



UNIWERSYTET ŚLĄSKI
W KATOWICACH

**Wydział Nauk Społecznych
Instytut Nauk Politycznych**

mgr Jacek Kiera

**WOJNA INFORMACYJNA W POLITYCE
ZAGRANICZNEJ FEDERACJI ROSYJSKIEJ
WOBEC POLSKI W LATACH 2010-2022**

ROZPRAWA DOKTORSKA

Promotor rozprawy doktorskiej:
prof. dr hab. Miron Lakomy

Promotor pomocniczy rozprawy doktorskiej:
dr hab. Katarzyna Czornik, prof. UŚ

Katowice 2025

Podziękowania

Serdeczne podziękowania składam mojemu Promotorowi, panu profesorowi Mironowi Lakomemu, za szczególną cierpliwość, zawsze okazywane wsparcie oraz wszelkie rady i wskazówki, które towarzyszyły mi na każdym etapie przygotowywania rozprawy.

Dziękuję również Promotorowi pomocniczemu, pani Profesor Katarzynie Czornik, za cenną pomoc, konstruktywne uwagi oraz dbałość o każdy szczegół rozprawy.

Spis treści

Wstęp	9
Rozdział 1. Pojęcie, uwarunkowania, cele i środki polityki zagranicznej.....	21
1.1. Pojęcie polityki zagranicznej	21
1.2. Uwarunkowania polityki zagranicznej	26
1.2.1. Uwarunkowania wewnętrzne o charakterze obiektywnym.....	28
1.2.2. Uwarunkowania wewnętrzne o charakterze subiektywnym	33
1.2.3. Uwarunkowania zewnętrzne o charakterze obiektywnym.....	36
1.2.4. Uwarunkowania zewnętrzne o charakterze subiektywnym	40
1.3. Cele polityki zagranicznej	42
1.3.1. Pojęcie interesu narodowego	43
1.3.2. Definicja celów polityki zagranicznej	52
1.3.3. Klasyfikacja celów polityki zagranicznej.....	57
1.4. Środki realizacji polityki zagranicznej	65
Rozdział 2. Wojna informacyjna jako instrument prowadzenia polityki zagranicznej ..	74
2.1. Pojęcie informacji	74
2.2. Wojna informacyjna w polityce zagranicznej	77
2.2.1. Definicja pojęcia wojny informacyjnej	78
2.2.2. Uwarunkowania wojny informacyjnej	86
2.2.3. Wybrane instrumenty wojny informacyjnej.....	93
2.2.4. Wybrani uczestnicy wojny informacyjnej.....	99
2.3. Propaganda i cyberataki jako instrumenty wojny informacyjnej	103
2.3.1. Propaganda jako instrument prowadzenia wojny informacyjnej	104
2.3.2. Cyberataki jako instrument prowadzenia wojny informacyjnej	120
Rozdział 3. Założenia metodologiczne badań	134
3.1. Problem badawczy	134
3.2. Cele badawcze	134
3.3. Hipotezy badawcze	136
3.4. Cezura czasowa badań.....	138
3.5. Metodologia badań	140
3.5.1. Założenia metodologiczne badań nad wojną informacyjną jako instrumentem polityki zagranicznej Federacji Rosyjskiej oraz polityką zagraniczną Federacji Rosyjskiej wobec Polski w latach 2010-2022	141

3.5.2. Założenia metodologiczne badań nad rosyjskimi atakami w cyberprzestrzeni wobec Polski w latach 2010-2022	146
3.5.3. Założenia metodologiczne badań nad rosyjskimi portalami informacyjnymi jako instrumentami wojny informacyjnej Federacji Rosyjskiej wobec Polski w latach 2010-2022.....	150
Rozdział 4. Wojna informacyjna w polityce zagranicznej Federacji Rosyjskiej	160
4.1. Polityka zagraniczna Federacji Rosyjskiej w XXI wieku	160
4.1.1. Geneza polityki zagranicznej Federacji Rosyjskiej	161
4.1.2. Uwarunkowania polityki zagranicznej Federacji Rosyjskiej	169
4.1.3. Cele polityki zagranicznej Federacji Rosyjskiej	185
4.2. Wojna informacyjna jako instrument polityki zagranicznej Federacji Rosyjskiej	194
4.2.1. Geneza i uwarunkowania wojny informacyjnej w polityce zagranicznej Federacji Rosyjskiej	194
4.2.2. Wybrane środki prowadzenia wojny informacyjnej w polityce zagranicznej Federacji Rosyjskiej	209
4.3. Wybrane przykłady wojny informacyjnej w polityce zagranicznej Federacji Rosyjskiej	214
Rozdział 5. Polska w polityce zagranicznej Federacji Rosyjskiej w latach 2010-2022 ..	220
5.1. Geneza stosunków polsko-radzieckich oraz polsko-rosyjskich	220
5.2. Uwarunkowania polityki zagranicznej Federacji Rosyjskiej wobec Polski.....	227
5.2.1. Uwarunkowania wewnętrzne polityki zagranicznej Federacji Rosyjskiej wobec Polski	228
5.2.2. Uwarunkowania zewnętrzne polityki zagranicznej Federacji Rosyjskiej wobec Polski	237
5.3. Zarys stosunków polsko-rosyjskich w latach 1992-2009.....	242
5.4. Cele polityki zagranicznej Federacji Rosyjskiej wobec Polski w latach 2010-2022 ..	246
5.5. Stosunki polsko-rosyjskie w kontekście występujących głównych kwestii spornych w latach 2010-2022	251
5.5.1. Polityka historyczna	252
5.5.2. Dywersyfikacja źródeł energii	256
5.5.3. Polityka bezpieczeństwa w Europie Środkowo-Wschodniej	260
5.5.4. Polityka bezpieczeństwa NATO	261
5.5.5. Katastrofa samolotu rządowego z Prezydentem Rzeczypospolitej Polskiej w Smoleńsku	265
5.5.6. Aneksja Półwyspu Krymskiego i wojna w Ukrainie	268
5.5.7. Program Partnerstwa Wschodniego	271

Rozdział 6. Cyberataki jako instrument wojny informacyjnej Federacji Rosyjskiej wobec Polski w latach 2010-2022	275
6.1. Cyberbezpieczeństwo Polski w latach 2010-2022	275
6.1.1. Stopień informatyzacji i digitalizacji w Polsce w latach 2010-2022	276
6.1.2. Zagrożenia dla bezpieczeństwa teleinformatycznego Polski w latach 2010-2022	281
6.1.3. Ewolucja systemu cyberbezpieczeństwa Polski w latach 2010-2022	296
6.2. Charakterystyka, przebieg i implikacje rosyjskich ataków teleinformatycznych wobec Polski w cyberprzestrzeni w latach 2010-2022	312
6.2.1. Charakterystyka, przebieg i implikacje rosyjskich ataków teleinformatycznych wobec Polski w cyberprzestrzeni w latach 2010-2013	314
6.2.2. Charakterystyka, przebieg i implikacje rosyjskich ataków teleinformatycznych wobec Polski w cyberprzestrzeni w latach 2014-2019	322
6.2.3. Charakterystyka, przebieg i implikacje rosyjskich ataków teleinformatycznych wobec Polski w cyberprzestrzeni w latach 2020-2022	341
Rozdział 7. Portale informacyjne jako instrument wojny informacyjnej Federacji Rosyjskiej wobec Polski w latach 2010-2022	364
7.1. Portal informacyjny Sputnik News International jako narzędzie wojny informacyjnej Federacji Rosyjskiej wobec Polski	364
7.1.1. Charakterystyka portalu informacyjnego Sputnik News International	364
7.1.2. Typy publikowanych treści na portalu informacyjnym Sputnik News International	367
7.1.3. Polsko-rosyjskie kwestie sporne w treściach publikowanych na portalu informacyjnym Sputnik News International	376
7.1.4. <i>Framing</i> treści na portalu informacyjnym Sputnik News International	387
7.1.5. Techniki propagandowe stosowane przez portal informacyjny Sputnik News International	393
7.2. Agencja informacyjna TASS jako narzędzie wojny informacyjnej Federacji Rosyjskiej wobec Polski	405
7.2.1. Charakterystyka agencji informacyjnej TASS	405
7.2.2. Typy publikowanych treści na witrynie internetowej agencji informacyjnej TASS	407
7.2.3. Polsko-rosyjskie kwestie sporne w treściach publikowanych na witrynie internetowej agencji informacyjnej TASS	413
7.2.4. <i>Framing</i> treści na witrynie internetowej agencji informacyjnej TASS	420
7.2.5. Techniki propagandowe stosowane na witrynie internetowej agencji informacyjnej TASS	425

Zakończenie	436
Summary	451
Bibliografia	454
Akty prawne, dokumenty państwowe i raporty	454
Monografie i prace zbiorowe	465
Artykuły naukowe i rozdziały w pracach zbiorowych	472
Artykuły prasowe	487
Źródła internetowe	501
Tytuły artykułów poddanych badaniom na portalu Sputnik News International.....	516
Tytuły artykułów poddanych badaniom na witrynie agencji informacyjnej TASS	529

Wstęp

Stosunki polsko-rosyjskie stanowią niezwykle złożone zagadnienie. Na przestrzeni ostatnich wieków charakteryzowały się one licznymi sporami, konfliktami oraz były kształtowane na płaszczyźnie politycznej, społecznej i kulturalnej. Wejście carskiej Rosji do europejskiej rywalizacji mocarstw było bezpośrednio związane z rozbiorem państwa polskiego, a w konsekwencji upadkiem Rzeczypospolitej Obojga Narodów. To właśnie w tamtym czasie Rosję zaczęto zaliczać na stałe do grona europejskich potęg. Słabość Polski jest więc dla Rosji zjawiskiem pożądanym, gdyż to właśnie ona znajdowała się i znajduje nadal na drodze Kremla do rozszerzania swojej strefy wpływów w Europie Środkowo-Wschodniej i dalej w całej Europie.

Dokonując analizy ostatnich kilkuset lat stosunków polsko-rosyjskich, można zauważyć, że „sprawa polska”, była dla Moskwy jednym z atrybutów jej imperialnej potęgi. Odzyskanie w 1918 roku przez Polskę niepodległości było dla carskiej Rosji, a chwilę później Związku Socjalistycznych Republik Radzieckich (ZSRR)¹, sytuacją zagrażającą w sposób istotny interesom narodowym Kremla. Zagrożenie to zostało opanowane wraz z zakończeniem II wojny światowej i w konsekwencji podporządkowaniem Polski ZSRR w ramach bloku wschodniego. Zakończenie okresu zimnej wojny, czego skutkiem było między innymi rozwiązanie Układu Warszawskiego (1991) i Rady Wzajemnej Pomocy Gospodarczej (1991) oraz wycofanie wojsk radzieckich z Polski (1993), ponownie spowodowało powstanie zagrożenia dla rosyjskich wpływów w regionie. Sytuację tę pogłębiło przede wszystkim wstąpienie Polski do Sojuszu Północnoatlantyckiego (NATO) (1999) oraz Unii Europejskiej (UE) (2004). Nie bez znaczenia pozostawało również polskie zaangażowanie w procesy polityczno-społeczne, zbliżające między innymi Ukrainę i Gruzję do członkostwa w Unii Europejskiej i NATO². Ważną była również kwestia dotycząca postrzegania przez Polskę i Rosję poszczególnych wydarzeń historycznych, głównie tych dotyczących II wojny światowej oraz roli, jaką każde z państw odegrało w jej rozpoczęciu i zakończeniu. Dla Kremla istotne stało się także przeciwdziałanie polskiej polityce dywersyfikacji źródeł energii, w konsekwencji której uniezależniała się ona od dostaw surowców energetycznych z Rosji. Katastrofa samolotu rządowego z Prezydentem Rzeczypospolitej Polskiej w Smoleńsku do

¹ Związku Socjalistycznych Republik Sowieckich.

² Zobacz szerzej: Pomarańczowa rewolucja na Ukrainie (2004-2005), wojna gruzińsko-rosyjska (2008), zainicjowanie z polskiej inicjatywy unijnego Programu Partnerstwa Wschodniego (2009), Euromajdan na Ukrainie (2013-2014).

której doszło dnia 10 kwietnia 2010 roku, wbrew oczekiwaniom niektórych środowisk politycznych nie spowodowała polsko-rosyjskiego pojednania, a wręcz przeciwnie. Aneksja Półwyspu Krymskiego w 2014 roku rozpoczęła definitywny impas w stosunkach bilateralnych, który pogłębiał się na przestrzeni lat wokół zagadnień dotyczących wojny na Ukrainie (trwającej na wschodzie tego państwa od 2014 roku oraz pełnoskalowo od 2022 roku), zwiększania obecności militarnej NATO na wschodniej flance Sojuszu oraz polityki bezpieczeństwa w Europie Środkowo-Wschodniej stanowiącej przeciwwagę dla wpływów rosyjskich w regionie.

Analizując powyższe wydarzenia można wskazać, że redefinicja celów polityki zagranicznej Kremla na przełomie XX i XXI wieku spowodowała, że Polska ponownie stała się dla Federacji Rosyjskiej przeszkodą do dalszego poszerzania swojej strefy wpływów. Współczesny schemat działania Kremla jest podobny do tego, który można było obserwować na przestrzeni ostatnich 300-400 lat historii stosunków polsko-rosyjskich. Zmianie uległy jedynie instrumenty w oparciu o które Federacja Rosyjska dąży do ciągłego i wielowymiarowego osłabiania Polski zarówno w sferze wewnętrznej (narodowej) oraz zewnętrznej (międzynarodowej), jak również rozszerzania swojej strefy wpływów w regionie Europy Środkowo-Wschodniej. Współcześnie instrumentem tym stała się w dużej mierze informacja, która od zawsze towarzyszyła napięciom, sporom i konfliktom międzynarodowym, jednak nigdy dotąd w historii jej zastosowanie do działań taktycznych, operacyjnych czy strategicznych nie było tak masowe i kompleksowe, zarówno w czasie wojny, jak i w czasie pokoju³. T. Aleksandrowicz określił informację zasobem krytycznym dla funkcjonowania państwa oraz wskazał, że musi być ona w dostateczny sposób chroniona na każdym etapie jej przetwarzania⁴. Narzędzia, które wykorzystuje Federacja Rosyjska w ramach prowadzonej wobec Polski polityki zagranicznej mają charakter niekonwencjonalny, asymetryczny. Za ich pomocą realizuje w niespotykanej dotąd skali działania w wymiarze offline⁵, ale przede wszystkim w sferze online. W tym przedmiocie opierają się one na wojnie informacyjnej zakładającej jednoczesne oddziaływanie informacyjne na odbiorców

³ Zobacz szerzej: J. Darczewska: *Anatomia rosyjskiej wojny informacyjnej Operacja Krymska – studium przypadku*. „Punkt widzenia” 2014, nr 42. https://www.osw.waw.pl/sites/default/files/anatomia_rosyjskiej_wojny_informacyjnej.pdf (dostęp: 16.03.2025); J. Darczewska: *Wojna informacyjna Rosji z Zachodem. Nowe wyzwanie?* „Przegląd Bezpieczeństwa Wewnętrznego” 2015, Wydanie Specjalne; T. R. Aleksandrowicz: *Podstawy walki informacyjnej*. Warszawa 2016.

⁴ T. Aleksandrowicz: *Bezpieczeństwo informacyjne państwa*. „Studia Politologiczne” 2018 nr 49, s. 33-48.

⁵ Do przykładów można zaliczyć wywołanie kryzysu migracyjnego na granicy polsko-białoruskiej oraz działalność sabotażową i wywiadowczą. Źródło: gov.pl: *Uderzenie dezinformacyjne*. <https://www.gov.pl/web/sluzby-specjalne/uderzenie-dezinformacyjne> (dostęp: 09.03.2025); gov.pl: *Komisja ds. badania wpływów rosyjskich i białoruskich powołana*. <https://www.gov.pl/web/premier/komisja-ds-badania-wplywow-rosyjskich-i-bialoruskich-powolana> (dostęp: 09.03.2025).

w Internecie przy użyciu technik propagandowych oraz dokonywanie ataków w cyberprzestrzeni na infrastrukturę teleinformatyczną przeciwnika. Prowadzona przez Kreml wojna informacyjna stanowi coraz większe zagrożenie dla bezpieczeństwa Polski w wymiarze narodowym i międzynarodowym.

Zjawisko wojny informacyjnej zwraca uwagę wielu badaczy od kilkudziesięciu lat. Środowisko naukowe postrzega je przede wszystkim w kontekście oddziaływania informacyjnego na odbiorców w świecie cyfrowym bądź w kontekście przeprowadzania operacji przeciwko systemom teleinformatycznym przeciwnika. Problematyka ta była poruszana wśród autorów zagranicznych takich jak D. Ventre⁶ i D. E. Denning⁷ w kontekście dokonywanych cyberataków oraz przez M. C. Libickiego⁸, B. Cronina i H. Crawforda również w kontekście operacji informacyjnych⁹. Zjawisko rywalizacji w cyberprzestrzeni za pomocą ataków teleinformatycznych spotkało się również z dużym zainteresowaniem polskiego środowiska naukowego. Problematykę tę w swoich pracach prezentowali między innymi M. Madej¹⁰, H. Świeboda¹¹, T. Aleksandrowicz¹², K. Liedel¹³, K. Liderman¹⁴, P. Sienkiewicz¹⁵, czy Z. Modrzejewski¹⁶. W kontekście działalności Kremla tematykę tę poruszali

⁶ D. Ventre: *Information Warfare. 2nd Edition revised and Updated*. London – New York 2016.

⁷ D. E. Denning: *Wojna Informacyjna i bezpieczeństwo informacji*. Warszawa 2002.

⁸ M. C. Libicki: *What is information warfare?* Washington D.C. 1995.

⁹ B. Cronin, H. Crawford: *Information Warfare: Its Application in Military and Civilian Contexts*. „The Information Society” 1999, Vol. 15:4.

¹⁰ M. Madej: *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państwa i systemu międzynarodowego*. W: *Bezpieczeństwo Teleinformatyczne Państwa*. Red. M. Madej, M. Terlikowski. Warszawa 2009.

¹¹ P. Sienkiewicz, H. Świeboda: *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej*. W: *Bezpieczeństwo Teleinformatyczne Państwa*. Red. M. Madej, M. Terlikowski. Warszawa 2009.

¹² T. R. Aleksandrowicz: *Bezpieczeństwo informacyjne państwa*. „Studia Politologiczne” 2018, nr 49; T. R. Aleksandrowicz: *Podstawy walki informacyjnej*. Warszawa 2016; T. R. Aleksandrowicz: *Zagrożenia dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym. Budowanie zdolności defensywnych i ofensywnych w infosferze*. Warszawa 2021.

¹³ K. Liedel, P. Piasecka, T. R. Aleksandrowicz: *Analiza informacji. Teoria i praktyka*. Warszawa 2012; K. Liedel: *Zdolność prowadzenia działań ofensywnych w cyberprzestrzeni warunkiem bezpieczeństwa państwa*. W: *Niebezpieczny świat. Systemy Informacja Bezpieczeństwo*. Red. P. Sienkiewicz, H. Świeboda, E. Szczepaniuk. Warszawa 2015; M. Adamczuk, K. Liedel: *Doktryna cyberbezpieczeństwa*. „Przegląd Bezpieczeństwa Wewnętrznego” 2015, nr 12/7; K. Liedel, P. Piasecka: *Wojna cybernetyczna – wyzwanie XXI wieku*. „Bezpieczeństwo narodowe” 2011, nr I-2011/17.

¹⁴ K. Liderman: *Bezpieczeństwo informacyjne*. Warszawa 2012.

¹⁵ P. Sienkiewicz: *Wizje i modele wojny informacyjnej*. W: *Spółczesność informacyjna - wizja czy rzeczywistość?* Red. L. H. Haber. Kraków 2003; P. Sienkiewicz: *Ewaluacja informacji w społeczeństwie informacyjnym*. „Ekonomiczne Problemy Usług” 2011; P. Sienkiewicz: *Inżynieria systemów*. Warszawa 1983; P. Sienkiewicz: *Bezpieczeństwo cyberprzestrzeni państwa*. „Ekonomiczne Problemy Usług” 2012, nr 88; P. Sienkiewicz: *Część III – Techniczne uwarunkowania rozwoju społeczeństwa informacyjnego. Wizje i modele wojny informacyjnej*. <http://winntbg.bg.agh.edu.pl/skrypty2/0095/373-378.pdf> (dostęp: 04.03.2025).

¹⁶ Z. Modrzejewski: *Dezinformacja w służbie walki informacyjnej*. W: *Bezpieczeństwo informacyjne w dobie postprawdy*. Red. T. W. Grabowski, M. Lakomy, K. Oświecimski. Kraków 2018.

M. Lakomy¹⁷, S. Gardocki¹⁸ i A. Warchoń¹⁹. Z kolei wykorzystywaniem przez Federację Rosyjską narzędzi wojny informacyjnej zajmowali się w kontekście działań propagandowych K. Giles²⁰, A. Seaboyer²¹, E. Lucas i P. Pomerantsev²², R. Bebbber²³ oraz B. Nakayama²⁴. Opracowania tego zagadnienia pojawiły się również w polskiej literaturze specjalistycznej w publikacjach takich autorów jak M. Banasik²⁵, U. Soler²⁶, M. Wrzosek²⁷ J. Darczewska²⁸, A. Legucka²⁹ oraz M. Marek³⁰. Liczne badania na temat wykorzystania narzędzi wojny informacyjnej przez Rosję można odnaleźć również w raportach publikowanych przez organizacje pozarządowe i podmioty rządowe. Należy do nich zaliczyć przykładowo Centrum

¹⁷ M. Lakomy: *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*. Katowice 2015; M. Lakomy: *Zagrożenia dla bezpieczeństwa teleinformatycznego państw - przyczynek do typologii*. „Kwartalnik Naukowy OAP UW e-Politikon” 2013, nr 6; M. Lakomy: *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku*. „Stosunki Międzynarodowe” 2010, Tom 42, nr 3/4; M. Lakomy: *Polityka bezpieczeństwa teleinformatycznego Polski*. W: *Dylematy polityki zagranicznej Polski na początku XXI wieku*. Red. K. Czornik, M. Lakomy, M. Stolarczyk. Katowice 2014.

¹⁸ S. Gardocki, H. Worona: *Wykorzystanie przez Rosję cyberprzestrzeni w konfliktach hybrydowych a rosyjska polityka cyberbezpieczeństwa*. „Colloquium Pedagogika – Nauki o Polityce i Administracji” 2020, nr 2(38)/2020.

¹⁹ A. Warchoń: *Rola cyberprzestrzeni w wojnie Rosji z Ukrainą*. „Nowa Polityka Wschodnia” 2023, nr 4 (39).

²⁰ K. Giles: *The Next Phase of Russian Information Warfare*. NATO Strategic Communications Centre of Excellence. Riga 2016; K. Giles: *Handbook of Russian Information Warfare. Fellowship Monograph Research Division NATO Defense College*. 2016, Vol. 9.

²¹ K. Giles, A. Seaboyer: *The Russian Information Warfare Construct*. Technical Report, Report number: DRDC-RDDC-2019-C241Affiliation: Defence Research and Development. Ontario 2019.

²² E. Lucas, P. Pomerantsev: *Winning the Information War. Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe. A Report by CEPA's Information Warfare Project in Partnership with the Legatum Institute*. Washington D.C. 2016.

²³ R. Bebbber: *Information War and Rethinking Phase 0*. „Journal of Information Warfare” 2016, Vol. 15 (Issue 2).

²⁴ B. Nakayama: *American Influence on Russian Information Warfare*. „E-International Relations” 2020. <https://www.e-ir.info/2020/09/24/american-influence-on-russian-information-warfare/> (dostęp: 07.12.2024).

²⁵ M. Banasik: *Teoria i praktyka wojny informacyjnej stosowanej przez Federację Rosyjską*. W: *Informacja czynnikiem warunkującym bezpieczeństwo. Kontekst rosyjski*. Red. M. Banasik. Warszawa 2021.

²⁶ U. Soler, A. Makuch, K. Chałubińska-Jentkiewicz: *Disinformation in Polish Society in 2021 – Trends, Topics, Channels of Transmission*. „Polish Political Science Yearbook” 2023, nr 1 (52).

²⁷ M. Wrzosek: *Rosyjska dominacja informacyjna w sferze militarnej*. W: *Informacja czynnikiem warunkującym bezpieczeństwo. Kontekst rosyjski*. Red. M. Banasik. Warszawa 2021; M. Wrzosek: *Rosyjska dezinformacja w konflikcie zbrojnym w Ukrainie*. „Bezpieczeństwo Narodowe” 2024, nr 44.

²⁸ J. Darczewska: *Miedzy jawną dezinformacją a niejawną praktyką. Gry rosyjskich służb*. „Punkt widzenia” 2019, nr 73. https://www.osw.waw.pl/sites/default/files/PW_73_PL_Miedzy-jawna-dezinformacja_net.pdf (dostęp: 14.03.2025); J. Darczewska: *Anatomia rosyjskiej wojny informacyjnej Operacja Krymska – studium przypadku*. „Punkt widzenia” 2014, nr 42. https://www.osw.waw.pl/sites/default/files/anatomia_rosyjskiej_wojny_informacyjnej.pdf (dostęp: 14.03.2025); J. Darczewska: *Dezinformacja – rosyjska broń strategiczna*. „Biuletyn Kwartalny Rządowego Centrum Bezpieczeństwa” 2017, nr 19; J. Darczewska: *Diabeł tkwi w szczegółach. Wojna informacyjna w świetle doktryny wojennej Rosji*. „Punkt widzenia” 2015, nr 50. https://www.osw.waw.pl/sites/default/files/pw_50_pl_diabel_tkwi_net.pdf (dostęp: 14.03.2025); J. Darczewska: *Rosyjskie Siły zbrojne na froncie walki informacyjnej. Dokumenty strategiczne*. „Prace OSW” 2016, nr 57. https://www.osw.waw.pl/sites/default/files/prace_57_pl_sily_zbrojne_net.pdf (dostęp: 14.03.2025); J. Darczewska, P. Żochowski: *Środki aktywne. Rosyjski towar eksportowy*. „Punkt Widzenia” 2017, nr 64. https://www.osw.waw.pl/sites/default/files/pw_64_pl_srodki_aktywne_net.pdf (dostęp: 14.03.2025).

²⁹ A. Legucka: *Walka z rosyjską dezinformacją w Unii Europejskiej*. „Biuletyn Polskiego Instytutu Spraw Międzynarodowych” 2019, nr 111 (1859). <https://pism.pl/upload/images/artykuly/0414d618-2799-421d-8510-b1130a66303e/1570904090174.pdf> (dostęp: 14.03.2025); A. Legucka: *Dezinformacja jako element wojny informacyjnej Federacji Rosyjskiej – założenia i efektywność*. „Sprawy Międzynarodowe” 2020, nr 4, T. 73.

³⁰ M. Marek: *Wojna informacyjna Federacji Rosyjskiej przeciwko Ukrainie, Polsce i NATO*. Warszawa 2025.

Analiz Propagandy i Dezinformacji³¹ (w zakresie operacji informacyjnych) oraz Zespół CERT Polska³² i Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV³³ (w zakresie dokonywanych cyberataków). Oprócz powyższego, należy zauważyć, iż z oczywistych względów bardzo dużym zainteresowaniem środowiska naukowego cieszy się tematyka polityki zagranicznej Federacji Rosyjskiej oraz stosunków polsko-rosyjskich. Problematykę tę w różnych okresach podejmowali uznani polscy naukowcy w tym S. Bieleń³⁴, M. Raś³⁵, A. Bryc³⁶, A. Skrzypek³⁷, A. Legucka³⁸, M. Stolarczyk³⁹, R. Zięba⁴⁰, J. Diec⁴¹, J. Wiatr⁴² czy S. Gardocki⁴³, ale również wielu innych badaczy stosunków polsko-rosyjskich oraz polityki zagranicznej Federacji Rosyjskiej wobec Polski⁴⁴. Wskazane zagadnienia są

³¹ K. Wóycicki, M. Kowalska, A. Lelonek: *Raport Rosyjska wojna dezinformacyjna przeciwko Polsce*. Warszawa 2017. <https://pulaski.pl/wp-content/uploads/2023/06/RAPORT-Rosyjska-wojna-dezinformacyjna-przeciwko-Polsce.pdf> (dostęp: 14.03.2025); M. Kowalska, A. Lelonek: *Jak budować odporność społeczną w przestrzeni informacyjnej i cyberprzestrzeni: przeciwdziałanie propagandzie i dezinformacji*. Raport Centrum Analiz Propagandy i Dezinformacji. Warszawa 2017. https://capd.pl/images/dokumenty/Raport_CSEU_CAPD.pdf (dostęp: 14.03.2025).

³² CERT Polska: *Publikacje CERT Polska*. <https://cert.pl/publikacje/> (dostęp: 03.03.2025).

³³ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raporty o stanie bezpieczeństwa cyberprzestrzeni RP*. <https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi> (dostęp: 03.03.2025).

³⁴ S. Bieleń: *Identyfikacja Rosji w stosunkach międzynarodowych*. W: *Polityka zagraniczna Rosji*. Red. S. Bieleń, M. Raś. Warszawa 2008; S. Bieleń, M. Raś (Red.): *Polityka zagraniczna Rosji*. Warszawa, 2008; S. Bieleń: *Tożsamość międzynarodowa Federacji Rosyjskiej*. Warszawa 2006; S. Bieleń: *Polityka zagraniczna Rosji*. W: *Federacja Rosyjska 1991-2001*. Red. J. Adamowski, A. Skrzypek. Warszawa 2002.

³⁵ M. Raś: *Cele oddziaływań politycznych Federacji Rosyjskiej*. W: *Rosja wobec państw Europy Środkowej i Wschodniej: zagrożenia pozamilitarne*. Red. T. Stępniewski. Lublin 2020; M. Raś: *Polska w stosunkach międzynarodowych*. W: *Polska i Rosja w zmieniającej się Europie*. Red. K. A. Wojtaszczyk, I. N. Novikova. Warszawa 2022; M. Raś: *Polityka Rosji wobec Europy Środkowo-Wschodniej*. „Prace Instytutu Europy Środkowo-Wschodniej” 2010, Tom 16.

³⁶ A. Bryc: *Rosja w XXI wieku. Gracz światowy czy koniec ery?* Warszawa 2009; A. Bryc: *Mechanizm polityki zagranicznej Federacji Rosyjskiej*. W: *Polityka zagraniczna Federacji Rosyjskiej. Wybrane aspekty stosunków z Polską, Ukrainą i Białorusią*. Red. L. Zyblikiewicz, M. Czajkowski, P. Bajor. Kraków 2010; A. Bryc: *Cele polityki zagranicznej Federacji Rosyjskiej*. Toruń 2004.

³⁷ S. Bieleń, A. Skrzypek (Red.): *Pamięć i polityka historyczna w stosunkach polsko-rosyjskich*. Warszawa 2017; S. Bieleń, A. Skrzypek (Red.): *Rosja. Rozważania imperiologiczne*. Warszawa 2015.

³⁸ A. Legucka: *Rosja wobec Partnerstwa Wschodniego Unii Europejskiej*. „Rocznik Instytutu Europy Środkowo-Wschodniej” 2019, nr 17 (2019), Zeszyt 2; A. Legucka: *Polityka zagraniczna Polski wobec Rosji po aneksji Krymu*. „Wschód Europy” 2019, Vol. 5, 1/2019.

³⁹ M. Stolarczyk: *Rosja w polityce zagranicznej Polski w latach 1992-2015*. Katowice 2016.

⁴⁰ R. Zięba: *Główne problemy w stosunkach polsko-rosyjskich*. „Stosunki Międzynarodowe – International Relations” 2018, nr 3 (T. 54); R. Zięba: *Współczesne stosunki polsko-rosyjskie: uwarunkowania, problemy, implikacje*. „Przegląd Politologiczny” 2011, nr 3 (2011).

⁴¹ J. Diec: *Geostrategiczny wybór Rosji u zarania trzeciego tysiąclecia. Tom 1 Doktryna rosyjskiej polityki zagranicznej. Partnerzy najbliżsi i najdalsi*. Kraków 2015.

⁴² J. Wiatr: *Bezpieczeństwo narodowe Polski a stosunki polsko-rosyjskie*. Poznań 2017.

⁴³ S. Gardocki (Red.): *Rosja i jej sąsiedzi. Studia i szkice*. Toruń 2015; S. Gardocki: *Polityka zagraniczna Rosji. Determinanty, interesy i środki*. „Studia Orientalne” 2020, nr 2 (18).

⁴⁴ A. Wierzbicki: *Russkij mir jako projekt restauracyjny imperium*. W: *Rosja. Rozważania imperiologiczne*. Red. S. Bieleń, A. Skrzypek. Warszawa 2015; K. Fedorowicz: *Polityka Polski wobec Rosji, Ukrainy i Białorusi w latach 1989-2010*. Poznań 2011; J. M. Fiszer: *Zadania i cele polityki zagranicznej Władimira Putina*. „Myśl Ekonomiczna i Polityczna” 2016, nr 1 (52); *Polska i Rosja w zmieniającej się Europie*. Red. K. A. Wojtaszczyk, I. N. Novikova. Warszawa 2022.

bardzo dobrze opracowane w literaturze specjalistycznej, a podane przykłady stanowią jedynie niewielką część prac naukowych na ten temat.

Choć zjawisko wykorzystania wojny informacyjnej jako narzędzia realizacji polityki zagranicznej Federacji Rosyjskiej wobec Polski zyskało na znaczeniu szczególnie po rozpoczęciu przez Kreml pełnoskalowej inwazji na Ukrainę w 2022 roku, to nadal omawiane zagadnienie nie doczekało się kompleksowego ujęcia w literaturze specjalistycznej. Należy również podkreślić, że większość dotychczasowych opracowań ujmowało rosyjską wojnę informacyjną jako działalność z zakresu oddziaływania informacyjnego na odbiorców w Internecie albo jako przeprowadzanie ataków w cyberprzestrzeni. Z kolei wnioski z dotychczas przeprowadzonych badań dowodzą, że rosyjskie postrzeganie wojny informacyjnej ujmuje łącznie powyższe rodzaje działalności i traktuje je wobec siebie komplementarnie⁴⁵. Wobec tego, prowadzenie badań w tym zakresie powinno być realizowane z perspektywy koncepcji rosyjskich, ale również z perspektywy koncepcji polityki zagranicznej Federacji Rosyjskiej wobec Polski, gdyż tylko w ten sposób będzie możliwe oddanie ich pełnego spektrum. Dotychczasowe badania przedmiotową aktywność Rosji omawiały jednak rozłącznie, wobec czego niniejsza rozprawa wypełni istniejącą lukę badawczą. Ponadto należy zauważyć, że większość prac dotyczących omawianych zagadnień nie realizuje badań w długim czasie. Z kolei tylko kompleksowe ujęcie tego zjawiska w odpowiednio długiej cezurze czasowej, zgodnie z rosyjskimi koncepcjami wojny informacyjnej, umożliwi objęcie go perspektywą realizacji celów polityki zagranicznej Federacji Rosyjskiej wobec Polski. To natomiast pozwoli na lepsze zrozumienie natury zachodzących procesów w ramach stosunków polsko-rosyjskich.

Konkludując, nie zostały dotąd podjęte na szeroką skalę badania dotyczące uwarunkowań, implikacji oraz charakteru rosyjskiej wojny informacyjnej jako narzędzia polityki zagranicznej wobec Polski w latach 2010-2022. W tym zakresie nie istnieją badania, które ujmowałyby omawiane zjawisko dwupłaszczyznowo, tj. poprzez oddziaływanie informacyjne na odbiorców w Internecie oraz dokonywanie ataków w cyberprzestrzeni. Uwzględniając dużą ilość materiału badawczego, działalność Rosji polegającą na wykorzystywaniu wojny informacyjnej jako narzędzia w ramach prowadzonej polityki zagranicznej oraz luki w dyskursie, przeprowadzenie badań w przedmiotowym zakresie jest

⁴⁵ R. Bebbler: *Information War and Rethinking Phase 0*. „Journal of Information Warfare” 2016, Vol. 15 (Issue 2); I. Panarin: *СМИ, пропаганда и информационные войны*. Москва 2012; J. Messner: *Хочешь Мира, Победи Мятёжевойну!* Москва 2005.

w pełni uzasadnione. Temat rozprawy doktorskiej nie znalazł swojego opracowania w literaturze specjalistycznej.

Przedmiotem badań niniejszej rozprawy są uwarunkowania, charakter oraz implikacje wojny informacyjnej Federacji Rosyjskiej jako instrumentu polityki zagranicznej wobec Polski w latach 2010-2022⁴⁶. Wojna informacyjna jest ściśle związana z rosyjską kulturą polityczną i realizowaną przez Kreml polityką zagraniczną. Ma trwałe cechy wypracowane na przestrzeni dziesiątek lat, które utrwaliły się w systemie ustrojowym Związku Socjalistycznych Republik Radzieckich, a współcześnie ewoluują w systemie ustrojowym Federacji Rosyjskiej. Federacja Rosyjska traktuje wojnę informacyjną w sposób szczególny, realizując ją w skali globalnej przy użyciu znacznych zasobów organizacyjnych i finansowych, widocznie wyróżniając się przy tym na tle innych państw⁴⁷. Zjawiska takie jak globalizacja oraz dynamiczny rozwój technologii i systemów teleinformatycznych sprzyjają coraz częstszemu wykorzystywaniu narzędzi właściwych dla wojny informacyjnej, ale również zwiększają jej znaczenie w polityce zagranicznej państw. Federacja Rosyjska bywa bardzo często kojarzona jako państwo, które było i jest nieprzystosowane do postępującej rewolucji informacyjnej. Jest to jednak założenie całkowicie błędne. Zmiany zachodzące w ramach wskazanych wyżej przemian nie były niezrozumiałe ani pomijane przez decydentów politycznych zarówno w Związku Radzieckim jak i w Federacji Rosyjskiej⁴⁸. Rozpad ZSRR z oczywistych względów zahamował postępującą w tym państwie rewolucję informacyjną. Nie nastąpiło to jednak w takim stopniu, aby nie móc określić Federacji Rosyjskiej jako współinicjatorce przemian technologicznych w omawianym zakresie. Działania Rosji są ukierunkowane na odbudowę swojej pozycji jako mocarstwa na świecie oraz strefy wpływów na arenie międzynarodowej. Władze Kremla, realizując te

⁴⁶ W pracy pojęcie wojny informacyjnej jest postrzegane w kontekście oddziaływania informacyjnego na odbiorców w Internecie, jak i w kontekście dokonywania przez określone podmioty ataków w cyberprzestrzeni. Ponadto rozprawa odnosi się do koncepcji wojny informacyjnej, nie natomiast walki informacyjnej. Kwestie terminologiczne związane ze wskazanymi pojęciami, w szczególności uzasadnienie ich rozróżnienia, zostały omówione w dalszej części pracy w rozdziale czwartym. Zobacz szerzej: R. Bebbler: *Information War and Rethinking Phase 0*. „Journal of Information Warfare” 2016, Vol. 15 (Issue 2); I. Panarin: *СМИ, пропаганда и информационные войны*. Москва 2012; J. Darczewska: *Anatomia rosyjskiej wojny informacyjnej Operacja Krymska – studium przypadku*. „Punkt widzenia” 2014, nr 42. https://www.osw.waw.pl/sites/default/files/anatomia_rosyjskiej_wojny_informacyjnej.pdf (dostęp: 14.03.2025); V. Volkoff: *Krótką historia dezinformacji. Od konia trojańskiego do Internetu*. Bielany Wrocławskie – Kobierzyce 2022; M. Wojnowski: *Koncepcja wojny sieciowej Aleksandra Dugina jako narzędzie realizacji celów geopolitycznych Federacji Rosyjskiej*. „Przegląd Bezpieczeństwa Wewnętrznego” 2017, Vol. 9; J. Messner: *Хочешь Мира, Победи Матеревую войну!* Москва 2005; J. Kiera: *Implikacje koncepcji wojen buntowniczych Jewgienija Messnera dla doktryny bezpieczeństwa Federacji Rosyjskiej w XXI wieku*. W: *Perspektywy zagrożeń dla bezpieczeństwa międzynarodowego kreowanych przez Federację Rosyjską*. Red. M. Banasik, A. Rogozińska. Warszawa 2019.

⁴⁷ Zobacz szerzej: J. Darczewska: *Anatomia rosyjskiej wojny informacyjnej Operacja Krymska – studium przypadku*. „Punkt widzenia” 2014, nr 42. https://www.osw.waw.pl/sites/default/files/anatomia_rosyjskiej_wojny_informacyjnej.pdf (dostęp: 14.03.2025).

⁴⁸ Zobacz szerzej: Y. Harrel: *Rosyjska Cyber-strategia*. Warszawa 2015.

dążenia, wykorzystują do tego wojnę informacyjną jako narzędzie realizacji polityki zagranicznej, w tym polityki zagranicznej wobec Polski⁴⁹.

Głównym celem badawczym niniejszej rozprawy jest określenie uwarunkowań, charakteru oraz implikacji wojny informacyjnej Federacji Rosyjskiej wobec Polski w latach 2010-2022. Praca zmierza przede wszystkim do określenia i scharakteryzowania jej uwarunkowań oraz celów pośrednich i bezpośrednich, jakie dzięki niej realizuje Federacja Rosyjska. Ponadto, rozprawa dąży do określenia instrumentów jakie do tego wykorzystuje, a także do wskazania najważniejszych implikacji powyższych działań. Należy również zaznaczyć, że w ramach niniejszej rozprawy rosyjska wojna informacyjna jest postrzegana zarówno jako oddziaływanie propagandowe na odbiorców w Internecie, jak i jako działania prowadzone w cyberprzestrzeni poprzez dokonywanie cyberataków. W związku z tym, celem pracy jest omówienie narzędzi i technik propagandowych jakie są wykorzystywane w prorosyjskich kanałach informacyjnych w Internecie, w przekazach dotyczących polski i relacji polsko-rosyjskich, jak również przedstawienie cech charakterystycznych rosyjskich cyberataków na Polskę w cyberprzestrzeni.

W ramach rozprawy, weryfikacji została poddana następująca główna hipoteza badawcza. Wojna informacyjna jako instrument polityki zagranicznej prowadzonej przez Federację Rosyjską stale zyskuje na znaczeniu, co należy odnieść również do stosunków polsko-rosyjskich. Rosja, w ramach prowadzonej wojny informacyjnej wobec Polski, wykorzystuje techniki i narzędzia propagandowe, które służą oddziaływaniu informacyjnemu na odbiorcę. Działania te podejmowane są za pośrednictwem rosyjskich portali informacyjnych. Wojna informacyjna Federacji Rosyjskiej wobec Polski przejawia się również przeprowadzaniem cyberataków na Polskę w cyberprzestrzeni. Działania podejmowane w ramach wskazanych wymiarów są komplementarne względem siebie. Celem podejmowanych przez Rosję operacji jest przede wszystkim osłabianie struktur wewnątrzpaństwowych, pogłębianie podziałów społecznych, marginalizowanie pozycji Polski na arenie międzynarodowej, kreowanie jej negatywnego wizerunku na arenie międzynarodowej, a przede wszystkim realizowanie własnych interesów.

Cezura czasowa badań obejmuje okres od 2010 do 2022 roku z uwagi na kluczowe wydarzenia w stosunkach polsko-rosyjskich, poczynając od katastrofy smoleńskiej z 2010 roku, do pełnowymiarowej inwazji Federacji Rosyjskiej na Ukrainę w 2022 roku. Choć początkowo katastrofa smoleńska mogła sugerować szansę na pojednanie obu państw, szybko

⁴⁹A. Łomanowski, B. Musiałowicz: *Kierunki rosyjskiej polityki zagranicznej*. „Bezpieczeństwo Narodowe” 2006, nr II – 2006/2, s. 17-40.

stała się punktem zapalnym w relacjach bilateralnych, prowadząc do wzajemnych oskarżeń. W latach 2011-2013 kluczowym tematem spornym były przyczyny katastrofy, a następnie aneksja Krymu (2014) oraz sprzeciw Rosji wobec integracji Ukrainy z Unią Europejską. Polska, dążąc do dywersyfikacji źródeł energii i uniezależnienia się od Rosji, a także zacieśniając współpracę z Ukrainą i NATO, prowadziła coraz bardziej konfrontacyjną politykę wobec Kremla. Istotnym tematem pozostawała również polityka historyczna, dotycząca przede wszystkim wydarzeń związanych z II wojną światową. Kulminacją napięć stała się rosyjska agresja na Ukrainę w 2022 roku, co pogłębiło impas w stosunkach polsko-rosyjskich. Do najważniejszych kwestii spornych w badanym okresie należy zaliczyć przede wszystkim: politykę historyczną, dywersyfikację źródeł energii, politykę bezpieczeństwa w Europie Środkowo-Wschodniej, politykę bezpieczeństwa NATO, katastrofę rządowego samolotu z Prezydentem Rzeczypospolitej Polskiej w Smoleńsku, aneksję Półwyspu Krymskiego i wojnę w Ukrainie oraz Program Partnerstwa Wschodniego. Szczegółowe uzasadnienie wyboru cezur czasowej badań zawarto w rozdziale metodologicznym rozprawy.

W tym miejscu należy zaznaczyć, że praca zawiera rozdział metodologiczny w którym szczegółowo scharakteryzowano główny cel badawczy oraz główną hipotezę badawczą. Ponadto zawarto w nim szczegółowe cele badawcze oraz odpowiadające im szczegółowe hipotezy badawcze. Wskazany rozdział obejmuje również założenia metodologiczne badań nad wojną informacyjną Federacji Rosyjskiej wobec Polski w latach 2010-2022 w kontekście działań z zakresu oddziaływania informacyjnego na odbiorców w Internecie, jak również dokonywanych względem Polski ataków w cyberprzestrzeni.

Struktura rozprawy ma charakter problemowy. W rozdziale pierwszym, o charakterze teoretycznym, zatytułowanym „Pojęcie, uwarunkowania, cele i środki polityki zagranicznej” omówione zostało pojęcie polityki zagranicznej, jej uwarunkowania wewnętrzne oraz zewnętrzne o charakterze obiektywnym oraz subiektywnym. Następnie zdefiniowano pojęcie interesu narodowego, celów polityki zagranicznej państwa oraz wskazano ich klasyfikację. Na koniec przedstawiono środki realizacji polityki zagranicznej przez państwa.

W rozdziale drugim pod tytułem „Wojna informacyjna jako instrument prowadzenia polityki zagranicznej” zdefiniowano pojęcie informacji i pojęcie wojny informacyjnej. Opisano jej genezę, uwarunkowania, instrumenty oraz uczestników. Poczyniono również rozważania niezwykle istotne z punktu widzenia założeń metodologicznych pracy, a mianowicie w zakresie wątpliwości terminologicznych dotyczących pojęcia wojny informacyjnej oraz walki informacyjnej. Następnie wskazano sposoby prowadzenia wojny informacyjnej w kontekście dwóch płaszczyzn jej występowania. Pierwsza z nich dotyczy oddziaływania informacyjnego

na odbiorcę w Internecie za pomocą technik propagandowych. W związku z tym wskazano definicje propagandy, genezę zjawiska propagandy, jej rodzaje, funkcje i zasady oraz techniki i metody stosowania propagandy. Druga z płaszczyzn odnosi się do przeprowadzanych w cyberataków w przestrzeni teleinformatycznej. Omówiono więc pojęcia i cech cyberprzestrzeni, pojęcia cyberataków oraz technik ich przeprowadzania.

W rozdziale trzecim, zatytułowanym „Założenia metodologiczne badań”, omówiony został zarys problemu badawczego. Następnie przedstawiony został główny cel badawczy oraz pięć szczegółowych celów badawczych, jak również odpowiadająca im główna hipoteza badawcza oraz szczegółowe hipotezy badawcze. Wreszcie dokonano uzasadnienie czasy czasowej badań, obejmującej lata 2010-2022. Na samym końcu przedstawiono szczegółową metodologię w zakresie badań nad rosyjską aktywnością wobec Polski w przestrzeni teleinformatycznej, jak również oddziaływaniem propagandowym na odbiorców w Internecie, z wykorzystaniem rosyjskich portali informacyjnych.

W rozdziale czwartym, zatytułowanym „Wojna informacyjna w polityce zagranicznej Federacji Rosyjskiej”, dokonano analizy kluczowych aspektów polityki zagranicznej Kremla w XXI wieku. Przedstawiono jej genezę, uwarunkowania oraz cele. Opisano historyczne i współczesne aspekty tej polityki, uwzględniając zmieniające się otoczenie międzynarodowe oraz wewnętrzne czynniki wpływające na procesy decyzyjne. W kolejnej części rozdziału wojna informacyjna została ukazana jako jeden z kluczowych instrumentów prowadzenia polityki zagranicznej przez Federację Rosyjską. Przeanalizowano jej genezę oraz uwarunkowania, które stanowiły tło dla rozwoju tej strategii. Szczególną uwagę poświęcono znaczeniu wojny informacyjnej, której celem jest nie tylko manipulowanie opinią publiczną, ale także wpływanie na procesy polityczne i społeczne w innych państwach. Omówione zostały także różne koncepcje rosyjskiej wojny informacyjnej.

W rozdziale piątym, zatytułowanym „Polska w polityce zagranicznej Federacji Rosyjskiej w latach 2010-2022”, omówiono stosunki polsko-rosyjskie w kontekście polityki zagranicznej Federacji Rosyjskiej w latach 2010-2022. Pierwsza część rozdziału dotyczy genezy stosunków polsko-radzieckich oraz polsko-rosyjskich, analizując ich historyczny rozwój i wpływ na obecne relacje między oboma państwami. W dalszej części przedstawiono uwarunkowania polityki zagranicznej Rosji wobec Polski, zarówno wewnętrzne, jak i zewnętrzne. Następnie omówiono stan stosunków polsko-rosyjskich w latach 1992-2009, aby nakreślić tło dla wydarzeń, które miały miejsce po 2010 roku. W tej części szczególnie zwrócono uwagę na zmieniające się dynamiki polityczne i gospodarcze. W kolejnej części rozdziału przedstawiono cele polityki zagranicznej Rosji wobec Polski w latach 2010-2022.

Rozdział omawia również główne kwestie sporne w stosunkach polsko-rosyjskich w tym okresie, takie jak: polityka historyczna, dywersyfikacja źródeł energii, polityka bezpieczeństwa w Europie Środkowo-Wschodniej, oraz rola NATO w regionie. Szczególnie ważne w tym kontekście są także wydarzenia, które miały wpływ na stosunki obu państw, jak katastrofa smoleńska z 2010 roku, aneksja Krymu przez Rosję w 2014 roku oraz wojna w Ukrainie, które dodatkowo pogłębiły napięcia. Ponadto zostały omówione działania Polski w ramach Programu Partnerstwa Wschodniego, które miały na celu wzmacnianie relacji z państwami postradzieckimi i przeciwdziałanie wpływowi Rosji w regionie.

W rozdziale szóstym szczególnie cennym badawczo, jako że o charakterze empirycznym, pod tytułem „Cyberataki jako instrument wojny informacyjnej Federacji Rosyjskiej wobec Polski w latach 2010-2022”, scharakteryzowane zostało cyberbezpieczeństwo Polski w latach 2010-2022. Określony został stopień informatyzacji i digitalizacji Polski, bezpieczeństwo polskiej infrastruktury krytycznej, zagrożenia dla bezpieczeństwa teleinformatycznego Polski oraz system cyberbezpieczeństwa Polski. Następnie omówione zostały wybrane rosyjskie cyberataki na Polskę cyberprzestrzeni w latach 2010-2022 w odniesieniu do cyberataków dokonywanych na wybrane sektory, jak: administracji centralnej i samorządowej, służb specjalnych i sił zbrojnych, infrastruktury krytycznej, publicznych podmiotów gospodarczych oraz na sektor prywatny. Wskazany rozdział jest kluczowy dla realizacji celu pracy jakim jest określenie podatności Polski na prowadzoną przez Rosję wojnę informacyjną w cyberprzestrzeni, jak również potencjału państwa polskiego w zakresie zapewnienia cyberbezpieczeństwa oraz wykrywania i zwalczania cyberataków.

W rozdziale siódmym o charakterze empirycznym, niezwykle cennym badawczo, zatytułowanym „Portale informacyjne jako instrument wojny informacyjnej Federacji Rosyjskiej wobec Polski w latach 2010-2022”, scharakteryzowane zostały dwa anglojęzyczne rosyjskie portale informacyjne, tj. portal internetowy Sputnik News International oraz witryna agencji informacyjnej TASS. Omówione zostały typy publikowanych przez nie treści, rodzaje poruszanych kwestii spornych w stosunkach polsko-rosyjskich, typ stosowanego *framingu* treści oraz wykorzystywane wybrane techniki propagandowe. Zawarte zostały również przykłady w powyższym zakresie. Rozdział ten jest istotny z punktu widzenia celów rozprawy, które sprowadzają się między innymi do zidentyfikowania głównych kanałów oddziaływania propagandowego, które są wykorzystywane w Internecie przez Federację Rosyjską wobec Polski oraz określenia technik propagandowych które są w tym zakresie stosowane.

W rozprawie wykorzystano literaturę polskojęzyczną, anglojęzyczną oraz rosyjskojęzyczną, obejmującą monografie, artykuły naukowe oraz raporty instytucji

badawczych rządowych i pozarządowych. Ponadto skorzystano między innymi z oficjalnych dokumentów państwowych publikowanych przez Kreml w zakresie koncepcji polityki zagranicznej państwa, doktryny wojennej oraz strategii działania w cyberprzestrzeni. Źródła te dostarczyły wiedzy na temat zagadnień teoretycznych oraz praktycznych, dotyczących narzędzi oferowanych przez wojnę informacyjną oraz ich wykorzystania w ramach polityki zagranicznej Federacji Rosyjskiej realizowanej wobec Polski w latach 2010-2022.

Rozdział 1. Pojęcie, uwarunkowania, cele i środki polityki zagranicznej

1.1. Pojęcie polityki zagranicznej

Pojęcie *polityka* jest terminem wieloaspektowym. Występuje w różnych postaciach, cechując się uniwersalnym charakterem w przestrzeni publicznej, a określenie jej początku i końca nie wydaje się możliwe⁵⁰. Arystoteles w swojej rozprawie „Polityka” zdefiniował to pojęcie jako sztukę rządzenia państwem⁵¹, które to z kolei jest wyposażone w autorytet i rząd⁵². W nauce nowożytnej definicję polityki sformułował jeden z najwybitniejszych jej teoretyków M. Weber, który stwierdził, że jest to dążenie do wywierania wpływu na podział władzy pomiędzy jednostkami czy państwami⁵³. Nie można jednak mówić o enumeratywnym katalogu definicji pojęcia polityka. Jak zaznaczył A. Heywood, „istnieje prawie tyle definicji polityki, ile autorytetów, które chcą się w tej sprawie wypowiadać”⁵⁴. W jego ocenie politykę można definiować jako proces podejmowania decyzji, wykonywanie władzy, działalność społeczną, relacje międzyludzkie czy sposób rozwiązywania konfliktów⁵⁵. Wieloaspektowość pojęcia polityka powoduje konieczność jego odniesienia do wielu płaszczyzn funkcjonowania człowieka, jak choćby do stosunków międzynarodowych, gdzie występuje ona pod nazwą *polityka zagraniczna*.

Polityka zagraniczna stanowi zewnątrz przejaw aktywności państw, będących pierwotnymi oraz głównymi uczestnikami stosunków międzynarodowych. Jest jednym z jego podstawowych atrybutów warunkujących zdolność do nawiązywania i utrzymywania stosunków międzynarodowych. Zdolność ta postrzegana jest również jako przesłanka do uznania podmiotowości państwa w rozumieniu prawa międzynarodowego publicznego, a więc

⁵⁰ S. Bieleń: *Polityka w stosunkach międzynarodowych*. Warszawa 2010, s. 13-14.

⁵¹ Dokonując próby zdefiniowania pojęcia państwo, spośród wielu definicji sformułowanych przez badaczy w literaturze specjalistycznej, należy przede wszystkim przywołać tę, której autorem jest G. Jelinek. Stwierdził on, że o państwie mówimy wtedy gdy dany podmiot posiada trzy określone cechy takie jak: terytorium (1), zamieszkałe przez ludność (2) oraz władzę (3) sprawującą nad nimi kontrolę. Definicja ta jest powszechnie akceptowalna w nauce o stosunkach międzynarodowych oraz na gruncie prawa międzynarodowego publicznego. W XX wieku przytoczona definicja została rozbudowana poprzez dodanie jeszcze jednego, czwartego elementu, szczególnie istotnego z punktu widzenia stosunków międzynarodowych, a którym jest zdolność podmiotu do nawiązywania i utrzymywania stosunków dyplomatycznych. Podmiot posiadający wskazane powyżej cztery atrybuty może zostać zdefiniowany jako państwo. Zobacz szerzej: G. Jelinek: *Nauka o państwie*. Warszawa 1921, s. 312; D. Kondrakiewicz: *Państwo. W: Międzynarodowe stosunki polityczne*. Red. M. Pietraś. Lublin 2007, s. 65-91; *Montevideo Convention on the Rights and Duties of States Signed at Montevideo, 26 December 1933 Entered into Force, 26 December 1934 Article 8 reaffirmed by Protocol, 23 December 1936*.

⁵² Zobacz szerzej: Arystoteles: *Polityka*. Wrocław 1953.

⁵³ M. Weber: *Polityka jako zawód i powołanie*. Kraków 1998, s. 37-38.

⁵⁴ A. Heywood: *Teoria polityki. Wprowadzenie*. Warszawa 2009, s. 60.

⁵⁵ Ibidem, s. 60.

wiąże się z przyznaniem danemu tworowi praw podmiotowych w jakie wyposażone jest każde państwo⁵⁶.

T. Łoś-Nowak wskazała, że w XVIII i XIX wieku politykę zagraniczną postrzegano przede wszystkim jako przejaw działalności dyplomatycznej państw będących wyłącznymi uczestnikami stosunków międzynarodowych. Dopiero czasy współczesne, ukazując złożoność oraz stopień skomplikowania stosunków międzynarodowych, których uczestnikami nie są już wyłącznie państwa, wymusiły zredefiniowanie tego pojęcia i dostosowanie go do aktualnie panującej sytuacji na arenie międzynarodowej⁵⁷.

Podobnie jak w odniesieniu do pojęcia polityki, tak i w odniesieniu do definicji polityki zagranicznej należy stwierdzić, że w dyskursie naukowym nie została sformułowana jednoznaczna definicja tego pojęcia, zawierająca wszystkie jego aspekty w sposób wyczerpujący i enumeratywny. Dokonując omówienia pojęcia polityki zagranicznej należy rozpocząć od przytoczenia kilku definicji występujących w nauce o stosunkach międzynarodowych. Współcześnie wskazuje się, że polityka zagraniczna stanowi środek realizacji interesów i celów danego państwa w środowisku międzynarodowym, oczywiście przy uwzględnieniu poszczególnych jej uwarunkowań. Działalność państwa na arenie międzynarodowej cechuje się trwałością i ciągłością, wzajemnym oddziaływaniem podmiotów, ale przede wszystkim (oczywiście w zależności od zdolności danego państwa) możliwością kształtowania stosunków międzynarodowych⁵⁸.

W polskiej nauce o stosunkach międzynarodowych definicje polityki zagranicznej państwa są stosunkowo szeroko omówione, toteż można wyróżnić kilka najczęściej występujących. W. Kostecki zdefiniował politykę zagraniczną jako „układ lub wzór celów i środków jawnych lub ukrytych w działaniach danego państwa wobec innych państw lub ich członków”⁵⁹. Podobną definicję sformułował J. Stefanowicz określając politykę zagraniczną jako „proces racjonalnego myślenia decydentów, warunkowanego przez ich sposób odczytania interesu narodowego, motywacje szczegółowe, analizę sytuacji międzynarodowej oraz bilansową ocenę własnych możliwości”⁶⁰.

Znaczna część badaczy w polskiej nauce o stosunkach międzynarodowych formułuje definicje polityki zagranicznej państwa nadając szczególne znaczenie płaszczyznom na jakich

⁵⁶ Zobacz szerzej: *Montevideo Convention on the Rights and Duties of States Signed at Montevideo, 26 December 1933 Entered into Force, 26 December 1934 Article 8 reaffirmed by Protocol, 23 December 1936.*

⁵⁷ T. Łoś-Nowak: *Stosunki międzynarodowe. Teorie – systemy – uczestnicy.* Wrocław 2006, s. 257-258.

⁵⁸ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych stosunków międzynarodowych.* Warszawa 2004, s. 106.

⁵⁹ W. Kostecki: *Polityka zagraniczna: teoretyczne podstawy badań.* Warszawa 1988, s. 50.

⁶⁰ M. Dobroczyński, J. Stefanowicz: *Polityka zagraniczna.* Warszawa 1984, s. 14.

się ona realizuje, tj. wewnętrznej oraz zewnętrznej. Jednym z nich jest R. Zięba, który określił politykę zagraniczną jako „część ogólnej polityki państwa, która jakkolwiek jest kształtowana w jego systemie wewnętrznym, to jednak realizuje się w systemie międzynarodowym”⁶¹. Wskazał również na otoczenie w jakim jest ona realizowana stwierdzając, że środowisko polityki zagranicznej jest bardzo szerokie, ponieważ składają się na nie elementy systemowe zarówno o charakterze wewnętrznym (państwowe) jak i zewnętrznym (międzypaństwowe). Podkreślił także, że wszystkie wartości zmienne występujące w stosunkach międzynarodowych mają znaczenie, gdyż kształtują w większym bądź mniejszym stopniu treści oraz formę prowadzonej przez państwa polityki zagranicznej⁶². Z. J. Pietraś z kolei zdefiniował politykę zagraniczną jako „proces formułowania i realizacji celów zewnątrzpaństwowych, odzwierciedlających interesy narodu i jego części składowych”⁶³. Inną definicję proponuje J. Kukułka, który stwierdza, że polityka zagraniczna to „działalność zmierzająca do obrony i maksymalizacji uznawanych i preferowanych systemów wartości oraz interesów wewnątrz państwa i w środowisku międzynarodowym”⁶⁴. Z kolei R. Kuźniar definiuje ją jako „zorganizowany i skierowany na zewnątrz wysiłek państwa, podporządkowany osiągnięciu jego żywotnych interesów, który wyraża się w kształtowaniu jego zewnętrznego otoczenia (tworzeniu relacji oraz sytuacji korzystnych, zapobieganiu i usuwaniu sytuacji niekorzystnych)”⁶⁵. T. Łoś-Nowak w swojej definicji szczególną rolę nadaje środowisku w jakim realizuje się polityka zagraniczna pisząc, że jest to „dynamiczny proces formułowania i realizacji interesów narodowych w poliarchicznym i policentrycznym środowisku międzynarodowym”⁶⁶.

Jeszcze inne podejście zaprezentował S. Bieleń wychodząc od polityki zagranicznej państw do polityki w stosunkach międzynarodowych stwierdzając przy tym, że „nie jest ani sztuką rządzenia, ani metodą prawomocnego, legalnego stosowania przemocy, ani tym bardziej autokratywnym podziałem dóbr czy wartości. Jest to przede wszystkim sztuka wpływania na innych w celu zaspokojenia potrzeb i interesów uczestników życia międzynarodowego, którzy

⁶¹ R. Zięba: *Uwarunkowania polityki zagranicznej państwa*. W: *Wstęp do teorii polityki zagranicznej państwa*. Red. R. Zięba. Toruń 2005, s. 17.

⁶² Ibidem, s. 17.

⁶³ Z. J. Pietraś: *Polityka zagraniczna państwa*. W: *Współczesne stosunki międzynarodowe*. Red. T. Łoś-Nowak. Wrocław 1992, s. 52.

⁶⁴ J. Kukułka: *Polityka zagraniczna a polityka wewnętrzna*. W: *Polityka zagraniczna państwa*. Red. J. Kukułka, R. Zięba. Warszawa 1992, s. 19.

⁶⁵ R. Kuźniar: *Międzynarodowe stosunki polityczne*. W: *Stosunki międzynarodowe – geneza, struktura, dynamika*. Red. E. Haliżak, R. Kuźniar. Warszawa 2000, s. 112.

⁶⁶ T. Łoś-Nowak: *Stosunki międzynarodowe...*, s. 192.

koncentrują się na takich wartościach jak: bezpieczeństwo, suwerenność, integralność, tożsamość, ład, sprawiedliwości, wolność, stabilność, rozwój czy dobrobyt”⁶⁷.

Definicje formułowane przez polskich badaczy stosunków międzynarodowych wykazują wiele zbieżności z ich zagranicznymi odpowiednikami, toteż poglądowo należy przytoczyć kilka wybranych. I tak na przykład J. Frankel określił pojęcie polityki zagranicznej jako „rodzaj działań i podejmowanych decyzji w stosunkach międzynarodowych”⁶⁸. W. Wallace odniósł politykę zagraniczną do przestrzeni stwierdzając, że jest to „obszar zachowań politycznych państwa, rodzaj pomostu pomiędzy sprawami wewnętrznymi państwa a jego środowiskiem międzynarodowym”⁶⁹.

Dokonując analizy powyższych definicji należy wskazać na kilka istotnych kwestii. Po pierwsze, polityka zagraniczna jest bezpośrednio związana z polityką wewnętrzną państwa. Po drugie, polityka zagraniczna to proces, w którym zderzają się interesy państw na arenie międzynarodowej. Po trzecie, jest określana przez władzę wykonawczą, która formułuje i realizuje interesy narodowe. Po czwarte, stanowi zbiór hierarchicznie ułożonych celów, które są determinowane przez hierarchicznie ułożone interesy narodowe. Po piąte, polityka zagraniczna państwa realizuje się w policentrycznym oraz poliarchicznym środowisku międzynarodowym. Po szóste, podstawowym celem polityki zagranicznej państwa jest realizowanie jej celów podstawowych, na które składają się takie wartości jak: bezpieczeństwo, potęga, rozwój, integralność czy dobrobyt. I wreszcie po siódme, polityka zagraniczna państwa to jego działalność wewnętrzna realizowana na zewnątrz w systemie międzynarodowym.

Pojęcie polityki zagranicznej należy również odnieść do przestrzeni teoretycznej oraz umiejscowić je w trzech dominujących modelach analitycznych. Najstarszy z nich, model realistyczny, zakorzeniony jest w dziełach N. Machiavellego oraz T. Hobbesa. Model ten rozwinęli wspólnie H. Morgenthau, E. Carr czy R. Niebuhr. W ich rozumieniu najistotniejszym elementem polityki zagranicznej jest rywalizacja państw w przestrzeni międzynarodowej. W teorii realistycznej wskazuje się na nieuchronne konkurowanie ze sobą państw oraz anarchizację stosunków międzynarodowych. Kluczowym narzędziem realizacji polityki zagranicznej w ocenie realistów jest siła militarna państwa gwarantująca jego bezpieczeństwo oraz skuteczność podejmowanych działań⁷⁰.

⁶⁷ S. Bieleń: *Polityka w stosunkach...*, s. 21.

⁶⁸ J. Frankel: *The Making of Foreign Policy*. London 1963, s. 1-10.

⁶⁹ W. Wallace: *Foreign Policy and Political Process*. London 1971, s. 7.

⁷⁰ T. Łoś-Nowak: *Polityka zagraniczna – stale i zmienne komponenty procesu formułowania i realizacji*. W: *Polityka zagraniczna: aktorzy, potencjały, strategie*. Red. T. Łoś-Nowak. Warszawa 2011, s. 21-24.

Swego rodzaju ograniczoność realizmu w zakresie badań nad stosunkami międzynarodowymi spowodowała powstanie nowego modelu analitycznego jakim był modernizm. W tym podejściu, którego przedstawicielami byli tacy badacze jak J. Burton, M. Doyle czy J. N. Rosenau, poddano pod wątpliwość badania odnoszące się przede wszystkim do państwa jako podstawowego uczestnika stosunków międzynarodowych⁷¹. Nowe podejście umożliwiło rozpoczęcie badań nad innymi uczestnikami takimi jak organizacje międzynarodowe, ruchy społeczne i polityczne, narody nieposiadające własnego państwa czy korporacje międzynarodowe. Na utratę pozycji państwa jako uczestnika stosunków międzynarodowych wskazał J. N. Rosenau, który w swojej pracy skupił się przede wszystkim na dynamice zmian jaka towarzyszy stosunkom międzynarodowym i jej wpływie na kreowanie polityki zagranicznej. Ponadto, odniósł się również do efektywności działań podejmowanych przez państwa oraz do prawa publicznego międzynarodowego⁷².

Innym nurtem szczególnie zakorzenionym w nauce o stosunkach międzynarodowych jest neoliberalizm. Wskazywał on na istotną rolę państwa w stosunkach międzynarodowych, jednak podkreślał również rolę pozostałych podmiotów, zwłaszcza odnosząc ich znaczenie do międzynarodowych stosunków gospodarczych. Zjawisko globalizacji oraz postępujące w jej wyniku zatarcie klasycznego podziału na politykę wewnętrzną i zewnętrzną państwa spowodowało pojawienie się zjawiska uspołecznienia polityki zagranicznej. Według neoliberalów, na politykę oddziałują nie tylko takie podmioty jak państwa i korporacje transnarodowe, ale również opinia publiczna, organizacje pozarządowe, narody (bez państwa), czy poszczególne grupy interesów. Podkreśla się również występujące współzależności międzynarodowe zaznaczając, że dynamiczny rozwój ekonomiczny państw wymusza lokowania kapitału w wymiarze transnarodowym, a nie głównie narodowym jak miało to miejsce dotychczas. Korzyści wynikające z takich działań to przede wszystkim generowanie zysku poprzez działalność międzynarodową, co z kolei przekłada się na małą skłonność do stosowania środków przymusu międzynarodowego, takich jak użycie siły zbrojnej, stosowanie groźby czy sankcje. Innym istotnym elementem teorii neoliberalizmu są relacje zachodzące pomiędzy państwem a społeczeństwem. Różne warstwy społeczne prezentują różne interesy.

⁷¹ R. Jackson, G. Sorensen: *Introduction to International relations. Theories and Approaches*. New York 2003, s. 109-115.

⁷² J. N. Rosenau: *Comparative Foreign Policy: Fad, Fantasy or Field?* "International Studies Quarterly" 1968, Vol. 12, s. 296-329.

Dążąc do ich realizacji oddziałują one na państwa, stając się współuczestnikiem tworzenia stosunków międzynarodowych⁷³.

Reasumując rozważania dotyczące zagadnienia polityki zagranicznej państwa należy wskazać na dwie najpełniejsze oraz najbardziej użyteczne definicje polityki zagranicznej państwa sformułowane przez R. Ziębę oraz S. Bielenia. Ich zestawienie pozwala na wskazanie, że polityką zagraniczną państwa jest jego działalność wewnętrzna podlegająca poszczególnym uwarunkowaniom, skierowana na zewnątrz i tam wykonywana, a której celem jest realizacja i ochrona podstawowych interesów oraz własnych wartości takich jak bezpieczeństwo, potęga, integralność, rozwój czy przetrwanie. Dalej wskazać należy, że w wyniku prowadzonej przez poszczególne państwa polityki zagranicznej może dochodzić do ścierania się sprzecznych ze sobą interesów, co może stanowić przyczynę napięć, kryzysów oraz konfliktów.

1.2. Uwarunkowania polityki zagranicznej

Przestrzeń w jakiej kształtuje się polityka zagraniczna jest bardzo szeroka, a określenie jej początku i końca wydaje się być bardzo trudne, a wręcz niemożliwe. Mnogość i dynamika procesów zachodzących na arenie międzynarodowej w wyniku realizowanych przez państwa ich własnych polityk zagranicznych skłania do sformułowania twierdzenia, że środowisko polityki zagranicznej może być, a w zasadzie jest, warunkowane przez pewne czynniki. Powstaje więc konieczność ich nazwania oraz określenia w jaki sposób determinują one działalność państw w środowisku międzynarodowym w ramach prowadzonej przez nie polityki zagranicznej. W literaturze specjalistycznej czynniki te nazywane są *determinantami*, *wyznacznikami*, *kontekstami*, *przesłankami* czy *uwarunkowaniami*⁷⁴.

R. Zięba stosując ujęcie systemowe wskazał, że elementy otoczenia polityki zagranicznej należy badać przy uwzględnieniu ich genezy. Przyjął więc, że czynniki oddziałujące na politykę zagraniczną stanowią jej uwarunkowania, na które składają się czynniki warunkujące oraz czynniki sprawcze⁷⁵. Takie założenie wydaje się słuszne, gdyż pojęcie uwarunkowań jest zdecydowanie szersze od występujących w literaturze pojęć wyznaczników⁷⁶, czynników, determinantów czy przesłanek⁷⁷.

⁷³ R. Tenerowicz: „Nowy liberalizm”. W: *Teorie i podejścia badawcze w nauce o stosunkach międzynarodowych*. Red. R. Zięba, S. Bielen, J. Zajac. Warszawa 2015, s. 29-43.

⁷⁴ S. Bielen: *Polityka w stosunkach...*, s. 13-14; R. Zięba: *Uwarunkowania polityki zagranicznej państwa*. W: *Wstęp do teorii polityki...*, s. 17-19.

⁷⁵ R. Zięba: *Uwarunkowania polityki zagranicznej państwa*. W: *Wstęp do teorii polityki...*, s. 17.

⁷⁶ J. Pietraś: *Podstawy teorii stosunków międzynarodowych*. Lublin 1986, 83-105.

⁷⁷ M. Dobroczyński, J. Stefanowicz: *Polityka zagraniczna...*, s. 9-12.

Określenie uwarunkowań polityki zagranicznej państwa jest zadaniem bardzo trudnym. Uzależnione jest bowiem ono od wielu czynników, takich jak chociażby wielkość państwa, jego zasoby, stopień rozwoju gospodarczego, potencjał demograficzny, otoczenie międzynarodowe czy położenie, a to tylko niektóre z nich, gdyż katalog ten nie jest enumeratywny. W związku z tym w pierwszej kolejności należałoby dokonać klasyfikacji uwarunkowań z uwagi na obszar materii, której one dotyczą. Znaczna część badaczy dokonuje podziału wyróżniając determinanty polityki zagranicznej o charakterze wewnętrznym (krajowe) oraz o charakterze zewnętrznym (międzynarodowe)⁷⁸. Inni z kolei proponują klasyfikację uwzględniającą uwarunkowania takie jak: międzynarodowe, rządowe i krajowe⁷⁹. Wreszcie jedną z propozycji klasyfikacji, szczególnie rozpowszechnioną w nauce amerykańskiej, zaproponowali M. Sprout i H. Sprout dokonując wyodrębnienia sfery psychologicznej oraz sfery operacyjnej. Pierwsza z nich odnosi się do oczekiwań i wyobrażeń decydentów politycznych w zakresie realizowanej polityki zagranicznej. Z kolei druga z nich odnosi się do rzeczywistych możliwości w kontekście oddziaływania na inne podmioty na arenie międzynarodowej⁸⁰. Wydaje się, że spośród wszystkich klasyfikacji uwarunkowań polityki zagranicznej państwa najszerzej rozpropagowana oraz najbardziej użyteczna jest ta występująca głównie w nauce europejskiej. Klasyfikacja ta zakłada bowiem podział uwarunkowań na obiektywne i subiektywne oraz wewnętrzne i zewnętrzne, dopuszczając jednocześnie ich wzajemne nakładanie się na siebie. Wyodrębnione zostały zatem następujące uwarunkowania polityki zagranicznej państwa takie jak: uwarunkowania wewnętrzne o charakterze obiektywnym, uwarunkowania wewnętrzne o charakterze subiektywnym, uwarunkowania zewnętrzne o charakterze obiektywnym oraz uwarunkowania zewnętrzne o charakterze subiektywnym⁸¹.

R. Zięba odnosząc się do wskazanej teorii stwierdził, że stosując taką klasyfikację niezbędne jest w pierwszej kolejności jej pogrupowanie. Zaproponował dokonanie tego w sposób następujący: „Biorąc za punkt wyjścia tezę głoszącą, że polityka zagraniczna stanowi publiczną działalność celową państwa skierowaną na środowisko międzynarodowe – prymat należy przyznać uwarunkowaniom wewnętrznym przed zewnętrznymi, a w każdej z tych grup – obiektywnym przed subiektywnymi”⁸². Odnosząc się do powyższej tezy zastrzegł, że ma

⁷⁸ G. Modelski: *A Theory of Foreign Policy: An Analysis of Decision-Making*. London 1963, s. 54-94; A. F. K. Organski: *World Politics*. New York 1958, s. 78-79; H. Sprout, M. Sprout: *An Ecological Paradigm for Study of International Politics*. Princeton 1968, s. 30-33.

⁷⁹ M. Webber, M. Smith: *Foreign Policy in a Transformed World*. Harlow 2002, s. 30-38.

⁸⁰ R. Zięba: *Uwarunkowania polityki zagranicznej państwa. W: Wstęp do teorii...*, s. 18-35. Zobacz szerzej: H. Sprout, M. Sprout: *Man – Milieu Relationship Hypotheses in the Context of International Politics*. Princeton 1956.

⁸¹ Ibidem, s. 18-35.

⁸² Ibidem, s. 19.

ona „charakter ogólny, a nie mechanistyczny. Możliwe są bowiem sytuacje, w których uwarunkowania obiektywne lub subiektywne mogą w głównej mierze determinować działania polityki zagranicznej państwa”⁸³.

Omawiając klasyfikację uwarunkowań polityki zagranicznej państwa należy również odnieść się do sposobu analizy jej poszczególnych typów. J. N. Rosenau wyodrębnia trzy sposoby analizy takie jak: wertykalny, horyzontalny oraz diagonalny. Pierwszy z nich zakłada, że działania podejmowane przez państwo mogą być wynikiem kontynuacji działań podejmowanych w przeszłości, a zatem konieczne jest przeprowadzanie analizy wybranych, ewoluujących w czasie uwarunkowań. Drugi typ analizy (horyzontalny) uwzględnia z kolei czynniki oddziałujące na politykę zagraniczną w danym momencie. Ostatni, trzeci z typów analizy uwarunkowań polityki zagranicznej (diagonalny), stanowi kompilację dwóch poprzednich, umożliwiając jej dokonanie zarówno odnosząc się do stanu faktycznego (danej sytuacji), jak i jego genezy⁸⁴.

Na gruncie niniejszej rozprawy przyjęto klasyfikację uwarunkowań polityki zagranicznej zaproponowaną i rozpowszechnioną w nauce europejskiej oraz dokonującą wyodrębnienia następujących uwarunkowań takich jak: uwarunkowań wewnętrznych o charakterze obiektywnym, uwarunkowań wewnętrznych o charakterze subiektywnym, uwarunkowań zewnętrznych o charakterze obiektywnym oraz uwarunkowań zewnętrznych o charakterze subiektywnym.

1.2.1. Uwarunkowania wewnętrzne o charakterze obiektywnym

Na uwarunkowania wewnętrzne o charakterze obiektywnym składają się: środowisko geograficzne państwa, potencjał ludnościowy, potencjał gospodarczy i naukowo-techniczny, system społeczno-polityczny⁸⁵, czynniki militarne⁸⁶. Ponad powyższe można wyróżnić inne uwarunkowania takie jak: kulturowo-cywilizacyjne, kulturowe, ideologiczne, etniczno-narodowe⁸⁷, działalność instytucji i organizacji międzynarodowych, historyczne⁸⁸ oraz osobowościowe (wybitne jednostki)⁸⁹.

⁸³ Ibidem, s. 19.

⁸⁴ J. N. Rosenau: *The Scientific Study of Foreign Policy*. London 1980, s. 320-321.

⁸⁵ R. Zięba: *Uwarunkowania polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 20.

⁸⁶ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych...*, s. 108-111.

⁸⁷ A. Czarnocki: *Czynniki międzynarodowych stosunków politycznych*. W: *Międzynarodowe stosunki polityczne*. Red. M. Pietraś. Lublin 2007, s. 44-64.

⁸⁸ J. Kukułka: *Międzynarodowe stosunki polityczne*. Warszawa 1982, s. 89-92.

⁸⁹ J. Bryła: *Czynniki kształtujące stosunki międzynarodowe*. W: *Międzynarodowe stosunki polityczne*. Red. W. Malendowski, Cz. Mojsiewicz. Poznań 1996, s. 35-36.

Uwarunkowania wewnętrzne o charakterze obiektywnym wiodą prym pośród wszystkich ich rodzajów. Wynika to przede wszystkim z faktu, że to uwarunkowania wewnętrzne występujące w danym państwie, mające jednocześnie charakter obiektywnych, a więc rzeczywistych, mogą w największym stopniu oddziaływać na dynamikę i ewolucję prowadzonej przez państwo polityki zagranicznej. To właśnie w strukturach wewnątrzpaństwowych, na poziomie rządowym, podejmowane są decyzje co do kierunków prowadzonej polityki zagranicznej oraz celów jakie ma ona pełnić. Realizacja przyjętych założeń będzie z kolei zależać od rzeczywistych (obiektywnych) zdolności danego państwa do oddziaływania na innych uczestników stosunków międzynarodowych.

Pierwszym typem uwarunkowań wewnętrznych o charakterze obiektywnym jest środowisko geograficzne państwa. Środowisko geograficzne państwa obejmuje przede wszystkim obszar państwa (jego wielkość), rzeźbę terenu na jakim się ono znajduje (np. góry, morza, doliny, płaskowyże, pustynie itp.), klimat (np. umiarkowany, tropikalny, wysokogórski itp.), faunę oraz florę (występowanie określonych gatunków zwierząt i roślinności), a przede wszystkim zasoby naturalne (stałe, odnawialne, nieodnawialne)⁹⁰. W nauce o stosunkach międzynarodowych środowisko geograficzne państwa zajmuje szczególne miejsce w kształtowaniu jego polityki zagranicznej⁹¹. Poglądy postulujące wyjaśnianie zjawisk politycznych czynnikami geograficznymi zyskały do tego stopnia na znaczeniu, że w literaturze specjalistycznej pojawiła się teoria determinizmu geograficznego⁹². Teoria ta zakłada wyjaśnianie zjawisk na arenie międzynarodowej, a w szczególności prowadzonej przez państwa polityki zagranicznej, na podstawie zajmowanego przez dane państwo terytorium na którym to występuje określony klimat, fauna, flora oraz zasoby naturalne. Teoria ta ma jednak zasadniczą wadę, o której pisał R. Bierzanek wskazując, że „teorie te należy zaliczyć do rzędu poglądów wyjaśniających złożone zjawiska społeczne jednym tylko czynnikiem, podczas gdy w rzeczywistości czynników tych jest wiele”⁹³. Należy zgodzić się z zaprezentowanym poglądem uwzględniając przy tym w szczególności dynamikę zmian występującą we współczesnych stosunkach międzynarodowych, które nie są zależne jedynie od środowiska geograficznego państwa. Nie ulega jednak wątpliwości, że czynniki geograficzne z pewnością decydują o realizowanej przez dane państwo strategii polityczno-militarnej. Dostęp do morza oraz jego zakres będzie warunkował rozwój floty morskiej. Z kolei kraj kontynentalny będzie

⁹⁰ Ibidem, s. 108-109.

⁹¹ J. Frankel: *The Making of Foreign...*, s. 57-61; M. Merle: *Sociologie des relations internationales*. Paris 1974, s. 149-158.

⁹² C. Jean: *Geopolityka*. Wrocław 2003, s. 60-97.

⁹³ R. Bierzanek: *Współczesne stosunki międzynarodowe*. Warszawa 1980, s. 40.

prowadził politykę zakładającą rozbudowę przede wszystkim sił lądowych. Podobnie państwo posiadające znaczne zasoby naturalne będzie miało większy potencjał gospodarczy, a jednocześnie być może stanie się polem rywalizacji innych państw o posiadane przez nie surowce⁹⁴.

Charakter środowiska geograficznego jako uwarunkowanie polityki zagranicznej państwa ulega zmianom również w związku z postępującym rozwojem technologicznym. Należy to odnieść przede wszystkim do znaczenia wielkości obszaru danego państwa. Przez wiele wieków decydujące znaczenie dla bezpieczeństwa miała rozległość oraz dostępność terytorium. Współcześnie, dzięki zaawansowanym technologiom (np. lotnictwo, pociski balistyczne, nawigacja satelitarna itp.), czynnik ten ma znaczenie jedynie na obszarach słabo rozwiniętych, gdzie państwa nie dysponują zaawansowaną technologią cywilną lub wojskową⁹⁵.

Drugim typem ze wskazanych uwarunkowań jest potencjał ludnościowy (demograficzny) państwa. Zjawiska demograficzne na które składa się: liczba ludności, wysokość przyrostu naturalnego, kształt piramidy wieku oraz migracje mogą w różnym stopniu kształtować realizowaną przez państwa politykę zagraniczną. Potencjał ludnościowy miał szczególne znaczenie w XIX wieku, kiedy potęga państw w stosunkach międzynarodowych była w dużym stopniu zależna od wielkości posiadanych przez nie sił zbrojnych. Te z kolei były tworzone przede wszystkim w oparciu o powszechny pobór do służby wojskowej, a więc im więcej ludności posiadało dane państwo, tym większe siły było w stanie wystawić do walki. Wydaje się, że współcześnie potencjał ludnościowy traci coraz bardziej na znaczeniu. Dysproporcja liczby ludności pomiędzy danymi państwami nie stanowi już o ich potędze jak miało to miejsce w przeszłości. I tak do państw mocarstwowych zaliczymy zarówno Francję posiadającą ponad 60 milionów ludności jak i Chiny, gdzie liczba ta wynosi ponad 1,4 miliarda⁹⁶. Należy jednak podkreślić, że pomimo iż rozwój technologii wojskowych spowodował spadek znaczenia potencjału demograficznego, to jednak państwo aspirujące do roli mocarstwa powinno dysponować dostateczną jego ilością. Wysokość przyrostu naturalnego oraz kształt piramidy wieku determinuje potencjał ludnościowy poprzez jest wzrost lub spadek. Migracje z kolei mogą stanowić czynnik powstawania napięć i konfliktów, spowodowanych problemem asymilacji ludności napływowej z rodzimą⁹⁷.

⁹⁴ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych...*, s. 108-109.

⁹⁵ J. Bryła: *Czynniki kształtujące stosunki międzynarodowe*. W: *Międzynarodowe stosunki...*, s. 29-30.

⁹⁶ R. Kuźniar: *Stosunki międzynarodowe – istota, uwarunkowania, badanie*. W: *Stosunki międzynarodowe – geneza, struktura, dynamika*. Red. E. Haliżak, R. Kuźniar. Warszawa 2000, s. 23-24.

⁹⁷ A. Czarnocki: *Czynniki międzynarodowych stosunków politycznych*. W: *Międzynarodowe stosunki...*, s. 45-47.

Trzecim typem jest potencjał gospodarczy i naukowo-techniczny, którego wzrost znaczenia nastąpił wraz z początkiem ery przemysłowej. Jego elementami składowymi są przede wszystkim: zdolność produkcyjna, wymiana handlowa, wielkość kapitału na rynku, rodzaj i skala inwestycji czy rozwój nowych technologii. Należy również podkreślić, że potencjał gospodarczy i naukowo-techniczny będzie stanowił o sile państwa o ile jest on umiejętnie wykorzystywany. Globalizacja spowodowała internacjonalizację procesów ekonomicznych. Więzy gospodarcze występujące pomiędzy państwami zacieśniają się, wzrasta wymiana handlowa oraz przepływ kapitału. Skutkiem tego jest zwiększenie powiązań oraz współzależności gospodarek państw w skali całego świata. Współzależności te często determinują realizację celów polityki zagranicznej poprzez oddziaływanie państw silniejszych (wysoko rozwiniętych) na państwa słabsze⁹⁸. Potrzeby ekonomiczne państw kształtują cele polityki zagranicznej, a z drugiej strony posiadany potencjał gospodarczy i naukowo-techniczny umożliwia skuteczniejszy wpływ na procesy zachodzące na arenie międzynarodowej⁹⁹. Omawiając wpływ ekonomii na stosunki międzynarodowe nie sposób pominąć roli korporacji transnarodowych. Zdarza się bowiem, że ich cele krzyżują się z celami ekonomicznymi państw, powodując wzajemne oddziaływanie. Inną istotną kwestią którą należy poruszyć jest podział świata na bogatą północ i biedne południe. Różnice w poziomie życia mogą powodować poczucie społecznej niesprawiedliwości i w konsekwencji oddziaływać konfliktogennie na stosunki międzynarodowe. Z jednej bowiem strony wyróżniamy społeczeństwa bogate, dążące do masowego, konsumpcjonistycznego zaspokajania swoich potrzeb, a z drugiej strony społeczeństwa biedne, stanowiące większą część na świecie, które z kolei dążą do zaspokajania przede wszystkim swoich elementarnych potrzeb, co może po ich stronie rodzić frustrację, a w konsekwencji chęć zmiany tak ukształtowanego systemu społecznego¹⁰⁰.

Czwartym typem uwarunkowań wewnętrznych o charakterze obiektywnym jest system społeczno-polityczny państwa. Jest on istotny przede wszystkim z uwagi na fakt, że to w jego wnętrzu podejmowane są decyzje warunkujące założenia i kształt polityki zagranicznej. Na system społeczno-polityczny składają się następujące jego części: administracja rządowa i samorządowa, obowiązujący porządek prawny (system prawny), forma rządów, reżim polityczny, ustrój terytorialny, organizacje społeczne, elity rządzące i nierządzące, grupy

⁹⁸ Ibidem, s. 32-34.

⁹⁹ R. Bierzanek: *Współczesne stosunki...*, s. 46-56.

¹⁰⁰ A. Czarnocki: *Czynniki międzynarodowych stosunków politycznych*. W: *Międzynarodowe stosunki...*, s. 47-48.

interesów i nacisku oraz opinia publiczna¹⁰¹. W odniesieniu do powyższych elementów R. Zięba słusznie zauważył, że „wymienione elementy systemu społeczno-politycznego państwa ujmowane łącznie stanowią mechanizm artykulacji potrzeb i interesów, które na szczeblu centralnym stanowią podstawę do formułowania celów polityki zagranicznej”¹⁰². System społeczno-polityczny determinuje określanie celów oraz metod realizacji polityki zagranicznej państwa. Wydaje się również, że szczególną rolę należy przypisać tutaj elementowi, którym jest ustrój państwa. W zależności od tego czy państwo jest rządzone demokratycznie albo totalitarnie bądź autorytarnie, co z kolei sprowadza się do rządów niedemokratycznych, procesy decyzyjne w zakresie polityki zagranicznej mogą być podejmowane przez różne grupy, o różnej strukturze oraz w różny sposób. I tak w przypadku rządów demokratycznych będą to elity rządzące, ale poddane konstytucyjnej kontroli parlamentów lub innych uprawnionych do tego organów państwa, a także kontroli społecznej, która prowadzona jest przez opinię publiczną. Z kolei w przypadku rządów niedemokratycznych, kształtowanie realizowanej polityki zagranicznej skupione będzie w wąskim kręgu elit rządzących, niepodlegających niczyjej kontroli. W odniesieniu do powyższego E. Cziomer słusznie stwierdził, że „sprawny i spójny system sprzyja aktywnej oraz elastycznej polityce zagranicznej, natomiast wszelkie reżimy niedemokratyczne i biurokratyczno-autorytarne prowadzą do nadmiernej centralizacji, a w konsekwencji także niskiej efektywności”¹⁰³.

Ostatnim, piątym z typów uwarunkowań wewnętrznych o charakterze obiektywnym które należy omówić są czynniki militarne. Składają się na nie takie elementy jak: liczebność sił zbrojnych, zaawansowanie technologiczne armii, rodzaje posiadanych sił zbrojnych, zdolności taktyczne i operacyjne, a współcześnie przede wszystkim dostęp do broni masowego rażenia (broni jądrowej). Siły wojskowe państw, bez względu na epokę historyczną, miały niepodważalny oraz zasadniczy wpływ na kształtowanie stosunków międzynarodowych. Było to szczególnie widoczne w okresie, kiedy prowadzenie wojen nie było nielegalne z punktu widzenia prawa międzynarodowego publicznego¹⁰⁴. Przyjęte w XX wieku regulacje prawnomiędzynarodowe w znacznym stopniu ograniczyły możliwość stosowania groźby lub użycia siły przez państwa, dopuszczając jednak pewne wyjątki od tej zasady, a możliwość ich zastosowania oddając pod rozstrzygnięcie Organizacji Narodów Zjednoczonych (Rady

¹⁰¹ R. Zięba: *Uwarunkowania polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 24-26.

¹⁰² Ibidem, s. 25.

¹⁰³ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych...*, s. 110.

¹⁰⁴ Zobacz szerzej: *Karta Narodów Zjednoczonych, Statut Międzynarodowego Trybunału Sprawiedliwości i Porozumienie ustanawiające Komisję Przygotowawczą Narodów Zjednoczonych* (Dz.U. 1947 nr 23 poz. 90).

Bezpieczeństwa)¹⁰⁵. Znaczenie sił zbrojnych w realizowanej polityce zagranicznej państw uległo w związku z tym istotnym i daleko posuniętym zmianom. Stały się one elementem polityki odstraszania, pozostając w nieustannej gotowości do ich użycia. Przejawem takiego stanu rzeczy na arenie międzynarodowej może być wyścig zbrojeń, widoczny szczególnie w okresie zimnowojennym¹⁰⁶.

Wraz z zakończeniem II wojny światowej, u schyłku której Stany Zjednoczone Ameryki (USA) dokonały rzutu bomb jądrowych na japońskie miasta Hiroszima (6 sierpnia 1945) oraz Nagasaki (9 sierpnia 1945), rozpoczęła się era broni jądrowej. Koniecznym stało się dokonanie rozgraniczenia broni na taką o charakterze konwencjonalnym oraz nuklearnym (jądrowym). Postępujące upowszechnianie broni jądrowej wśród wielu państw w okresie zimnowojennym (1947-1991) doprowadziło do powstania zjawiska samoograniczania jej wykorzystania. Było to skutkiem między innymi powstania doktryny wzajemnego zagwarantowanego zniszczenia oraz doktryny odstraszania¹⁰⁷. Zakończenie zimnej wojny zminimalizowało ryzyko użycia broni jądrowej, jednak jej posiadanie nadal jest wyznacznikiem pozycji mocarstwowej na arenie międzynarodowej. Ponadto, większość państw nadal przeznacza ogromne środki na zbrojenia, co dowodzi istotnej roli jaką pełnią siły zbrojne w realizowanej polityce zagranicznej. Skutkiem takich działań jest oczywiście zwiększanie swoich zdolności w zakresie oddziaływania na uczestników stosunków międzynarodowych¹⁰⁸.

1.2.2. Uwarunkowania wewnętrzne o charakterze subiektywnym

Do uwarunkowań wewnętrznych o charakterze subiektywnym zaliczamy: koncepcje polityki zagranicznej, percepcje środowiska międzynarodowego przez własne społeczeństwo i państwo oraz postawy społeczne wobec innych państw i narodów, jakość oraz aktywność własnej służby zagranicznej i dyplomacji¹⁰⁹.

Pierwszym z uwarunkowań wewnętrznych o charakterze obiektywnym są koncepcje polityki zagranicznej państwa. Przez koncepcje polityki zagranicznej należy rozumieć formułowanie przez decydentów politycznych wizji realizacji polityki zagranicznej.

¹⁰⁵ J. Kukułka: *Międzynarodowe stosunki...*, s. 88-89.

¹⁰⁶ J. Bryła: *Czynniki kształtujące stosunki międzynarodowe. W: Międzynarodowe stosunki...*, s. 34-35.

¹⁰⁷ Doktryna wzajemnego zagwarantowanego zniszczenia zakładała, że w przypadku użycia przez jakiekolwiek państwo broni jądrowej lub też rozpoczęcia konfliktu nuklearnego, doszłoby do zagłady wszystkich jego stron. Doktryna wzajemnego zagwarantowanego zniszczenia opiera się na teorii odstraszania, która zakłada, że jedynym sposobem na uniknięcie wrogiego ataku jest posiadanie arsenału większego niż potencjalny przeciwnik.

¹⁰⁸ J. Bryła: *Czynniki kształtujące stosunki międzynarodowe. W: Międzynarodowe stosunki...*, s. 34-35.

¹⁰⁹ R. Zięba: *Uwarunkowania polityki zagranicznej państwa. W: Wstęp do teorii...*, s. 26-29.

Decydentami w zależności od występującego w danym państwie systemu politycznego może być rząd lub prezydent, czy też innego rodzaju powołane do tego organy. Wybór koncepcji polityki zagranicznej może być dokonywany poprzez wybór jednej z wielu zaproponowanych, bądź też wypracowanie zupełnie nowej koncepcji, stanowiącej efekt połączenia kilku z nich¹¹⁰. Jak pisze R. Zięba, koncepcja polityki zagranicznej państwa „stanowi pewien przemyślany, wyważony stan rzeczy i spraw, który, zdaniem jej autorów, powinien stać się realny”¹¹¹. Wskazuje również, że koncepcja polityki zagranicznej „jest więc kategorią należną do sfery świadomości społecznej: wyraża wartości i interesy społeczeństwa (narodu), które mają być realizowane poprzez stosunki państwa ze środowiskiem międzynarodowym”¹¹². Należy również zaznaczyć, że koncepcja polityki zagranicznej państwa nie pozostaje w całości jawna wobec opinii publicznej państw. Opinia publiczna ma dostęp do doktryny polityki zagranicznej, która zawiera uszeregowane pod kątem ich znaczenia cele polityki zagranicznej. Te z kolei mogą być uszczegółowione i zawarte w programach, skąd wynikają kierunki, płaszczyzny, środki oraz metody działania państwa. Część jawna koncepcji polityki zagranicznej jest bardzo często zawierana w publikowanych przez właściwe organy państwowe aktach prawnych i oficjalnych dokumentach rządowych, takich jak na przykład: koncepcje, doktryny, strategie czy białe księgi¹¹³. Wizje, koncepcje i programy polityki zagranicznej, jak pisze E. Cziomer, muszą „nie tylko zawierać ogólne i zhierarchizowane cele, lecz wskazywać przy pomocy jakich metod, instrumentów i środków można je będzie realizować”¹¹⁴.

Drugim z uwarunkowań wewnętrznych o charakterze subiektywnym jest percepcja środowiska międzynarodowego przez własne społeczeństwo i państwo oraz postawy społeczne wobec innych państw i narodów. Percepcja otoczenia międzynarodowego odnosi się do tego, w jaki sposób elity rządzące, grupy interesów, media oraz społeczeństwo postrzegają innych uczestników na arenie międzynarodowej. Postrzeganie to, jak pisze E. Cziomer, może być uzależnione od „tradycji historycznej, poziomu wykształcenia, kultury politycznej oraz dominujących w społeczeństwie ideologii, religii, poglądów oraz przekonań i świadomości politycznej”¹¹⁵. Percepcja stanowi również zainicjowanie procesu pozyskiwania wiedzy o środowisku międzynarodowym, a w konsekwencji umożliwia prawidłowe formułowanie

¹¹⁰ R. Zięba: *Uwarunkowania polityki zagranicznej polski na początku drugiej dekady XXI wieku*. „Stosunki międzynarodowe – International Relations” 2011, nr 1-2 (T.43), s. 20.

¹¹¹ R. Zięba: *Uwarunkowania polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 27.

¹¹² Ibidem, s. 27.

¹¹³ W. J. Szczepański: *Europa myśli politycznej de Gaulle’a. Próby analizy systemowej*. Warszawa 1979, s. 55-69.

¹¹⁴ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych...*, s. 111.

¹¹⁵ Ibidem, s. 110.

ocen oraz wniosków w kontekście realizowanej przez dane państwo polityki zagranicznej¹¹⁶. Należy zatem stwierdzić, że przyjęcie prawidłowej percepcji środowiska międzynarodowego warunkuje sposób działania państwa na arenie międzynarodowej, a im bardziej złożone są koncepcje polityki zagranicznej państwa, tym jego percepcja powinna być szersza i głębsza, a nadto uwzględniać ocenę rezultatów działań podejmowanych przez to państwo¹¹⁷. Szczególnym składnikiem omawianego uwarunkowania na który należy zwrócić uwagę jest czynnik historyczny, przez który należy rozumieć wszelkiego rodzaju obciążenia historyczne, dotyczące stosunków pomiędzy poszczególnymi państwami. Nie mają one charakteru przejściowego, lecz utrzymują się przez bardzo długi czas, kształtują stereotypy i uprzedzenia, a w wielu przypadkach mogą i będą oddziaływać na procesy decyzyjne w ramach realizowanej polityki zagranicznej. W konsekwencji skutkować będą podejmowaniem nieracjonalnych lub nieadekwatnych działań z punktu widzenia interesów danego państwa. Dlatego też podkreśla się, jak ważna jest działalność edukacyjna realizowana przez organizacje polityczne, społeczne i kulturalne, a których celem powinno być przełamywanie istniejących obciążeń historycznych występujących pomiędzy uczestnikami stosunków międzynarodowych¹¹⁸.

Trzecim i ostatnim z uwarunkowań wewnętrznych o charakterze subiektywnym jest jakość oraz aktywność własnej służby zagranicznej i dyplomacji. Jest ona jednym z głównych elementów wykonawczych prowadzonej przez państwo polityki zagranicznej, stanowiąc całokształt systemu organizacyjnego, w skład którego wchodzi służba zagraniczna oraz dyplomacja. Jest swego rodzaju procesem oraz zespołem czynności polegających na kształtowaniu otoczenia międzynarodowego przez państwo. Zwolennicy behawioryzmu wskazują na szczególne znaczenie czynnika ludzkiego w służbie zagranicznej oraz dyplomacji, przez który należy rozumieć kwalifikacje, predyspozycje czy cechy osobowościowe polityków oraz urzędników realizujących politykę zagraniczną państwa¹¹⁹. Jak wskazuje R. Zięba, „wpływ polityków: przywódców państw, szefów rządów, ministrów spraw zagranicznych czy parlamentarzystów na politykę zagraniczną, jest bezpośredni i bardzo duży, gdyż to właśnie oni są jej aktorami i decydentami”¹²⁰. Potwierdza się zatem kolejny pogląd behawiorystów uznający istotną rolę wybitnych jednostek, które działając w charakterze decydentów politycznych formułują koncepcje działań zewnętrznych państwa, realizując w konsekwencji

¹¹⁶ R. Zięba: *Polityki zagraniczna Polski w strefie euroatlantyckiej*. Warszawa 2013, s. 24-25.

¹¹⁷ J. Kukułka: *Polityka zagraniczna jako element procesu oddziaływań międzynarodowych*. W: *Zmienność i instytucjonalizacja stosunków międzynarodowych*. Red. J. Kukułka. Warszawa 1988, s. 153-154.

¹¹⁸ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych...*, s. 111.

¹¹⁹ R. Bierzanek, *Współczesne stosunki...*, s. 94-99.

¹²⁰ R. Zięba: *Polityki zagraniczna Polski...*, s. 32.

politykę zagraniczną¹²¹. Innym istotnym czynnikiem w zakresie jakości i aktywności służby zagranicznej państwa jest wykwalfikowanie i przygotowanie jej kadr, wspomaganych przez zaplecze nowoczesnych technologii¹²². Jak pisze E. Cziomer, chodzi tu o „system doboru, weryfikacji, zasady rotacji służby dyplomatycznej, poziom merytoryczny, predyspozycje indywidualne i kwalifikacje dyplomatów oraz ekspertów, jak też utrzymanie sprawności organizacyjnej oraz wyposażenie centrali i placówek w nowoczesny sprzęt i urządzenia”¹²³. Służba zagraniczna oraz podejmowane przez nią działania dyplomatyczne służą bezpośredniej realizacji koncepcji polityki zagranicznej państwa, a więc wywieraniu wpływu celem powstania określonych zmian w systemach wartości czy postawach i zachowaniach uczestników stosunków międzynarodowych¹²⁴. Wywieranie wpływu jest złożonym oraz długotrwałym, ale również niepewnym procesem. Decydenci polityczni, będący realizatorami polityki zagranicznej, podejmują działania, które mogą w dłuższej perspektywie przynieść zamierzony skutek, bądź też może on nie wystąpić w ogóle¹²⁵.

1.2.3. Uwarunkowania zewnętrzne o charakterze obiektywnym

Na uwarunkowania zewnętrzne o charakterze obiektywnym składają się: trendy ewolucji najbliższego danemu państwu środowiska międzynarodowego, pozycja państwa w systemie stosunków i ról międzynarodowych, struktura i zasięg umownych powiązań międzynarodowych państwa oraz obowiązujące prawo międzynarodowe. Uwarunkowania zewnętrzne o charakterze obiektywnym stanowią pierwszą grupę czynników zewnętrznych działalności państwa na arenie międzynarodowej, obok uwarunkowań zewnętrznych o charakterze subiektywnym¹²⁶.

Pierwszym z uwarunkowań, które R. Zięba klasyfikuje jako najistotniejsze w zakresie wpływu na politykę zagraniczną, są trendy ewolucji najbliższego danemu państwu środowiska międzynarodowego¹²⁷. Każde państwo będące uczestnikiem stosunków międzynarodowych musi uwzględniać oddziaływanie, któremu jest poddawane ze strony innych państw czy podmiotów. Oddziaływanie to jest warunkowane przez strukturę oraz procesy zachodzące w systemie międzynarodowym, jednak może ono występować w różnym stopniu jego

¹²¹ J. Kukułka: *Międzynarodowe stosunki...*, s. 91.

¹²² J. Bryła: *Czynniki kształtujące stosunki międzynarodowe*. W: *Międzynarodowe stosunki...*, s. 35.

¹²³ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych...*, s. 111.

¹²⁴ S. Bieleń: *Polityka w stosunkach...*, s. 37.

¹²⁵ R. Cooper: *Pęknięcie granic. Porządek i chaos w XXI wieku*. Poznań 2005, s. 127.

¹²⁶ R. Zięba: *Uwarunkowania polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 30-33.

¹²⁷ Ibidem, s. 30-31.

nasilenia. Czynnikiem, które go określają są atrybuty siły państwa oraz zdolność wpływu na innych uczestników stosunków międzynarodowych. Należy w związku z tym stwierdzić, że państwa posiadające duży potencjał ekonomiczny bądź militarny nie muszą w znacznym stopniu obawiać się oddziaływania na nie przez środowisko międzynarodowe, a wręcz przeciwnie – posiadają duże zdolności do jego samodzielnego kształtowania (oddziaływania). Z kolei państwa posiadające mały potencjał ekonomiczny lub militarny będą narażone w większym stopniu na zmiany w trendach ewolucji sytuacji międzynarodowej i zagrożone przez działalność innych państw, w szczególności mocarstw¹²⁸. Powyższy pogląd podziela E. Cziomer wskazując, że „mocarstwa i państwa silne, o ile nie są głównymi siłami sprawczymi powyższych ewolucji, w o wiele mniejszym stopniu są podatne na określone zmiany polityki zagranicznej”¹²⁹. Podkreśla jednak, że „i one w dłuższej perspektywie czasowej nie mogą ignorować zachodzących zmian w systemie międzynarodowym”¹³⁰. Taki wniosek uzasadnia pogląd, że państwa, bez względu na swoją pozycję i pełnione role na arenie międzynarodowej, muszą liczyć się ze zmianami w trendach ewolucji stosunków międzynarodowych.

Kolejnym z uwarunkowań jest pozycja państwa w systemie stosunków i ról międzynarodowych. Jest ona uzależniona przede wszystkim od uwarunkowań obiektywnych wewnętrznych, które ją determinują¹³¹. R. Zięba oraz E. Cziomer wyróżnili trzy typy pozycji państwa takie jak: centralna, kluczowa oraz peryferyjna. Z kolei zajmowanie danej pozycji przez państwo na arenie międzynarodowej określa jego role międzynarodowe¹³². Należy zatem dokonać zdefiniowania tego pojęcia. J. Z. Pietraś określa role międzynarodowe jako „spójny system wybranych przez państwo działań w stosunkach zewnętrznych”¹³³. Z kolei J. Zając pisze, że jest to „system działań i oddziaływań na arenie międzynarodowej, determinowany głównie międzynarodową pozycją oraz tożsamością państwa”¹³⁴. Wskazuje jednak, że pozycja ta uzależniona jest od faktu, czy dane państwo umiejętnie i czynnie z niej korzysta. Co ważne, pozycja państwa determinuje to jakie role będą mu przypisywane bądź narzucane z zewnątrz,

¹²⁸ R. Zięba: *Polityki zagraniczna Polski...*, s. 33-34.

¹²⁹ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych...*, s. 112.

¹³⁰ Ibidem, s. 112.

¹³¹ Do najważniejszych z nich należy zaliczyć środowisko geograficzne państwa; potencjał ludnościowy, gospodarczy i naukowo-techniczny; system społeczno-polityczny; percepcje środowiska międzynarodowego przez społeczeństwo i państwo oraz postawy społeczne wobec innych państw i narodów; koncepcje polityki zagranicznej; jakość i aktywność własnej służby zagranicznej i dyplomacji. Zobacz szerzej: 1.2.1. *Uwarunkowania wewnętrzne o charakterze obiektywnym*; 1.2.2. *Uwarunkowania wewnętrzne o charakterze subiektywnym*.

¹³² R. Zięba: *Uwarunkowania polityki zagranicznej państwa. W: Wstęp do teorii...*, s. 31; E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych...*, s. 112.

¹³³ J. Z. Pietraś: *Pojęcie i klasyfikacja ról międzynarodowych*. Lublin 1989, s. 18.

¹³⁴ J. Zając: *Teorie ról międzynarodowych. W: Teorie i podejścia badawcze w nauce o stosunkach międzynarodowych*. Red. R. Zięba, S. Bieleń, J. Zając. Warszawa 2015, s. 135.

ale również to, jakie oczekiwania innych uczestników stosunków międzynarodowych będą wobec niego formułowane¹³⁵. Rola międzynarodowa jaką pełni dane państwo uzależniona jest dodatkowo od jego tożsamości międzynarodowej, a więc od tego w jaki sposób państwo to się postrzega w odniesieniu do jego niezależności od innych państw oraz przypisywanych mu przez nie poszczególnych cech. S. Bieleń stwierdził, że na tożsamość międzynarodową składa się tożsamość wewnętrzna, wyrażająca się w trwałości części składowych państwa oraz tożsamość zewnętrzna, która odnosi się do jego niezależności względem innych uczestników stosunków międzynarodowych. Tożsamość międzynarodowa jest więc samoświadomością państwa co do umiejscowienia państwa na arenie międzynarodowej¹³⁶. Z kolei J. Kukułka zaznaczył, że determinantami tożsamości międzynarodowej są przede wszystkim czynniki: historyczne, kulturowe, przestrzenne, ekonomiczne, geograficzne, militarne, ideologiczne oraz psychologiczne¹³⁷. Dlatego też tożsamość międzynarodowa państwa jest współzależna z pełnionymi przez nie rolami międzynarodowymi¹³⁸. Należy przytoczyć również trafną prawidłowość, którą zauważył E. Cziomer pisząc, że „im wyższy jest poziom rozwoju społeczno-gospodarczego oraz wielkość państwa, tym bardziej atrakcyjnym staje się ono sojusznikiem polityczno-wojskowym oraz partnerem handlowym gospodarczym itp.”¹³⁹. Dodał, że „nie bez znaczenia jest w tym przypadku także jego atrakcyjność społeczno-ustrojowa oraz zdolność adaptacyjna zmian”¹⁴⁰.

Ostatnim z uwarunkowań zewnętrznych o charakterze obiektywnym jest struktura i zasięg umownych powiązań międzynarodowych państwa oraz obowiązujące prawo międzynarodowe. Wydaje się trafnym przyjęcie, że podstawowe znaczenie będzie mieć tutaj prawo publiczne międzynarodowe¹⁴¹. Prawem publicznym międzynarodowym jest „zespół norm regulujących wzajemne stosunki między państwami oraz organizacjami międzynarodowymi i innymi uczestnikami stosunków międzynarodowych mającymi zdolność do działania w stosunkach międzynarodowych”¹⁴². Prawo międzynarodowe powinno być tutaj rozumiane szeroko, a więc odnosić się również, obok umów międzynarodowych i zwyczaju międzynarodowego (będących podstawowymi źródłami prawa międzynarodowego), do innych

¹³⁵ Ibidem, s. 136-138.

¹³⁶ S. Bieleń: *Tożsamość międzynarodowa Federacji Rosyjskiej*. Warszawa 2006, s. 25-27.

¹³⁷ J. Kukułka: *Pojmowanie i istota tożsamości narodowej pod koniec XX wieku*. W: *Nowa tożsamość Niemiec i Rosji w stosunkach międzynarodowych*. Red. S. Bieleń, W. Góralski. Warszawa 1999, s. 11-15.

¹³⁸ J. Kukułka: *Postrzeganie międzynarodowe*. „Stosunki międzynarodowe – International Relations” 1992, T.16, s. 91-103.

¹³⁹ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych...*, s. 112.

¹⁴⁰ Ibidem, s. 112.

¹⁴¹ R. Zięba: *Uwarunkowania polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 31.

¹⁴² R. Bierzanek, J. Symonides: *Prawo Międzynarodowe Publiczne*. Warszawa 2005, s. 18.

źródeł takich jak uchwały organów organizacji międzynarodowych, porozumień dwustronnych niebędących umowami międzynarodowymi¹⁴³ czy orzecznictwa sądów międzynarodowych i doktryny¹⁴⁴. Najpowszechniejszą formą zabezpieczenia interesów państw w ramach realizowanej polityki zagranicznej są dwustronne oraz wielostronne umowy międzynarodowe. Szczególnie istotne są tutaj umowy wielostronne powołujące do życia uniwersalne i regionalne organizacje międzynarodowe, których przykładem może być Organizacja Narodów Zjednoczonych, Liga Narodów, Rada Europy, Organizacja Państw Amerykańskich, Liga Państw Arabskich czy Organizacja Bezpieczeństwa i Współpracy w Europie¹⁴⁵. Takie podejście prezentują w szczególności instytucjonaliści, którzy postrzegają działania państw na arenie międzynarodowej jako funkcję instytucji międzynarodowych, których państwo to jest członkiem. W ich ocenie uczestnictwo państwa w instytucjach międzynarodowych determinuje jego pozycję oraz role jakie pełni ono w stosunkach międzynarodowych¹⁴⁶.

Immanentną cechą prawa międzynarodowego publicznego jest ograniczanie swobody działalności państw na arenie międzynarodowej. Jedną z jego podstawowych zasad jest zasada *pacta sunt servanda*, zgodnie z którą państwowi uczestnicy stosunków międzynarodowych nie mogą w wyniku jednostronnych decyzji uwalniać się od zaciągniętych zobowiązań. Z powyższą zasadą należy powiązać zasadę wzajemności, zgodnie z którą państwo dokonujące naruszenia normy prawa międzynarodowego względem innego podmiotu musi liczyć się z podjęciem podobnych działań przez stronę względem której nastąpiło naruszenie. Innym rodzajem reakcji może być nałożenie sankcji międzynarodowych przez uprawnione do tego podmioty (np. przez Radę Bezpieczeństwa Organizacji Narodów Zjednoczonych) na państwa naruszające normy prawa międzynarodowego¹⁴⁷.

Omawiając powyższe zagadnienie nie sposób nie wspomnieć o normach *ius cogens*, a więc normach bezwzględnie obowiązujących, których nie można wyłączyć od stosowania żadną normą międzynarodową¹⁴⁸. Zaliczamy do nich na przykład: zakaz użycia siły oraz stosowania groźby (z wyjątkiem postanowień zawartych w Karcie Narodów Zjednoczonych), zakaz ludobójstwa, zakaz niewolnictwa czy zakaz ingerencji w wewnętrzne sprawy państw¹⁴⁹. W odniesieniu do ostatniej z wymienionych norm warto przytoczyć słowa setkarza stanu USA

¹⁴³ A. Czarnocki: *Czynniki międzynarodowych stosunków politycznych*. W: *Międzynarodowe stosunki...*, s. 53-55.

¹⁴⁴ R. Bierzanek, J. Symonides: *Prawo Międzynarodowe...*, s. 110-114.

¹⁴⁵ R. Zięba: *Uwarunkowania polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 32; Ibidem, s. 301-336.

¹⁴⁶ B. White: *Understanding European Foreign Policy*. Houndmills 2001, s. 29-30.

¹⁴⁷ R. Zięba: *Uwarunkowania polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 32.

¹⁴⁸ Za wyjątkiem postanowień zawartych w Karcie Narodów Zjednoczonych. Zobacz szerzej: *Karta Narodów Zjednoczonych, Statut Międzynarodowego Trybunału Sprawiedliwości i Porozumienie ustanawiające Komisję Przygotowawczą Narodów Zjednoczonych* (Dz.U. 1947 nr 23 poz. 90).

¹⁴⁹ Zobacz szerzej: Ibidem.

H. Kissingera, który stwierdził, że w kontekście realizowania przez państwa polityki zagranicznej, zakaz ingerencji w ich wewnętrzne sprawy pozostaje ciekawą kwestią akademicką¹⁵⁰.

Przestrzeganie przez uczestników stosunków międzynarodowych norm prawa międzynarodowego skutkuje ich postrzeganiem na arenie międzynarodowej, a tym samym ich pozycją oraz przypisywanym rolom. Jak można trafnie zauważyć, postępowanie zgodne z prawem powoduje wzrost znaczenia państwa i jego autorytetu. Niezbędne jest jednak podejmowanie przez nie czynnych działań w tym zakresie, takich jak udział w konferencjach międzynarodowych, członkostwo w organizacjach międzynarodowych, czy zdolność do negocjowania korzystnych umów międzynarodowych¹⁵¹.

1.2.4. Uwarunkowania zewnętrzne o charakterze subiektywnym

Do uwarunkowań zewnętrznych o charakterze subiektywnym zaliczamy: międzynarodową percepcję danego państwa i narodu oraz oczekiwania i wymagania stawiane danemu państwu przez inne państwa, koncepcje polityki zagranicznej innych państw, jakość oraz aktywność służby zagranicznej i dyplomacji innych państw¹⁵². Dokonując analizy poszczególnych typów uwarunkowań polityki zagranicznej można zauważyć, że uwarunkowania zewnętrzne o charakterze subiektywnym stanowią odzwierciedlenie uwarunkowań wewnętrznych o charakterze subiektywnym z tą różnicą, że pierwsze z nich odnoszą się do percepcji wewnętrznej danego państwa, z kolei drugie do percepcji środowiska międzynarodowego względem tego państwa.

W pierwszej kolejności spośród uwarunkowań zewnętrznych o charakterze subiektywnym należy omówić międzynarodową percepcję danego państwa i narodu oraz oczekiwania i wymagania stawiane danemu państwu przez inne państwa. Kształtuje się ona w wyniku obserwacji dokonywanych przez inne państwa, rządy, parlamenty, obywateli czy media, gdzie ich przedmiotem są wszystkie uwarunkowania, zarówno wewnętrzne jak i zewnętrzne. Skutkiem tych obserwacji jest wykreowanie wizerunku danego państwa, przy czym może przybrać on różny charakter. J. Kukułka wyróżnia wizerunek pełny, ułomny (niepełny), nieadekwatny przeidealizowany bądź katastroficzny¹⁵³. Wizerunek ułomny

¹⁵⁰ A. Czarnocki: *Czynniki międzynarodowych stosunków politycznych*. W: *Międzynarodowe stosunki...*, s. 54.

¹⁵¹ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych...*, s. 112.

¹⁵² R. Zięba: *Uwarunkowania polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 33-35.

¹⁵³ J. Kukułka: *Postrzeganie międzynarodowe...*, s. 95.

powstaje w sytuacji, w której proces dokonanych obserwacji nie przebiegł w sposób prawidłowy, a został zniekształcony w wyniku funkcjonujących stereotypów, uprzedzeń czy obciążeń historycznych. Może on również wynikać z posiadania błędnych informacji, które wpłynęły na świadomość podmiotów prowadzących obserwację i ich ostateczny skutek. Jak zauważa R. Zięba, przytoczonym sytuacjom może sprzyjać brak wiedzy w zakresie przedmiotu postrzegania, czy też izolacja obserwowanego bądź obserwującego społeczeństwa. Dlatego podkreśla się, jak istotna jest działalność edukacyjna realizowana przez organizacje polityczne, społeczne i kulturalne, której celem jest ich przewyciężanie. Psychologowie zauważają również, że mimo iż całkowite wyeliminowanie negatywnych wpływów nie jest możliwe, to decydenci polityczni pomimo tego powinni działać na rzecz ich marginalizowania, tak by nie zakłócały one stosunków międzypaństwowych¹⁵⁴.

Należy również podkreślić, że negatywna percepcja danego państwa nie zawsze musi być wynikiem czynników leżących po stronie obserwatora. Zdarza się, że postrzeganie państwa przez innych uczestników stosunków międzynarodowych jest spowodowane popełnianymi przez decydentów politycznych tego państwa błędami w polityce wewnętrznej lub zewnętrznej. Zdarza się również, że negatywne postrzeganie przez inne podmioty może być wynikiem działań podejmowanych przez samych obywateli państwa będącego przedmiotem obserwacji. W konsekwencji skutkuje to brakiem akceptacji na arenie międzynarodowej¹⁵⁵.

Następnym z uwarunkowań są koncepcje polityki zagranicznej państwa. Jak zostało już omówione, koncepcje polityki zagranicznej stanowią wypadkową formułowanych przez grupy rządzące wizji sposobu realizowania polityki zagranicznej. Decydentami, w zależności od występującego w danym państwie systemu politycznego, może być rząd lub prezydent czy też innego rodzaju organy. Z kolei wybór koncepcji polityki zagranicznej może być dokonywany zarówno poprzez wybór jednej z wielu zaproponowanych, bądź też w oparciu o wypracowanie zupełnie nowej koncepcji, będącej efektem połączenia kilku z nich¹⁵⁶. Znajomość koncepcji polityki zagranicznej innych państw powinna stanowić jeden z najistotniejszych elementów działalności uczestników stosunków międzynarodowych. Stanowią one bowiem swego rodzaju wyznaczniki w zakresie formułowania celów, podejmowania decyzji oraz realizowania działań w ramach prowadzonej polityki zagranicznej przez poszczególne państwa. Ich nieznajomość po stronie decydentów politycznych będzie skutkować brakiem możliwości ustosunkowania

¹⁵⁴ R. Zięba: *Uwarunkowania polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 33; J. Kukułka: *Polityka zagraniczna jako element procesu oddziaływań międzynarodowych*. W: *Zmienność i instytucjonalizacja...*, s. 153-154.

¹⁵⁵ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych...*, s. 113.

¹⁵⁶ Zobacz szerzej: 1.2.2. *Uwarunkowania wewnętrzne o charakterze subiektywnym*.

się do tych koncepcji poprzez odpowiednie sformułowanie własnych celów, podjęcie adekwatnych decyzji i zaplanowanie działań, a więc w konsekwencji w zakresie realizowania własnej polityki zagranicznej. Chodzi zatem nie tylko o pozyskanie informacji na dany temat, ale również o wyciągnięcie prawidłowych wniosków, między innymi poprzez zaangażowanie ekspertów i naukowców¹⁵⁷.

Ostatnim z uwarunkowań zewnętrznych o charakterze obiektywnym jest jakość oraz aktywność służby zagranicznej i dyplomacji innych państw. Współczesna dyplomacja podlega stałej ewolucji, co z kolei jest skutkiem postępu technologicznego oraz profesjonalizacji służby zagranicznej. Co więcej, zwłaszcza w okresie pozimnowojennym, nastąpiła zmiana form i metod jej działania, co można zaobserwować poprzez wzrost roli dyplomacji wielostronnej, realizowanej chociażby poprzez organizowanie konferencji międzynarodowych¹⁵⁸. Innym trendem ewolucyjnym jest z kolei wzrost znaczenia personelu dyplomatycznego wyspecjalizowanego do spraw naukowych, ekonomicznych, kulturalnych czy ekologicznych. Wreszcie należy wskazać na dyplomację prewencyjną, a więc taką, gdzie istotną rolę pełnią organizacje międzynarodowe, takiej jak Organizacja Narodów Zjednoczonych, Unia Europejska czy Organizacja Traktatu Północnoatlantyckiego (NATO), ale również inne organizacje regionalne. Celem takiej dyplomacji jest podejmowanie działań polegających na wyeliminowaniu możliwości powstawania przyszłych zagrożeń dla bezpieczeństwa narodowego i międzynarodowego państwa¹⁵⁹. Reasumując należy podkreślić, że działalność służby zagranicznej polega przede wszystkim na prowadzeniu stałej oraz kompleksowej obserwacji w zakresie celów, kierunków oraz płaszczyzn działania uczestników stosunków międzynarodowych. Z kolei dopiero weryfikacja pozyskanych informacji umożliwia adekwatną ocenę deklarowanych oraz rzeczywistych celów polityki zagranicznej danego państwa, by w konsekwencji móc ukazać jej mocne i słabe strony¹⁶⁰.

1.3. Cele polityki zagranicznej

Działalność zewnętrzna państwa to przede wszystkim podejmowane przemyślane decyzje oraz ich skuteczne realizowanie. Aby móc mówić o powodzeniu takiego działania

¹⁵⁷ J. Kukułka: *Polityka zagraniczna jako element procesu oddziaływań międzynarodowych*. W: *Zmienność i instytucjonalizacja...*, s. 153-154; R. Zięba: *Uwarunkowania polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 34.

¹⁵⁸ G. R. Berridge: *Diplomacy: Theory and Practice*. Houndmills 2002, s. 146-164.

¹⁵⁹ R. Zięba: *Uwarunkowania polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 34.

¹⁶⁰ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych...*, s. 113.

konieczne jest dostateczne określenie własnych potrzeb, aspiracji, interesów, możliwości oraz zagrożeń występujących w stosunkach międzynarodowych. Ponadto, działalność państwa ma charakter celowy, a więc zmierza do zrealizowania przyjętych przez nie koncepcji polityki zagranicznej. Cele polityki zagranicznej wynikają więc z przyjętych koncepcji¹⁶¹. Koncepcje z kolei są determinowane interesami narodowymi państwa. Jak pisze H. Morgenthau, „cele polityki zagranicznej muszą być definiowane przez pryzmat interesu narodowego, najczęściej utożsamianego z dążeniem do zapewniania bezpieczeństwa, potęgi, przetrwania”¹⁶². Co więcej, państwa będąc świadomym uczestnikiem stosunków międzynarodowych dokonują hierarchizacji celów polityki zagranicznej, poczynając od tych najistotniejszych (żywotnych), a więc zapewniających im możliwość przetrwania¹⁶³. W ramach niniejszego podrozdziału zostało zdefiniowane oraz omówione pojęcie *interesu narodowego* oraz *celów polityki zagranicznej*, a ponadto wskazana i scharakteryzowana została ich klasyfikacja.

1.3.1. Pojęcie interesu narodowego

Zagadnienie interesu narodowego pozostaje w bezpośrednim związku z celami polityki zagranicznej państw o czym pisał G. Modelski, autor klasycznej teorii polityki zagranicznej. Posługuje się on jednak pojęciem interesu, a nie interesu narodowego, które jego zdaniem jest niejasne i trudne do zdefiniowania. Píše on, że interesy są „zadaniami, życzeniami i pragnieniami odnoszonymi do zachowania się innych państw; są formułowane po to, aby były przyjęte do realizacji przez polityków”¹⁶⁴. G. Modelski stwierdza, że nadają one treści celom, a cele określają formę i kształt interesów. Zarówno interesy jak i cele stanowią wynik oczekiwań względem innych państw, jednak te pierwsze nie wyrażają oczekiwań tak ogólnie jak cele. Wskazując również na ich charakter stwierdza, że interesy mogą nie być konkretne w przeciwieństwie do celów, które ze swej istoty i znaczenia powinny być jasno wyartykułowane oraz skoordynowane pomiędzy sobą, a przede wszystkim dostosowane do możliwości operacyjnych państwa w zakresie prowadzonej polityki zagranicznej¹⁶⁵. Jak wskazuje R. Zięba, znaczna część badaczy anglosaskich determinuje cele polityki zagranicznej istnieniem określonych interesów narodowych¹⁶⁶. Przedstawiciele szkoły realizmu

¹⁶¹ T. Łoś-Nowak: *Wstęp do teorii stosunków międzynarodowych*. Poznań 1999, s. 134-136.

¹⁶² H. Morgenthau: *Politics among Nations*. New York 1954, s. 528.

¹⁶³ T. Łoś-Nowak: *Wstęp do teorii stosunków...*, s. 136-139.

¹⁶⁴ G. Modelski: *A Theory of Foreign Policy...*, s. 65.

¹⁶⁵ Ibidem, 118-119.

¹⁶⁶ R. Zięba: *Uwarunkowania polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 39.

politycznego określają interes narodowy synonimem bezpieczeństwa, przetrwania, potęgi i pochodnych¹⁶⁷. Jeden z czołowych jego twórców, H. Morgenthau, wskazywał, że „cele polityki zagranicznej muszą być definiowane przez pryzmat interesu narodowego, najczęściej utożsamianego z dążeniem do zapewniania bezpieczeństwa, potęgi, przetrwania”¹⁶⁸. Interes narodowy pozostaje więc w bezpośrednim związku z celami polityki zagranicznej państwa. Ciekawy pogląd sformułował również J. Kukułka pisząc, że są one „formą wyrażania i ukierunkowania realizowanych potrzeb, a zarazem tworzą ogniwo łączące owe potrzeby z celami narodów, państw czy ich grup kierowniczych. Dlatego interesy noszą zwykle subiektywne piętno wyrażających je podmiotów, które swoje oceny, wyobrażenia i aspiracje wiążą z określoną rzeczywistością. Subiektywna wola realizacji danego interesu prowadzi do formułowania celu aktywności podmiotu. W ten sposób współzależność potrzeb, interesów i celów tworzy wewnętrzny mechanizm wszystkich procesów oddziaływań międzynarodowych”¹⁶⁹.

Odnosząc się z kolei do działań podejmowanych przez realizatorów polityki zagranicznej, a więc decydentów politycznych na arenie międzynarodowej, można zauważyć, że interesy narodowe legitymizują ich postępowanie, stanowiąc punkt wyjścia dla każdej podejmowanej aktywności¹⁷⁰. S. Bieleń pisze nawet, że interesy narodowe są dla decydentów polityki zagranicznej „uświadamianymi preferencjami państw, które powstają jako rezultat zarówno wewnętrznych warunków materialnych, jak i potrzeb funkcjonalnych. Preferencje te powstają również pod wpływem czynników zewnętrznych, często jako wynik naśladownictwa oraz uczenia się na wzorach sprawdzonych bądź przeżytym doświadczeniu innych uczestników stosunków międzynarodowych”¹⁷¹. Dalej stwierdza, że „są wreszcie interesy pochodną ról i utrwalonych wzorców zachowań państw w środowisku międzynarodowym”¹⁷².

Interesy narodowe (państwa) stanowią główny czynnik motywacyjny realizowanej polityki zagranicznej przez państwa, będące uczestnikami stosunków międzynarodowych. S. Bieleń stwierdza, że „są one odzwierciedleniem naturalnych tendencji do obrony posiadanych wartości oraz instrumentów mobilizujących, integrujących i konsolidujących

¹⁶⁷ O. R. Holsti: *Theories of International Relations and Foreign Policy: Realism and Its Challengers*. W: *Controversies in International relations Theory: Realism and the Neoliberal Challenge*. Red. Ch. W. Kegley. New York 1995, s. 37.

¹⁶⁸ H. Morgenthau: *Politics among...*, s. 528.

¹⁶⁹ J. Kukułka: *Zaspokajanie potrzeb i rozwiązywanie konfliktów w stosunkach międzynarodowych*. W: *Stosunki międzynarodowe. Geneza, struktura, dynamika*. Red. E. Halizak, R. Kuźniar, Warszawa 2006, s. 253.

¹⁷⁰ T. Łoś-Nowak: *Polityka zagraniczna – stale i zmienne komponenty procesu formułowania i realizacji*. W: *Polityka zagraniczna: aktorzy...*, s. 48-51.

¹⁷¹ S. Bieleń: *Polityka w stosunkach...*, s. 76.

¹⁷² *Ibidem*, s. 76.

zamieszkujące je zbiorowości”¹⁷³. Z. J. Pietraś formułuje etymologiczną definicję interesu narodowego wskazując, że są to pewnego rodzaju relacje pomiędzy potrzebami jakiegoś podmiotu, a stanem rzeczy, w którym to mogą one zostać zaspokojone¹⁷⁴. Z kolei zgodnie z inną definicją interesem narodowym są „ogólne, długookresowe i kontynuowane cele funkcjonalne w stosunku do celu ostatecznego”¹⁷⁵. Interes narodowy definiowany jest również jako dążenie do realizacji celów w określonych warunkach czasowo-przestrzennych czego skutkiem jest zaspokojenie maksymalnej ilości potrzeb¹⁷⁶. Następna definicja zakłada, że jest to zaspokojenie zestawienia rozmaitych potrzeb jednostki, społeczeństwa oraz państwa¹⁷⁷. W ujęciu socjologiczno-historycznym interes narodowy ujmowany jest w odniesieniu do grupy społecznej o unitarnej kulturze, wspólnym języku, religii czy tradycji¹⁷⁸.

T. Łoś-Nowak stwierdza, że „to właśnie przez pryzmat interesu narodowego formułowane są cele, metody działania i środki realizacji polityki zagranicznej państwa”¹⁷⁹. Należy więc stwierdzić, że interesy narodowe stanowią jedyne kryterium słuszności podejmowanych przez państwa działań w stosunkach międzynarodowych oraz że są jedynym miernikiem ich skuteczności¹⁸⁰. I. Popiuk-Rysińska zauważa, że interesy narodowe państw są odzwierciedleniem wzajemnych relacji (zależności) uczestników stosunków międzynarodowych. W jej ocenie określają pożądane stany stosunków pomiędzy uczestnikami oraz środowiskiem międzynarodowym, wyrażają pożądane stany zjawisk i procesów międzynarodowych oraz środowiska międzynarodowego, a wreszcie wskazują na pożądane przez uczestników pozycje, statusy oraz role międzynarodowe¹⁸¹.

Interesy narodowe, jak już zostało niejednokrotnie wspomniane, mogą stanowić czynnik konfliktogenny w stosunkach międzynarodowych. Słuszne zatem spostrzeżenie poczynił R. Skarżyński pisząc, że „państwa współdziałają ze sobą wyłącznie tam, gdzie łączą je wspólne interesy albo nie mają innego wyjścia. W pozostałych przypadkach rywalizują przy wykorzystaniu wszystkich dających się użyć środków. Realia stosunków w ramach systemu międzynarodowego określa fakt, że strony same nadal je określają, nie tylko gospodarczą

¹⁷³ Ibidem, s. 73-74.

¹⁷⁴ Z. J. Pietraś: *Podstawy teorii stosunków...*, s. 144.

¹⁷⁵ Ch. O. Lerche, A. A. Said: *Concept of International Politics*. Englewood Cliffs 1963, s. 6 i 15.

¹⁷⁶ J. Wiatr: *Socjologia polityki*. Warszawa 1999, s. 119.

¹⁷⁷ Cz. Maj: *Wartości polityczne w stosunkach międzynarodowych*. Lublin 1992, s. 23.

¹⁷⁸ S. Bieleń: *Polityka w stosunkach...*, s. 74.

¹⁷⁹ T. Łoś-Nowak: *Polityka zagraniczna – stałe i zmienne komponenty procesu formułowania i realizacji*. W: *Polityka zagraniczna: aktorzy...*, s. 48-49.

¹⁸⁰ H. Morgenthau: *Polityka między narodami. Walka o potęgę i pokój*. Warszawa 2010, s. 20-44.

¹⁸¹ I. Popiuk-Rysińska: *Uczestnicy stosunków międzynarodowych, ich interesy i oddziaływania*. W: *Stosunki międzynarodowe. Geneza, struktura, dynamika*. Red. E. Halizak, R. Kuźniar. Warszawa 2006, s. 107-108.

i kulturowo, ale także czysto fizycznie (przemocą lub groźbą jej użycia), pomimo ograniczeń narzucanych przez prawo międzynarodowe i obyczaje”¹⁸².

Ciekawą koncepcję interesu narodowego zaproponował V. Udalov, który wywiódł istotę tego pojęcia z rozważań badaczy dwóch przeciwstawnych bloków państw z okresu zimnej wojny, wschodniego pod prymatem Związku Socjalistycznych Republik Radzieckich oraz zachodniego pod przewodnictwem USA. W jego ocenie definicja interesu narodowego występująca we wskazanych państwach korelowała z postępującą rywalizacją na arenie międzynarodowej. I tak badacze amerykańscy postrzegają interes narodowy jako potrzeby, teologiczne determinanty oraz niepodlegające negocjacji przyczyny ludzkich zachowań, od percepcji pojedynczej jednostki po percepcję międzynarodową. Interesem narodowym w ich ocenie jest przetrwanie, bezpieczeństwo oraz tożsamość. Z kolei badacze radzieccy rozważają interes narodowy jako główny element motywacji, gdzie prym wiedzie ludzkie myślenie i działanie, które to z kolei formułuje postawy, cele i intencje¹⁸³. Szczególnego podkreślenia wymaga również fakt, że w ujęciu radzieckim interes narodowy jest elementem realizowanej polityki zagranicznej państwa, nie mając przy tym charakteru autonomicznego¹⁸⁴.

Interes narodowy może przybierać różne wymiary. A. Kortunov i A. Volodin piszą, że ma on wymiar ogólny, ponadczasowy, metafizyczny oraz praktyczny, konkretny i doraźny. Wyróżniają dwa aspekty postrzegania interesu narodowego, określając je mianem holistycznego oraz pozytywistycznego. Pierwszy z nich, holistyczny, przejawia się w akcentowaniu wyjątkowości danego państwa, jego historii oraz przeznaczenia. Czynniki te są z kolei zakorzenione w kulturze, historii oraz położeniu geopolitycznym państwa. Dalej wskazują, że państwo, które neguje swoje przeznaczenie, jest z góry skazane na porażkę. W ich ocenie celem decydentów politycznych jest bowiem kreowanie, artykułowanie, a w konsekwencji narzucanie wzorców zachowań całemu społeczeństwu w zgodzie z przyjętą strategią rozwoju. Drugim z wymiarów jest wymiar pozytywistyczny, który jest charakterystyczny i stosunkowo dobrze rozpowszechniony wśród społeczeństw (państw) demokratycznych. W państwach tych artykulacja interesów następuje przy wykorzystaniu rozmaitych mechanizmów konstytucyjnych, a więc w granicach i na podstawie prawa. Dzięki temu możliwe jest uwzględnienie interesów jak największej liczby grup społecznych

¹⁸² R. Skarżyński: *Czy istnieje porządek międzynarodowy? Jak starożytne i średniowieczne wzorce myślowe określają terminologię współczesnej nauki o stosunkach międzynarodowych*. W: *Wybrane problemy globalnej i regionalnej polityki międzynarodowej*. Red. E. Kuźlewska, K. Stefanowicz. Toruń 2009, s. 156.

¹⁸³ V. Udalov: *National Interests and Conflict Reduction*. W: *Cooperative Security. Reducing Third World Wars*. Red. I. W. Zartman, V. A. Kremenyuk. New York 1995, s. 61–77.

¹⁸⁴ I. Popiuk-Rysinska: *Uczestnicy stosunków międzynarodowych, ich interesy i oddziaływania*. W: *Stosunki międzynarodowe...*, s. 108.

i wypracowanie rozwiązania będącego satysfakcjonujące dla jak największej liczby z nich¹⁸⁵. Z zaprezentowanego podejścia można zatem wywnioskować, że wymiar holistyczny będzie cechował reżimy (państwa) autorytarne, w których wybrane grupy jednostek (bądź jednostki) kreują poszczególne działania. Wymiar ten będzie również dotyczył młodych demokracji, w których mechanizmy konstytucyjne nie zostały jeszcze w sposób dostateczny wykształcone, aby móc w pełni realizować swoje zadania. Aspekt holistyczny można również odnieść do tradycji platońskich, w których to wąskie gremia władzy podejmowały decyzje dotyczące całej zbiorowości. Z kolei aspekt pozytywistyczny wydaje się bliski tradycji arystotelesowskiej, gdzie interes narodowy jest kształtowany w drodze debaty publicznej¹⁸⁶.

Ujęcia interesu narodowego zaproponowane przez wskazanych wyżej badaczy wydają się nawiązywać do koncepcji zaproponowanych przez J. Frankela. Wyróżniał on bowiem interes w ujęciu aspiracyjnym oraz operacyjnym. Pierwsze z nich odnosiło się do wizji lepszego życia oraz ideału celów, które dane państwo chce realizować na arenie międzynarodowej. Wymiar aspiracyjny określa również kierunek działań decydentów politycznych, aby poprzez dokonanie odpowiednich zmian w środowisku międzynarodowym, przekształcić interes narodowy w interes możliwy do jego realizacji. Interesy o charakterze aspiracyjnym są zakorzenione w filozofii, historii oraz ideologii, których rozwój określa w konsekwencji główne cele prowadzonej polityki zagranicznej. Następnie wskazać należy, że zasadniczą rolę pełnią tutaj elity rządzące, które realizują wykreowane przez siebie założenia polityki zagranicznej, choć co istotne niekoniecznie muszą być one zgodne z realnymi możliwościami danego państwa. Drugim z ujęć wyróżnionych przez J. Frankela jest ujęcie operacyjne, w którym interes narodowy stanowi zestawienie dążeń oraz rzeczywiście realizowanych polityk. Charakteryzują się one doraźnością oraz są określane przez realne możliwości państwa, a w mniejszym stopniu przez wolę decydentów politycznych, jak ma to z kolei miejsce w przypadku ujęcia aspiracyjnego¹⁸⁷. J. Frankel wyróżnił również trzecie ujęcie – polemiczne, które to z kolei odnosi się do dokonywania politycznej argumentacji, racjonalizacji, oceniania, krytyki zachowań bądź wyjaśniania działalności państw na arenie międzynarodowej¹⁸⁸.

Polski badacz teorii stosunków międzynarodowych J. Kukułka wyróżnił z kolei trzy płaszczyzny identyfikacji interesu narodowego. Zaliczył do nich poziom społeczny,

¹⁸⁵ A. Kortunov, A. Wolodin: *Contemporary Russia: National Interests and Emerging Foreign Policy Perceptions. Berichte des Bundesinstituts für Ostwissenschaftliche und Internationale Studien*. Köln 1996, s. 3-22.

¹⁸⁶ T. A. Columbus, J. H. Wolfe: *Introduction to International Relations: Power and Justice*. Englewood Cliffs 1986, s. 107-108.

¹⁸⁷ S. Bieleń: *Polityka w stosunkach...*, s. 83; Zobacz szerzej: J. Frankel: *National Interest*. London 1970.

¹⁸⁸ J. Frankel: *Contemporary International Theory and the Behavior of States*. London 1973, s. 78-79.

decydentów politycznych oraz uczestników stosunków międzynarodowych. Na płaszczyźnie społecznej, interes narodowy nie jest łatwo rozpoznawalny. Związane jest to z faktem, że poszczególni obywatele, w wyniku oddziaływania na nich różnych czynników zewnętrznych jak i wewnętrznych, nie są w stanie w prawidłowy sposób dokonać wnikliwej analizy interesów narodowych danego, czy też własnego państwa. Decydenci polityczni z kolei posiadają zdolności w zakresie kreowania, ale i manipulowania wartościami, które kształtują interesy narodowe państwa. Wykreowane w ten sposób interesy mogą zastosowane zarówno na użytek wewnętrzny jak i zewnętrzny w polityce danego państwa. Na ostatnim z wyróżnionych poziomów J. Kukulka wskazuje, że interes narodowy jest narzędziem służącym perswazji, propagandzie, a przede wszystkim legitymizowaniu działań podejmowanych przez rządy państw. Stwierdzić jednak należy, że poszczególne interesy jakie występują w stosunkach międzynarodowych uzależnione są nie tylko od działań podejmowanych przez decydentów politycznych, ale również, a być może przede wszystkim od ich postrzegania przez pozostałych uczestników stosunków międzynarodowych¹⁸⁹.

W literaturze specjalistycznej można wyróżnić wiele klasyfikacji typów interesów narodowych państw. I tak K. Deutsch oraz H. Morgenthau wyróżnili interesy podstawowe, które obejmują wartości takie jak przetrwanie państwa, ochronę jego integralności terytorialnej, tożsamości narodowej oraz suwerenności. V. van Dyke z kolei wyróżnił interesy egoistyczne, które odnoszą się do interesów państwa (społeczeństwa) oraz altruistyczne, dotyczące solidarności międzynarodowej czy pomocy państwom słabiej rozwiniętym. A. Wolfers wyszczególnił natomiast interesy egoistyczne, altruistyczne oraz samozachowawcze. Ostatnie z nich odnoszą się do dążenia państwa, do rozszerzania wpływów na arenie międzynarodowej, współdziałanie z innymi uczestnikami stosunków międzynarodowych oraz utrzymanie pokoju i *status quo* na świecie¹⁹⁰. J. Frankel zaproponował koncepcję, w ramach której wyodrębnił trzy szczeble interesu narodowego takie jak: aspiracyjny, operacyjny oraz polemiczny. Stwierdził również, że interesy aspiracyjne oddziałują na problemy polityczne oraz wytyczają pewne cele i kierunki polityki zagranicznej państwa¹⁹¹.

W polskiej nauce o stosunkach międzynarodowych M. Dobroczyński i J. Stefanowicz zaproponowali dokonanie klasyfikacji poprzez wyróżnienie dwóch zespołów interesów narodowych takich jak tożsamości i bezpieczeństwa oraz współpracy i współzawodnictwa¹⁹².

¹⁸⁹ S. Bieleń: *Polityka w stosunkach...*, s. 84; T. Łoś-Nowak: *Stosunki międzynarodowe. Teorie – systemy – uczestnicy*. Wrocław 2006, s. 267-268.

¹⁹⁰ Z. J. Pietraś: *Podstawy teorii stosunków...*, s. 146.

¹⁹¹ J. Frankel: *National Interest...*, s. 31-32.

¹⁹² M. Dobroczyński, J. Stefanowicz: *Polityka zagraniczna*. Warszawa 1984, s. 15-32.

Wydaje się, że najpełniejszą z klasyfikacji interesu narodowego zaproponował J. Kukułka, który sformułował trzy enumeratywne typy interesów narodowych takie jak: egzystencjalne, koegzystencjalne oraz funkcjonalne. Klasyfikacja ta wydaje się niezwykle przydatna, przede wszystkim z uwagi na fakt, że pozwala na pogrupowanie poszczególnych typów interesów nie tylko z uwagi na ich znaczenie dla danego państwa, ale i charakter wewnętrzny oraz zewnętrzny w kontekście prowadzonej przez państwo polityki zagranicznej. Interesy egzystencjalne państwa stanowią podstawową grupę interesów narodowych, którym każde państwo powinno nadać pierwsze miejsce w ogólnej hierarchii oraz realizować w pierwszej kolejności (czasem również kosztem innych interesów narodowych). Zaliczamy do nich przede wszystkim zachowanie integralności terytorialnej, przetrwanie na arenie międzynarodowej, zapewnienie bezpieczeństwa państwa oraz przystosowanie do aktualnie panujących warunków w ramach stosunków międzynarodowych. Następną grupę interesów stanowią interesy koegzystencjalne, które koncentrują się na uczestnictwie państwa w systemie międzynarodowym, roli jaką dane państwo w nim pełni lub do pełnienia jakiej roli aspiruje, współpracy państwa z innymi uczestnikami stosunków międzynarodowych oraz normatywizacją stosunków międzynarodowych. Ostatnim z typów interesów wyróżnionych przez J. Kukułkę są interesy funkcjonalne. Odnoszą się one przede wszystkim do aktywności poszczególnych uczestników stosunków międzynarodowych w systemie międzynarodowym oraz innowacyjności i skuteczności podejmowanych przez nich działań¹⁹³.

Mając na uwadze powyższe rozważania dotyczące interesu narodowego oraz jego znaczenia w polityce zagranicznej państwa należy również podkreślić, że interesy w zależności od typów oraz uwarunkowań polityki zagranicznej państwa mogą ulegać w mniejszym bądź większym stopniu ewolucji. Jak zauważa T. Łoś-Nowak, przykładem opisanego wyżej zjawiska może być zredefiniowanie interesów Polski po 1989 roku. T. Łoś-Nowak pisze, że „przykładem jest redefinicja interesów państwowych RP w fazie transformacji ustrojowej po roku 1989. Objęła ona zarówno interesy egzystencjalne (bezpieczeństwo zewnętrzne – nowe sojusze, członkostwo w NATO), koegzystencjalne (uczestnictwo w UE, OECD, nowe formy współpracy), jak i funkcjonalne (aktywność na arenie międzynarodowej, idee nowego regionalizmu)”¹⁹⁴. Zauważa również, że „pełna rekonstrukcja interesów państwa bywa niezwykle złożona. W realnym wymiarze polityki zagranicznej państwo często podejmuje działania na wielu płaszczyznach i różnych kierunkach, próbując dyskontować ewentualne

¹⁹³ J. Kukułka: *Problemy teorii stosunków międzynarodowych*. Warszawa 1978, s. 258-270.

¹⁹⁴ T. Łoś-Nowak: *Stosunki międzynarodowe...*, s. 272-273.

niepowodzenia na jednej płaszczyźnie sukcesami na innej lub też za pomocą jednego działania realizować kilka różnych interesów”¹⁹⁵.

Poruszając zagadnienia związane z pojęciem interesu narodowego nie sposób nie odnieść się do jego części składowej jaką jest racja stanu. Rozpoczynając od genezy tego zagadnienia należy wskazać, że historycznie racja stanu nie była częścią pojęcia interesu narodowego, a raczej je zastępowała. Współcześnie jest ona definiowana jako nadrzędny, żywotny interes państwowy, który wiedzie prym pośród wszystkich innych jakie dane państwo posiada. Należy jednak dość jednoznacznie stwierdzić, że oba terminy odnosiły się do zabezpieczenia najważniejszych oraz podstawowych potrzeb i wartości egzystencjalnych państwa. Racja stanu, podobnie jak interes narodowy, oddziałuje na prowadzoną przez państwo politykę zagraniczną, będąc swego rodzaju wyznacznikiem kierunku w jakim powinna być ona prowadzona, ale również przy użyciu jakich środków powinno się to odbywać. Ewolucja racji stanu będzie z kolei oddziaływać na prowadzoną przez państwo politykę zagraniczną, a zmiany w środowisku międzynarodowym powodować jej redefiniowanie¹⁹⁶.

Pojęcie racji stanu zostało po raz pierwszy użyte w XVI wieku przez G. della Casa, który wzywał króla Karola V do kierowania się moralnością i uczciwością, a nie brutalnym stosowaniem siły¹⁹⁷. Z kolei za twórcę nowożytnej koncepcji racji stanu, która ewoluując trwa do czasów współczesnych, uważa się N. Machiavellego. W swojej rozprawie „Książę” utożsamiał rację stanu z wolą księcia, interesami dynastii oraz nadrzędnością korony¹⁹⁸. W okresie absolutyzmu racja stanu służyła do uzasadniania samowładności monarchów, a jedną z najwybitniejszych postaci, która stosowała ten typ argumentacji był francuski kardynał A. J. Richelieu¹⁹⁹. Schyłek XVIII wieku, który wraz z początkiem Wielkiej Rewolucji Francuskiej (1789) rozpoczął proces zmian w systemie międzynarodowym, odbił się również na rozumieniu pojęcia racji stanu, w związku z czym zaczęła być ona utożsamiana z takimi kryteriami jak: wola ogółu, interes polityczny czy honor narodowy²⁰⁰. Pojęcie racji stanu oraz jego korelacja z zagadnieniem interesu narodowego stale ewoluowało oraz nadal ewoluuje. Współcześnie racja stanu stanowi element składowy interesów narodowych, będąc jego najistotniejszym z ogniw. E. Sadowski pisze, że: „charakter (status) racji stanu pojmuje się i interpretuje w płaszczyźnie historycznej bądź w świetle bieżących wydarzeń i procesów

¹⁹⁵ Ibidem, s. 272-273.

¹⁹⁶ S. Bieleń: *Polityka w stosunkach...*, s. 86-90.

¹⁹⁷ Ibidem, s. 86-87.

¹⁹⁸ E. Sadowski: *Racja stanu w polityce zagranicznej współczesnego państwa. W: Zmienność i instytucjonalizacja stosunków międzynarodowych*. Red. J. Kukułka. Warszawa 1988, s. 166-173.

¹⁹⁹ S. Bieleń: *Polityka w stosunkach...*, s. 86-87.

²⁰⁰ E. Sadowski: *Racja stanu w polityce zagranicznej współczesnego państwa. W: Zmienność...*, s. 167.

politycznych. Z pierwszej perspektywy, racji stanu przypisuje się trwałość i ciągłość. Z drugiej zaś, w znaczeniu racji stanu akcentuje się jej aktualne treści i polityczną zmienność, dynamikę²⁰¹. Racja stanu jest zatem nie tylko ogólnym kryterium działania uwarunkowanego bieżącą sytuacją polityczną, w ramach której decydenci polityczny podejmują decyzje, ale wynika również z wydarzeń historycznych i uzyskanego w ich wyniku doświadczenia²⁰².

Omawianemu pojęciu należy przypisać również walor uniwersalności, choć z drugiej strony jest ono przecież związane z konkretnym państwem, które racje stanu może postrzegać w różnoraki sposób. Uniwersalność racji stanu należy więc przede wszystkim odnieść do wspólnych wszystkim państwom wartości takich jak: zapewnianie bezpieczeństwa państwa, ochrony jego suwerenności oraz integralności terytorialnej. Taki pogląd przedstawia również T. Pióro, który pisze, że „nie ma takiego rządu, który nie czułby się zobowiązany do zapewniania bezpieczeństwa swemu narodowi, nie tylko przez politykę sojuszy z sąsiadami, ale również przez utrzymywanie instytucji bezpieczeństwa to – przynajmniej we własnym przekonaniu – zapewniających. Takie zobowiązanie nie wymaga żadnego moralnego usprawiedliwienia, wynika z samego istnienia państwa narodowego i jego suwerenności; jest ono i długo pozostanie nieuniknioną koniecznością państwowej egzystencji”²⁰³.

Omawiając pojęcie racji stanu warto również przytoczyć pogląd sformułowany przez S. Bielenia, który pisze, że ma ona „charakter ponadklasowy i ponadsektorowy; nie ulega też zasadom etyki i moralności. W polityce zagranicznej, jak w każdej polityce, obowiązuje wyłącznie kierowanie się względami realnych interesów, racjonalnych przewencji i wyborów, kalkulacji zysków i strat”²⁰⁴. Tym samym wyprowadza on wniosek, że „stąd nie znajduje uzasadnienia ani przesadne moralizatorstwo, ani jakakolwiek ideologizacja zachowań politycznych. Z tych względów w sytuacjach ekstremalnych (koniecznych i wyjątkowych) racja stanu uzasadnia i usprawiedliwia pozaprawne i pozamoralne działania polityczne, co nie oznacza, że jej treści nie podlegają kwalifikacjom etycznym”²⁰⁵. Należy zgodzić się z tak sformułowanym stwierdzeniem, gdyż istotą racji stanu jest przecież poświęcanie dobra niższego rzędu na rzecz dobra wyższego rzędu. Dobro to powinno podlegać szczególnej ochronie, ponieważ zmierza ono do zachowania suwerenności i integralności państwa w stosunkach międzynarodowych.

²⁰¹ Ibidem, s. 167.

²⁰² K. Grzybowski: *Historia doktryn politycznych i prawnych*. Warszawa 1969, s. 312.

²⁰³ T. Pióro: *Wojsko – nasze wojsko?* „Res Publica” 1990, nr 5, s. 4.

²⁰⁴ S. Bielen: *Polityka w stosunkach...*, s. 89-90.

²⁰⁵ Ibidem, s. 89-90.

Wreszcie na gruncie niniejszych deliberacji należy dokonać rozróżnienia pomiędzy pojęciem interesu narodowego a racji stanu czego dokonuje T. Łoś-Nowak. Píše ona, że interes narodowy to wartość, na którą składają się „elementy obiektywnego i subiektywnego postrzegania państwa i potrzeb, możliwości w środowisku, wreszcie samego środowiska i świadomości potrzeby jak najlepszego wykorzystania istniejących uwarunkowań polityki zagranicznej państwa. Zawsze jednak ma charakter potencjalny”²⁰⁶. Dalej wskazuje, że „racja stanu zaś to coś, co może być częścią interesów państwowych, tą najważniejszą, ale nie jedyną. Jako taka jawi się więc jako potrzeba wyższego rzędu, wyjątkowa konieczność, imperatywny wybór”²⁰⁷. W wymiarze podmiotowym interes narodowy jest więc sprzężony z racją stanu, przy czym interes odnosi się oraz obejmuje swoim zakresem całe społeczeństwo, z kolei racja stanu związana jest współcześnie przede wszystkim z elitami rządzącymi. W ujęciu przedmiotowym realizowanie interesów narodowych oraz racji stanu zmierza do zabezpieczenia najważniejszych potrzeb państwa, zarówno w wymiarze wewnętrznym jak i zewnętrznym.

Reasumując poszczególne rozważania dotyczące zagadnienia interesu narodowego, zgodzić należy się ze spostrzeżeniem poczynionym przez A. Wielomskiego, który stwierdził, że z racji jego nieostrego i nieprecyzyjnego znaczenia „każdy polityk może interes ten inaczej definiować i interpretować”²⁰⁸. Interesy narodowe współcześnie wydają się być pojęciem znacznie szerszym, obejmującym swoim znaczeniem ambicje i cele nie tylko poszczególnych państw, ale ogółu społeczności międzynarodowej. Interesy narodowe są ściśle sprzężone z polityką wewnętrzną państwa, która je definiuje. Stanowią one zatem wyznacznik dla realizowanej przez państwo polityki zagranicznej, pośród której najwyższe miejsce w hierarchii zajmuje racja stanu, określając podstawowe (egzystencjalne) aspekty funkcjonowania państwa, których ochrona pozwala na zachowanie jego suwerenności oraz integralności. Polityka zagraniczna z kolei to działalność skierowana na zewnątrz w imię racji stanu i interesu narodowego.

1.3.2. Definicja celów polityki zagranicznej

Polityka zagraniczna to przede wszystkim działalność celowa państwa realizowana na arenie międzynarodowej, którą determinują określone potrzeby, wartości czy idee. Polityka

²⁰⁶ T. Łoś-Nowak: *Stosunki międzynarodowe...*, s. 271.

²⁰⁷ Ibidem, s. 271.

²⁰⁸ A. Wielomski: *Nacjonalizm francuski 1886-1940. Geneza, przemianu i istota filozofii politycznej*. Warszawa 2007, s. 19.

zagraniczna jest określania przez decydentów politycznych, choć należy zaznaczyć, że istotną rolę odgrywa tutaj również świadomość społeczna, stanowiąca czynnik programujący, motywacyjny oraz organizujący. Omawiając pojęcie celów polityki zagranicznej państwa nie sposób nie wspomnieć o roli jaką sprawuje w jej formułowaniu i realizacji nauka o stosunkach międzynarodowych. Pełni ona bowiem funkcję informacyjną, prognostyczną, ekspercko-doradczą oraz ideologiczną²⁰⁹. Zagadnienie celów polityki zagranicznej państw nie jest opisane w literaturze specjalistycznej o stosunkach międzynarodowych w sposób jednoznaczny, a sam proces ich formułowania ma charakter niezwykle skomplikowany oraz złożony, toteż wymaga szczegółowego scharakteryzowania i omówienia²¹⁰. Rozpoczynając rozważania dotyczące definicji celów polityki zagranicznej państwa, należy w pierwszej kolejności dokonać określić, co należy rozumieć pod pojęciem cel. W najogólniejszym znaczeniu jest to stan pożądaný, do którego dany podmiot zmierza w oparciu o przyjęte strategie działania. Do celu dąży się zatem poprzez świadome działanie podejmowane przez podmioty, którymi mogą być osoby fizyczne, organizacje, przedsiębiorstwa, społeczeństwa, a na gruncie niniejszej rozprawy przede wszystkim uczestnicy stosunków międzynarodowych²¹¹.

Jedną z najbardziej rozpowszechnionych definicji celów polityki zagranicznej państwa, również w polskiej nauce o stosunkach międzynarodowych, jest definicja wywodząca się z literatury anglosaskiej zaproponowana przez K. J. Holstiego. Stwierdził on, że cel polityki zagranicznej to „wyobrażenie przyszłego stanu spraw oraz przyszłego oznaczenia warunków, które rządy za pośrednictwem indywidualnych twórców polityki zamierzają spowodować poprzez wywieranie wpływu na zewnątrz oraz poprzez zmianę lub podtrzymanie zachowania innych państw”²¹². R. Zięba w ramach wskazanej definicji sformułował następujące wnioski. Po pierwsze, w jego ocenie cele polityki zagranicznej są efektem dążeń elit rządzących do ich zrealizowania poprzez oddziaływanie na środowisko międzynarodowe, a zatem mają charakter celowy oraz są tym samym w sposób dostateczny uzasadnione. Podziela on również pogląd wyrażony przez F. Frankela który wskazał, że są one formułowane przez indywidualnych decydentów politycznych, jednak nie można ich zaliczyć do analizy zachowań poszczególnych jednostek²¹³. Stwierdza bowiem, że cele polityki zagranicznej są rezultatem długiego oraz złożonego procesu realizowanego przez elity rządzące. Po drugie, R. Zięba stwierdza, że cele

²⁰⁹ R. Zięba: *Cele polityki zagranicznej państwa*. W: *Wstęp do teorii polityki zagranicznej państwa*. Red. R. Zięba. Toruń 2005, s. 37.

²¹⁰ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych...*, s. 113.

²¹¹ R. Zięba: *Cele polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 37.

²¹² K. J. Holsti: *International Politics: A Framework for Analysis*. Englewood Cliffs 1967, s. 126.

²¹³ J. Frankel: *National Interest...*, s. 24-25.

polityki zagranicznej stanowią wyobrażenie jakiegoś indywidualnego stanu faktycznego w danym państwie, który to z kolei jest uwarunkowany obecną oraz przyszłą formą systemu międzynarodowego. Po trzecie, wskazuje, że organy państwa powinny realizować politykę zagraniczną w oparciu o przyjęte cele, gdyż są one formułowane jako dyrektywy działań. I wreszcie po czwarte, cele polityki zagranicznej państwa są kierowane do adresatów zewnętrznych, a więc uczestników stosunków międzynarodowych. W związku z tym zmierzają one do wywierania określonego wpływu, a w konsekwencji do urzeczywistnienia określonych planów, strategii, doktryn, założeń czy koncepcji. Osiągnięcie realizowanego celu polityki zagranicznej będzie więc zależało w dużej mierze od samych adresatów względem których są kierowane oczekiwania państwa (cele), ale również możliwości bądź chęci adresatów w zakresie ich przyjęcia (zrealizowania)²¹⁴. R. Zięba pisze również, że „pierwotnie są potrzeby, które wyartykułowane i przystosowane do realizacji stają się interesami uczestników stosunków międzynarodowych. Na podstawie tych interesów ośrodek decyzyjny formułuje cele, które stają się następnie bodźcami podejmowania przez państwo działań na forum międzynarodowym”²¹⁵. Dalej stwierdził, że „cele są elementem ukierunkowującym działania polityki zagranicznej państwa, zmierzające do zaspokojenia potrzeb i interesów wyartykułowanych w jego systemie wewnętrznym, a związanych z uczestnictwem państwa w określonym środowisku międzynarodowym”²¹⁶. Odwołując się do powyższych rozważań E. Cziomer zaproponował zdefiniowanie pojęcia celów polityki zagranicznej państwa poprzez wskazanie, że jest to „świadome i systematyczne działanie oraz dążenie państwa do adaptacji środowiska międzynarodowego dla własnych potrzeb i interesów”²¹⁷.

W nauce o stosunkach międzynarodowych można wyróżnić wiele innych definicji celów polityki zagranicznej, przy czym należy podkreślić, że znaczna część z nich obejmuje elementy i obszary, na które wskazuje już K. J. Holsti. Toteż zaproponowaną przez niego definicję należy określić mianem najpełniejszej i najbardziej użytecznej na gruncie niniejszej rozprawy.

Przechodząc wreszcie do charakterystyki celów polityki zagranicznej należy ponownie odwołać się do faktu ich nierozzerwalnego związku z interesami narodowymi państwa. Jak pisał H. Morgenthau, „cele polityki zagranicznej muszą być definiowane przez pryzmat interesu narodowego, najczęściej utożsamiane z dążeniem do zapewnienia bezpieczeństwa, potęgi,

²¹⁴ R. Zięba: *Cele polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 38.

²¹⁵ Ibidem, s. 43.

²¹⁶ Ibidem, s. 43.

²¹⁷ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych...*, s. 113.

przetrwania”²¹⁸. Choć formułując powyższy pogląd H. Morgenthau odwołał się przede wszystkim do celów podstawowych jakie powinno realizować państwo (bezpieczeństwo, przetrwanie, potęga), to nie należy ograniczać związku interesów narodowych jedynie do nich. Ważne spostrzeżenie w zakresie korelacji celów oraz interesów poczynił z kolei G. Modelski pisząc, że interesy narodowe stanowią odzwierciedlenie różnego rodzaju potrzeb, dostarczając tym samym treści celom, a te z kolei nadają kształt interesom. Korelacja pomiędzy interesami narodowymi i celami polityki zagranicznej stanowi więc swego rodzaju obieg zamknięty, w którym zaburzenie jednego z elementów uniemożliwia prawidłowe funkcjonowanie całego mechanizmu²¹⁹. W odniesieniu do procesu formułowania celów i interesów R. Zięba pisał, że „podczas gdy interesy mogą być niesprecyzowane lub nawet niewyartykułowane – cele powinny być jasno określone, skoordynowane między sobą i przystosowane do działalności operacyjnej”²²⁰. Dalej stwierdził, że „cele reprezentują polityczne zrealizowanie interesów danej wspólnoty, czyli przesunięcie bodźców i życzeń na konkretny kierunek działania polityki zagranicznej”²²¹. Reasumując powyższe poglądy koniecznym jest sformułowanie wniosku, że zmiany w zakresie interesów państwa będą powodować zmianę celów realizowanej przez nie polityki zagranicznej.

Proces formułowania celów polityki zagranicznej choć z pozoru wydawać by się mogło prosty, w rzeczywistości jest niezwykle skomplikowany. Kreowanie celów jest bowiem uzależnione od wielu różnych uwarunkowań, zarówno o charakterze wewnętrznym jak i zewnętrznym, które to z kolei można podzielić na uwarunkowania o charakterze subiektywnym i obiektywnym²²². Wskazać należy, że istotnym czynnikiem o charakterze wewnętrznym w zakresie formułowania celów polityki zagranicznej jest system polityczny danego państwa. W zależności od jego typu cele mogą być przyjmowane w oparciu o stan stosunków występujący pomiędzy rywalizującymi bądź współpracującymi ugrupowaniami politycznymi, ale może również wynikać z porządku konstytucyjnego obowiązującego w danym państwie. W związku z tym, operacjonalizacja celów polityki zagranicznej może przybierać różne formy. Z kolei identyfikacja poszczególnych celów polityki zagranicznej państwa jest determinowana dynamicznym charakterem stosunków międzynarodowych, a więc relacjami zewnętrznymi zachodzącymi pomiędzy ich uczestnikami. Zdolność realizacji celów będzie z kolei

²¹⁸ H. Morgenthau: *Politics among...*, s. 528.

²¹⁹ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych...*, s. 113; Zobacz szerzej: G. Modelski: *A Theory of Foreign Policy...*

²²⁰ R. Zięba: *Cele polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 42.

²²¹ Ibidem, s. 42.

²²² R. Zięba: *Uwarunkowania polityki zagranicznej państwa*. W: *Wstęp do teorii polityki...*, s. 17-36.

uzależniona od potęgi danego państwa (a więc zdolności do samodzielnego oddziaływania na inne podmioty), ale może być również zależna od ich współdziałania na arenie międzynarodowej²²³. T. Łoś-Nowak wskazała również, że „mając na względzie percepcję polityki zagranicznej w środowisku międzynarodowym, ogromną rolę odgrywają zarówno sposób formułowania celów, jak i forma ich werbalizacji. Analiza polityki zagranicznej pod tym kątem może np. dać odpowiedź na pytanie, jakie role w polityce międzynarodowej państwo ogrywa, chce odgrywać lub – jaki status zajmuje w świecie realnej polityki”²²⁴. Dalej pisze, że „role deklarowane przez przywódców politycznych państwa mogą być przejawem ich wyobrażeń o możliwościach kształtowania stosunków międzynarodowych oraz polityki innych państw”²²⁵.

W ramach omawianego zagadnienia nie bez znaczenia pozostaje sam problem identyfikacji czynników oddziałujących na proces formułowania celów polityki zagranicznej państwa. T. Łoś-Nowak pisze, że J. Kukułka „wyprowadza je wprost z potrzeb uczestników stosunków międzynarodowych”²²⁶. Dalej stwierdza, że „potrzeby państwa (na przykład politycznej niezależności, przetrwania, rozwoju gospodarczego czy międzynarodowego uznania) stanowią więc według J. Kukułki główny motyw w procesie formułowania celów w polityce zagranicznej”²²⁷. J. Kukułka stwierdza więc, że cele polityki zagranicznej są wprost determinowane przez potrzeby uczestników międzynarodowych, które mogą przybierać różne wymiary. W nieco innym tonie wypowiedzieli się badacze: Z. J. Pietraś, R. Zięba, J. Stefanowicz czy M. Dobroczyński oraz zdecydowana większość teoretyków nauki o stosunkach międzynarodowych. T. Łoś-Nowak pisze, że przyjęli oni, iż cele polityki zagranicznej należy w pierwszej kolejności wiązać z interesami, które to z kolei są determinowane przez określone potrzeby²²⁸. Pogląd ten wydaje się o wiele słuszniejszy, gdyż uwzględnia istotną rolę interesów narodowych w procesie formułowania celów polityki zagranicznej państwa, a na co wielokrotnie w niniejszym rozdziale wskazywano.

Cele polityki zagranicznej mogą stanowić również zarzewie konfliktu o charakterze wewnętrznym (np. pomiędzy ugrupowaniami politycznymi), ale przede wszystkim o charakterze zewnętrznym (np. pomiędzy państwami). Wynika to z faktu, że przyjęte

²²³ T. Łoś-Nowak: *Wstęp do teorii stosunków...*, s. 135-136.

²²⁴ T. Łoś-Nowak: *Polityka zagraniczna – stałe i zmienne komponenty procesu formułowania i realizacji. W: Polityka zagraniczna: aktorzy...*, s. 53.

²²⁵ Ibidem, s. 53.

²²⁶ T. Łoś-Nowak: *Stosunki międzynarodowe...*, s. 267-268; Zobacz szerzej: J. Kukułka: *Problemy teorii...*, s. 259-263.

²²⁷ Ibidem, s. 267-268.

²²⁸ T. Łoś-Nowak: *Stosunki międzynarodowe...*, s. 268; Z. J. Pietraś: *Podstawy teorii stosunków...*, s. 143-145.

i realizowane cele polityki zagranicznej mogą być sprzeczne z interesami (celami) innych uczestników stosunków międzynarodowych²²⁹. Bezsprzecznym pozostaje bowiem fakt, że państwa realizując politykę zagraniczną w wyniku podejmowanych działań zmierzają przede wszystkim do osiągnięcia własnych korzyści, niejednokrotnie, a być może głównie, kosztem innych uczestników stosunków międzynarodowych. Niekiedy też pomiędzy państwami może dochodzić do sprzeczności w zakresie realizacji ich celów podstawowych. Najważniejszym z nich jest zapewnienie bezpieczeństwa obywatelom danego państwa. W dalszej kolejności jest to zapewnienie ekonomicznego rozwoju, kreowanie pozytywnych warunków w państwie (tzw. środowiska politycznego) czy zapewnianie spójności wewnętrznej poprzez unikanie działań zmierzających do wytwarzania podziałów społecznych. W takiej sytuacji trudno oczekiwać ustępstw ze strony poszczególnych podmiotów, co z kolei może prowadzić do eskalacji napięć, a w konsekwencji konfliktu²³⁰.

Wreszcie wskazać należy, że cele polityki zagranicznej nie są również bytami samoistnymi, gdyż mogą stanowić wypadkową istnienia innych celów bądź też oddziaływać na siebie w określonym stopniu, a to z kolei będzie uzależnione od aktualnej sytuacji międzynarodowej. Cele polityki zagranicznej są również klasyfikowane pod względem ich ważności dla państwa, w wyniku czego tworzy się swoista ich hierarchia. Co jednak istotne, hierarchia ta nieustannie ewoluuje wymuszając podejmowanie rozmaitych działań na arenie międzynarodowej przez decydentów politycznych²³¹.

1.3.3. Klasyfikacja celów polityki zagranicznej

Jak już zostało wyżej wspomniane, cele polityki zagranicznej państw mogą przybierać różne wymiary w zależności od ich ustroju społeczno-politycznego, formy rządów, sytuacji geopolitycznej, historii, posiadanych zasobów czy relacji z innymi państwami. W nauce o stosunkach międzynarodowych można wyróżnić wiele typologii celów polityki zagranicznej. Dokonanie ich klasyfikacji służy ich uporządkowaniu w zależności od roli jaką pełnią w państwie które je formułuje, ale przede wszystkim pod kątem roli jaką pełnią w stosunku do innych uczestników stosunków międzynarodowych. W ramach niniejszego podrozdziału

²²⁹ T. Łoś-Nowak: *Polityka zagraniczna – stale i zmienne komponenty procesu formułowania i realizacji*. W: *Polityka zagraniczna: aktorzy...*, s. 51-54.

²³⁰ J. Nowiak: *Polityka zagraniczna*. W: *Międzynarodowe stosunki polityczne*. Red. W. Malendowski, Cz. Mojsiewicz. Poznań 1996, s. 62.

²³¹ T. Łoś-Nowak: *Polityka zagraniczna – stale i zmienne komponenty procesu formułowania i realizacji*. W: *Polityka zagraniczna: aktorzy...*, s. 51-54; T. Łoś-Nowak: *Wstęp do teorii stosunków...*, s. 265-266.

przedstawione zostaną klasyfikacje celów polityki zagranicznej, które w największym stopniu znalazły uznanie w nauce o stosunkach międzynarodowych.

Klasyfikacje celów polityki zagranicznej państwa dokonywane są poprzez zastosowanie przez ich autorów konkretnych kryteriów. W nauce anglosaskiej można wyróżnić wiele typologii o charakterze dychotomicznym w ramach których poszczególne cele polityki zagranicznej są klasyfikowane w oparciu o ich zawartość (prezentowane treści), formę wyrażania (uzewnętrzniania), adresata czy okresu obowiązywania. A. F. K. Organski wyróżnił cztery kategorie celów polityki zagranicznej takie jak: siła, dobrobyt, pokój oraz znaczenie kulturalne. Nadto, wyszczególnił kilka przeciwstawnych par celów polityki zagranicznej wyróżniając: cele współzawodnictwa i cele absolutne; cele, wokół których społeczeństwo jest zjednoczone i podzielone; cele narodowe i humanitarne; cele długookresowe i bezpośrednie; cele ogólne i specyficzne; cele określone i bieżące; cele *status quo* oraz dynamiczne²³². Inną klasyfikację spośród badaczy anglosaskich zaproponował J. Stoessinger dokonując rozróżnienia celów polityki zagranicznej przy uwzględnieniu kryterium dychotomicznego. Sformułowany przez niego podział obejmuje cztery pary celów polityki zagranicznej takie jak: cele współzawodnictwa i absolutne; cele jasno określone i nieokreślone; cele deklarowanie i działania; cele statyczne i dynamiczne²³³. Jeden z czołowych badaczy anglosaskich, G. Modelski, dokonał prostego podziału celów polityki zagranicznej wyróżniając cele defensywne oraz ofensywne²³⁴. W odniesieniu do powyższych klasyfikacji, zgodzić należy się z poglądem jaki wyraził R. Zięba pisząc, że „wydaje się, że klasyfikacje dychotomiczne są zbyt scholastyczne i nie potwierdzają się w praktyce polityki zagranicznej państw. Właściwie to niewiele one wyjaśniają, a raczej komplikują proces myślenia i analizy naukowej”²³⁵. W jego ocenie zdecydowanie bardziej użyteczne zdają się być klasyfikacje celów polityki zagranicznej o charakterze ogólnym, co z kolei pozwala na uwzględnienie całej struktury celów sformułowanych przez dane państwo. Takie koncepcje prezentowali tacy badacze jak A. Wolfers, W. F. Hanrieder oraz K. J. Holsti²³⁶.

Jedną z najpowszechniej stosowanych klasyfikacji celów polityki zagranicznej jest ta zaproponowana przez K. J. Holstiego. Dokonał on podziału celów polityki zagranicznej

²³² A. F. K. Organski: *World Politics*. New York 1958, s. 53-56, 63-77; R. Zięba: *Cele polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 44.

²³³ J. Stoessinger: *The Might of Nations. World Politics in Our Time*. New York 1965, s. 21-31; R. Zięba: *Cele polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 44.

²³⁴ G. Modelski: *A Theory of Foreign Policy...*, s. 91-93.

²³⁵ R. Zięba: *Cele polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 44.

²³⁶ Ibidem, s. 44.

państwa wyróżniając takie cele jak: podstawowe, średniofalowe oraz długofalowe²³⁷. Pierwszą grupę celów stanowią cele podstawowe. Zajmują one najwyższe miejsce w hierarchii celów, w ramach prowadzonej polityki zagranicznej. W imię ich realizacji, elity rządzące czy też cały naród są w stanie ponieść największe ofiary. Cele te związane są z żywotnymi interesami państwa, a więc takimi bez których realizacji nie będzie ono w stanie przetrwać na arenie międzynarodowej²³⁸. R. Zięba stwierdza, że teoria ta nawiązuje do pojęć wyodrębnianych przez realistów pisząc: „zauważyć należy, że ta kategoria nawiązuje do wielu pojęć wyodrębnionych przez przedstawicieli realizmu politycznego, takich jak: koncepcja twardego jądra interesu narodowego z teorii H. J. Morgenthau²³⁹, pojęcie żywotnych interesów, o których pisał między innymi F. Hartmann²⁴⁰, czy też kategoria bezpośrednich celów-interesów z prac K. von Vorysa”²⁴¹. Drugą grupę celów stanowią cele średniofalowe zwane również średniookresowymi. Są to przede wszystkim cele zmierzające do zabezpieczenia publicznych interesów państwa, prywatnych grup nacisku oraz międzynarodowego prestiżu państwa, z kolei poszczególne cele zawierają oczekiwania względem innych uczestników stosunków międzynarodowych. Charakter tej grupy celów można określić zatem jako ekspansywny, gdyż ich realizacja związana jest bezpośrednio z oddziaływaniem na inne podmioty międzynarodowe, często kosztem ich interesów²⁴². Trzecim i ostatnim z zaproponowanych przez H. J. Holstiego typu celów polityki zagranicznej państwa są cele długofalowe. Nie są one jednoznacznie sprecyzowane, a ich istota może ulegać nieustannej ewolucji w zależności od realizowanej przez dane państwo polityki zagranicznej bądź funkcjonującego systemu międzynarodowego²⁴³. Jak pisze R. Zięba, cele te mają charakter uniwersalny, gdyż zawierają „wizje i plany odnoszące się do politycznej i (lub) ideologicznej organizacji systemu międzynarodowego oraz reguł zachowania się państw na forum międzynarodowym”²⁴⁴. Powyższa klasyfikacja celów polityki zagranicznej państwa H. J. Holstiego, scharakteryzowana przez R. Ziębę, została również opisana przez T. Łoś-Nowak, która wskazała z kolei, że H. J. Holsti wyróżnił cele podstawowe (występujące pod analogiczną nazwą w opracowaniu R. Zięby), cele ekspansywne (odpowiadające celom średniofalowym czy średniookresowym

²³⁷ K. J. Holsti: *International Politics...*, s. 131-146.

²³⁸ Ibidem, s. 131-146.

²³⁹ H. Morgenthau: *Dilemmas of Politics*. Chicago 1958, s. 65-69.

²⁴⁰ F. Hartmann: *The Relations of Nations*. New York 1962, s. 6, 14.

²⁴¹ K. von Vorys: *The Concept of National Interest. W: Some Approaches and Concepts Used in the Teaching of International Politics*. Red. V. van Dyke. Iowa City 1957, s. 51.

²⁴² K. J. Holsti: *International Politics...*, s. 131-146; T. Łoś-Nowak: *Stosunki międzynarodowe...*, s. 267; R. Zięba: *Cele polityki zagranicznej państwa. W: Wstęp do teorii...*, s. 45.

²⁴³ K. J. Holsti: *International Politics...*, s. 138-146.

²⁴⁴ R. Zięba: *Cele polityki zagranicznej państwa. W: Wstęp do teorii...*, s. 45.

według R. Zięby) oraz cele uniwersalne (odpowiadające celom długofalowym w klasyfikacji R. Zięby)²⁴⁵.

Z kolei jedną z najbardziej rozpowszechnionych w polskiej nauce o stosunkach międzynarodowych typologii celów polityki zagranicznej państwa jest ta zaproponowana przez J. Kukułkę. Wyróżnił on trzy typy celów takie jak: egzystencjalne, koegzystencjalne oraz funkcjonalne²⁴⁶. Cele egzystencjalne stanowią pierwszy oraz podstawowy typ wyróżnionych przez J. Kukułkę. Obejmują one kwestie związane z zabezpieczeniem oraz realizacją materialnych i świadomościowych potrzeb danego państwa. Realizacja celów egzystencjalnych powinna następować w odpowiednim stopniu zaangażowania państwa, tak by zapewnić jego przetrwanie, bezpieczeństwo, jednolitość oraz rozwój. Działanie takie jest więc nieustannie trwającym procesem zmierzającym do maksymalizacji szans jego przetrwania i rozwoju. Należy więc stwierdzić, że ich cechą jest dynamika oraz nieustanna ewolucja²⁴⁷. Następnie J. Kukułka wskazał na cele koegzystencjalne pisząc, że zmierzają one do zaspokojenia „materialnych i świadomościowych potrzeb państwa w zakresie przynależności, łączności, współżycia, współpracy, współzawodnictwa i zorganizowania międzynarodowego”²⁴⁸. Cele koegzystencjalne mogą mieć więc charakter okresowy lub długotrwały oraz oddziaływać na siebie wzajemnie²⁴⁹. Ostatnim z typów są cele funkcjonalne, które to z kolei odnoszą się do uczestnictwa państwa w środowisku międzynarodowym. Dążą więc do zaspokajania potrzeb państwa w zakresie międzynarodowej informacji, regulacji, decyzji, percepcji, sprawności oraz skuteczności na arenie międzynarodowej. J. Kukułka podkreślił, że sprawna realizacja celów funkcjonalnych przyczynia się do zdolności państwa w zakresie realizowania celów egzystencjalnych i koegzystencjalnych, toteż w związku z tym będą one charakteryzować się największą dynamiką zmian oraz elastycznością²⁵⁰.

Dokonując porównania typologii celów polityki zagranicznej państwa zaproponowanej przez H. J. Holstiego oraz J. Kukułki, można wskazać na pewne elementy wspólne. Należy przede wszystkim zwrócić uwagę na fakt, że dokonali oni podziału celów na trzy typy, gdzie pierwszy z nich wydaje się być najistotniejszy, gdyż obejmuje cele, których realizowanie przez państwo powinno być kluczowe (cele podstawowe). Pogląd taki podzielił również R. Zięba

²⁴⁵ T. Łoś-Nowak: *Stosunki międzynarodowe...*, s. 267.

²⁴⁶ J. Kukułka: *Problemy polityki zagranicznej państw i współczesnych stosunków międzynarodowych. W: Zmienność i instytucjonalizacja stosunków międzynarodowych*. Red. J. Kukułka. Warszawa 1988, s. 150-153.

²⁴⁷ Ibidem, s. 151.

²⁴⁸ Ibidem, s. 152.

²⁴⁹ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych...*, s. 114; Ibidem, s. 152.

²⁵⁰ J. Kukułka: *Problemy polityki zagranicznej państw i współczesnych stosunków międzynarodowych. W: Zmienność i instytucjonalizacja...*, s. 152.

pisząc, że „zaniedbania w tym zakresie prowadzą bowiem do powstania zagrożeń dla prowadzenia polityki zagranicznej i osiągnięcia jej pozostałych celów”²⁵¹. Elementy wspólne odnoszą się również do hierarchizacji wymienionych typów celów polityki zagranicznej w kontekście ich ważności dla danego państwa. Jako pierwsze wymienione są cele podstawowe, następnie cele średniofalowe czy też średniookresowe (ekspansywne), które z kolei odpowiadają celom koegzystencjalnym zaproponowanym przez J. Kukułkę, by wreszcie wskazać na cele długofalowe (uniwersalne), które J. Kukułka nazywa funkcjonalnymi.

Jak już zostało wielokrotnie wspomniane w niniejszym rozdziale, działalność państwa ma charakter celowy, a więc co do zasady planowy oraz nastawiony na osiągnięcie konkretnych skutków (rezultatów). J. Kukułka, wyróżniając poszczególne cele polityki zagranicznej państwa wskazał również, że „wszystkie typy celów ukierunkowują więc procesy działań zewnętrznych państwa, wyznaczają ich przybliżony zakres oraz determinują ich dynamikę w długim lub krótkim horyzoncie czasowym”²⁵². Zaznaczył też, że „łączą także rację stanu i odpowiadające jej koncepcje polityki zagranicznej”²⁵³. Z takim wnioskiem nie sposób się nie zgodzić, gdyż państwa, urzeczywistniając cele polityki zagranicznej, dążą do zrealizowania pożądanego skutku, co w konsekwencji może oznaczać na przykład zmianę *status quo* albo jego utrzymanie.

Bez względu na przyjętą typologię celów polityki zagranicznej państwa wskazać należy, że wymienione wyżej typy celów stanowią cele zbiorcze, a te z kolei składają się z celów szczegółowych²⁵⁴. Realizacja celów szczegółowych dokonywana jest przez uczestników stosunków międzynarodowych w wyniku ukierunkowanych na nie procesów. W tym zakresie zgodzić należy się z poglądem J. Kukułki, który pisał, że „dopiero system procesów obejmujący system działań jest w stanie zapewnić realizację celów zbiorczych, które tworzą podstawowe typy celów zewnętrznych państwa”²⁵⁵.

Dokonując analizy poszczególnych typologii celów polityki zagranicznej występujących zarówno w światowej jak i polskiej nauce o stosunkach międzynarodowych należy wyprowadzić wniosek, że większość podziałów jest dokonywanych z uwagi na hierarchię (ważność) poszczególnych celów i ich grup. Jak stwierdza R. Zięba, wielu badaczy

²⁵¹ R. Zięba: *Cele polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 46.

²⁵² J. Kukułka: *Problemy polityki zagranicznej państw i współczesnych stosunków międzynarodowych*. W: *Zmienność i instytucjonalizacja...*, s. 152.

²⁵³ Ibidem, s. 152.

²⁵⁴ R. Zięba: *Cele polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 46.

²⁵⁵ J. Kukułka: *Problemy polityki zagranicznej państw i współczesnych stosunków międzynarodowych*. W: *Zmienność i instytucjonalizacja...*, s. 152-153.

dokonuje podziału celów polityki zagranicznej wyróżniając cele podstawowe (pierwotne), przez które należy rozumieć najważniejsze interesy państwa, których nieprawidłowa realizacja, lub w ogóle jej brak, może doprowadzić do jego unicestwienia. Choć pozostałe interesy określane mianem wtórnych obejmują swym zasięgiem znacznie więcej celów polityki zagranicznej, o charakterze mniej lub bardziej istotnym dla państwa, to jednak należy zaznaczyć, że zmierzają one do realizacji celów podstawowych (pierwotnych). Państwo, podejmując się formułowania celów polityki zagranicznej, powinno zatem dokonać ich hierarchizacji, gdzie na szczycie swoistej piramidy znajdować powinny się cele żywotne dla istnienia danego państwa, z kolei niżej cele o mniejszej wadze i znaczeniu²⁵⁶. Podstawowym celem polityki zagranicznej państwa jest zapewnienie mu szeroko rozumianego bezpieczeństwa. W tym miejscu zgodzić należy się z poglądem zaprezentowanym przez R. Ziębę, który stwierdził, że „mimo zintensyfikowania na początku XXI wieku procesów internacjonalizacji różnych dziedzin życia społecznego a nawet przyspieszenia procesów integracyjnych w niektórych regionach świata – naczelnym celem polityki zagranicznej współczesnych państw pozostaje nadal zapewnienie szeroko rozumianego ich bezpieczeństwa”²⁵⁷.

J. Kukułka zaproponował natomiast następującą typologię podstawowych celów polityki zagranicznej państwa. Wyróżnił on takie cele jak: zapewnienie bezpieczeństwa państwa, wzrost jego siły oraz pozycji i prestiżu międzynarodowego. Stwierdził również, że cele te powinno realizować każde państwo, gdyż zmierzają one do zachowania jego suwerenności, integralności terytorialnej oraz pozycji na arenie międzynarodowej. Z kolei brak ich realizacji lub niedostateczne zaangażowanie w tym zakresie może być wykorzystane przez innych uczestników stosunków międzynarodowych oraz prowadzić do unicestwienia danego państwa²⁵⁸. R. Zięba, dokonując analizy typologii celów podstawowych zaproponowanej przez J. Kukułkę, słusznie zauważył, że pokrywa się ona w znacznej części z innymi typologiami występującymi w światowej nauce o stosunkach międzynarodowych, jednakże pomija on dość istotną grupę celów²⁵⁹. R. Zięba pisze, że chodzi o „historycznie zmienną, ale stale występującą grupę interesów i celów o charakterze koegzystencjalnym i funkcjonalnym, takich jak: współpraca międzynarodowa, instytucjonalizacja stosunków międzynarodowych (w tym tworzenie prawa), ochrona i umacnianie pokoju, solidarność międzynarodowa, ochrona praw

²⁵⁶ R. Zięba: *Cele polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 47.

²⁵⁷ R. Zięba: *Wpływ tendencji globalizacyjnych na bezpieczeństwo narodowe*. „Rocznik Nauk Politycznych” 2001, T. 3, s. 54-55.

²⁵⁸ J. Kukułka: *Międzynarodowe stosunki...*, s. 43-44.

²⁵⁹ R. Zięba: *Cele polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 49-50.

człowieka itp.”²⁶⁰. W związku z tym wyodrębnia on obok trzech grup celów podstawowych polityki zagranicznej państwa J. Kukułka czwartą grupę jaką jest kształtowanie i optymalizacja reguł funkcjonowania środowiska międzynarodowego²⁶¹.

Dokonując analizy rozważań zawartych w niniejszym rozdziale wydaje się, że najistotniejszym celem polityki zagranicznej każdego państwa jest zapewnienie mu odpowiedniego poziomu bezpieczeństwa, co nie powinno wymagać szerszego uzasadnienia. R. Zięba stwierdził, że „w najogólniejszym znaczeniu bezpieczeństwo można więc określić jako pewność istnienia i przetrwania, stanu posiadania oraz funkcjonowania i rozwoju podmiotu”²⁶². Wskazał jednocześnie, że pewność tego stanu jest zmienna w czasie oraz powstaje lub zanika wskutek działalności danego podmiotu, bądź w skutek oddziaływania innego podmiotu na ten podmiot²⁶³. J. Kukułka pisał, że „bez zaspokojenia tych potrzeb nie może być mowy o prowadzeniu polityki zagranicznej i osiąganiu kolejnych jej celów”²⁶⁴. Dalej stwierdził, że to właśnie z tego powodu „państwa gotowe są w swojej polityce zagranicznej ograniczać inne potrzeby i cele, jeśli ma to służyć ich bezpieczeństwu”²⁶⁵. Takie poglądy potwierdzają wyjątkowość potrzeby jaką jest bezpieczeństwo oraz konieczności jej realizacji na każdym płaszczyźnie funkcjonowania danego podmiotu. W kontekście omawianego pojęcia należy również zasygnalizować, że bezpieczeństwo jako zjawisko cechuje się nieustanną ewolucją horyzontalną i wertykalną. S. Wojciechowski wskazał, że „w pierwszym przypadku oznacza to, że zmienia ono swój zakres wraz np. ze zwiększeniem się liczby podmiotów, których dotyczy (wymiar horyzontalny). Aspekt wertykalny to z kolei konieczność przeciwdziałania coraz to nowym wyzwaniom i zagrożeniom występującym w sferze bezpieczeństwa”²⁶⁶.

Powyższe stwierdzenia prowadzą również do wniosku, że przez zapewnianie bezpieczeństwa państwa w stosunkach międzynarodowych należy rozumieć ochronę istotnych dla danego narodu wartości wewnętrznych przed zagrożeniami zewnętrznymi. Należy zatem dokonać określenia owych wartości. W koncepcji zaproponowanej przez J. Kukułkę wyróżnia on: przetrwanie państwa, integralność terytorialną, niezależność polityczną oraz jakość życia.

²⁶⁰ Ibidem, s. 50.

²⁶¹ Ibidem, s. 50.

²⁶² R. Zięba: *O tożsamości nauk o bezpieczeństwie*. „Zeszyty Naukowe Akademii Obrony Narodowej” 2012, nr 1 (86), s. 7-8.

²⁶³ Ibidem, s. 7-8.

²⁶⁴ J. Kukułka: *Międzynarodowe stosunki...*, s. 43-44.

²⁶⁵ Ibidem, s. 43-44.

²⁶⁶ S. Wojciechowski: *Teoretyczne i praktyczne aspekty bezpieczeństwa Polski. 1.1. Wprowadzenie*. W: *Współczesne bezpieczeństwo Polski. Międzynarodowy wymiar instytucjonalny*. Red. A. Wejksznar, S. Wojciechowski. Warszawa 2019, s. 15.

Pierwsza z wymienionych wartości – przetrwanie, jest postrzegana przez badaczy stosunków międzynarodowych jako najważniejszą spośród wszystkich wymienionych, gdyż pozwala ona na trwanie danego państwa jako niezależnego bytu, narodu jako grupy etnicznej czy biologiczne przeżycie ludności. Następna z wartości – integralność terytorialna, odnosi się do zdolności państwa do utrzymania kontroli nad jego terytorium. Niezależność polityczna z kolei oznacza zdolność do samostanowienia, a więc posiadane przez państwo atrybutu suwerenności. Ostatnia z wartości – jakość życia, odnosi się do poziomu dobrobytu w społeczeństwie, rozwoju gospodarczego, systemu kulturalnego oraz dalszych perspektyw ich wzrostu²⁶⁷.

Następnym celem polityki zagranicznej państwa zaliczanych przez J. Kukulkę do celów podstawowych jest wzrost siły państwa. Przez wskazany cel należy przede wszystkim rozumieć dążenie do zapewniania wsparcia poprzez realizowaną politykę zagraniczną dla działań podejmowanych przez społeczeństwo oraz państwo, a zmierzających do szeroko rozumianego rozwoju państwa. Prowadzona polityka zagraniczna powinna zmierzać zatem również do realizacji kluczowych (egzystencjonalnych) potrzeb narodu, a zatem do podnoszenia poziomu życia obywateli, zapewnienia sprawnego funkcjonowania systemu wewnętrznego, a w konsekwencji zwiększania zdolności w zakresie przeciwdziałania potencjalnym zagrożeniom zewnętrznym, ale również wpływu na innych uczestników stosunków międzynarodowych²⁶⁸.

Kolejnym z celów podstawowych polityki zagranicznej państwa jest wzrost jego pozycji międzynarodowej i prestiżu. R. Zięba pisał o nim, że „koegzystencjalne interesy wyrastają z potrzeb: uczestnictwa w systemie międzynarodowym, znaczenia i miejsca wśród innych narodów, współpracy i współzawodnictwa z innymi państwami i narodami, potwierdzania suwerenności państwa i wzrostu jego roli międzynarodowej”²⁶⁹. E. Cziomer stwierdził z kolei, że jest on „ściśle uzależnionym od wielu czynników obiektywnych i subiektywnych, o charakterze wewnętrznym i międzynarodowym”²⁷⁰, zwłaszcza od dobrych wskaźników efektywności rozwoju społeczno-gospodarczego, sprawnego funkcjonowania demokratycznego systemu politycznego oraz jego instytucji: potencjału militarnego i jakości sił zbrojnych”²⁷¹.

²⁶⁷ J. Kukulka: *Bezpieczeństwo a współpraca europejska: współzależność i sprzeczność interesów*. „Sprawy międzynarodowe” 1982, nr 7, s. 34.

²⁶⁸ J. Kukulka: *Międzynarodowe stosunki...*, s. 43-44, 381.

²⁶⁹ R. Zięba: *Cele polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 53-54.

²⁷⁰ R. Zięba w *Uwarunkowania polityki zagranicznej państwa*. W: *Wstęp do teorii polityki zagranicznej państwa*. Red. R. Zięba. Toruń 2005. R. Zięba czynniki wskazane przez E. Cziomera określał mianem uwarunkowań wewnętrznych i zewnętrznych o charakterze obiektywnym i subiektywnym. Kwestie te omówiono we wcześniejszych częściach pracy.

²⁷¹ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych...*, s. 115.

Ostatnim z podstawowych celów polityki zagranicznej państwa, którego sformułowanie postulował R. Zięba po dokonaniu analizy dyskursu międzynarodowego w tym zakresie, a przede wszystkim celów zaproponowanych przez J. Kukułkę, jest kształtowanie i optymalizacja reguł funkcjonowania środowiska międzynarodowego²⁷². Współcześnie interesami tymi są na przykład takie wartości jak współpraca międzynarodowa, wymiana informacyjna, prawo, rozbrojenie, pokój, prawa człowieka, ochrona środowiska czy solidarność międzynarodowa. Należy przy tym zauważyć, że istotną rolę w realizacji powyższego celu będzie odgrywać prawo międzynarodowe publiczne, którego zadaniem jest ochrona oraz wspieranie powyższych wartości. Słusznie zauważył przy tym R. Zięba pisząc, że „każde państwo może być zainteresowane umacnianiem systemu stosunków międzynarodowych, jego stabilizacją, bądź takim przekształcaniem, aby ten system sprzyjał osiągnięciu przez państwa głównych celów ich polityki zagranicznej (tj. bezpieczeństwa, wzrostu siły i pozycji międzynarodowej)”²⁷³. Dalej wskazał, że „państwa podchodzą instrumentalnie do środowiska międzynarodowego, ale muszą też uzgadniać pewne podstawowe reguły jego funkcjonowania”²⁷⁴. Z powyższych rozważań można wyprowadzić wniosek który podzielił również E. Cziomer wskazując, że kształtowanie i optymalizacja funkcjonowania środowiska międzynarodowego jest niezbędne do efektywnego realizowania sformułowanych celów podstawowych takich jak zapewnienie bezpieczeństwa państwa, wzrost siły państwa oraz wzrost pozycji międzynarodowej i prestiżu państwa²⁷⁵. Wydaje się być zatem trafnym spostrzeżenie, że państwa chcąc aktywnie uczestniczyć w kształtowaniu systemu międzynarodowego, ale również dążąc do zabezpieczenia realizacji swoich partykularnych interesów, są zmuszone do uczestnictwa w tworzeniu norm i instytucji w środowisku międzynarodowym, a także stosowania się do już istniejących.

1.4. Środki realizacji polityki zagranicznej

Wielokrotnie już wskazywano, że realizacja polityki zagranicznej przez państwa jest działaniem celowym, toteż w tym miejscu należy zwrócić uwagę na niezwykle skomplikowany proces jej realizacji. Istotnymi jego częściami są nie tylko materialne zasoby siły tzw. *hard*

²⁷² Zobacz szerzej: J. Kukułka: *Międzynarodowe stosunki polityczne*. Warszawa 1982, s. 89-92; R. Zięba: *Uwarunkowania polityki zagranicznej państwa*. W: *Wstęp do teorii polityki zagranicznej państwa*. Red. R. Zięba. Toruń 2005, s. 48-50.

²⁷³ R. Zięba: *Cele polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 55-58.

²⁷⁴ Ibidem, s. 55-58.

²⁷⁵ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych...*, s. 115.

power, ale również zasoby tzw. *soft power* i *smart power*, takie jak skuteczna dyplomacja, otwarcie na środowisko międzynarodowe, atrakcyjność przedkładanych ofert i ich wartość w kontekście stabilności i bezpieczeństwa (regionalnego lub globalnego). T. Łoś-Nowak stwierdziła, że „tak rozumiana siła państwa niezbędna do zapewnienia mu nie tylko wąsko rozumianego bezpieczeństwa, ale szans na rozwój, dobrobyt jego obywateli i rozwój cywilizacyjny jest wypadkową możliwości państwa i jego zdolności do posługiwania się nimi w środowisku międzynarodowym”²⁷⁶. Niezbędne jest zatem, obok sformułowanych celów polityki zagranicznej, dokonanie określenia środków jej realizacji. Bez tego podejmowane przez uczestników stosunków międzynarodowych działania będą mało skuteczne lub w ogóle nieskuteczne²⁷⁷. T. Łoś-Nowak pisze, że dobór środków jest determinowany takimi czynnikami jak: wielkość, zakres oraz kompatybilność celów; intensywność ich przejawiania się; relatywne możliwości jakimi państwo dysponuje albo społecznym przyzwoleniem na rezygnację z innych celów; ich pilność; możliwość zastąpienia jednego z nich lub modyfikacją w odpowiedzi na presję zewnętrzną lub wewnętrzną; skalę ryzyka jakie państwo jego gotowe ponieść dla ich realizacji; przekonanie, że cele będą osiągnięte²⁷⁸.

Środki realizacji polityki zagranicznej należy więc postrzegać jako instrumenty, które zmierzają do osiągnięcia poszczególnych jej celów. J. Zając definiuje ich pojęcie jako „wszystkie zasoby i instrumenty, przy użyciu których państwa starają się kształtować pożądane postawy i działania zagranicznych podmiotów oraz pożądane stany zjawisk i procesów międzynarodowych”²⁷⁹. W odniesieniu do pojęcia środków, J. Zając definiuje również termin *instrument*. Jest on stosunkowo szeroko stosowany w nauce o stosunkach międzynarodowych, w szczególności w literaturze zachodniej, jednakże wydaje się on być kategorią podrzędną względem środka polityki zagranicznej. Uzasadniając taki pogląd stwierdza, że w odniesieniu do jednego typu środka, można wyróżnić kilka instrumentów w wyniku których stosowania dany środek będzie realizowany²⁸⁰. Ponadto, od pojęcia środków i instrumentów należy odróżnić termin *metody*. Metodami są bowiem sposoby posługiwania się przez uczestników stosunków międzynarodowych środkami. Z. J. Pietraś dzieli je na metody pozytywne (nakłanianie), negatywne (przymus) oraz neutralne²⁸¹.

²⁷⁶ T. Łoś-Nowak: *Polityka zagraniczna – stale i zmienne komponenty procesu formułowania i realizacji*. W: *Polityka zagraniczna: aktorzy...*, s. 54-55.

²⁷⁷ T. Łoś-Nowak: *Wstęp do teorii stosunków...*, s. 140.

²⁷⁸ T. Łoś-Nowak: *Stosunki międzynarodowe...*, s. 273.

²⁷⁹ J. Zając: *Środki i metody polityki zagranicznej państwa*. W: *Wstęp do teorii polityki zagranicznej państwa*. Red. R. Zięba. Toruń 2005, s. 79.

²⁸⁰ Ibidem, s. 79.

²⁸¹ Z. J. Pietraś: *Podstawy teorii stosunków...*, s. 86.

Dokonując wyodrębnienia poszczególnych środków polityki zagranicznej należałoby w dalszej kolejności posłużyć się kryteriami ich oddziaływania. W tym zakresie najczęściej stosowanym i wydaje się, że najprzydatniejszym, jest kryterium podmiotowe, które pozwala wyróżnić takie środki jak: polityczne, ekonomiczne, wojskowe oraz kulturowo-ideologiczne²⁸². W ramach powyższych kategorii nie dokonano wyszczególnienia środków prawnych, uzasadniając to faktem, że zastosowanie każdej z powyższych grup środków może przybierać formę prawną. Należy zgodzić się z takim poglądem, gdyż prawo międzynarodowe publiczne pełni rolę służebną wobec stosunków międzynarodowych, w wyniku czego poszczególne typy środków polityki zagranicznej państwa zazębiają się ze środkami prawnymi. Kolejnym z kryteriów jest kryterium czasowe, które określa czas w jakim środki polityki zagranicznej są realizowane. Wyróżniamy środki krótkofalowe, średniofalowe oraz długofalowe. Następnie wskazać należy na kryterium sposobu oddziaływania, przez co należy rozumieć środki polityki zagranicznej państwa o charakterze dwustronnym oraz wielostronnym, stosowane przez państwa lub organizacje międzynarodowe²⁸³.

Opisując środki realizacji polityki zagranicznej, nie sposób nie odnieść się do rezultatów jakie mogą zostać osiągnięte wyniku ich zastosowania. Oczywistym jest bowiem fakt, że nie zawsze zastosowane środki, zmierzające do zrealizowania określonego celu, wywołają pożądany przez danego uczestnika stosunków międzynarodowych skutek. J. Kukułka stwierdził, że zastosowane przez państwa środki mogą przynieść rezultat zamierzony (prosty) lub niezamierzony (uboczny). Porównanie zamierzonego celu oraz osiągniętego wyniku pozwala z kolei na ocenę skuteczności podejmowanych działań. Dalej J. Kukułka zaproponował wyróżnienie czterech rodzajów wyników działań zewnętrznych państwa, takich jak: stabilizujące (konserwacyjne), profilaktyczne, konstruktywne oraz destrukcyjne. Pierwszy z nich – stabilizujący, zwany również konserwacyjnym, przejawia się w utrzymaniu istniejącego w danym momencie *status quo*, a więc wynika z niego, że podejmowane przez państwo działania utrwaliły istniejący stan rzeczy. Drugim z wyników jest wynik profilaktyczny, objawiający się w skutecznym zapobiegnięciu wystąpienia danych stanów faktycznych, które charakteryzują się cechami negatywnymi. Następny z wyników, będący wynikiem konstruktywnym, oznacza dokonanie zmiany o charakterze pozytywnym, a więc wykreowanie w danym stanie rzeczy cech, które będą oceniane w sposób dodatni dla danego podmiotu. I wreszcie, czwarty z wyników – destrukcyjny, polega na powstaniu w wyniku

²⁸² J. Zajac: *Środki i metody polityki zagranicznej państwa. W: Wstęp do teorii...*, s. 81-82.

²⁸³ Ibidem, s. 82.

zastosowanych środków stanu faktycznego o charakterze negatywnym²⁸⁴. Należy również zauważyć, że wynik konkretnych działań należy oceniać nie tylko w kontekście rzeczywiście wywołanych skutków (pozytywnych, neutralnych czy negatywnych), lecz przede wszystkim w kontekście zamierzonych przez dany podmiot celów.

Katalog środków realizacji polityki zagranicznej państwa nie ma charakteru enumeratywnego. Co więcej, katalog ten ulega stałej ewolucji w wyniku zachodzących zmian społecznych, w tym w ramach stosunków międzynarodowych²⁸⁵. Na potrzeby niniejszej rozprawy przyjęto następujące typy środków realizacji polityki zagranicznej państwa: środki polityczne, środki wojskowe, środki ekonomiczne oraz środki kulturowo-ideologiczne. Uzasadnieniem wyboru powyższych typów jest ich rozpowszechnienie w nauce o stosunkach międzynarodowych jako tych, które są najczęściej stosowane przez państwa w ramach realizowanej przez nie polityki zagranicznej. Środki polityczne (zwane również środkami dyplomatycznymi²⁸⁶) realizacji polityki zagranicznej państwa stanowią istotę stosunków międzynarodowych, oraz najczęściej stosowany środek przez ich uczestników. W korelacji ze środkami politycznymi pozostają środki prawne (zwane też normatywnymi), które pełnią wobec nich rolę służebną²⁸⁷.

Najogólniej rzecz ujmując, środki polityczne to ogół stosunków dyplomatycznych, poczynając od klasycznych form dyplomacji, poprzez działania negocjacyjne (również konferencyjne), po udział w organizacjach międzynarodowych i sojuszach²⁸⁸. W związku z tym stwierdzić należy, że środki polityczne obejmują wszelkiego rodzaju oświadczenia i deklaracje polityczne uczestników stosunków międzynarodowych, składane przede wszystkim w oparciu o służbę dyplomatyczną (zagraniczną) danego państwa. Dyplomacja stanowi więc działalność zewnętrzną państwa umożliwiającą nawiązywanie i utrzymywanie stosunków między państwami przy jednoczesnej ochronie jego interesów²⁸⁹. Jak pisze J. Zając, może ona przybierać różne formy „stosując metodę pozytywną, w której wykazują dobrą wolę, obiecują korzyści, zachęcają dane państwo na nawiązania bliższych kontaktów oraz metodę negatywną, używając formy przymusu, perswazji, groźby oraz podstęp”²⁹⁰. Dalej wskazuje, że „istnieją

²⁸⁴ J. Kukułka: *Problemy polityki zagranicznej państw i współczesnych stosunków międzynarodowych*. W: *Zmienność i instytucjonalizacja...*, s. 157-158.

²⁸⁵ R. Kuźniar: *Międzynarodowe stosunki polityczne*. W: *Stosunki międzynarodowe...*, s. 116-117.

²⁸⁶ T. Łoś-Nowak: *Wstęp do teorii stosunków...*, s. 142-143.

²⁸⁷ E. Cziomer, L. W. Zyplikiewicz: *Zarys współczesnych stosunków międzynarodowych*. Warszawa 2004, s. 122; J. Zając: *Środki i metody polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 81-82.

²⁸⁸ J. Kukułka: *Międzynarodowe stosunki...*, s. 45.

²⁸⁹ J. Sutor: *Prawo dyplomatyczne i konsularne*. Warszawa 1996, s. 28; R. Bierzanek, J. Symonides: *Prawo Międzynarodowe...*, s. 172-176.

²⁹⁰ J. Zając: *Środki i metody polityki zagranicznej państwa*. W: *Wstęp do teorii...*, s. 82-83.

także metody neutralne, do których można zaliczyć konsultacje oraz wymianę informacji, należące do rutynowych metod działalności dyplomatycznej”²⁹¹. Dyplomacja jest działalnością co do zasady uregulowaną w prawie międzynarodowym publicznym przede wszystkim przez Konwencję wiedeńską o stosunkach dyplomatycznych z 18 kwietnia 1961 roku. Zawiera ona podstawowe zasady międzynarodowego prawa dyplomatycznego, które powinno stosować państwo będące sygnatariuszem konwencji, w kontaktach dyplomatycznych z innymi uczestnikami stosunków międzynarodowych²⁹². Działalność dyplomatyczna obejmuje przede wszystkim pokojowe załatwianie sporów międzynarodowych, co może następować w drodze rokowań bezpośrednich, dobrych usług i mediacji, komisji badań oraz koncyliacji²⁹³.

Środki wojskowe (militarne) zawsze stanowiły i będą stanowić jeden z kluczowych elementów realizacji polityki zagranicznej państwa, co przy ich zestawieniu z historią konfliktów zbrojnych wydaje się nie potrzebować szerszego uzasadnienia. Jest jednak faktem, że współcześnie środki te stale tracą na znaczeniu co jest spowodowane, przede wszystkim ograniczeniem możliwości ich stosowania, w związku z obowiązującymi normami prawa międzynarodowego. Niemniej jednak siła militarna nadal pozostaje bezsprzecznie jednym z najczęściej wykorzystywanych przez państwa środków realizacji polityki zagranicznej²⁹⁴. J. Kukułka wskazał, że na zdolność wykorzystania przez państwo środków wojskowych składają się takie czynniki jak wielkość i jakość armii, stan jej uzbrojenia, rozmieszczenia oraz morale. Z kolei przejawem ich stosowania na arenie międzynarodowej jest wyścig zbrojeń, szczególnie widoczny po II wojnie światowej²⁹⁵. Podobny pogląd podzielił E. Cziomer, który do uwarunkowań wykorzystania środków wojskowych zaliczył również położenie geopolityczne państwa oraz przynależność państwa do sojuszy militarnych. Omawiając zakres zastosowania środków militarnych wskazał, że mogą „być stosowane bezpośrednio, prowadzą wtedy do interwencji lub innej formy działań zbrojnych łącznie z wojną, bądź też pośrednio, polegają wówczas na wspieraniu ruchów odśrodkowych (podczas wojen domowych), nielegalnym dostarczaniu broni lub innej pomocy wojskowej”²⁹⁶. Wspomniany przez J. Kukułkę wyścig zbrojeń jako przejaw stosowania przez państwo środków militarnych był szczególnie widoczny w okresie zimnowojennym, kiedy to posiadanie broni masowego rażenia stanowiło wyznacznik pozycji państwa na arenie międzynarodowej oraz skutkowało

²⁹¹ Ibidem, s. 82-83.

²⁹² Zobacz szerzej: *Konwencja wiedeńska o stosunkach dyplomatycznych, sporządzona w Wiedniu dnia 18 kwietnia 1961 roku* (Dz.U. 1965 nr 37 poz. 232).

²⁹³ R. Bierzanek, J. Symonides: *Prawo Międzynarodowe...*, s. 341-349.

²⁹⁴ Ibidem, s. 379-440.

²⁹⁵ J. Kukułka: *Międzynarodowe stosunki...*, s. 45-46.

²⁹⁶ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych...*, s. 123.

odstraszaniem potencjalnego przeciwnika²⁹⁷. Siła zbrojna stanowiła oraz stanowi również element presji oraz wymuszania ustępstw ze strony innych państw. W tym kontekście należy wskazać, że środki wojskowe występują najczęściej łącznie ze środkami politycznymi²⁹⁸.

Do środków ekonomicznych, nazywanych również gospodarczymi, należy zaliczyć przede wszystkim te instrumenty, które polegają na wykorzystaniu potencjału ekonomicznego państwa, a zwłaszcza stopnia rozwoju jego przemysłu, handlu czy finansów. O posiadanych przez dane państwo środkach ekonomicznych będzie świadczyć również ilość posiadanych przez nie zasobów surowcowych, w szczególności energetycznych. Państwo mające dobrą kondycję gospodarczą oraz posiadające dostateczną ilość zasobów będzie w większym stopniu samowystarczalne, a więc w mniejszym stopniu zależne od importu z innych państw. Taki stan rzeczy najczęściej będzie skutkował również dużymi możliwościami w zakresie eksportu, a tym samym posiadaniu zdolności oddziaływania w tym zakresie na innych uczestników stosunków międzynarodowych²⁹⁹.

Dokonując analizy powyższego poglądu należy przytoczyć trafnie spostrzeżenie R. Kuźniara który wskazał, że „instrumenty gospodarcze obejmują zarówno znajdujące się w dyspozycji państw zasoby, jak i sposoby posługiwania się nimi w polityce zagranicznej. Należy je jednak odróżniać od normalnych, wynikających z prawidłowego rozwoju i funkcjonowania gospodarki narodowej, stosunków gospodarczych (handlowych, finansowych, technicznych itp.) z zagranicą. Środki i metody gospodarcze stają się instrumentem polityki zagranicznej, gdy za ich pomocą państwo chce osiągnąć polityczne cele”³⁰⁰. Podobnie jak w kontekście innych środków realizacji polityki zagranicznej państwa tak i w przypadku środków ekonomicznych można wyróżnić ich aspekt pozytywny oraz negatywny. T. Łoś-Nowak pisze, że do środków o charakterze pozytywnym zaliczamy chociażby: redukcję taryf celnych, przyznawanie licencji, gwarancje dla prywatnego kapitału inwestującego w danym państwie, korzystne kredyty czy zwolnienia z opłat. Z kolei do środków o charakterze negatywnym zalicza ona: *embargo*, bojkot gospodarczy, *dumping* cen, dyskryminacje w przyznawaniu taryf celnych, zamrożenie handlu, opodatkowanie wymiany czy cofnięcie zgody na kontyngenty w handlu³⁰¹. W odniesieniu do skutków stosowania przez państwa środków ekonomicznych E. Cziomer wskazał, że „mogą one być wykorzystywane do różnych celów, które ochraniają interesy i wzmacniają pozycję własnego państwa w sposób legalny oraz

²⁹⁷ Zobacz szerzej: *Mutual Assured Destruction*.

²⁹⁸ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych...*, s. 123.

²⁹⁹ J. Kukułka: *Międzynarodowe stosunki...*, s. 45.

³⁰⁰ R. Kuźniar: *Międzynarodowe stosunki polityczne*. W: *Stosunki międzynarodowe...*, s. 117.

³⁰¹ T. Łoś-Nowak: *Wstęp do teorii stosunków...*, s. 143.

zgodnie z umowami międzynarodowymi, bądź też narażają na straty partnerów i kontrahentów poprzez różne formy nacisku i szantażu, nie wkluczając ich uzależnienia”³⁰².

Polityka zagraniczna wielu państw opiera się na stosowaniu środków kulturowo-ideologicznych, które służą przede wszystkim podnoszeniu prestiżu danego państwa, a tym samym jego pozycji na arenie międzynarodowej. Termin *kultura* może być definiowany jako całokształt materialnego i niematerialnego dorobku człowieka czy też danej zbiorowości. Oddziaływanie międzynarodowe przy użyciu środków kulturalnych określa się mianem dyplomacji kulturalnej, której działania są podstawą obowiązujących w danym momencie celów polityki kulturalnej państwa³⁰³. W związku z powyższym należy wskazać na pogląd sformułowany przez J. Zając która pisze, że „poprzez promocję własnego sposobu myślenia i działania państwa próbują zdobyć wpływy w wielu regionach świata i podnieść swoją pozycję na arenie międzynarodowej”³⁰⁴.

Odnosząc się wreszcie do pojęcia ideologii, definiowanej najogólniej rzecz ujmując jako zbiór światopoglądów, należy zaznaczyć, że kształtuje się ona na gruncie kultury³⁰⁵. Z kolei środki ideologiczne, jak pisze J. Kukułka, stanowią proces oddziaływania za pomocą własnej ideologii „na świadomość i ideologię innych narodów, państw i rządów”³⁰⁶. W jego ocenie „najbardziej znanymi postaciami takiego oddziaływania są różne formy zagranicznej informacji, propagandy i polityki kulturalnej stosowane w bilateralnych i wielostronnych stosunkach z innymi państwami”³⁰⁷. Oddziaływanie za pomocą ideologii może przybierać różne formy. Wyróżnić można oddziaływanie o konsekwencjach realnych oraz oddziaływanie o skutkach intencjonalnych. Pierwszą grupę form stanowią propaganda międzynarodowa, dywersja ideologiczna oraz doktryny polistrategiczne, z kolei do drugiej zaliczamy koncepcje społeczno-polityczne, mity ideologiczne, teorie społeczno-naukowe oraz wielkie religie³⁰⁸. Wreszcie, wykorzystanie środków kulturowo-ideologicznych może przybrać formę pozytywną albo negatywną. Forma pozytywna występuje wtedy, kiedy oddziaływanie polega na wytwarzaniu świadomych oraz trwałych podstaw współpracy międzynarodowej oraz skutkuje łagodzeniem napięć międzynarodowych, a co jest szczególnie widoczne w państwach wysokorozwiniętych. Z kolei forma negatywna prowadzi do wytworzenia zagrożeń dla dóbr

³⁰² E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych...*, s. 122.

³⁰³ G. Michałowska: *Zmienność i instytucjonalizacja międzynarodowych stosunków kulturalnych*. Warszawa 1991, s. 253.

³⁰⁴ J. Zając: *Środki i metody polityki zagranicznej państwa. W: Wstęp do teorii...*, s. 91.

³⁰⁵ G. Michałowska: *Międzynarodowe stosunki kulturalne*. Warszawa 1986, s. 29.

³⁰⁶ J. Kukułka: *Międzynarodowe stosunki...*, s. 45.

³⁰⁷ Ibidem, s. 45.

³⁰⁸ J. Zając: *Środki i metody polityki zagranicznej państwa. W: Wstęp do teorii...*, s. 92.

kultur narodowych. Przykładem takiego zjawiska może być polityka kulturalna prowadzona przez USA, które wykorzystują ją jako narzędzie wpływu. Jej skutkiem jest przyjmowanie w wielu regionach świata amerykańskiego stylu życia (również dążenie do niego), oglądanie amerykańskich filmów czy przejmowanie amerykańskich świąt. Wykorzystanie środków kulturowo-ideologicznych w formie negatywnej może przejawiać się również w dywersji ideologicznej, totalnej propagandzie czy instrumentalnym wykorzystaniem zasad religijnych. Niebezpiecznym zjawiskiem jest również starcie dwóch przeciwstawnych ideologii, czego przykładem może być rywalizacja Wschodu i Zachodu podczas zimnej wojny³⁰⁹.

Jedną z form środków kulturowo-ideologicznych mogą być również instrumenty (środki) określane mianem psychospołecznych. R. Kuźniar pisze, że polegają one na wykorzystaniu „kultury, nauki, informacji, atrakcyjności ideologii czy modelu społecznego w działalności promocyjnej, propagandowej, informacyjnej prowadzonej przez dane państwo wobec swego otoczenia”³¹⁰. Dalej stwierdza, że „stosowanie środków psychospołecznych służy niekiedy dezinformacji, dywersji lub też przybiera postać czarnej propagandy zmierzającej do uzależnienia lub podbicia innego państwa”³¹¹. Warto zaznaczyć, że omawiane instrumenty należy zaliczyć do narzędzi wojny informacyjnej. E. Cziomer pisząc z kolei o środkach psychospołecznych stwierdza, że „stanowią one ogromny wachlarz działania państw od zagranicznej polityki kulturalnej, współpracy naukowej, polityki informacyjnej itp.”³¹². W swoich rozważaniach podziela pogląd, że mogą być one stosowane zarówno w sposób pozytywny jak i negatywny. Sposób pozytywny w jego ocenie przejawia się w wymianie kulturalnej w której wyniku następuje zbliżanie się państw i narodów, zacieśnianiu współpracy naukowej, czy też szerzeniu informacji skutkującej kreowaniem obrazu współpracujących ze sobą społeczeństw i narodów. Z kolei sposób negatywny stanowi zaprzeczenie pozytywnego oraz polega na szerzeniu dyskryminacji, nienawiści oraz negatywnego obrazu innych państw i obywateli. E. Cziomer stwierdza również, że „państwa, zwłaszcza demokratyczne, nie są wyłącznymi dysponentami wymienionych wyżej środków (np. mediów, instytucji naukowych itp.), które, wykorzystując wolność słowa i druku, mogą propagować własne oceny na temat sąsiadów i innych państw lub poszczególnych zagadnień niezgodnych z polityką zagraniczną danego państwa. Jest ono wtedy zobowiązane do podjęcia środków zaradczych o charakterze

³⁰⁹ Ibidem, s. 93.

³¹⁰ R. Kuźniar: *Międzynarodowe stosunki polityczne*. W: *Stosunki międzynarodowe...*, s. 118.

³¹¹ Ibidem, s. 118.

³¹² E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych...*, s. 123.

politycznych lub prawnych, szczególnie gdy działania powyższe są sprzeczne z prawem lub racją stanu i wychodzą z grona marginalnych ugrupowań i sił politycznych”³¹³.

³¹³ Ibidem, s. 123.

Rozdział 2. Wojna informacyjna jako instrument prowadzenia polityki zagranicznej

2.1. Pojęcie informacji

Pojęcie *informacji* w potocznym rozumieniu tego terminu wydaje się być całkowicie oczywiste i nie wymagać szerszego omówienia. Jednakże inaczej sytuacja wygląda w dyskursie naukowym, gdzie bywa ono definiowane niejednoznacznie, co wynika przede wszystkim z jego interdyscyplinarnego charakteru. W zależności zatem od poszczególnych dziedzin i dyscyplin nauki, termin ten będzie definiowany w sposób odmienny³¹⁴. Na potrzeby rozprawy przytoczonych zostało kilka wybranych definicji wskazanego pojęcia, które najpełniej oddają jego znaczenie w kontekście omawianego problemu badawczego.

Pierwszą definicją jaką można przytoczyć, cechującą się jednocześnie charakterem uniwersalnym, jest ta wskazująca, że informacja to „pojęcie, w zasadzie niedefiniowalne ze względu na jego pierwotny, elementarny charakter; rozpatrywana najczęściej w trzech aspektach: syntaktycznym (dotyczy ilości informacji, jaka może być potencjalnie zawarta w danej wiadomości), semantycznym (znaczenia i zawartości treściowej wiadomości) i pragmatycznym (przydatności informacji, tj. wartości informacji zawartej w wiadomości ze względu na realizowany przez odbiorcę cel)”³¹⁵. Inny pogląd odnosi pojęcie informacji do faktów dotyczących danej sytuacji, osoby czy zdarzenia³¹⁶. Jest ona definiowana również jako wiedza zdobywana o kimś lub o czymś, ale również fakty lub szczegóły dotyczące danego zagadnienia³¹⁷. Warto również przytoczyć pogląd, zgodnie z którym współcześnie nie jest możliwe określenie uniwersalnych metod analizy terminu informacja pod kątem semantycznym i pragmatycznym. Jest możliwe jednak dokonanie tego w sensie syntaktycznym, gdzie informację definiuje się poprzez ich ilość (miarę), bądź też postrzega się jako synonim pojęcia *dana*³¹⁸. Inna z definicji słownikowych stwierdza, że „informacja jest zwykle utożsamiana z przedmiotami myślowymi, odzwierciedlającymi wszelkie wiadomości, wieści, nowiny lub rzeczy zakomunikowane”³¹⁹.

³¹⁴ A. D. Madden: *A definition of information*. „Aslib Proceedings” 2000, Vol. 52, No. 9, s. 343-348.

³¹⁵ Encyklopedia PWN: *informacja*. <https://encyklopedia.pwn.pl/haslo/informacja;3914686.html> (dostęp: 01.10.2022).

³¹⁶ Cambridge Dictionary: *information*. <https://dictionary.cambridge.org/dictionary/english/information> (dostęp: 01.10.2022).

³¹⁷ Britannica Dictionary: *information*. <https://www.britannica.com/dictionary/information> (dostęp: 01.10.2022).

³¹⁸ Encyklopedia PWN: *informacja*. <https://encyklopedia.pwn.pl/haslo/informacja;3914686.html> (dostęp: 01.10.2022).

³¹⁹ M. Wrzosek, Sz. Markiewicz, Z. Modrzejewski (Red.): *Informacyjny wymiar wojny hybrydowej*. Warszawa 2019, s. 89.

L. Ciborowski odniósł z kolei pojęcie informacji do swego rodzaju bodźca, który oddziałuje na „układ recepcyjny człowieka, powodujący wytwarzanie w jego wyobraźni przedmiotu myślowego, odzwierciedlającego obraz rzeczy materialnej lub abstrakcyjnej (przedmiotu, procesu, zjawiska, pojęcia), który w jego przekonaniu (świadomości) kojarzy się z tym bodźcem”³²⁰. Informacja to również „obiekt abstrakcyjny, który może być w postaci zakodowanej zapisywany (na nośnikach informacji), przesyłany, przetwarzany za pomocą programów komputerowych i używany do sterowania urządzeniami”³²¹. N. Wiener pisał z kolei, że jest ona treścią „zaczepniętą ze świata zewnętrznego w procesie naszego dostosowania się do niego i przystosowania się do niego naszych zmysłów”³²². P. Sienkiewicz natomiast w swoich rozważaniach zdefiniował informację jako „zbiór faktów, zdarzeń, cech itp. określonych obiektów (rzeczy, procesów, systemów) zawarty w wiadomości (komunikacie), tak ujęty i podany w takiej postaci (formie), że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działania umysłowe lub fizyczne”³²³. Inny badacz, A. Webster, określił ją jako „wiedzę przekazywaną przez innych ludzi bądź uzyskiwaną przez studia, obserwację, badania”³²⁴. Natomiast w terminologii wojskowej omawiany termin jest definiowany jako wszelkiego rodzaju wiedza, która będąc pozyskiwana poprzez dokonanie „interpretacji danych w ustalonym kontekście ma określone znaczenie i dotyczy obiektów, takich jak fakty, zdarzenia, przedmioty, zjawiska, procesy i idee; także nieprzetworzone dane każdego rodzaju, które mogą być wykorzystane do opracowań wywiadowczych (rozpoznawczych)”³²⁵. Z kolei w „Słowniku terminów i definicji NATO” została określona stosunkowo w sposób ogólny jako „nieprzetworzone dane każdego rodzaju, które mogą być wykorzystane do opracowań wywiadowczych/rozpoznawczych”³²⁶.

Analizując powyższe definicje można zauważyć, że traktują one informację nie tylko jako zasób, ale również jako środek, który może być zastosowany do działań o charakterze ofensywnym. Takie postrzeganie informacji jest szczególnie widoczne na gruncie rosyjskiej literatury specjalistycznej. W takim bowiem kontekście wypowiedzieli się między innymi emerytowani rosyjscy wojskowi I. Vorobyov oraz V. Kiselyov, którzy wskazują wręcz, że

³²⁰ L. Ciborowski: *Walka informacyjna*. Toruń 1999, s. 50.

³²¹ Encyklopedia PWN: *informacja*. <https://encyklopedia.pwn.pl/haslo/informacja;3914687.html> (dostęp: 01.09.2021).

³²² N. Wiener: *Cybernetyka i społeczeństwo*. Warszawa 1961, s. 16.

³²³ P. Sienkiewicz: *Ewaluacja informacji w społeczeństwie informacyjnym*. „Ekonomiczne Problemy Usług” 2011, nr 67, s. 127; Zobacz szerzej: P. Sienkiewicz: *Inżynieria systemów*. Warszawa, 1983.

³²⁴ K. Liedel, P. Piasecka, T. R. Aleksandrowicz: *Analiza informacji. Teoria i praktyka*. Warszawa 2012, s. 34.

³²⁵ J. Kaczmarek, W. Łepkowski, B. Zdrodowski (Red.): *Słownik terminów z zakresu bezpieczeństwa narodowego*. Warszawa 2008, s. 51.

³²⁶ Biuro Standaryzacji NATO: *Słownik terminów i definicji NATO AAP-6 (2017)*. 2017, s. 244.

informacja jest rodzajem broni. Podobnie jej charakter nakreślił politolog I. Panarin, który pisze o światowej konfrontacji informacyjnej, obejmującej takie elementy jak: strategiczną analizę polityczną (uzyskanie informacji o przeciwniku oraz warunkach wojny informacyjnej), wpływ informacji (np. blokowanie dostępu do informacji, przetwarzanie informacji, działania dezinformacyjne), opór informacyjny (np. przeciwdziałanie dezinformacji, kształtowanie opinii publicznej)³²⁷.

Dokonując rozważań w zakresie pojęcia informacji, należy również wskazać na kilka jego cech charakterystycznych, które wyróżnił K. Liderman. Stwierdził, że informacja „jest przede wszystkim towarem, i to często o znaczeniu strategicznym (dla państwa, firmy, ale także konkretnej osoby); (...) jest podstawowym elementem procesów biznesowych; (...) służy do sterowania procesami w zautomatyzowanych procesach wytwórczych i usługowych o kluczowym znaczeniu dla gospodarki i społeczeństwa; (...) bywa chroniona na mocy obowiązującego prawa lub zawartych umów”³²⁸. Dalej pisał, że aby informacja spełniała wskazane wyżej pierwsze trzy funkcje, musi być dobrej jakości, a więc musi cechować się takimi kryteriami jak: relewantność, dokładność, aktualność, kompletność, spójność, odpowiedniość formy oraz wirylność³²⁹. Oczywiście podkreślić należy, że waga poszczególnych kryteriów postrzegania informacji będzie różna w zależności od sposobu jej wykorzystania, a więc od dziedziny w której występuje, na przykład w polityce, prawie, ekonomii, czy siłach zbrojnych.

Interpretując powyższe rozważania terminologiczne można zauważyć, że pojęcie informacji jest definiowane przy uwzględnieniu jej konkretnych oraz wybranych właściwości, które odnoszą się z kolei do poszczególnych dziedzin nauki. W związku z tym warto przytoczyć trafne spostrzeżenie J. L. Kulikowskiego, który stwierdził, że „pojęcie informacji już dawno wykroczyło poza ścisłe, lecz wąskie definicje – stało się po prostu kategorią filozoficzną niemal tak ogólną, jak pojęcie materii lub ruchu. Specjalista w każdej dziedzinie dostrzega na ogół w tym pojęciu tylko niektóre aspekty, stąd też niekończące się spory terminologiczne i odmiennosc interpretacji tego, co pozornie wydaje się powszechne i oczywiste”³³⁰. Tym samym można zauważyć, że J. L. Kulikowski przypisuje pojęciu informacji charakter pierwotny i jako taki wyklucza jednocześnie możliwość jego jednoznacznego zdefiniowania, bez względu na płaszczyznę na jakiej występuje.

³²⁷ M. Wrzosek, Sz. Markiewicz, Z. Modrzejewski (Red.): *Informacyjny wymiar...*, s. 90-91.

³²⁸ K. Liderman: *Bezpieczeństwo informacyjne*. Warszawa 2012, s. 18.

³²⁹ Ibidem, s. 18.

³³⁰ J. L. Kulikowski: *Informacja i świat w którym żyjemy*. Warszawa 1978, s. 11.

2.2. Wojna informacyjna w polityce zagranicznej

Informacja, nieprzerwanie od początków istnienia ludzkości, w mniejszym bądź większym zakresie była traktowana jako zasób, z kolei wraz z początkiem rewolucji informacyjnej przypisano jej walor zasobu o znaczeniu strategicznym. Postęp technologiczny spowodował zasadnicze zmiany w procesach gospodarczych i społecznych państw, ich polityce (wewnętrznej i zewnętrznej) oraz strategiach, jak również w zakresie prowadzonych konfliktów zbrojnych³³¹. Wykorzystanie informacji nigdy nie było tak kompleksowe, z kolei postrzeganie jej jako zasobu determinowało szerokie zastosowanie do działań taktycznych, operacyjnych i strategicznych. Wykorzystana jako broń, cechuje się niskim kosztem wytworzenia, uniwersalnym charakterem, łatwą dostępnością oraz nieograniczonym zasięgiem. Przede wszystkim nie uznaje ona granic państwowych, a jej kontrola w dzisiejszym społeczeństwie informacyjnym jest w znacznym stopniu utrudniona, aby nie powiedzieć, że niemożliwa³³². Co ważne, informacja musi być postrzegana również jako zasób o charakterze krytycznym dla funkcjonowania państwa, co z kolei wymusza konieczność zapewnienia jej dostatecznej ochrony na każdym etapie przetwarzania³³³. Tym samym informacja stała się również zasobem służącym do prowadzenia wojen, określanym mianem informacyjnych, które to z kolei stanowią jeden ze środków (instrumentów) prowadzenia przez państwa ich polityki zagranicznej. Wojna informacyjna od wielu lat jest prowadzona przez światowe mocarstwa takie jak USA³³⁴, Federacja Rosyjska³³⁵ oraz Chiny³³⁶, czy przez organizacje terrorystyczne, na

³³¹ M. Madej: *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państwa i systemu międzynarodowego*. W: *Bezpieczeństwo Teleinformatyczne Państwa*. Red. M. Madej, M. Terlikowski. Warszawa 2009, s. 17-18.

³³² Zobacz szerzej: J. Darczeńska: *Anatomia rosyjskiej wojny informacyjnej Operacja Krymska – studium przypadku*. „Punkt widzenia” 2014, nr 42. https://www.osw.waw.pl/sites/default/files/anatomia_rosyjskiej_wojny_informacyjnej.pdf (dostęp: 07.12.2024); J. Darczeńska: *Wojna informacyjna Rosji z Zachodem. Nowe wyzwanie?* „Przegląd Bezpieczeństwa Wewnętrznego” 2015, Wydanie Specjalne.

³³³ T. R. Aleksandrowicz: *Bezpieczeństwo informacyjne państwa*. „Studia Politologiczne” 2018, nr 49, s. 34.

³³⁴ B. Nakayama: *American Influence on Russian Information Warfare*. „E-International Relations” 2020. <https://www.e-ir.info/2020/09/24/american-influence-on-russian-information-warfare/> (dostęp: 07.12.2024). CyberDefence24.pl: *Amerykanie "idą" na wojnę informacyjną*. <https://www.cyberdefence24.pl/amerykanie-ida-na-wojne-informacyjna> (dostęp: 07.12.2024).

³³⁵ Zobacz szerzej: K. Wóycicki, M. Kowalska, A. Lelonek: *Raport Rosyjska wojna dezinformacyjna przeciwko Polsce*. Warszawa 2017. <https://pulaski.pl/wp-content/uploads/2023/06/RAPORT-Rosyjska-wojna-dezinformacyjna-przeciwko-Polsce.pdf> (dostęp: 07.12.2024); J. Darczeńska: *Anatomia rosyjskiej wojny informacyjnej Operacja Krymska – studium przypadku*. „Punkt widzenia” 2014, nr 42. https://www.osw.waw.pl/sites/default/files/anatomia_rosyjskiej_wojny_informacyjnej.pdf (dostęp: 07.12.2024).

³³⁶ T. Wójtowicz: *Od doktryny wojny ludowej do doktryny wojny informacyjnej. Rola nowych technologii w transformacji Chińskiej Armii Ludowo-Wyzwoleńczej*. „Kultura i Polityka” 2014, nr 16, s. 127-141; CyberDefence24.pl: *Chiny zwycięzcą wojny informacyjnej z USA?* <https://www.cyberdefence24.pl/chiny-zwyciezca-wojny-informacyjnej-z-usa> (dostęp: 07.12.2024).

przykład Państwo Islamskie (ISIS)³³⁷. Powyższe rozważania można skonkludować stwierdzeniem, że „wojna informacyjna, wrogie działania w cyberprzestrzeni, manipulacja informacją oraz dezinformacja jednostek i grup społecznych stają się narzędziami wpływu, ingerencji, a nawet agresji, stosowanymi zarówno przez państwa (np. Federacja Rosyjska, Chińska Republika Ludowa, Koreańska Republika Ludowo-Demokratyczna), jak i – znacznie częściej – podmioty pozapaństwowe: i te dobrze zorganizowane, jak np. Państwo Islamskie albo Anonimowi (Anonymous), i te działające indywidualnie (hakerzy)”³³⁸.

2.2.1. Definicja pojęcia wojny informacyjnej

Sun Tzu napisał, że „osiągnąć sto zwycięstw w stu bitwach nie jest szczytem osiągnięć. Największym osiągnięciem jest pokonanie wroga bez walki. (...) Dlatego najwyższą sztuką jest zwyciężyć armię wroga bez wydania bitwy. Zająć miasto wroga bez oblegania i zająć tereny jego państwa bez inwazji”³³⁹. Analiza przytoczonej wyżej wypowiedzi słynnego starożytnego chińskiego myśliciela w kontekście omawianego problemu badawczego skłania do stwierdzenia, że to właśnie w taki sposób prowadzone są wojny informacyjne, bez bitew i bez walk, jakie znamy z konfliktów o charakterze konwencjonalnym. Taka wojna może mieć miejsce w przestrzeni informacyjnej w ramach której oddziałuje na zachodzące w niej procesy. Jak zauważają P. Sienkiewicz oraz H. Świeboda, „procesy informacyjne są obiektem zewnętrznych zagrożeń, zarówno losowych (niemożliwych bądź trudnych do przewidzenia), jak i deterministycznych (dzielących się na kumulacyjne oraz świadome)”³⁴⁰. Wojnę informacyjną można z pewnością zaliczyć do ostatniej ze wskazanych kategorii, mianowicie zagrożeń świadomych, będących efektem zaplanowanego działania ze strony danego podmiotu lub podmiotów, których celem jest wywołanie określonych skutków – negatywnych z punktu widzenia bezpieczeństwa informacyjnego. Samo pojęcie wojny informacyjnej, podobnie jak pojęcie informacji, nie zostało dotychczas zdefiniowane w literaturze specjalistycznej w sposób jednoznaczny, toteż konieczne jest jego omówienie oraz przytoczenie wybranych definicji, formułowanych zarówno przez badaczy zachodnich, jak i rosyjskich.

³³⁷ M. Lakomy: *Recruitment and Incitement to Violence in the Islamic State's Online Propaganda: Comparative Analysis of Dabiq and Rumiyah*. „Studies in Conflict & Terrorism” 2019, nr 44(7), s. 565-580.

³³⁸ P. Bajor, A. Gruszcak: *Między wiedzą a władzą – o związkach między informacją, wiedzą i bezpieczeństwem*. W: *Między wiedzą a władzą. Bezpieczeństwo w erze informacji*. Red. P. Bajor, A. Gruszcak. Kraków 2019, s. 10.

³³⁹ Sun Tzu: *Sztuka wojny*. Warszawa 1994, s. 35-37.

³⁴⁰ P. Sienkiewicz, H. Świeboda: *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej*. W: *Bezpieczeństwo Teleinformatyczne Państwa*. Red. M. Madej, M. Terlikowski. Warszawa 2009, s. 79-80.

Znaczące problemy związane z definiowaniem pojęcia wojny informacyjnej miały miejsce na przełomie lat osiemdziesiątych i dziewięćdziesiątych XX wieku, co było związane z pojawieniem się nowych technologii (rewolucji informacyjnej), a w konsekwencji wymuszało redefiniowanie omawianego terminu³⁴¹. W tym kontekście jedną z bardziej powszechnych definicji wojny informacyjnej sformułowała D. E. Denning pisząc, że są to „działania, których celem jest zdobycie lub wykorzystanie zasobów informacyjnych”³⁴². Definicja wydaje się stosunkowo uniwersalna, jednak jej dalsza część obejmuje również, jak pisze autorka, podział *zasobów*, który z kolei należy odnieść do wykorzystywania informacji (w zależności od pełnionej funkcji). W związku z tym D. E. Denning wyróżniła pięć klas zasobów takich jak: pojemniki, transportery, czujniki, rejestratory i procesory³⁴³. Pojemniki – zwane również kontenerami – pełnią zadania magazynu przechowując poszczególne informacje o określonej strukturze. Przykładem pojemnika może być: pamięć ludzka, dyskietka, drukowane środki przekazu, czy współcześnie dysk twardy, pamięć przenośna, płyta CD/DVD, czy chmura obliczeniowa. Transportery służą do przekazywania (przenoszenia) informacji, co dokonywane jest przy użyciu fizycznych środków transportu (np. samochód czy samolot), systemów komunikacyjnych lub sieci Internet. Czujniki są natomiast urządzeniami wychytującymi dane z innych przedmiotów (np. zmysły ludzkie, aparat fotograficzny czy telefon – smartfon). Następną klasą wyróżnioną przez D. E. Denning są rejestratory, które umieszczają daną informację w pojemniku (kontenerze), a ostatnią procesory, czyli obiekty które nią manipulują (np.: ludzie, urządzenia komputerowe i oprogramowanie)³⁴⁴. Inną definicję wojny informacyjnej zaproponował M. C. Libicki, który uznał, że jest to „ciąg działań wywołanych potrzebą modyfikacji przepływu informacji, kierowanych do drugiej strony, przy jednoczesnej ochronie własnych; takie działania obejmują atak fizyczny, atak radioelektroniczny, ataki na systemy i czujniki, kryptografię, ataki na komputery i operacje psychologiczne”³⁴⁵. Wskazał również na złożoność zagadnienia wojny informacyjnej stwierdzając, że nie istnieje ona jako odrębna technika prowadzenia wojny, gdyż w rzeczywistości składa się na nią łącznie siedem różnych. Zaliczył do nich wojnę dowodzenia i kontroli, wojnę wywiadowczą, wojnę elektroniczną, wojnę psychologiczną, wojnę hakerską, ekonomiczną wojnę informacyjną oraz cyberwojnę³⁴⁶. W swoich rozważaniach, podejmując próbę stworzenia, jak sam określił, dobrej

³⁴¹ D. Ventre: *Information Warfare. 2nd Edition revised and Updated*. London – New York 2016, s. X.

³⁴² D. E. Denning: *Wojna Informacyjna i bezpieczeństwo informacji*. Warszawa 2002, s. 23.

³⁴³ Należy przy tym podkreślić, że poszczególne zasoby mogą pełnić jednocześnie wiele funkcji.

³⁴⁴ D. E. Denning: *Wojna Informacyjna...*, s. 23-24.

³⁴⁵ D. Ventre: *Information Warfare...*, s. 4.

³⁴⁶ M. C. Libicki: *What is information warfare?* Washington D.C. 1995, s. X.

definicji wojny informacyjnej, przytoczył tę zaproponowaną przez T. Ronana, który wskazał, że jest to „rywalizacja na poziomie strategicznym, operacyjnym i taktycznym w całym spektrum pokoju, kryzysu, eskalacji kryzysu, konfliktu, wojny, zakończenia wojny i rekonstrukcji/odbudowy, prowadzona między konkurentami, przeciwnikami lub wrogami przy użyciu środków informacyjnych do osiągnięcia swoich celów”³⁴⁷. I choć M. C. Libicki uznał, że jest ona zbyt szeroka³⁴⁸, bo obejmuje większość ludzkich zachowań, to jednocześnie należy zauważyć, że posiada wiele elementów wspólnych z występującymi współcześnie koncepcjami rosyjskimi w zakresie omawianego terminu³⁴⁹. A. Borden z kolei określa wojnę informacyjną jako „wszelkie działania mające na celu negowanie, wykorzystywanie, uszkodzanie lub niszczenie informacji przeciwnika i jej funkcji; ochronę przed tymi działaniami oraz wykorzystywanie własnych wojskowych funkcji informacyjnych”³⁵⁰. Dla V. Volkoffa jest to natomiast „ofensywne i defensywne używanie informacji i systemów informacyjnych, by wykorzystywać, psuć i niszczyć informacje i systemy informacyjne przeciwnika, chroniąc zarazem własne informacje i własne systemy”³⁵¹. Mogą być też to „działania podejmowane dla osiągnięcia przewagi informacyjnej poprzez wpływanie na informacje przeciwnika, procesy oparte na przetwarzaniu informacji, systemy informacyjne oraz sieci komputerowe przy jednoczesnej ochronie własnych informacji, procesów opartych na przetwarzaniu informacji, systemów informacyjnych oraz sieci komputerowych”³⁵². Natomiast W. Schwartau wskazał na trzy poziomy na jakich może występować wojna informacyjna, zaliczając do nich: osobisty, korporacyjny oraz globalny³⁵³. A. Lelonek zaproponował jego uzupełnienie o dodatkowe dwie płaszczyzny – militarną i cywilną. W jego ocenie celem wojny informacyjnej jest przecież dokonywanie ataków, których rezultaty niekoniecznie będą od razu widoczne, przy czym „chodzi tu zarówno o ataki cybernetyczne, ale i szeroki aspekt narzędzi oddziaływania psychologicznego”³⁵⁴. Powyższe definicje niewątpliwie, co do zasady, ujmują wojnę

³⁴⁷ Ibidem, s. 4. Tłumaczenie własne. Tekst w oryginale: „The strategic, operation, and tactical level competitions across the spectrum of peace, crisis, crisis escalation, conflict, war, war termination, and reconstitution/restoration, waged between competitors, adversaries or enemies using information means to achieve their objectives”.

³⁴⁸ Ibidem, s. 4.

³⁴⁹ Koncepcje rosyjskie zostaną omówione w dalszej części pracy.

³⁵⁰ A. Borden: *What is Information Warfare?* <https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/borden.pdf> (dostęp: 01.10.2022). Tłumaczenie własne. Tekst w oryginale: „any action to Deny, Exploit, Corrupt or Destroy the enemy’s information and its functions; protecting ourselves against those actions and exploiting our own military information functions”.

³⁵¹ V. Volkoff: *Krótką historia dezinformacji. Od konia trojańskiego do Internetu*. Bielany Wrocławskie – Kobierzyce 2022, s. 235-236.

³⁵² A. Lelonek: *Wojna informacyjna, operacje informacyjne i psychologiczne: pojęcia, metody i zastosowanie*. W: *Potencjał słowa. Międzynarodowe stosunki i komunikacja: stan i perspektywy*. Red. A. Lelonek. Warszawa – Lwów 2016, s. 69.

³⁵³ Ibidem, s. 70.

³⁵⁴ Ibidem, s. 70.

informacyjną w sferze działalności człowieka o charakterze militarnym. Należy jednak zauważyć, że w tym kontekście wypowiedzieli się w latach dziewięćdziesiątych XX wieku B. Cronin i H. Crawford, którzy zauważyli, że wojna informacyjna jest zbyt ważna, aby tę domenę działalności człowieka pozostawić wyłącznie wojsku³⁵⁵.

Ponadto wskazać należy, że pojęcie wojny informacyjnej bywa bardzo często utożsamiane z pojęciem walki informacyjnej, niejednokrotnie traktowane zamiennie bądź uzupełniająco. P. Sienkiewicz i H. Świeboda wskazali za R. Szpyrą, że „wojna informacyjna jest kategorią obejmującą wszystkie formy walki: zbrojną, informacyjną ekonomiczną itd. Współcześnie słusznie uważa się, że *cyberwar*, *infowar*, walka informacyjna, cyberterroryzm, *netwar*, informacyjni wojownicy, informacyjna dominacja, obrona w cyberprzestrzeni (*cyberspace defense*) czy informacyjny chaos to tylko neologizmy, dotyczące tego samego, ale bardzo szerokiego pojęcia wojny ery informacyjnej (*information age warfare*)”³⁵⁶.

P. Sienkiewicz zdefiniował wobec tego pojęcie walki informacyjnej jako „całokształt działań ofensywnych i defensywnych koniecznych do uzyskania przewagi informacyjnej nad przeciwnikiem i osiągnięcia zamierzonych celów militarnych (politycznych)”³⁵⁷. Inna z definicji zakłada, że jest to forma „konfliktu w którym bezpośrednie atakowanie systemów informacyjnych jest środkiem atakowania wiedzy i przekonań przeciwnika. Walka informacyjna może być prowadzona jako element działań wojennych – w postaci wojny sieciowej (*netwar*) lub cyberwojny (*cyberwar*) – lub może przybrać formę walki samodzielnej”³⁵⁸. W znaczeniu wojskowym jest to z kolei „zorganizowana w formie przemocy militarna aktywność zewnętrzna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływającej przez nie informacji oraz aktywność zapewniająca ochronę własnych systemów informacyjnego komunikowania i przesyłania (...) przed podobnym działaniem przeciwnika”³⁵⁹. A. Żebrowski, w ślad za P. Gawliczkiem i J. Pawłowskim pisał, że „walka informacyjna to działania informacyjne prowadzone w okresie kryzysu lub konfliktu zbrojnego z zamiarem promowania określonego celu

³⁵⁵ B. Cronin, H. Crawford: *Information Warfare: Its Application in Military and Civilian Contexts*. „The Information Society” 1999, Vol. 15:4, s. 257.

³⁵⁶ P. Sienkiewicz, H. Świeboda: *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej*. W: *Bezpieczeństwo Teleinformatyczne Państwa*. Red. M. Madej, M. Terlikowski. Warszawa 2009, s. 80-81.

³⁵⁷ K. Liedel, P. Piasecka, T. R. Aleksandrowicz: *Analiza informacji...*, s. 20.

³⁵⁸ P. Sienkiewicz, H. Świeboda: *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej*. W: *Bezpieczeństwo Teleinformatyczne Państwa*. Red. M. Madej, M. Terlikowski. Warszawa 2009, s. 81. Zobacz szerzej: R. Szafranski: *Cyberwar: A Theory of Information Warfare: Preparing for 2020*. W: *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Red. A. D. Campen, D. H. Deart, R. T. Coodden. Fairfax 1996.

³⁵⁹ J. Kaczmarek, W. Łepkowski, B. Zdrodowski (Red.): *Słownik terminów...*, s. 157.

politycznego lub wojskowego w odniesieniu do wskazanego przeciwnika lub przeciwników”³⁶⁰. Mogą być to również „działania informacyjne, prowadzone dla obrony własnej informacji i systemów informacyjnych lub dla atakowania i wywarcia wpływu na informację lub systemy informacyjne przeciwnika”³⁶¹. Kolejna definicja, postrzegająca informację jako zasób, definiuje walkę informacyjną jako użycie „informacji dla osiągnięcia własnych narodowych celów. Podobnie jak dyplomacja, ekonomiczna rywalizacja czy użycie sił zbrojnych, informacja jest kluczowym czynnikiem narodowej potęgi. Ponadto, co jeszcze ważniejsze, informacja staje się głównym narodowym zasobem, który wspiera dyplomację, ekonomiczną rywalizację oraz przemoc militarną. Walka informacyjna w tym sensie może być postrzegana jako konflikt między państwami lub narodami, prowadzony częściowo przez globalną infrastrukturę informacyjną i komunikacyjną”³⁶². Natomiast „Słownik terminów i definicji NATO” wyróżnia jedynie pojęcie *działań informacyjnych*, przez które należy rozumieć kształtowanie informacji lub systemów informacyjnych³⁶³, jednakże zauważono, że środowisko informacyjne może być również przestrzenią walki³⁶⁴.

Powracając do pojęcia wojny informacyjnej, należy zauważyć, że zdecydowanie odmienne koncepcje w tym zakresie można znaleźć w literaturze rosyjskiej. Termin ten jest tam definiowany jako oddziaływanie na masową świadomość opinii publicznej w ramach występującej rywalizacji państw na arenie międzynarodowej poprzez uzyskanie kontroli nad zasobami informacji i wykorzystanie ich w charakterze broni³⁶⁵. Definicja wojny informacyjnej wypracowana przez badaczy rosyjskich może być więc postrzegana jako przeciwstawna do tych formułowanych przez badaczy zachodnich, przede wszystkim w kontekście celu jaki realizuje oraz sfer aktywności człowieka w których występuje. Odwołuje się bowiem do rywalizacji systemów cywilizacyjnych, czym nawiązuje do okresu zimnej wojny. W literaturze rosyjskiej podkreśla się również, że rosyjska wojna informacyjna jest wojną będącą odpowiedzią na działania podejmowane przez państwa zachodnie, które zagrażają żywotnym interesom Federacji Rosyjskiej³⁶⁶. Ponadto, koncepcje wojny informacyjnej w literaturze

³⁶⁰ A. Żebrowski: *Determinanty walki informacyjnej*. W: *Walka informacyjna: uwarunkowania, incydenty, wyzwania*. Red. H. Batorowska. Kraków 2017, s. 93.

³⁶¹ P. Sienkiewicz, H. Świeboda: *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej*. W: *Bezpieczeństwo Teleinformatyczne Państwa*. Red. M. Madej, M. Terlikowski. Warszawa 2009, s. 81.

³⁶² Ibidem, s. 81.

³⁶³ Biuro Standaryzacji NATO: *Słownik terminów...*, s. 244.

³⁶⁴ Ibidem, s. 77.

³⁶⁵ Zobacz szerzej: I. Panarin: *СМИ, пропаганда и информационные войны*. Москва 2012.

³⁶⁶ Zobacz szerzej: J. Darczewska: *Anatomia rosyjskiej wojny informacyjnej Operacja Krymska – studium przypadku*. „Punkt widzenia” 2014, nr 42 https://www.osw.waw.pl/sites/default/files/anatomia_rosyjskiej_wojny_informacyjnej.pdf (dostęp: 07.12.2024); J. Darczewska: *Wojna informacyjna Rosji z Zachodem. Nowe wyzwanie?* „Przegląd Bezpieczeństwa Wewnętrznego” 2015, Wydanie Specjalne.

rosyjskiej jak i oficjalnych dokumentach rządowych nie ograniczają się wyłącznie do działań prowadzonych w trakcie wojny, jak ma to miejsce w przypadku definicji badaczy zachodnich. Wręcz przeciwnie, Rosjanie postrzegają prowadzenie działań z zakresu oddziaływania informacyjnego przede wszystkim poza otwartym konfliktem zbrojnym, a bardzo często poniżej granicy otwartego konfliktu zbrojnego³⁶⁷. Następuje zatem tutaj swego rodzaju przemieszanie porządku militarnego z porządkiem pozamilitarnym³⁶⁸, w ramach którego wojna informacyjna w ujęciu rosyjskim będzie realizować takie same cele jak prowadzenie wojny konwencjonalnej, z tym że na innej płaszczyźnie³⁶⁹.

W odniesieniu do wspomnianych płaszczyzn, tutaj również należy wskazać na odmienności występujące w definicjach omawianego terminu. Badacze zachodni ograniczają się bowiem do postrzegania wojny informacyjnej przede wszystkim w sferze militarnej (np. poprzez dostarczanie błędnych informacji dowódcom przeciwnika czy paraliżowanie jego wojskowych systemów teleinformatycznych), natomiast Rosjanie podejmują działania w powyższych sferach, a jednocześnie rozszerzają je o sferę polityki, wywiadu, dyplomacji, propagandy, psychologii, edukacji, kultury czy religii³⁷⁰. J. Darczewska sprowadziła cele rosyjskiej wojny informacyjnej do podporządkowania „elit i społeczeństw innych państw w sposób niezauważalny, przy wykorzystaniu różnych tajnych i jawnych kanałów (służb specjalnych, dyplomatycznych, medialnych), oddziaływania psychologicznego, dywersji ideologicznej i politycznej”³⁷¹. Nawiązując z kolei do przytoczonych wyżej definicji walki informacyjnej, należy zauważyć, że pojęcie to występuje również w terminologii rosyjskiej, będąc definiowane jako „kompleks przedsięwzięć obejmujących wsparcie, przeciwdziałanie i obronę informacyjną, prowadzonych według jednolitej koncepcji i planu, w celu wywalczenia i utrzymania panowania nad przeciwnikiem w dziedzinie informacyjnej podczas przygotowania operacji wojskowych oraz prowadzonych działań bojowych”³⁷². Można zatem zauważyć, że również w rosyjskim ujęciu walki informacyjnej wskazuje się na podejmowanie działań zarówno poza otwartym konfliktem zbrojnym, jak i w jego trakcie.

³⁶⁷ K. Giles, A. Seaboyer: *The Russian Information Warfare Construct*. Technical Report, Report number: DRDC-RDDC-2019-C241Affiliation: Defence Research and Development. Ontario 2019, s. 5.

³⁶⁸ J. Darczewska: *Anatomia rosyjskiej wojny...*, s. 12.

³⁶⁹ Z. Modrzejewski: *Dezinformacja w służbie walki informacyjnej*. W: *Bezpieczeństwo informacyjne w dobie postprawdy*. Red. T. W. Grabowski, M. Lakomy, K. Oświecimski. Kraków 2018, s. 106.

³⁷⁰ K. Giles: *The Next Phase of Russian Information Warfare*. NATO Strategic Communications Centre of Excellence. Riga 2016, s. 2; M. Banasik: *Teoria i praktyka wojny informacyjnej stosowanej przez Federację Rosyjską*. W: *Informacja czynnikiem warunkującym bezpieczeństwo. Kontekst rosyjski*. Red. M. Banasik. Warszawa 2021, s. 56; J. Darczewska: *Anatomia rosyjskiej wojny...*, s. 10.

³⁷¹ J. Darczewska: *Anatomia rosyjskiej wojny...*, s. 5.

³⁷² A. Żebrowski: *Bezpieczeństwo informacyjne Polski a walka informacyjna*. „Roczniki Kolegium Analiz Ekonomicznych” 2013, nr 29/2013, s. 454.

Wreszcie podnieść należy, że wojna informacyjna nie może być traktowana wyłącznie jako samoistne zjawisko. Jak trafnie zaważył L. Ciborowski, „nigdy nie może występować w oderwaniu, bo nigdy też sama dla siebie nie może stanowić celu. Jej cel wynika zawsze z charakteru i celu walki wspieranej”³⁷³. Z kolei odnosząc się do koncepcji rosyjskich, K. Giles oraz A. Seaboyer za V. Kvachkovem³⁷⁴ wskazali, że wojna informacyjna składa się w rzeczywistości z dwóch rodzajów, przy czym każdy z nich realizuje inne cele. I tak pierwszy z nich to „wojna informacyjno-psychologiczna (mająca na celu oddziaływanie na personel sił zbrojnych i ludność), która prowadzona jest w warunkach naturalnej konkurencji, czyli stale”³⁷⁵ oraz drugi, czyli „wojna informacyjno-technologiczna (mająca na celu oddziaływanie na systemy techniczne odbierające, gromadzące, przetwarzające i przekazujące informacje), która prowadzona jest w czasie wojen i konfliktów zbrojnych”³⁷⁶.

Choć rosyjskie koncepcje omawianego terminu zostaną omówione szerzej w kolejnych rozdziałach pracy, to już w tym momencie można stwierdzić, że wojna informacyjna w tym ujęciu wychodzi znacznie szerzej poza zakres działań o charakterze militarnym. Po pierwsze, wojna informacyjna polega na wykorzystywaniu informacji przede wszystkim poza polem walki oraz przez podmioty polityczne, gospodarcze, służby specjalne czy porządkowe (np. policję) – przy czym katalog tych podmiotów nie jest enumeratywny. Po drugie, wojna informacyjna może być prowadzona w okresie pokoju pomiędzy danymi państwami (wobec braku formalnego wypowiedzenia wojny) oraz pomimo, iż ma charakter walki niezbrojnej, to może prowadzić do fizycznej destrukcji w sposób pośredni lub bezpośredni³⁷⁷.

Wreszcie wskazać należy, że mając na względzie całokształt powyższych rozważań, zastosowanie na gruncie niniejszej rozprawy pojęcia wojny informacyjnej, nie natomiast walki informacyjnej, wydaje się być całkowicie uzasadnione. Wojna informacyjna jest bowiem terminem zdecydowanie szerszym, obejmującym wiele form oddziaływania informacyjnego. Ponadto stanowi pojęcie przyjęte i ugruntowane w literaturze specjalistycznej, a co najistotniejsze – takim terminem posługują się Rosjanie, nie tylko w publikacjach dotyczących wojny informacyjnej, ale w ogóle w działalności z tym związanej. Trzeba również podkreślić,

³⁷³ L. Ciborowski: *Mechanizmy i przestrzenie walki informacyjnej*. W: *Informacja w walce zbrojnej*. Red. G. Nowacki, Warszawa 2002, s. 45.

³⁷⁴ Zobacz szerzej: V. Kvachkov: *Специализация России*. http://militera.lib.ru/science/kvachkov_vv/index.html (dostęp 02.10.2022).

³⁷⁵ K. Giles, A. Seaboyer: *The Russian Information Warfare...*, s. 9.

³⁷⁶ Ibidem, s. 9.

³⁷⁷ Zobacz szerzej: K. Giles: *The Next Phase of Russian Information Warfare*. NATO Strategic Communications Centre of Excellence. Riga 2016; K. Giles: *Handbook of Russian Information Warfare. Fellowship Monograph Research Division NATO Defense College*. 2016, Vol. 9; J. Darczewska: *Anatomia rosyjskiej wojny informacyjnej Operacja Krymska – studium przypadku*. „Punkt widzenia” 2014, nr 42. https://www.osw.waw.pl/sites/default/files/anatomia_rosyjskiej_wojny_informacyjnej.pdf (dostęp: 07.12.2024).

że omawianego terminu nie należy interpretować jako tożsamego z pojęciem klasycznej wojny w stosunkach międzynarodowych. Nie ma tutaj bowiem elementu kinetyczności oraz określonego, konkretnego charakteru, z którym mamy do czynienia w przypadku zorganizowanych konfliktów zbrojnych pomiędzy państwami, narodami czy też innymi podmiotami. Niemniej jednak powyższe stwierdzenia nie mogą prowadzić do wniosku, że wojna informacyjna nie jest również instrumentem polityki zagranicznej państw. Biorąc pod uwagę problem badawczy prezentowany w pracy, przyjęcie terminu walki zamiast wojny nie oddałoby właściwego oraz całościowego znaczenia omawianych zagadnień. Ma to szczególne znaczenie wobec faktu, że przedmiotem rozprawy są nie tylko działania polegające na oddziaływaniu informacyjnym na odbiorcę, ale również na dokonywaniu ataków w cyberprzestrzeni³⁷⁸.

Z uwagi na definicję i zakres, wojnę informacyjną może określić szerokie i kompleksowe pojęcie, które obejmuje wszystkie aspekty działań mających na celu wykorzystanie informacji jako narzędzia konfliktu na dużą skalę. Może dotyczyć zarówno konfliktów zbrojnych, jak i rywalizacji politycznej, ekonomicznej czy społecznej. Walka informacyjna to bardziej ograniczone pojęcie, odnoszące się do konkretnych działań w ramach wojny informacyjnej. Obejmuje operacje skierowane na uzyskanie przewagi na określonym polu. Następnie, w przypadku wojny informacyjnej, celem jest długoterminowa destabilizacja przeciwnika, wpływanie na opinię publiczną, kontrola przepływu informacji oraz zmiana zachowań grup społecznych lub całych państw. Może obejmować także niszczenie infrastruktury informacyjnej przeciwnika. Z kolei celem walki informacyjnej jest osiągnięcie lokalnej lub tymczasowej przewagi informacyjnej, np. poprzez zakłócanie przepływu informacji w danej sytuacji, dezinformację lub wywiad w ramach konkretnej operacji. Wojna informacyjna ma więc charakter strategiczny i długoterminowy. Jest prowadzona na szeroką skalę, obejmując różne obszary działalności (wojskowy, polityczny, gospodarczy, społeczny), z kolei walka informacyjna jest ograniczona w czasie i przestrzeni. Może być prowadzona w ramach jednej operacji wojskowej. Wojna informacyjna to na przykład propaganda na poziomie globalnym, cyberataki na kluczowe systemy informacyjne, wykorzystywanie

³⁷⁸ Zobacz szerzej: E. Lucas, P. Pomerantsev: *Winning the Information War. Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe. A Report by CEPA's Information Warfare Project in Partnership with the Legatum Institute*. Washington D.C. 2016; K. Giles, A. Seaboyer: *The Russian Information Warfare Construct*. Technical Report, Report number: DRDC-RDDC-2019-C241Affiliation: Defence Research and Development. Ontario 2019; R. Bebb: *Information War and Rethinking Phase 0*. „Journal of Information Warfare” 2016, Vol. 15 (Issue 2); J. Darczewska: *Anatomia rosyjskiej wojny informacyjnej Operacja Krymska – studium przypadku*. „Punkt widzenia” 2014, nr 42. https://www.osw.waw.pl/sites/default/files/anatomia_rosyjskiej_wojny_informacyjnej.pdf (dostęp: 01.10.2022).

mediów tradycyjnych i społecznościowych do wpływania na społeczeństwa, z kolei walka informacyjna to przykładowo zakłócanie komunikacji wroga na polu bitwy, rozpowszechnianie fałszywych informacji w konkretnych operacjach, czy zbieranie i analizowanie danych przeciwnika w celu uzyskania przewagi w danym obszarze³⁷⁹.

W związku z tym, na potrzeby niniejszej rozprawy przyjęto, że wojna informacyjna to działania podejmowane przez podmioty państwowe i niepaństwowe, polegające na oddziaływaniu na odbiorców (świadomość opinii publicznej) w Internecie z wykorzystaniem metod i technik propagandowych, jak i poprzez prowadzenie działań w cyberprzestrzeni polegających na dokonywaniu cyberataków na infrastrukturę teleinformatyczną innego państwa bądź podmiotu.

2.2.2. Uwarunkowania wojny informacyjnej

Z całą pewnością wojna informacyjna może być jednym z instrumentów prowadzonej przez państwa polityki zagranicznej, toteż podobnie jak ona podlega poszczególnym uwarunkowaniom. W związku z tym na potrzeby niniejszej rozprawy wyszczególniono kilka wybranych (najistotniejszych) z nich jak: bezpieczeństwo informacji (poziom bezpieczeństwa informacyjnego), stopień z informatyzowania państwa (infrastruktura informacyjna) oraz występowanie społeczeństwa informacyjnego, charakter przestrzeni medialnej państwa, charakter cyberprzestrzeni państwa – zdolności w zakresie jej wykorzystania tj. prowadzenia działalności operacyjnej (ofensywnej i defensywnej).

Pierwszym i najistotniejszym z uwarunkowań jest bezpieczeństwo informacji, które należy definiować jako działania podejmowane w celu ochrony danych, informacji i systemów informacyjnych. Jest to również współzależność wielu narzędzi służących ochronie informacji poprzez: antywirusową ochronę urządzeń i ich zasobów; zabezpieczenie techniczne wszelkich postaci danych osobowych, tajemnicy lekarskiej, poufności bankowej, karalności, gwarancji tajemnicy korespondencji sieciowej; ochronę parametrów komputerów zarządzających systemami w przemyśle, bankowości, ochronie zdrowia, energetyce i łączności; procedury reagowania na ataki hakerskie i cyberterrorystyczne; ochronę prawną zasobów i systemów

³⁷⁹ Zobacz szerzej: P. Sienkiewicz, H. Świeboda: *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej*. W: *Bezpieczeństwo Teleinformatyczne Państwa*. Red. M. Madej, M. Terlikowski. Warszawa 2009; K. Liedel, P. Piasecka, T. R. Aleksandrowicz: *Analiza informacji. Teoria i praktyka*. Warszawa 2012; R. Szafranski: *Cyberwar: A Theory of Information Warfare: Preparing for 2020*. W: *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Red. A. D. Campen, D. H. Deart, R. T. Coodden, Fairfax 1996; A. Żebrowski: *Determinanty walki informacyjnej*. W: *Walka informacyjna: uwarunkowania, incydenty, wyzwania*. Red. H. Batorowska. Kraków 2017.

informacyjnych³⁸⁰. Od pojęcia bezpieczeństwa informacji można odróżnić pojęcie bezpieczeństwa teleinformatycznego, którym są działania podejmowane przez określone podmioty w celu ochrony sieci informatycznych o znaczeniu strategicznym, poprzez tworzenie i stosowanie procedur zarządzania i obrony systemów teleinformatycznych³⁸¹.

Informacja w stosunkach międzynarodowych będąc zasobem o znaczeniu strategicznym dla ich uczestników, jest również zasobem krytycznym dla funkcjonowania każdego państwa. W związku z tym musi być ona w dostateczny sposób chroniona na każdym etapie jej przetwarzania. Informacja posiada określoną wartość, a jej kreowanie pociąga za sobą określone koszty wytworzenia i wykorzystania. Brak informacji powoduje zmniejszenie skuteczności funkcjonowania państwa, a w kontekście bezpieczeństwa – obniżenie jego walorów obronnych³⁸². Tym samym można wskazać na najważniejsze zagrożenia dla bezpieczeństwa informacyjnego, teleinformatycznego oraz informacji. Ich źródłami może być przede wszystkim: działalność państw, grup przestępczych, organizacji terrorystycznych, hakerów, hakywistów. Do zagrożeń systemów teleinformatycznych można zaliczyć: *hacking*, hakywizm, cyberprzestępczość, cyberterroryzm, cyberszpiegostwo, zbrojne wykorzystanie cyberprzestrzeni³⁸³. K. Liderman przyjął stosunkowo szeroki katalog źródeł zagrożeń dla bezpieczeństwa informacji przyjmując, że są to „katastrofy naturalne; błędy ludzi wykorzystujących lub obsługujących systemy informacyjne; błędy w organizacji pracy i procedurach; celowe, szkodliwe działania ludzi skierowane na systemy informacyjne; awarie sprzętu (elementów i podzespołów mechanicznych, elektronicznych, elektromechanicznych) i wady oprogramowania”³⁸⁴. Katalog ten nie jest oczywiście enumeratywny.

Umiejętności w zakresie przeciwdziałania wskazanym wyżej zagrożeniom zapewnia funkcjonujący w danym państwie system bezpieczeństwa informacyjnego. Zwykle posiada on bardzo rozbudowaną strukturę, łącząc szereg elementów organizacyjnych, technicznych oraz ludzkich. Sprawne funkcjonowanie systemu bezpieczeństwa informacyjnego (w tym przypadku państwa) nie może mieć miejsca bez zapewnienia „odpowiedniego poziomu ochrony informacji i elementów systemu przetwarzających bądź przechowujących informacje; utrzymania pod kontrolą zmian w systemie; spełnienia wymogów różnych przepisów prawnych, które w sposób jawny nakładają obowiązek posiadania przez organizacje (...)

³⁸⁰ J. Kaczmarek, W. Łepkowski, B. Zdrodowski (Red.): *Słownik terminów...*, s. 51.

³⁸¹ Ibidem, s. 21.

³⁸² T. R. Aleksandrowicz: *Bezpieczeństwo informacyjne państwa*. „Studia Politologiczne” 2018, nr 49, s. 33-40.

³⁸³ M. Lakomy: *Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek do typologii*. „Kwartalnik Naukowy OAP UW e-Politikon” 2013, nr 6, s. 102-110.

³⁸⁴ K. Liderman: *Bezpieczeństwo informacyjne...*, s. 33.

dokumentów nazwanych „polityka bezpieczeństwa”, „instrukcje i procedury bezpieczeństwa” lub podobnie”³⁸⁵. Przygotowany w powyższy sposób system bezpieczeństwa informacyjnego powinien być dobrze udokumentowany poprzez przyjęcie i wdrożenie polityki bezpieczeństwa informacyjnego³⁸⁶, planu bezpieczeństwa informacyjnego³⁸⁷, instrukcji bezpieczeństwa teleinformatycznego³⁸⁸ oraz planu zapewnienia ciągłości działania³⁸⁹. Na początku niniejszego podrozdziału wskazano, że bezpieczeństwo informacji jest jednym z najistotniejszych uwarunkowań wojny informacyjnej. Dotyczy ono zarówno podmiotów wykorzystujących środki z zakresu wojny informacyjnej, jak i podmiotów które przed nimi się bronią, przy czym poziom bezpieczeństwa informacyjnego będzie szczególnie istotny dla tych drugich. Jego miarę można określić na podstawie zdolności danego podmiotu do przeciwdziałania zagrożeniom dla bezpieczeństwa informacyjnego (również w zakresie prewencji względem tych zagrożeń), co z kolei będzie przekładać się na możliwości działań defensywnych oraz ofensywnych w zakresie prowadzonej wojny informacyjnej. Posiadanie sprawnego systemu bezpieczeństwa informacyjnego determinuje zdolności państwa w powyższym zakresie, pozwalając na obronę własnej, szeroko rozumianej przestrzeni informacyjnej.

Kolejnym z uwarunkowań wymagającym szerszego omówienia jest stopień z informatyzowania państwa oraz społeczeństwa (stopień rozwoju społeczeństwa informacyjnego), przez co można rozumieć przede wszystkim występującą w danym państwie infrastrukturę informacyjną. Na początku lat dziewięćdziesiątych XX wieku dostęp do sieci internetowej posiadało kilka milionów użytkowników, aby pod koniec wieku osiągnąć liczbę ponad 250 milionów³⁹⁰. Tym samym Internet stał się globalną siecią transmisji danych, do której przykładowo w 2019 roku miało dostęp ponad 4,39 miliarda osób³⁹¹. W samej Polsce, liczącej około 38 milionów mieszkańców³⁹², w 2019 roku dostęp do Internetu posiadały ponad 33 miliony użytkowników³⁹³. Powyższe zmiany spowodowały, że na przełomie XX i XXI wieku rozpoczęło się kształtowanie tzw. społeczeństwa informacyjnego. Jest to społeczeństwo,

³⁸⁵ Ibidem, s. 120.

³⁸⁶ Dokumenty określające najistotniejsze, ogólne ustalenia w zakresie ochrony informacji, ale również zasady ich przetwarzania. Ibidem, s. 121.

³⁸⁷ Dokument zawierający szczegółowy plan budowy systemu bezpieczeństwa informacyjnego. Ibidem, s. 121.

³⁸⁸ Dokument określający reguły zachowania podmiotów w zakresie bezpieczeństwa teleinformatycznego. Ibidem, s. 121.

³⁸⁹ Dokument z instrukcjami i zasadami postępowania na wypadek wystąpienia zdarzeń kryzysowych, tj. zdarzeń tworzących lub mogących tworzyć zagrożenia dla bezpieczeństwa informacyjnego państwa. Ibidem, s. 121.

³⁹⁰ M. Lakomy: *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*. Katowice 2015, s. 45-47.

³⁹¹ *Global Digital Report 2019*: <https://wearesocial.com/global-digital-report-2019> (dostęp: 11.12.2021).

³⁹² Główny Urząd Statystyczny: *Podstawowe dane*. <https://stat.gov.pl/podstawowe-dane/> (dostęp: 9.12.2021).

³⁹³ Główny Urząd Statystyczny: *Spółeczeństwo Informacyjne w Polsce w 2019 roku*. <https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2019-roku,2,9.html> (dostęp: 9.12.2021).

w którym informacja jako wytwór niematerialny jest równie ważna co wytwory materialne, zyskując tym samym znaczną wartość ekonomiczną. Społeczeństwo informacyjne charakteryzuje się umiejętnościami wytwarzania, przetwarzania i zdalnego przesyłania informacji z wykorzystaniem zaawansowanych systemów teleinformatycznych. Występuje w nim również wysoki stopień z informatyzowania życia społecznego. Trudno jest bowiem wyobrazić sobie funkcjonowanie współczesnego świata bez komputerów, urządzeń czy też innych elektronicznych podzespołów wspomagających i ułatwiających nasze codzienne życie³⁹⁴.

J. S. Nowak uznał natomiast, że społeczeństwo informacyjne to „społeczeństwo charakteryzujące się przygotowaniem i zdolnością do użytkowania systemów informatycznych, skomputeryzowane i wykorzystujące usługi telekomunikacji do przesyłania i zdalnego przetwarzania informacji”³⁹⁵. Jest to również „społeczeństwo, które nie tylko posiada rozwinięte środki przetwarzania informacji i komunikowania, lecz środki te są podstawą tworzenia dochodu narodowego i dostarczają źródła utrzymania większości społeczeństwa”³⁹⁶. Nie bez znaczenia jest zatem funkcjonująca w państwie infrastruktura informacyjna, która mając współcześnie charakter globalny (poprzez połączenie infrastruktury krajowej z infrastrukturami innych państw), umożliwia w coraz łatwiejszy sposób prowadzenie różnego rodzaju działań w przestrzeni informacyjnej, w tym działań z zakresu wojny informacyjnej. P. Sienkiewicz wskazał, że na potencjał informacyjny państwa składają się „wszelkie zasoby informacyjne (dane, informacje, wiedza), które tworzą infosferę określonego systemu działania (organizacji, instytucji), ale także systemy informacyjne (informatyczne, telekomunikacyjne) niezbędne do efektywnego prowadzenia określonych, zamierzonych działań”³⁹⁷. A. Żebrowski z kolei zauważył, że „infrastruktura informacyjna przeciwnika i własna składa się z danych, informacji, sprzętu, wyposażenia pomocniczego, systemów telekomunikacyjnych i ludzi. To także zbiór różnych sieci i serwisów, do których zalicza się m.in.: Internet, sieci telefonii publicznej i komórkowej, publiczną sieć danych, komercyjne sieci satelitarne, sieci rozgłośni radiowych i telewizyjnych, wojskowe sieci danych, urządzenia szyfrujące, satelitarne systemy telewizyjnej transmisji bezpośredniej, serwisy online, usługi wydawnicze i rozrywkowe, sieci

³⁹⁴ W. Krztoń: *XXI wiek – Wiekiem Społeczeństwa Informacyjnego*. „Modern Management Review” 2015, nr 22 (3/2015), s. 101-111; Zobacz szerzej: F. Webster: *Theories of the information society*. New York 2006.

³⁹⁵ J. S. Nowak: *Społeczeństwo informacyjne – geneza i definicje*. W: *Społeczeństwo informacyjne. Krok naprzód, dwa kroki wstecz*. Red. P. Sienkiewicz, J. S. Nowak. Katowice 2008, s. 25.

³⁹⁶ T. Goban-Klas, P. Sienkiewicz: *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*. Kraków 1999, s. 53.

³⁹⁷ P. Sienkiewicz: *Część III – Techniczne uwarunkowania rozwoju społeczeństwa informacyjnego. Wizje i modele wojny informacyjnej*. <http://winntbg.bg.agh.edu.pl/skrypty2/0095/373-378.pdf> (dostęp: 01.10.2022).

finansowe i usługi bankowe, sieci zasilania w energię, sieci transportowe, sieci bezpieczeństwa publicznego, usługi nawigacyjne, meteorologiczne, rządowe itp.”³⁹⁸. Niezwykle trafnym spostrzeżeniem, jest również to, że „skuteczne funkcjonowanie infrastruktury informacyjnej (w tym informatycznej) zależy jednak od czynnika ludzkiego. To człowiek bezpośrednio obsługuje systemy i sieci teleinformatyczne”³⁹⁹.

Istotną rolę w prowadzeniu wojen informacyjnych, zwłaszcza w odniesieniu do oddziaływania informacyjnego w Internecie, odgrywają media, które z kolei funkcjonują w przestrzeni medialnej. Należy zatem dokonać zdefiniowania pojęć *przestrzeń medialna* oraz *media* w ujęciu prezentowanego w pracy problemu badawczego. Pierwsze z nich – pojęcie przestrzeni medialnej – należy rozumieć jako sferę, w której funkcjonuje system medialny, z kolei w jego wnętrzu znajduje się człowiek, otaczany przez poszczególne media. H. Pietrzak pisał, że „to w niej rodzą się, narastają, a potem zanikają olbrzymie zbiory informacji, które decydują o naszym postrzeganiu otaczającej nas rzeczywistości, reprezentujących ją zjawisk społecznych, politycznych i kulturowych. Wszystkie one kreują nowe zdarzenia w przestrzeni społecznej, ale przede wszystkim tworzą „tło” – aktualny kontekst do interpretacji przekazywanych informacji. Są więc w tym sensie źródłem naszych inspiracji i imaginacji, jakie powstają w świadomości pojedynczego człowieka oraz grup społecznych”⁴⁰⁰. Definiując z kolei pojęcie mediów trzeba zauważyć, że są one bezpośrednimi uczestnikami procesu informacyjnego, który realizuje między innymi cele sprowadzające się do pozyskiwania informacji, jak i zniekształcania poszczególnych przekazów poprzez propagandę, manipulację, dezinformację czy też dezintegrację różnych środowisk, przy użyciu określonych metod i technik. Prowadzenie wojny informacyjnej z wykorzystaniem mediów w skali globalnej jest stosunkowo nowym zjawiskiem, gdyż stało się możliwe dopiero dzięki nowym technologiom, czego konsekwencją było powstanie społeczeństwa informacyjnego⁴⁰¹.

Kluczową rolę w zakresie działalności mediów w przestrzeni medialnej odgrywa wykorzystywana przez nie infrastruktura informacyjna. D. E. Denning pisze, że składają się na nią przede wszystkim zasoby informacyjne wraz z systemami komunikacji, które są

³⁹⁸ K. Liedel: *Zdolność prowadzenia działań ofensywnych w cyberprzestrzeni warunkiem bezpieczeństwa państwa*. W: *Nie-bezpieczny świat. Systemy Informacja Bezpieczeństwo*. Red. P. Sienkiewicz, H. Świeboda, E. Szczepaniuk. Warszawa 2015, s. 175.

³⁹⁹ A. Żebrowski: *Walka informacyjna w asymetrycznym środowisku bezpieczeństwa międzynarodowego. Wybrane problemy*. Kraków 2016, s. 260-261.

⁴⁰⁰ H. Pietrzak: *Wybrane zagadnienia mierzalności przestrzeni medialnej*. „Nierówności Społeczne a Wzrost Gospodarczy” 2011, nr 22, s. 336.

⁴⁰¹ A. Żebrowski, M. Żmigrodzka: *Media uczestnikami walki informacyjnej*. „Doctrina. Studia społeczno-polityczne” 2012, nr 9/2012, s. 371.

wykorzystywane przez człowieka⁴⁰². Rozwijając powyższą myśl, do infrastruktury informacyjnej zaliczymy zatem: nośniki danych (np. dyski twarde, pamięć przenośna), urządzenia biurowe (np. faksy czy drukarki), konsumenckie urządzenia elektroniczne (np. kamery, aparaty), urządzenia telekomunikacyjne (np. telefony stacjonarne i komórkowe, komputery, kable, sieci bezprzewodowe). Infrastruktura informacyjna to również sieci, a więc: Internet, sieć telefonii komórkowej, sieci satelitarne, sieci radiowe oraz telewizyjne, czy sieci wojskowe⁴⁰³. Nie wydaje się zatem wymagać szerszego uzasadnienia spostrzeżenie, że poziom zaawansowania technologicznego infrastruktury informacyjnej (tzn. zakres zastosowania nowych technologii, powszechności sieci – przede wszystkim Internetu, czy ilość poszczególnych mediów, tj. stacji telewizyjnych, gazet, rozgłośni radiowych, portali internetowych itp.), wpływa na skalę oraz efektywność prowadzonych wojen informacyjnych, zarówno w odniesieniu do działań o charakterze ofensywnym jak i defensywnym.

Powracając do mediów należy wskazać, że ich kluczową rolę w wojnie informacyjnej trafnie podsumowali A. Żebrowski oraz M. Żmigrodzka pisząc, że media „wykorzystując postęp w dziedzinie teleinformatyki posiadają możliwości dotarcia praktycznie do każdego odbiorcy w czasie niemal rzeczywistym. Ich aktywność jest widoczna wszędzie, a forma prezentowanego materiału wpływa na ocenę zachodzących zmian w otoczeniu wewnętrznym i zewnętrznym państwa. Zdolność człowieka do oceny zjawisk, zdarzeń czy osób zależy nie tylko od naszej aktualnej wiedzy, ale i mocy oddziaływania mediów. Media, będące aktywnymi uczestnikami walki informacyjnej, to nie tylko przekazywanie informacji, ale możliwość kształtowania naszej opinii poprzez zakłócanie informacyjne i obronę informacyjną. Pamiętać przy tym należy o tym, że media również są obiektem analogicznych działań ze strony przeciwnika”⁴⁰⁴.

Kolejnym istotnym uwarunkowaniem prowadzenia wojen informacyjnych (czy to poprzez oddziaływanie informacyjne na odbiorców w Internecie czy też poprzez dokonywanie cyberataków) jest potencjał do działania cyberprzestrzeni. W tym miejscu koniecznym jest wskazanie, że jednym z podstawowych celów każdego państwa – zwłaszcza w dobie globalnej rewolucji informacyjnej – powinien być rozwój cyberprzestrzeni oraz zwiększanie swoich zdolności do jej aktywnego zagospodarowywania⁴⁰⁵, a w konsekwencji zapewnienie

⁴⁰² D. E. Denning: *Wojna Informacyjna...*, s. 24-25.

⁴⁰³ A. Żebrowski, M. Żmigrodzka: *Media uczestnikami walki...*, s. 380-382.

⁴⁰⁴ Ibidem, s. 387-388.

⁴⁰⁵ Cyberprzestrzeń to najogólniej rzecz ujmując ogół powiązań o charakterze wirtualnym, które powstały w wyniku ludzkiej działalności wykorzystującej technologie informacyjne. Pojęcie cyberprzestrzeni zostało omówione szerzej w dalszej części pracy.

odpowiedniego poziomu bezpieczeństwa (cyberbezpieczeństwa⁴⁰⁶). Trzeba zgodzić się ze stwierdzeniem jakie poczynił T. R. Aleksandrowicz wskazując, że „cyberprzestrzeń jest niemal naturalną sferą walki informacyjnej, bowiem *ex definitione* służy do przekazywania, przetwarzania i przechowywania informacji”⁴⁰⁷.

Decydenci polityczni w każdym państwie powinni mieć zatem świadomość, że wraz z rozwojem infrastruktury informacyjnej (co jest z kolei skutkiem postępującej globalnej rewolucji cyfrowej), wzrastają zagrożenia w cyberprzestrzeni, która zresztą nieustannie się powiększa. Wobec powyższego, cyberprzestrzeń odgrywa zasadniczą rolę w prowadzeniu przez poszczególne podmioty (w tym państwa) wojen informacyjnych. Podejmowane przez nie działania mogą przybierać formę oddziaływania informacyjnego na odbiorców w Internecie z wykorzystaniem technik propagandowych, ale również polegać na dokonywaniu cyberataków (przede wszystkim na infrastrukturę krytyczną państwa) w cyberprzestrzeni. Przez oddziaływanie informacyjne na odbiorców w Internecie należy rozumieć co do zasady występowanie takich zjawisk jak propaganda, dezinformacja czy *fake news*. Ich nośnikiem są media internetowe, portale informacyjne, blogi, fora oraz portale społecznościowe, przy czym wiele z nich funkcjonuje w oparciu o pewien profil nacechowany ideologiczne oraz odwołujący się na przykład do wartości lewicowych, prawicowych, nacjonalistycznych czy narodowych⁴⁰⁸. Reasumując powyższe rozważania, koniecznym jest wyprowadzenie wniosku, że oddziaływanie informacyjne będzie współzależne od występującej w danym państwie struktury przestrzeni medialnej. Działalność mediów odwołujących się do poszczególnych ideologii w znaczeniu *sensu stricto*, czy też sprzyjających rządowi w danym państwie, będzie determinować sposób i zakres zniekształcania przekazu medialnego⁴⁰⁹.

Wreszcie odnosząc się do wojny informacyjnej rozumianej jako przeprowadzanie cyberataków w cyberprzestrzeni można zauważyć, że podstawowym elementem warunkującym takie działania są zdolności ofensywne oraz defensywne danego podmiotu (państwa). Zdolności te kształtowane są przede wszystkim przez właściwości techniczne cyberprzestrzeni, na które składają się między innymi urządzenia tworzące przestrzeń teleinformatyczną oraz sieci komputerowe w ramach których dokonuje się wymiana

⁴⁰⁶ Cyberbezpieczeństwo to ogół działań zmierzających do ochrony cyberprzestrzeni danego podmiotu – w szczególności sieci, urządzeń oraz programów. Pojęcie cyberbezpieczeństwa zostało omówione szerzej w dalszej części pracy.

⁴⁰⁷ T. R. Aleksandrowicz: *Podstawy walki informacyjnej*. Warszawa 2016, s. 174.

⁴⁰⁸ M. Kowalska, A. Lelonek: *Jak budować odporność społeczną w przestrzeni informacyjnej i cyberprzestrzeni: przeciwdziałanie propagandzie i dezinformacji*. Raport Centrum Analiz Propagandy i Dezinformacji, Warszawa 2017, s. 2-11.

⁴⁰⁹ Ibidem, s. 2-11.

poszczególnych informacji⁴¹⁰. Innym istotnym składnikiem cyberprzestrzeni są również systemy teleinformatyczne do których zaliczymy takie elementy jak: „informację, która jest przetwarzana, przechowywana i przesyłana; urządzenia umożliwiające te działania, czyli komputery, pamięci zewnętrzne, łącza transmisji danych, routery, koncentratory itd.; elementy programowe, w tym systemy operacyjne, oprogramowanie narzędziowe czy aplikacje; infrastrukturę, czyli budynki, zasilanie (np. energetyczne) bądź systemy ochrony przed nieuprawnionym dostępem fizycznym; operatorów, którzy korzystają z możliwości oferowanych przez system, oraz administratorów technicznych”⁴¹¹. A zatem stopień zdolności ofensywnych oraz defensywnych danego podmiotu (państwa) w zakresie przeprowadzania cyberataków (jako części składowej wojny informacyjnej), będzie zależny od poziomu zaawansowania oraz liczby urządzeń tworzących przestrzeń teleinformatyczną, sieci komputerowe oraz systemy teleinformatyczne. Warto również wspomnieć, że poza powyższymi aspektami o charakterze fizycznym, kluczowa pozostaje świadomość decydentów politycznych danego państwa w zakresie jego potencjału w cyberprzestrzeni, a więc ich wewnętrzne przekonanie co do zdolności ofensywnych oraz defensywnych. W tym celu rządy w postaci publikowanych strategii, koncepcji oraz doktryn określają cele jakie realizują lub będą realizować w cyberprzestrzeni, występujące w niej zagrożenia dla cyberbezpieczeństwa państwa oraz działania, które podejmą w celu ich neutralizacji, jak również wyzwania jakie w tej materii przed nimi stoją. Wspomniane dokumenty stanowią zatem punkt wyjścia w tworzeniu zdolności ofensywnych oraz defensywnych każdego państwa⁴¹².

2.2.3. Wybrane instrumenty wojny informacyjnej

Zagadnienie wojny informacyjnej, szczególnie przy uwzględnieniu odmienności występujących w koncepcjach rosyjskich i zachodnich, jest zagadnieniem niezwykle złożonym. Samo pojęcie występujące od dawna w nauce o stosunkach międzynarodowych czy nauce o bezpieczeństwie doczekało się wielu definicji. Dokonując analizy wybranych z nich, co miało miejsce we wcześniejszych częściach pracy, można wyprowadzić wniosek, że każda zawiera

⁴¹⁰ M. Lakomy: *Cyberprzestrzeń jako nowy...*, s. 85-86.

⁴¹¹ Ibidem, s. 87.

⁴¹² Zobacz na przykład: *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej 2015*. Warszawa 2015. <https://www.bbn.gov.pl/pl/informacje-o-bbn/publikacje/6818,Doktryna-cyberbezpieczenstwa-RP.html> (dostęp: 01.10.2022); *Strategia Bezpieczeństwa Narodowego Federacji Rosyjskiej zatwierdzona 2 lipca 2021 roku*. Moskwa 2021. https://poland.mid.ru/pl/press-centre/news/strategia_bezpiecze_stwa_narodowego_federacji_rosyjskiej/ (dostęp: 24.10.2022); President of the United States: *National Security Strategy*. Washington D.C. 2017. <https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf> (dostęp: 01.10.2022).

pewne cechy charakterystyczne, które w istotny sposób wpływają na jej zrozumienie jako zjawiska. Dlatego też w niniejszym podrozdziale zostaną zdefiniowane wybrane instrumenty wojny informacyjnej, wymienione w literaturze specjalistycznej, takie jak: manipulacja, dezinformacja, operacje informacyjne, operacje psychologiczne, agentura wpływu oraz dywersja ideologiczna⁴¹³.

Pierwszym ze wskazanych pojęć jest *manipulacja*, która w potocznym znaczeniu oznacza „kontrolowanie kogoś lub czegoś na własną korzyść, często niesprawiedliwie lub nieuczciwie”⁴¹⁴ bądź też „wpływanie na poglądy i zachowania innych osób poza ich świadomością dla osiągnięcia własnych celów”⁴¹⁵. Definicje występujące w literaturze specjalistycznej zasadniczo nie odbiegają od tych przytoczonych wyżej, jednakże warto wskazać na kilka z nich, które opisują ten termin w sposób bardziej złożony. T. M. Wilkinson stwierdza, że jest to rodzaj wpływu, który omija i podważa racjonalne zdolności celu, a więc w pewien sposób znieważa autonomiczne podejmowanie decyzji przez daną osobę, która jest traktowana jako narzędzie. Wskazuje, że manipulacja to celowe i udane wywieranie na kogoś wpływu przy użyciu metod, które wypaczają wybór⁴¹⁶. R. Faden i T. Beauchamp z kolei wskazują na pojęcie manipulacji psychologicznej oraz że jest to każdorazowe zamierzone działanie, które z powodzeniem wpływa na odbiorcę w zakresie jego przekonań lub zachowań, w konsekwencji wywołania zmian w procesach umysłowych, odmiennych od tych zaangażowanych w rozumienie. Natomiast J. Raz zestawia terminy manipulacji i przymusu, stwierdzając, że pierwsze z pojęć nie ingeruje w możliwość wyboru, ale zamiast tego wypacza sposób w jaki odbiorca podejmuje decyzje oraz kształtuje swoje preferencje⁴¹⁷. J. Fras natomiast definiuje manipulację jako niejawne i podstępne, nierzetelne dobieranie środków językowych w celu wywarcia wpływu na nastroje, poglądy i opinie innych osób oraz uzyskanie możliwości kierowania ich zachowaniem, w celi realizacji własnych interesów⁴¹⁸.

Drugi z terminów wymagający omówienia – *dezinformacja* – jest ściśle związany z opisaną wyżej manipulacją, przy czym ma on wydźwięk o wiele bardziej konfrontacyjny. W terminologii wojskowej działalnością dezinformującą jest „rozpowszechnianie nieprawdziwych wiadomości i dokumentów dla wprowadzenia w błąd nieprzyjaciela co do

⁴¹³ Z uwagi na przedmiot rozprawy szczegółowe rozważania w zakresie zagadnienia propagandy oraz cyberataków zostaną przedstawione w kolejnych częściach pracy.

⁴¹⁴ Cambridge Dictionary: *manipulation*. <https://dictionary.cambridge.org/us/dictionary/english/manipulation> (dostęp: 06.10.2022). Tłumaczenie własne. Tekst w oryginale: „controlling someone or something to your own advantage, often unfairly or dishonestly”.

⁴¹⁵ SJP.pl: *manipulacja*. <https://sjp.pl/manipulacja> (dostęp: 06.10.2022).

⁴¹⁶ C. R. Sunstein: *Fifty Shades of Manipulation*. „Journal of Marketing Behavior” 2016, 213, s. 10.

⁴¹⁷ Ibidem, s. 10-11.

⁴¹⁸ B. Dobek-Ostrowska, J. Fras, B. Ociepka: *Teoria i praktyka propagandy*. Wrocław 1997, s. 97-98.

faktycznego zamiaru, organizacji i prowadzenia operacji (walki, bitwy), a także składu wojsk własnych i charakteru ich działania”⁴¹⁹. Słownikowa, potoczna, definicja dezinformacji to działalność polegająca na rozpowszechnianiu fałszywych informacji w celu oszukania odbiorcy⁴²⁰. A. Golicyn uznał natomiast, że jest to (odnosząc oczywiście ten pogląd do nauki radzieckiej) „rozprowadzanie przez prasę i radio fałszywych danych w celu wprowadzenia w błąd opinii publicznej”⁴²¹. Bardzo ciekawe spostrzeżenie poczyniła J. Darczewska, która wskazała, że ujęciu rosyjskim „stanowi ona pojęcie zbiorcze różnych metod wykorzystywanych w przestrzeni fizycznej i informacyjnej, jest syntezą znacznie subtelniejszych niż zwykle oszustwo technik politycznych, wojskowych, wywiadowczych, biznesowych, dyplomatycznych medialnych, cybernetycznych, służących realizacji długoterminowych celów polityki Kremla”⁴²². Z terminem dezinformacji (ang. *disinformation*) nie należy mylić terminu *mylna informacja* (ang. *misinformation*). Różnica polega na tym, że o ile w przypadku dezinformacji nadawca komunikatu wie, iż jest on fałszywy o tyle w przypadku mylnej informacji nie jest tego świadom. Brak jest zatem tutaj zamiaru (celowości) działania, aby okłamać odbiorcę⁴²³.

Omawiając termin dezinformacji, warto również odnieść się do często pojawiającego się w jej kontekście pojęcia *fake news*. Jest ono używane zamiennie z pojęciami takimi jak *kopia*, *falszerstwo*, *podróbka* czy *nieautentyczny*⁴²⁴. *Fake news* nie jest kłamstwem, ponieważ jego część jest prawdziwa, tyle że zmodyfikowana, wyrwana z kontekstu. D. Elliot i Ch. Culver zdefiniowali omawiany termin jako czynność przekazania wiadomości bez użycia kłamstwa, ale z jednoczesnym ukryciem części informacji tak, aby doprowadzić do wykreowania po stronie odbiorcy fałszywego przekonania co do danego tematu⁴²⁵. Inne poglądy definicyjne w zakresie omawianego terminu nawiązują do okoliczności związanych z informacjami podawanymi do publicznej wiadomości przez dziennikarzy, którzy uprzednio je przetwarzają. W związku z tym H. Allcott i M. Gentzkow podzielają pogląd, że *fake news* to wiadomości,

⁴¹⁹ J. Kaczmarek, W. Łepkowski, B. Zdrodowski (Red.): *Słownik terminów...*, s. 31.

⁴²⁰ Cambridge Dictionary: *disinformation*. <https://dictionary.cambridge.org/dictionary/english/disinformation> (dostęp: 06.10.2022).

⁴²¹ A. Golicyn: *Nowe kłamstwa w miejsce starych*. Warszawa 2007, s. 5.

⁴²² J. Darczewska: *Dezinformacja – rosyjska broń strategiczna*. „Biuletyn Kwartalny Rządowego Centrum Bezpieczeństwa” 2017, nr 19, s. 6.

⁴²³ United Nations Educational, Scientific and Cultural Organization: *Journalism, 'Fake News' & Disinformation. Handbook for Journalism Education and Training*. Paris 2018, s. 44.

⁴²⁴ E. C. Tandoc Jr., Z. W. Lim, R. Ling: *Defining "Fake News" A typology of scholarly definitions*. „Digital Journalism” 2018, Vol. 6, Issue 2/2018, s. 4.

⁴²⁵ D. Elliot, C. Culver: *Defining and Analyzing Journalistic Deception*. „Journal of Mass Media Ethics” 1992, Vol. 7, s. 69-83.

które „celowo są fałszowane i mogą wprowadzać odbiorców w błąd”⁴²⁶. J. Gillin z kolei pisze, że *fake news* jest wiadomością medialną oraz że nie jest ani kłamstwem, ani prawdą, ponieważ bazując na dezinformacji zawiera elementy prawdziwe⁴²⁷. Reasumując, dezinformacja jest szerszym pojęciem, obejmującym wszelkie działania mające na celu świadome wprowadzenia w błąd, niezależnie od formy. *Fake news* to jeden z rodzajów dezinformacji, który koncentruje się głównie na fałszywych materiałach informacyjnych. Ponadto celem dezinformacji jest wpływanie na postawy i działania ludzi poprzez manipulowanie faktami, podczas gdy *fake newsy* często sprowadzają się do wywoływania sensacji, rozprzestrzenienia negatywnych emocji lub zamieszania.

Wreszcie należy omówić pojęcie *operacji informacyjnych*, które są „stosowane przez organizacje, państwa w celu zmanipulowania opinii publicznej i skłonienia jej do popierania strony przeprowadzającej te operacje. Operacje informacyjne to działania podejmowane w celu wpływania na informację oraz systemy informacyjne przeciwnika, przy jednoczesnej obronie własnych informacji i systemów informacyjnych”⁴²⁸. „Słownik terminów i definicji NATO” wyróżnia natomiast termin *działania informacyjne*, definiując je jako aktywności podmiotów mające kształtować informacje lub systemy informacyjne, jak również wskazując, że działania informacyjne może realizować dowolny podmiot, oraz że obejmują one środki ochrony⁴²⁹. Definicja amerykańska postrzega operacje informacyjne jako „zintegrowane wykorzystanie, podczas operacji wojskowych, zdolności związanych z informacją w połączeniu z innymi liniami operacyjnymi w celu wpływania, zakłócania, korumpowania lub uzurpowania podejmowanych decyzji przez przeciwników i potencjalnych przeciwników, przy jednoczesnej ochronie naszych własnych”⁴³⁰. Można zauważyć, że operacje informacyjne są przede wszystkim domeną działalności podmiotów o charakterze militarnym. Pozostają więc związane z zagadnieniem walki informacyjnej, która jest częścią składową wojny informacyjnej. Operacje informacyjne będą co do zasady prowadzone przede wszystkim w postaci cyberataków oraz w cyberprzestrzeni, z kolei działalność z zakresu oddziaływania informacyjnego jest domeną operacji psychologicznych, omówionych poniżej.

⁴²⁶ M. Aldwairi, A. Alwahedi: *Detecting Fake News in Social Media Networks*. „Procedia Computer Science” 2018, Vol. 141/2018, s. 215-221.

⁴²⁷ POLITIFACT: *Fact-checking fake news reveals how hard it is to kill pervasive ‘nasty weed’ online*. <https://www.politifact.com/article/2017/jan/27/fact-checking-fake-news-reveals-how-hard-it-kill-p/> (dostęp: 06.10.2022).

⁴²⁸ J. Kaczmarek, W. Łepkowski, B. Zdrodowski (Red.): *Słownik terminów...*, s. 87.

⁴²⁹ Biuro Standaryzacji NATO: *Słownik terminów...*, s. 224.

⁴³⁰ Chairman of the Joint Chiefs of Staff: *Joint Publication 3-13. Information Operations*. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf (dostęp: 06.10.2022).

Odmianą operacji informacyjnych są *operacje psychologiczne*. W ich przypadku największy nacisk położono na kwestie dotyczące oddziaływania informacyjnego na odbiorców, co odróżnia je od definicji terminu omówionego wyżej. A. Lelonek zauważył, że w rozumieniu amerykańskim, operacje informacyjne nie są tym samym czym operacje psychologiczne, mimo iż mogą być prowadzone w niewojskowym środowisku, jak na przykład media⁴³¹. W terminologii amerykańskiej operacje psychologiczne mają bowiem na celu „przekazanie wybranych informacji i sygnałów zagranicznym odbiorcom, aby wpłynąć na ich emocje, motyw, obiektywne rozumowanie, a ostatecznie na zachowanie zagranicznych rządów, organizacji, grup i jednostek. Celem operacji psychologicznych jest wywołanie lub wzmocnienie zagranicznych postaw i zachowań korzystnych dla celów inicjatora”⁴³². Operacje psychologiczne są również zestawiane z zagadnieniem wojny psychologicznej, w ramach której M. Libicki wyróżnił cztery kategorie operacji takie jak: przeciwko woli narodu, przeciwko dowództwu przeciwnika, przeciwko żołnierzom oraz konflikt kulturowy⁴³³. Operacje psychologiczne wykraczają poza zagadnienie propagandy, ponieważ są definiowane jako „wykorzystanie różnorodnych środków komunikacji, mające na celu przekazanie określonych informacji i danych (za pomocą dźwięku lub obrazu) dla zagranicznego audytorium, aby oddziaływać na jego emocje, motyw, obiektywne rozumowanie, a ostatecznie na zachowanie zagranicznych rządów, organizacji, grup i jednostek”⁴³⁴.

Przedostatni termin to *agentura wpływu*, który jest silnie związany z działalnością służb specjalnych. Agentura wpływu, a precyzyjniej mówiąc agent, jest osobą często narodowości obcej względem państwa w którym przebywa, niebędącą etatowym pracownikiem służb, ale działającą na ich rzecz. Taka współpraca sprowadza się przede wszystkim do dostarczania informacji wywiadowczych i kontrwywiadowczych⁴³⁵. Agentura stanowi pośrednią formę zdobywania informacji, ale również zapewnia infiltrację poszczególnych podmiotów. Samych agentów można podzielić na różne rodzaje takie jak agentów: głównych, nieświadomych, podwójnych, uśpionych czy potencjalnych⁴³⁶. Odnosząc się do powyższych rozważań nie wydaje się celowym, aby agenturę wpływu utożsamiać wyłącznie z działaniami o charakterze

⁴³¹ A. Lelonek: *Wojna informacyjna, operacje informacyjne...*, s. 78.

⁴³² Air Force Doctrine Center: *Psychological operations. Air Force Doctrine Document 2-5.3 27 August 1999*. Tłumaczenie własne. Tekst w oryginale: „convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives”.

⁴³³ M. C. Libicki: *What is information...*, s. 35.

⁴³⁴ A. Lelonek: *Wojna informacyjna, operacje informacyjne...*, s. 84-85.

⁴³⁵ A. Żebrowski: *Agentura wpływu uczestnikiem walki informacyjnej*. „Studia nad Autorytaryzmem i Totalitaryzmem” 2019, nr 1, T.40, s. 64.

⁴³⁶ Ibidem, s. 64-65.

militarnym. Biorąc bowiem po uwagę zakres działań prowadzonych w ramach wojny informacyjnej, agentem wpływu może być zarówno osoba działająca przeciwko siłom zbrojnym innego państwa, jak i osoba będąca pracownikiem gazety, stacji telewizyjnej, przedsiębiorstwa itp., czy też po prostu będąca zwykłym obywatelem⁴³⁷.

Wreszcie, należy przejść do pojęcia *dywersji ideologicznej*, szczególnie istotnego w działalności rosyjskiego aparatu informacyjnego. T. D. Schuman, a właściwie J. Bezmienow bo tak naprawdę nazywał się agent KGB zbiegły na Zachód, opowiedział w sposób bardzo szczegółowy jak działa dywersja ideologiczna w kontekście operacji realizowanych przez ZSRR. Wskazał, że dywersja w ujęciu rosyjskim nie ma takiego samego znaczenia jak na Zachodzie. Dywersant w tym ujęciu to student z wymiany międzyuczelnianej, dyplomata, dziennikarz czy aktor. W terminologii radzieckiej dywersja to odwracanie uwagi od wrogiej działalności, która została podjęta w celu zniszczenia wrogiego państwa (narodu). Ponadto, działania takie nie są penalizowane przez prawo państwa, w którym są dokonywane oraz pozostają jawne, będąc prowadzone wieloma kanałami komunikacyjnymi⁴³⁸. Reasumując rozważania J. Bezmienowa można wskazać, że przewrót ideologiczny (dywersja ideologiczna) to działania mające na celu zniszczenie tradycyjnego systemu wartości, światopoglądu, norm kulturowych oraz więzi społecznych przeciwnika. Dywersja polega więc na pokonaniu państwa od środka, na spustoszeniu jego struktur wewnętrznych, zarówno tych sformalizowanych jak i niesformalizowanych, aby w konsekwencji przejąć nad nim kontrolę. Działania takie są podejmowane w ramach prowadzonych wojen informacyjnych, a w przypadku Rosji poprzez wspieranie różnego rodzaju ideologii oraz grup w państwach na całym świecie.⁴³⁹

Zarysowane powyżej instrumenty, za pomocą których jest prowadzona wojna informacyjna, nie mają oczywiście charakteru enumeratywnego. Intencją autora było jedynie przedstawienie podstawowych z nich, o szczególnym znaczeniu w kontekście działań podejmowanych przez Federację Rosyjską⁴⁴⁰. Mając na względzie omówione powyżej instrumenty należy ponownie zauważyć, że uzasadnionym pozostaje zastosowanie w pracy pojęcia wojna informacyjna, nie natomiast walka informacyjna. Nie tylko z uwagi na fakt, że pierwszym z terminów posługują się Rosjanie, ale również z uwagi na to, że termin walka nie obejmuje swoim znaczeniem wszystkich omówionych wyżej instrumentów oraz nie traktuje

⁴³⁷ A. Lelonek: *Wojna informacyjna, operacje informacyjne...*, s. 75.

⁴³⁸ YouTube: *Jak napaść na państwo (całość) Jurij Bezmienow*. <https://www.youtube.com/watch?v=IWlpFvGrNak> (dostęp 06.10.2022).

⁴³⁹ M. Banasik: *Rywalizacja presja i agresja Federacji Rosyjskiej. Konsekwencje dla bezpieczeństwa międzynarodowego*. Warszawa 2021, s. 111.

⁴⁴⁰ Zobacz szerzej: *Rozdział 4. Wojna informacyjna w polityce zagranicznej Federacji Rosyjskiej*.

ich w sposób kompleksowy. Wojna informacyjna, będąc terminem zdecydowanie szerszym, pozwala na prawidłowe ujęcie omawianego w pracy problemu badawczego.

2.2.4. Wybrani uczestnicy wojny informacyjnej

Omawiając zagadnienie wojny informacyjnej wielokrotnie w sposób dość ogólny wskazywano, że jest ona prowadzona przede wszystkim przez państwa, zatem konieczne jest szczegółowe scharakteryzowanie poszczególnych jej uczestników, którzy operują w obrębie struktur krajowych. Podmioty państwowe są stosunkowo szeroką grupą bytów, spośród których wybrane z nich prowadzą działania z zakresu wojen informacyjnych, a ich katalog nie jest oczywiście enumeratywny. Na potrzeby rozprawy zostaną omówione najistotniejsze z nich do których zaliczono: władzę wykonawczą i ustawodawczą, służby dyplomatyczne, wywiad i kontrwywiad (w tym wojskowe oraz cywilne służby specjalne), siły zbrojne oraz media.

Działalność pierwszego z podmiotów, którym są organy egzekutywy oraz legislatury, sprowadza się przede wszystkim do formułowania i realizowania wewnętrznej oraz zewnętrznej działalności państwa, będąc przy tym jednocześnie aktywnym i biernym uczestnikiem wojny informacyjnej⁴⁴¹. To w ramach ich działalności odbywa się proces decyzyjny w zakresie formułowania interesów narodowych, a w konsekwencji celów polityki zagranicznej, w wyniku której dochodzi do oddziaływania decydentów politycznych na środowisko międzynarodowe⁴⁴². Nadmienić należy, że identyfikacja poszczególnych interesów narodowych nie jest oparta wyłącznie o to co najlepsze dla państwa (społeczeństwa), ale często stanowi wyraz realizacji partykularnych interesów rządzących⁴⁴³, przez co wojny informacyjne mogą być prowadzone w zasadzie wobec nieograniczonej liczby podmiotów. W zależności od ustroju politycznego występującego w danym państwie to właśnie te podmioty mają kluczowy wpływ⁴⁴⁴ na działania podejmowane przez dyplomację, wywiad, kontrwywiad, służby specjalne, siły zbrojne oraz media.

Służby dyplomatyczne są częścią władzy wykonawczej państwa, niemniej jednak z uwagi na ich specyfikę oraz znaczenie w realizowaniu polityki zagranicznej, zostały one omówione odrębnie. Służba dyplomatyczna, będąc zależną od władzy wykonawczej, realizuje

⁴⁴¹ A. Żebrowski: *Walka informacyjna w asymetrycznym...*, s. 182-186.

⁴⁴² R. Zięba: *Cele polityki zagranicznej państwa. W: Wstęp do teorii polityki zagranicznej państwa*. Red. R. Zięba. Toruń 2005, s. 37-38.

⁴⁴³ E. Furnis; R. C. Snyder: *An Introduction to American Foreign Policy*. New York 1955, s. 17.

⁴⁴⁴ R. Gilpin stwierdził wręcz, że interesy narodowe są determinowane wyłącznie przez dominujących w danym kraju decydentów politycznych, co z kolei przekłada się na realizowaną przez dane państwa politykę zagraniczną. Źródło: R. Gilpin: *War and Change in World Politics*. Cambridge 1981, s. 18-19.

zewnętrzne funkcje państwa. Jedną z nich jest prowadzenie działań polegających na zdobywaniu informacji, o czym stanowi Konwencja wiedeńska o stosunkach dyplomatycznych. Wskazuje, że funkcją misji dyplomatycznej jest „zaznajamianie się wszelkimi legalnymi sposobami z warunkami panującymi w państwie przyjmującym i z rozwojem zachodzących w nim wydarzeń oraz zdawanie z tego sprawy rządowi państwa wysyłającego”⁴⁴⁵. Zatem efektywne prowadzenie wojen informacyjnych nie byłoby możliwe bez sprawnego realizowania tej funkcji. Zakłada ona również przekazywanie organom państwa przyjmującego urzędowych informacji za pośrednictwem oficjalnych kanałów dyplomatycznych, organizację konferencji prasowych, odczytywanie dementi i sprostowań, czy też ocenę wzajemnych stosunków⁴⁴⁶. Są to oficjalne oraz w pełni legalne kanały kolportowania określonych treści przez dane państwo, które nie są jednak pozbawione instrumentów z zakresu oddziaływania informacyjnego. Ponadto dyplomacja pełni również funkcję preskrypcyjną, która polega na wskazywaniu najbardziej odpowiednich metod osiągania przez politykę zagraniczną jej celów oraz środków jakie powinny zostać do tego użyte⁴⁴⁷.

Następną grupą uczestników są służby wywiadowcze i kontrwywiadowcze do których należy zaliczyć przede wszystkim wojskowe oraz cywilne służby specjalne. Na ich podstawowe funkcje składa się między innymi: pozyskiwanie informacji oraz ich analiza, prowadzenie tajnych operacji, misji wywiadowczych, działań kontrwywiadowczych, wspieranie operacji dyplomatycznych oraz wojskowych, przeciwdziałanie zagrożeniom wewnętrznym i zewnętrznym⁴⁴⁸. T. R. Aleksandrowicz wskazał z kolei, że służby specjalne pełnią dwie podstawowe funkcje, tj. informacyjno-analityczną oraz kreatywną. Pierwsza z nich polega na pozyskiwaniu źródeł informacji dla decydentów politycznych oraz tworzeniu analiz i prognoz opartych na dostępnych źródłach informacji. Te z kolei stanowią podstawę dla strategii bezpieczeństwa narodowego, a zatem funkcja ta jest realizowana zarówno wewnątrz, jak i na zewnątrz państwa, w zależności od tego, gdzie posiada ono swoje interesy. Druga z nich – funkcja kreatywna – sprowadza się do podejmowania działań o charakterze wykonawczym, a więc działań wynikających z przyjętych przez państwo strategii bezpieczeństwa. Jest to więc

⁴⁴⁵ Konwencja wiedeńska o stosunkach dyplomatycznych, sporządzona w Wiedniu dnia 18 kwietnia 1961 roku (Dz.U. 1965 nr 37 poz. 232), artykuł 3.

⁴⁴⁶ R. Bierzanek, J. Symonides: *Prawo Międzynarodowe Publiczne*. Warszawa 2005, s. 174-175.

⁴⁴⁷ B. Molo: *Systemy, zasady i formy międzynarodowej współpracy politycznej*. W: *Międzynarodowe stosunki polityczne*. Red. E. Cziomer. Kraków 2008, s. 115.

⁴⁴⁸ Report Commission on the Roles and Capabilities of the United States Intelligence Community: *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*. March 1996. <https://www.govinfo.gov/app/details/GPO-INTELLIGENCE/context> (dostęp: 06.10.2022), s. 15-25.

przede wszystkim przeciwdziałanie zagrożeniom dla bezpieczeństwa państwa, ale również wywieranie wpływu na inne podmioty w celu osiągnięcia pożądanego skutku z punktu widzenia własnych interesów⁴⁴⁹. W odniesieniu do zagadnienia wojny informacyjnej, działalność służb specjalnych ma zasadnicze znaczenie w Federacji Rosyjskiej, gdzie stanowią one trzon podmiotów odpowiedzialnych za podejmowanie działań w tym zakresie⁴⁵⁰.

Kolejnym podmiotem będącym uczestnikiem wojny informacyjnej są siły zbrojne. Ich działalność może być utożsamiana z funkcjami realizowanymi przez służby specjalne z tym zastrzeżeniem, że działalność wojska ma przede wszystkim charakter militarny. Służby wywiadu oraz rozpoznawanie wojskowe odpowiadają za ofensywną walkę informacyjną, w wyniku której pozyskiwane są informacje o przyszłej płaszczyźnie funkcjonowania dyplomacji, służb specjalnych oraz wojska. Z kolei działalność kontrwywiadowcza jest nakierowana na pozyskiwanie oraz analizowanie informacji w celu zapewnienia bezpieczeństwa wewnętrznego państwa oraz sił zbrojnych przebywających poza granicami państwa⁴⁵¹. W odniesieniu do sił zbrojnych Rosji J. Darczewska wskazuje⁴⁵², że opisana działalność to działania defensywne „dla obrony integralności własnego systemu informacyjnego przed oddziaływaniem, niszczeniem i zakłócaniem przez przeciwnika (...), a jednocześnie działania ofensywne (mające na celu oddziaływanie, uszkodzanie i niszczenie systemu informacyjnego przeciwnika)”⁴⁵³. W tym ujęciu działalność sił zbrojnych będzie zatem polegać przede wszystkim na prowadzeniu walki informacyjnej (elektronicznej), będącej częścią wojny informacyjnej⁴⁵⁴. Tutaj należy zaznaczyć, że wraz ze wzrostem znaczenia tego rodzaju walki poszczególne państwa w ramach posiadanych sił zbrojnych rozpoczęły procesy tworzenia ich nowego rodzaju – wojsk obrony cyberprzestrzeni⁴⁵⁵.

⁴⁴⁹ T. R. Aleksandrowicz: *Wywiad jako narzędzie w koncepcji nowych wojen. Casus konfliktu ukraińskiego*. „Studia Politologiczne” 2017, Vol. 43, s. 187-189.

⁴⁵⁰ B. Smith: *Russian intelligence services and special forces*. „Briefing paper” 2018, Number CBP 8430 2018, s. 4-12; J. Darczewska: *Diabeł tkwi w szczegółach. Wojna informacyjna w świetle doktryny wojennej Rosji*. „Punkt widzenia” 2015, nr 50. https://www.osw.waw.pl/sites/default/files/pw_50_pl_diabel_tkwi_net.pdf (dostęp: 06.10.2022), s. 22-29.

⁴⁵¹ A. Żebrowski: *Walka informacyjna w asymetrycznym...*, s. 210.

⁴⁵² W przytoczonym fragmencie J. Darczewska opisuje działalność sił zbrojnych Federacji Rosyjskiej, jednak zaznacza, że nie odróżnia to armii rosyjskiej od armii innych państw na świecie.

⁴⁵³ J. Darczewska: *Rosyjskie Siły zbrojne na froncie walki informacyjnej. Dokumenty strategiczne*. „Prace OSW” 2016, nr 57. https://www.osw.waw.pl/sites/default/files/prace_57_pl_sily_zbrojne_net.pdf (dostęp: 06.10.2022), s. 11.

⁴⁵⁴ D. Kazimierczak: *Walka informacyjna we współczesnych konfliktach i jej społeczne konsekwencje*. „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate” 2017, nr 7, s. 111-128.

⁴⁵⁵ The Congressional Research Service: *Russian Cyber Units (IF11718)*. <https://crsreports.congress.gov/product/details?prodcode=IF11718> (dostęp: 06.10.2022); U.S. Cyber Command: *Our history*. <https://www.cybercom.mil/About/History/> (dostęp: 06.10.2022); GOV.UK: *Armed Forces announce launch of Cyber Regiment in major modernisation*. <https://www.gov.uk/government/news/armed-forces-announce-launch-of-first-cyber-regiment-in-major-modernisation> (dostęp: 06.10.2022); Ministre des Armées: *Le commandement de la cyberdéfense (COMCYBER)*. <https://www.defense.gouv.fr/ema/commandement->

Ostatnim z wybranych uczestników wojen informacyjnych, a jednocześnie jednym z najistotniejszych o którym należy wspomnieć, są media. Trzeba bowiem zauważyć, że media jak i wojna informacyjna są powszechnie obecne w naszym codziennym życiu. Ponadto, „kształtują percepcję jednostek i określonych środowisk krajowych i międzynarodowych. Wykorzystują technikę teleinformatyczną, do której powszechny dostęp zwiększa możliwości dotarcia do każdego odbiorcy w czasie niemal rzeczywistym”⁴⁵⁶. Co więcej, jak słusznie zaznacza w tym zakresie A. Żebrowski, „działalność mediów to nie tylko pozyskiwanie, interpretowanie i przekazywanie informacji, ale również dezorientowanie odbiorcy co do aktualnej sytuacji społecznej, politycznej, gospodarczej, naukowej, wojskowej czy zagrożeń”⁴⁵⁷. Wykorzystywanie mediów do prowadzenia działań z zakresu oddziaływania informacyjnego ma bardzo długą historię, a w odniesieniu do aktywności rosyjskiej występowało również w okresie zimnej wojny. Dla przykładu można wskazać na operacje Federacji Rosyjskiej w ramach których oskarżono USA o stworzenie wirusa AIDS w celach bojowych, FBI o zamach na M. L. Kinga, natomiast CIA o to, że próbowało dokonać zamachu na papieża Jana Pawła II⁴⁵⁸. Prokremlowskie media „uwypuklają ochronny, defensywny aspekt działalności służb; nielegalne zdobywanie informacji, manipulacyjne oddziaływanie na percepcję, zakłócanie przestrzeni informacyjnej i inne antagonistyczne działania są przypisywane służbom przeciwnika”⁴⁵⁹. Jak już wspomniano, współczesny postęp technologiczny umożliwia mediom (nie tylko rosyjskim) dotarcie do niemal każdego odbiorcy na świecie, w czasie w zasadzie rzeczywistym. Forma kształtowanego przekazu wpływa z kolei na ocenę poszczególnych zdarzeń przez każdego człowieka (odbiorcę). Jednocześnie mnogość podmiotów o charakterze medialnym w globalnej przestrzeni informacyjnej powoduje, że przeciwdziałanie omawianym wyżej zagrożeniom jest niezwykle trudne, a w zasadzie w pełni skutecznie niemożliwe⁴⁶⁰.

cyberdefense-comcyber (dostęp: 06.10.2022); Reuters: *Chinese military force to take lead on cyber, space defense*. <https://www.reuters.com/article/us-china-military-idUSKCN0V714B> (dostęp 06.10.2022); Ministerstwo Obrony Narodowej: *Wojska Obrony Cyberprzestrzeni rozpoczynają działalność*. <https://www.gov.pl/web/obrona-narodowa/wojska-obrony-cyberprzestrzeni-rozpoczynaja-dzialalnosc> (dostęp: 06.10.2022).

⁴⁵⁶ A. Żebrowski: *Walka informacyjna w asymetrycznym...*, s. 217.

⁴⁵⁷ Ibidem, s. 217.

⁴⁵⁸ E. Lucas, P. Pomerantsev: *Winning the Information War. Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe. A Report by CEPA's Information Warfare Project in Partnership with the Legatum Institute*. Washington D.C. 2016, s. 55.

⁴⁵⁹ J. Darczewska: *Między jawną dezinformacją a niejawną praktyką. Gry rosyjskich służb. „Punkt widzenia”* 2019, nr 73. https://www.osw.waw.pl/sites/default/files/PW_73_PL_Miedzy-jawna-dezinformacja_net.pdf (dostęp: 06.10.2022), s. 15.

⁴⁶⁰ A. Żebrowski, M. Żmigrodzka: *Media uczestnikami walki...*, s. 369-388.

Dokonując oceny powyższych rozważań można wyprowadzić wniosek, że najważniejszym z uczestników wojny informacyjnej pozostają niewątpliwie media. Wynika to z faktu, że ocena poszczególnych informacji przeprowadzana przez człowieka (czy też szerzej opinię publiczną), nie jest zależna jedynie od posiadanej przez niego wiedzy, ale przede wszystkim od stopnia oddziaływania mediów, a więc w gruncie rzeczy od sposobu, metod czy technik przekazywania przez nie informacji. To właśnie media odpowiadają w ogromnym stopniu za kształtowanie opinii oraz osądów w przestrzeni publicznej. Co również w tym kontekście istotne, media mogą stać się narzędziem wykorzystywanym władzę, służby specjalne, czy siły zbrojne. Co więcej, jak trafnie zauważyła D. E. Denning „we wszystkich operacjach wojny informacyjnej występują dwa zasadnicze typy graczy: gracz ofensywny, który rozpoczyna operację przeciw jakimś konkretnym zasobom informacyjnym, i gracz defensywny, który zamierza się bronić”⁴⁶¹. Pogląd ten należy utożsamiać ze stwierdzeniem, że każdy podmiot będący uczestnikiem wojen informacyjnych, bez względu na swój charakter podmiotowy, może być zarówno atakującym jak i obrońcą, a charakter podejmowanych przez poszczególnych uczestników działań będzie zależał z kolei od zadań jakie zostaną im przydzielone przez decydentów politycznych (elity rządzące)⁴⁶². Media odgrywają więc kluczową rolę w kształtowaniu opinii publicznej i percepcji rzeczywistości. Dzięki swojej zdolności do masowego przekazu informacji, oddziałują nie tylko na jednostki, ale także na całe społeczeństwa, wpływając na ich postawy, decyzje i zachowania. Zarówno media tradycyjne takie jak prasa, telewizja czy radio, jak i nowoczesne formy przekazu, w tym media internetowe, przyczyniają się do tego procesu, dostarczając informacji w sposób, który często ukierunkowuje odbiorców na określone poglądy. Techniki i metody stosowane przez media, w tym selekcja treści, sposób ich prezentacji czy stosowanie określonych narracji, mają kluczowe znaczenie w budowaniu określonych przekazów. W wyniku tego media mogą pełnić zarówno rolę edukacyjną, przekazując rzetelne informacje, jak i manipulacyjną, w sytuacji, gdy są wykorzystywane do realizacji interesów politycznych, gospodarczych, społecznych czy militarnych.

2.3. Propaganda i cyberataki jako instrumenty wojny informacyjnej

Z dotychczasowych rozważań można zauważyć, że wojny informacyjne nie stanowią jedynie domeny działań o charakterze militarnym, ale mogą być prowadzone w innych

⁴⁶¹ D. E. Denning: *Wojna Informacyjna...*, s. 28.

⁴⁶² Ibidem, s. 28-31.

przestrzeniach aktywności człowieka. Na gruncie niniejszej rozprawy przyjęto, że wojna informacyjna to oddziaływanie informacyjne na odbiorców w Internecie oraz dokonywanie cyberataków w cyberprzestrzeni. Podejmowanie powyższych działań nie może być określane mianem doraźnych czy przypadkowych, gdyż wynika najczęściej z precyzyjnie przygotowanego planu, rozpatrywanego jako element rywalizacji w stosunkach międzynarodowych. Wojna informacyjna ma również charakter kompleksowy, a sam termin jest zdecydowanie szerszy w porównaniu z pojęciem walki informacyjnej. Ponadto jest trwale ugruntowany w literaturze specjalistycznej, a przede wszystkim stosowany przez rosyjskich badaczy oraz teoretyków w kontekście omawianych w pracy zagadnień. Dzięki jego zastosowaniu w rozprawie, możliwe staje się ujęcie problemu badawczego w sposób syntetyczny oraz wyczerpujący. Zarówno rosyjskie oddziaływanie informacyjne na odbiorców, jak i przeprowadzane przez Kreml cyberataki pozostają skorelowane oraz uzupełniają się wzajemnie, wobec czego nie można tych zjawisk traktować oraz omawiać oddzielenie. Dlatego też w ramach następnego podrozdziału zostało omówione pojęcie *propagandy* jako instrumentu prowadzenia wojny informacyjnej ze wskazaniem jej definicji, rodzajów oraz wykorzystywanych technik i metod, a także scharakteryzowane zostało zjawisko *cyberataków*, ich pojęcie oraz cechy cyberprzestrzeni, jak również metody i techniki wykorzystywane do ich przeprowadzania.

2.3.1. Propaganda jako instrument prowadzenia wojny informacyjnej

Zjawisko przepływu informacji towarzyszy człowiekowi od zarania dziejów. Wraz z nim pojawiło się jego następstwo, jakim jest szeroko rozumiane zagadnienie zniekształcania informacji między innymi poprzez wszelkiego rodzaju manipulacje, dezinformację czy wreszcie propagandę. Rewolucja informacyjna z którą związany jest niespotykany dotąd w historii rozwój środków masowego przekazu oraz nowoczesnych technologii informacyjnych sprawia, że możliwe jest wręcz nieograniczone kolportowanie najróżniejszych treści, co z kolei może wywoływać daleko idące skutki, zwłaszcza w życiu społecznym (publicznym). O znaczeniu rozwoju środków masowego przekazu pisali już między innymi S. Kuśmierski oraz A. Frydrychowicz, którzy zauważyli, że „elektroniczny przekaz, wtargnąwszy do naszego domu dokonuje poważnych zmian w naszej świadomości i w sposobie naszego życia. Kolejne wynalazki będą pogłębiały te zmiany”⁴⁶³ oraz że „postęp w dziedzinie

⁴⁶³ S. Kuśmierski, A. Frydrychowicz: *Podstawy wiedzy o propagandzie*. Warszawa 1980, s. 12.

nowoczesnego przekazu i utrwalania informacji przeobraża nie tylko nasze życie codzienne, ale wywiera także wpływ na politykę międzynarodową⁴⁶⁴. Z kolei za sprawą masowego przekazu oraz technologii informacyjnych „kształtowane są stosunki międzynarodowe, realizowana jest polityka zagraniczna oraz kształtowane są poglądy obywateli i ich preferencje polityczne, społeczne uwarunkowania i wynikające z tego wybory kulturowe”⁴⁶⁵. Należy jednak zauważyć, że wyeliminowanie zjawiska zniekształcania informacji (bez względu na zastosowane środki) jest niemożliwe. Wskazuje na to V. Volkoff, który pisał, że „odmienność punktów widzenia niedoskonałość percepcji, różna ocena względnego znaczenia wydarzeń sprawia jednak, że każda lub niemal każda informacja zawiera w sobie pewien, chociażby najmniejszy ładunek dezinformacji”⁴⁶⁶. W jego ocenie informacja jest dezinformująca z samej swej natury i taka pozostanie. Dalej pisze, że przecież nawet prozaiczne przejrzenie się w lustrze nie może być pozbawione pewnej dozy dezinformacji, gdyż tafla szklana lustra, nasz wzrok, oświetlenie czy nasz nastrój w większym lub mniejszym stopniu dezinformują nasze postrzeganie lustrzanego odbicia⁴⁶⁷. To jakże trafne spostrzeżenie powinno zostać odniesione do przestrzeni publicznej, gdzie pojedyncze jednostki bądź ich grupy – będąc zainteresowane osiągnięciem konkretnych celów – podejmują działania zmierzające do wykreowania określonej oceny poszczególnych osób, zjawisk czy stanów rzeczy. Działania takie mogą być szczególnie niebezpieczne w państwach demokratycznych, gdzie opinia publiczna, będąc jednocześnie suwerenem, dokonuje wyboru władzy ustawodawczej, a pośrednio również wykonawczej i sądowniczej. Wybrani przez wyborców decydenci polityczni będą z kolei kreować cele oraz kierunki realizowanej przez państwo polityki zagranicznej. W odniesieniu do omawianego w niniejszej rozprawie problemu badawczego należy zauważyć, że przedsięwzięcia podejmowane przez wskazane wyżej jednostki bądź ich grupy mogą być częścią prowadzonych przez państwa wojen informacyjnych. Powyższe działania można nazwać mianem szeroko rozumianego oddziaływania informacyjnego na odbiorców z wykorzystaniem różnorodnych metod i technik, przy czym najczęściej w powyższym zakresie odnosi się to do zjawiska propagandy. W związku z tym w dalszej kolejności została omówiona definicja terminu propaganda, jej rodzaje oraz wykorzystywane techniki i metody.

⁴⁶⁴ Ibidem, s. 12.

⁴⁶⁵ R. Rajczyk: *Oblicza współczesnej propagandy. Przypadek chińsko-tajwańskiej wojny informacyjnej*. Katowice, 2019, s. 7-14.

⁴⁶⁶ V. Volkoff: *Dezinformacja. Oręż wojny*. Warszawa 1990, s. 5.

⁴⁶⁷ Ibidem, s. 5.

2.3.1.1. Definicja pojęcia propaganda

Propaganda nie jest zjawiskiem nowym, jednakże jej rozumienie i znaczenie ulega ciągłej ewolucji w dyskursie naukowym, toteż sam termin nie jest zdefiniowany w sposób jednoznaczny w literaturze. Omówienia pojęcia propagandy nie sposób nie rozpocząć od scharakteryzowania słownikowego znaczenia tego terminu. Propaganda, od łacińskiego *propagare*, oznacza *rozmnażać, siać, rozszerzać*. Jest to również „celowe oddziaływanie na zbiorowości i jednostki zmierzające do pozyskania zwolenników i sojuszników, wpojenia pożądanych przekonań i wywołania określonych dążeń i zachowań”⁴⁶⁸. Zdecydowanie bardziej rozbudowane definicje znajdują się w literaturze specjalistycznej.

M. Kolczyński zauważył, że kryteria nowoczesnej, ukierunkowanej na ogół obywateli propagandy, realizowanej przy użyciu środków masowego przekazu, spełniały działania podejmowane przez jej dysponentów w okresie I wojny światowej. Niemniej jednak pełnię swojego rozwoju propaganda osiągnęła w latach dwudziestych, trzydziestych i czterdziestych XX wieku. Wskazał również, że w „okresie międzywojennym sformułowano podstawowe koncepcje, stanowiące załączek współczesnych teorii komunikowania politycznego; szczególna rola w tym względzie przypadła dwóm amerykańskim ośrodkom badawczym: *The Institute for Propaganda Analysis* założonemu w 1937 roku (...) oraz *Bureau of Applied Social Research* w Columbia University — powstałe także w 1937 roku”⁴⁶⁹. S. Kuśmierski oraz A. Frydrychowicz wyróżnili natomiast trzy zasadnicze grupy definicji, dzieląc je na „odwołujące się do tradycji socjologicznej, na definicje określające zjawisko propagandy ze stanowiska psychologii społecznej i na definicje ujmujące fenomen propagandy w kategoriach politologicznych”⁴⁷⁰. Wskazują oni zatem, że definicje propagandy mogą być różne w zależności od stopnia nasycenia w nich elementów psychologicznych, socjologicznych oraz politologicznych. Wydaje się, że taki podział znajduje swoje uzasadnienie wobec faktu, że termin propaganda jest pojęciem interdyscyplinarnym, które w zależności od występowania w danym dziale nauki będzie realizować inne cele i funkcje oraz posługiwać się innymi środkami oraz metodami. J. Sztumski zdefiniował z kolei pojęcie propagandy jako metody „oddziaływania na dowolnie liczne zbiory ludzi, którego celem jest wywieranie wpływu na kształtowanie ich myślenia, postaw, przekonań i zachowań w stosunku do spraw publicznych

⁴⁶⁸ Encyklopedia PWN: *propaganda*. <https://encyklopedia.pwn.pl/haslo/propaganda;3962718.html> (dostęp: 23.12.2021).

⁴⁶⁹ M. Kolczyński: *Strategie komunikowania politycznego*. Katowice 2008, s. 74.

⁴⁷⁰ S. Kuśmierski, A. Frydrychowicz: *Podstawy wiedzy o propagandzie*. Warszawa 1980, s. 29.

lub określonych wartości politycznych, religijnych, moralnych itp., zgodnie z życzeniem tego, kto tym właśnie sposobem posługuje się lub go firmuje”⁴⁷¹. J. Kossecki natomiast określił propagandę jako „planowe oddziaływanie na psychikę ludzi za pomocą rozpowszechnianych w skali masowej bodźców o charakterze informacyjnym, zmierzające do ukształtowania u nich odpowiednich norm społecznych lub spowodowania odpowiednich działań”⁴⁷².

Podobnie termin propaganda jest definiowany w literaturze zagranicznej. V. O'Donnell i G. S. Jowett, rozpoczynając rozważania w zakresie definicji omawianego pojęcia, w pierwszej kolejności przytoczyli wydarzenia związane utworzeniem w 1622 roku przez Watykan *Sacra Congregatio de Propaganda Fide*, czyli Kongregacji do spraw Ewangelizacji Narodów. Nie przypadkowa pozostaje również data powstania wskazanej instytucji, gdyż jej podstawowym celem było szerzenie wiary chrześcijańskiej (Kościoła rzymskokatolickiego) w Nowym Świecie oraz przeciwstawienia wpływom protestantów w Europie. Dalej wskazują, że w związku z powyższym wydarzeniem słowo *propagare* utraciło swój neutralny wydźwięk przyjmując znaczenie pejoratywne⁴⁷³. Inny pogląd wyraził natomiast S. Macdonald, który stwierdził, że nastąpiło to dopiero wraz z pojawieniem się nazistów i komunistów⁴⁷⁴. Kolejny badacz L. Fraser pisze, że propaganda to „sztuka zmuszania ludzi do robienia tego, czego by nie zrobili, gdyby dysponowali wszystkimi danymi dotyczącymi sytuacji”⁴⁷⁵. Z kolei W. Schram definiuje ją jako modyfikowanie „postaw i opinii oraz efektów funkcjonowania w grupie”⁴⁷⁶. H. Lasswell postrzegał propagandę jaką zarządzanie zbiorowymi postawami poprzez manipulowanie istotnymi symbolami. W odniesieniu do tej definicji M. Bartoszewicz wskazał, że „do zadań propagandystów w takim ujęciu zaliczać się miały przede wszystkim: intensyfikacja postaw sprzyjających interesom dysponenta propagandy, odwracanie (neutralizacja) postaw wrogich, przyciąganie uwagi osób dotychczas obojętnych wobec poruszanej tematyki, a także zapobieganie wrogim zabiegom propagandowym”⁴⁷⁷. N. O'Shaughnessy z kolei określa propagandę jako emocjonalną manipulację mającą na celu przekazywanie idei oraz ideologii⁴⁷⁸. B. Dobek-Ostrowska przytoczyła natomiast jedną z ważniejszych definicji prezentowanego pojęcia, a sformułowaną przez W. W. Bidelle'a

⁴⁷¹ J. Sztumski: *Propaganda – jej problemy i metody*. Katowice 1990, s. 30.

⁴⁷² J. Kossecki: *Totalna wojna informacyjna XX wieku a II RP*. Kielce 1997, s. 2.

⁴⁷³ G. S. Jowett, V. O'Donnell: *Propaganda and Persuasion*. Thousand Oaks 2012, s. 2.

⁴⁷⁴ S. Macdonald: *Propaganda and Information Warfare in the Twenty-First Century. Altered images and deception operations*. Abingdon 2007, s. 32.

⁴⁷⁵ R. Rajczyk: *Nowoczesne wojny informacyjne*. Warszawa 2016, s. 24.

⁴⁷⁶ Ibidem, s. 24

⁴⁷⁷ M. Bartoszewicz: *Teorie propagandy w obliczu algorytmizacji internetowego komunikowania społecznego*. „Kultura Współczesna” 2019, nr 1(104), s. 84-86.

⁴⁷⁸ N. O'Shaughnessy: *Politics and propaganda. Weapons of mass seduction*. Manchester 2004, s. 37-49.

w 1931 roku zgodnie z którą „pod wpływem propagandy, każda jednostka zachowuje się tak, jak gdyby jej reakcje były wynikiem jej własnej decyzji. Wiele jednostek można zmusić do takiego samego zachowania, przy czym każdą pozornie kierują jej własne sądy”⁴⁷⁹. Sama zdefiniowała propagandę jako komunikowanie „jednostronne, zinstytucjonalizowanie, intencjonalne, które ma zaspokoić życzenia nadawcy, zaprogramowane i profesjonalnie realizowane informacyjno-perswazyjne, które nie polega na przemocy ani na przekupstwie, wspierane technikami marketingowymi i socjotechniką”⁴⁸⁰. Wreszcie przytoczyć należy poglądy „ojca *public relations*”, E. L. Bernays’a, który stwierdził, że „propaganda jest konsekwentnym, trwałym wysiłkiem tworzenia lub kształtowania wydarzeń w celu wpłynięcia na stosunek społeczeństwa do jakiegoś przedsięwzięcia, idei lub grupy”⁴⁸¹. Z kolei J. Ellul uważa, że propaganda to „zestaw metod stosowanych przez zorganizowaną grupę, która chce doprowadzić do czynnego lub biernego udziału ludzkich mas, wśród których dochodzi do wytworzenia jedności psychicznej w wyniku manipulacji i włączenia do organizacji”⁴⁸². V. O’Donnell i G. S. Jowett poza terminem propaganda wyróżnili również pojęcie *subpropagandy*, określanej mianem komunikacji ułatwiającej. Przez termin ten należy rozumieć prowadzenie w stosunku do odbiorcy działań polegających na utrzymaniu z nim stałego kontaktu, do czasu aż konieczne będzie rozpoczęcie przeciwko niemu właściwych działań propagandowych. Do przykładów można zaliczyć udzielanie pomocy finansowej podmiotom, wydawanie książek czy czasopism, prowadzenie zajęć, czy też po prostu prowadzenie kontaktów towarzyskich, wszystko po to, aby wytworzyć u odbiorcy przyjazną atmosferę relacji oraz poczucie zaufania, co w dogodnym momencie dysponent propagandy wykorzysta do realizacji własnych celów⁴⁸³.

Z powyższych definicji należy wywnioskować, że działalność propagandowa jaką prowadzi jej dysponent może przybrać charakter ofensywny, czy też kontekst militarny. Nie jest to jedynie hipotetyczne założenie, gdyż definicje omawianego pojęcia można odnaleźć również w dokumentach o ściśle wojskowym charakterze. I tak na przykład w „Słowniku terminów i definicji NATO” propaganda jest definiowana jako „informacje, szczególnie te o charakterze tendencyjnym lub wprowadzające w błąd, wykorzystywane w celach politycznych lub do promowania poglądów”⁴⁸⁴. W słowniku opracowanym przez Biuro

⁴⁷⁹ B. Dobek-Ostrowska: *Komunikowanie polityczne i publiczne. Podręcznik akademicki*. Warszawa 2007, s. 204.

⁴⁸⁰ Ibidem, s. 207.

⁴⁸¹ E. L. Bernays: *Propaganda*. New York 1928, s. 25.

⁴⁸² J. Ellul: *Propaganda: The formation of mens attitudes*. New York 1973, s. 61.

⁴⁸³ G. S. Jowett, V. O’Donnell: *Propaganda and Persuasion...*, s. 27-29.

⁴⁸⁴ Biuro Standaryzacji NATO: *Słownik terminów...*, s. 364.

Bezpieczeństwa Narodowego pojęcie propagandy jest utożsamiane z terminem dezinformacji i obejmuje „rozpowszechnianie zmanipulowanych lub sfabrykowanych informacji (albo kombinacji jednych i drugich), w celu skłonienia ich odbiorców do określonych zachowań korzystnych dla dezinformującego, lub też w celu odwrócenia ich uwagi od faktycznie zaistniałych wydarzeń”⁴⁸⁵. Z kolei w „Słowniku terminów z zakresu bezpieczeństwa narodowego” propaganda nie funkcjonuje jako samodzielne pojęcie, ale wskazuje się, że należy do niezbrojnych środków przemocy gospodarczej⁴⁸⁶ czy też rodzaju działalności dywersyjnej⁴⁸⁷.

Omawiając pojęcie propagandy należy również wspomnieć, że po II wojnie światowej termin ten zaprzestał być szeroko używany przez badaczy z uwagi na jego pejoratywny charakter. Jego negatywne konotacje spowodowały, że zaczęto zdecydowanie szerzej stosować pojęcie *komunikowanie polityczne*, które miało zdecydowanie bardziej neutralne zabarwienie. Nie zmienia to jednak faktu, że propaganda nadal pozostała propagandą, na co nie ma żadnego wpływu jej nazewnictwo⁴⁸⁸. Co więcej, w odniesieniu do zaprezentowanego problemu badawczego należy zaznaczyć, że wojnom informacyjnym zdecydowanie bliższe jest właśnie to pojęcie (propagandy), aniżeli stosowane zamienniki, które nie oddają w przedmiotowym kontekście właściwego charakteru tego terminu.

Uwzględniając powyższe rozważania terminologiczne dotyczące pojęcia propagandy sformułowano następującą jej definicję w oparciu o przyjęty problem badawczy. Propaganda to zaplanowana oraz zorganizowana działalność podmiotów państwowych oraz wysoko zorganizowanych, która jest realizowana w oparciu o szereg metod takich jak dezinformacja, manipulacja, perswazja oraz oddziaływanie emocjonalne na świadomość opinii publicznej, grup społecznych oraz jednostek. Jej celem jest kreowanie, ukierunkowywanie oraz modyfikowanie poszczególnych zachowań wymienionych wyżej podmiotów zgodnie z celem dysponenta propagandy. Ponad powyższe, przydatna na gruncie niniejszej rozprawy z uwagi na przyjęty problem badawczy będzie również definicja zaproponowana przez E. L. Bernaysa, który stwierdził, że „propaganda jest konsekwentnym, trwałym wysiłkiem tworzenia lub kształtowania wydarzeń w celu wpłynięcia na stosunek społeczeństwa do jakiegoś

⁴⁸⁵ Biuro Bezpieczeństwa Narodowego: (MINI)Słownik BBN. Propozycje nowych terminów z dziedziny bezpieczeństwa: propaganda. <https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html> (dostęp: 26.12.2021).

⁴⁸⁶ J. Kaczmarek, W. Łepkowski, B. Zdrodowski (Red.): *Słownik terminów...*, s. 78.

⁴⁸⁷ Ibidem, s. 34.

⁴⁸⁸ B. Dobek-Ostrowska, J. Fras, B. Ociepka: *Teoria i praktyka...*, s. 32.

przedsięwzięcia, idei lub grupy”⁴⁸⁹. Drugą przydatną oraz przyjętą w roli uzupełniającej definicją jest ta sformułowana przez J. Ellul, który zdefiniował propagandę jako „zestaw metod stosowanych przez zorganizowaną grupę, która chce doprowadzić do czynnego lub biernego udziału ludzkich mas, wśród których dochodzi do wytworzenia jedności psychicznej w wyniku manipulacji i włączenia do organizacji”⁴⁹⁰.

2.3.1.2. Rodzaje propagandy

J. Ellul twierdził, że termin propaganda jest niezwykle złożony i nie może zostać ujęty jedynie w prezentowanych wyżej definicjach. Co więcej, zauważył i wskazał na różnice jakie zachodzą w amerykańskim i rosyjskim rozumieniu pojęcia propaganda pod względem stosowanych metod i technik psychologicznych⁴⁹¹. Klasyczna typologia propagandy, będąca jednocześnie jedną z najpopularniejszych, obejmuje podział na propagandę białą, szarą oraz czarną, a więc jest to klasyfikacja ze względu na stopień zafałszowania treści oraz jego jawność⁴⁹². Jak pisze S. Kuśmierski i A. Frydrychowicz, propaganda biała jest łatwo rozpoznawalna oraz identyfikowalna. Dysponent propagandy nie ukrywa celu swojego działania, przedstawiając swoje poglądy jako najlepsze oraz budując poczucie zaufania wśród odbiorców. Dysponentem propagandy białej są najczęściej oficjalne instytucje państwowe firmujące swoją działalność na zewnątrz, zgodnie z faktycznym stanem rzeczy⁴⁹³. Doskonałym przykładem białej propagandy może być Radio Wolna Europa⁴⁹⁴ oraz Radio Moskwa⁴⁹⁵. Przeciwnieństwem propagandy białej jest propaganda czarna, która utrudnia lub uniemożliwia identyfikację źródła danego przekazu informacyjnego. Przekaz ten jest z kolei fałszywym wytworem dysponenta propagandy, a do jego cech charakterystycznych trzeba zaliczyć kolportowanie sfabrykowanych, zmanipulowanych oraz fałszywych treści. W związku z powyższym należy zauważyć, że rozpoznanie rzeczywistego nadawcy przekazu będzie wiązać się z nieuniknionym fiaskiem działań dysponenta propagandy w konsekwencji utraty zaufania przez odbiorcę⁴⁹⁶. Ostatnim z typów jest propaganda szara, która łączy w sobie elementy propagandy białej i czarnej, przez co należy rozumieć podejmowanie działań,

⁴⁸⁹ E. L. Bernays: *Propaganda...*, s. 25.

⁴⁹⁰ J. Ellul: *Propaganda: The formation of mens...*, s. 61.

⁴⁹¹ J. Ellul: *Propagandes*. Paris 1962, s. 75.

⁴⁹² G. S. Jowett, V. O'Donnell: *Propaganda and Persuasion...*, s. 17-27.

⁴⁹³ S. Kuśmierski, A. Frydrychowicz: *Podstawy wiedzy...*, s. 46-48.

⁴⁹⁴ B. Dobek-Ostrowska, J. Fras, B. Ociepka: *Teoria i praktyka...*, s. 33.

⁴⁹⁵ G. S. Jowett, V. O'Donnell: *Propaganda and Persuasion...*, s. 17.

⁴⁹⁶ H. M. Kula: *Propaganda współczesna. Istota – właściwość*. Warszawa 2005 s. 101.

w wyniku których ustalenie źródła komunikatu nie jest niemożliwe lub utrudnione, jednak sam przekaz jest nieprecyzyjny i nie jest w pełni fałszywy. Głównym celem jej stosowania jest podważanie wiarygodności i kompetencji oraz prawdomówności rywala⁴⁹⁷.

Następną typologią, którą można wyróżnić jest dokonanie podziału propagandy ze względu na rodzaje (sfery) oddziaływania. H. M. Kula przytacza tutaj propagandę werbalną (słowną), propagandę wizualną oraz propagandę realizowaną za pomocą środków masowego przekazu i środków technicznych⁴⁹⁸. Propaganda werbalna sprowadza się do wykorzystywania słowa jako narzędzia, a więc przede wszystkim jest stosowana podczas bezpośredniego kontaktu propagandzisty z odbiorcą. Propaganda wizualna z kolei wykorzystuje bodźce optyczne posługując się takimi elementami jak znak, symbol, barwa, światło, słowo przedstawione graficznie, czy ruch. Ostatni ze wskazanych typów propagandy obejmuje połączenie dwóch poprzednich poprzez wykorzystanie środków masowego przekazu jak prasa, radio, telewizja, a współcześnie Internet⁴⁹⁹. W odniesieniu do omawianej sfery oddziaływania, inną nazewniczo klasyfikację zaproponowała B. Dobek-Ostrowska dokując podziału na propagandę wizualną, audytywną oraz audiowizualną. Każdy z wymienionych wyżej typów odpowiada kolejno typom zaproponowanym przez H. M. Kulę⁵⁰⁰.

Kolejna typologia z uwagi na treść dokonuje podziału na propagandę społeczną (socjologiczną), polityczną, ekonomiczną, zdrowotną, naukową, edukacyjną, sportową itp., przy czym z uwagi na omawiany problem badawczy scharakteryzowane zostaną tylko dwa pierwsze z wymienionych typów⁵⁰¹. I tak na przykład J. Ellul stwierdził, że propaganda społeczna, inaczej zwana również socjologiczną, wychodzi poza granice zamkniętych kręgów społecznych, nie ograniczając się tym samym do jakiegoś konkretnego z nich. Jej zadaniem jest integracja jak największej liczby jednostek według określonego modelu oraz rozpowszechnianie określonego stylu życia wewnątrz danej zbiorowości. W jej obrębie znajdują się również inne rodzaje propagandy takie jak chociażby polityczna czy religijna oraz związana z innymi nurtami ideologicznymi. Jedną z najważniejszych cech propagandy społecznej jest jej spontaniczny charakter oraz brak struktur zarządzania, co odróżnia ją od propagandy politycznej. Nie ma tutaj zatem zorganizowanych kampanii i specjalistów, ponieważ każdy członek grupy może być potencjalnym propagandzistą (dysponentem

⁴⁹⁷ S. Kuśmierski, A. Frydrychowicz: *Podstawy wiedzy...*, s. 47-48.

⁴⁹⁸ H. M. Kula: *Propaganda współczesna...*, s. 89.

⁴⁹⁹ Ibidem, s. 90-92.

⁵⁰⁰ B. Dobek-Ostrowska: *Komunikowanie polityczne i publiczne...*, s. 228-231.

⁵⁰¹ B. Dobek-Ostrowska, J. Fras, B. Ociepka: *Teoria i praktyka...*, s. 30-31.

propagandy)⁵⁰². Odmienne założenia występują w przypadku propagandy politycznej. Jest to zorganizowany instytucjonalnie zbiór technik i metod wpływania na obywateli przez instytucje władzy państwowej, partie polityczne, administrację, elity polityczne, grupy nacisku oraz inne⁵⁰³. Jak piszą B. Dobek-Ostrowska, J. Fras oraz B. Ociepka, „realizacja tego typu propagandy opiera się zarówno na wolontariuszach, jak i aparacie do tego celu powołanym. Najlepiej zbadanymi i dobrze znanymi przykładami propagandy politycznej jest propaganda hitlerowska i stalinowska. Nie można jednak zapominać, że propaganda nie jest zarezerwowana jedynie dla systemów totalitarnych. Jest ona uprawiana także w systemach demokratycznych, i to z dużym powodzeniem”⁵⁰⁴. W odniesieniu do tego stwierdzenia, należy wskazać na szczególny rodzaj propagandy politycznej jakim jest propaganda wyborcza. Jest ona nieodłącznym elementem wszystkich kampanii wyborczych, a jej celem jest pozyskanie jak największej liczby głosów (wyborców), co z kolei ma zapewnić zdobycie władzy przez określone podmioty. Typ ten opiera się przede wszystkim na metodach i technikach z zakresu marketingu politycznego i wyborczego⁵⁰⁵.

Następna typologia to podział propagandy ze względu na kierunek jej oddziaływania, a więc na propagandę wewnętrzną i zewnętrzną. S. Kuśmierski i A. Frydrychowicz piszą, że przez propagandę wewnętrzną „rozumimy perswazyjne oddziaływanie na obywateli własnego państwa. Jest ono oparte na dobrowolnym nakłanianiu i uświadamianiu im celów i interesów oraz odpowiadających tym interesom działań służących całej wspólności obywateli, a także każdemu z nich z osobna”⁵⁰⁶. Działalność taka jest typowa dla wszystkich państw bez względu na występujący w nich ustrój polityczny. Propaganda zewnętrzna jest z kolei skierowana do społeczności (obywateli) innych państw oraz jest uwarunkowana aktualną sytuacją międzynarodową. Należy przez to rozumieć, że nawet drobna zmiana w stosunkach pomiędzy poszczególnymi państwami powoduje zmiany w zakresie formy i treści wymienianych pomiędzy nimi komunikatów⁵⁰⁷. Ponadto propaganda zewnętrzna jest „jednym ze środków wojny psychologicznej. Ten typ działalności propagandowej ma duże znaczenie w czasie wojny, choć występuje także w okresie pokoju”⁵⁰⁸. B. Dobek-Ostrowska poczyniła również w tym zakresie swoje spostrzeżenia pisząc, że „propaganda zewnętrzna to także działania

⁵⁰² J. Ellul: *Propagandes...*, s. 75-84.

⁵⁰³ J. Ellul: *Propaganda: The formation...*, s. 62-70.

⁵⁰⁴ B. Dobek-Ostrowska, J. Fras, B. Ociepka: *Teoria i praktyka...*, s. 31-32.

⁵⁰⁵ Ibidem, s. 32.

⁵⁰⁶ S. Kuśmierski, A. Frydrychowicz: *Podstawy wiedzy...*, s. 45.

⁵⁰⁷ H. M. Kula: *Propaganda współczesna...*, s. 98-99.

⁵⁰⁸ S. Kuśmierski, A. Frydrychowicz: *Podstawy wiedzy...*, s. 45.

w zakresie *public relations*, mające na celu promowanie i kształtowanie pozytywnego wizerunku państwa na scenie międzynarodowej”⁵⁰⁹.

Kolejną typologią jest podział z uwagi na sposób rozpowszechniania propagandy. Zaliczamy do niej propagandę bezpośrednią – interaktywną, a także pośrednią – impersonalną. Pierwsza z nich jest jednym z podstawowych typów, z kolei do czasu pojawienia się mediów masowych stanowiła w zasadzie jedyną dostępną formę kolportowania komunikatów propagandowych. Jej cechą charakterystyczną jest przede wszystkim bezpośredni kontakt dysponenta propagandy z odbiorcą komunikatu. Zaletą tej formy przekazu jest możliwość ciągłego kontrolowania słuchaczy i ewentualna zmiana formułowanego przekazu poprzez dostosowanie do reakcji audytorium. Do formy propagandy bezpośredniej zaliczamy spotkania z osobami publicznymi takimi jak politycy, funkcjonariusze państwowi, przedstawiciele aparatu władzy oraz innych struktur organizacyjnych, którzy stosują przekazy propagandowe. Zauważyć jednak należy, że „w dobie mediatyzacji społeczeństwa zaawansowania rozwoju nowych technologii w dziedzinie komunikowania masowego propaganda bezpośrednia, choć uważana za bardzo skuteczną, ma ograniczony zasięg oddziaływania. Współcześnie należy ją uznać za formę komplementarną, a nie zasadniczą wszelkich kampanii propagandowych”⁵¹⁰. Drugim z typów w ramach omawianej typologii jest propaganda pośrednia, a więc taka, której podstawą są środki masowego przekazu. Należy zatem wskazać, że wzrost jej znaczenia nastąpił wraz z postępującą od XX wieku rewolucją informacyjną oraz rozwojem nowych technologii, w szczególności technologii komunikowania. Owe masowe komunikowanie posiada pięć cech charakterystycznych na które wskazuje za J. R. Bittnerem B. Dobek-Ostrowska, pisząc o „istnieniu środków masowego przekazu, które są pośrednikami w procesie przenoszenia informacji od nadawcy do odbiorcy; ograniczonych kanałach sensorycznych zaangażowanych w proces przekazu propagandowego (wzrok i słuch); impersonalnym charakterze przekazu, polegającym na braku osobistego kontaktu autora tekstu propagandowego z odbiorcą; funkcji *gatekeepera* mediów, polegającej na dowolnej prezentacji materiału pochodzącego ze źródła propagandy (ograniczanie, rozszerzanie, reorganizacja lub reinterpretacja informacji skonstruowanej przez nadawcę pierwotnego); opóźnionym sprzężeniu zwrotnym, które nie pozwala autorowi propagandy na natychmiastową reakcję w razie szumów i zakłóceń w procesie przekazu”⁵¹¹. W odniesieniu do propagandy pośredniej należy również przytoczyć klasyfikację, na którą wskazują S. Kuśmierski i A. Frydrychowicz

⁵⁰⁹ B. Dobek-Ostrowska, J. Fras, B. Ociepka: *Teoria i praktyka...*, s. 36.

⁵¹⁰ Ibidem, s. 42.

⁵¹¹ Ibidem, s. 42-43; Zobacz szerzej: J. R. Bittner: *Mass Communication. And Introduction*. New Jersey 1989.

pisząc o propagandzie pośredniej: audiatywnej masowej (np. radio, płyty), audiatywnej stosowanej audytoryjnie (np. magnetofon), audiowizualnej masowej (np. film, telewizja), audiowizualnej audytoryjnej (np. udźwiękowione przeźrocza), wizualnej (np. prasa, plakat, transparent, fotografia)⁵¹². Choć z uwagi na rozwój nowych technologii wymienione wyżej urządzenia mogą nie być już powszechnie stosowane, to ich dzisiejsze odpowiedniki można zaklasyfikować zgodnie z powyższą typologią.

Jedynie uzupełniającą warto wspomnieć, że do innych typologii propagandy można zaliczyć również podział ze względu na przebieg procesu propagandowego w społeczeństwie. W tym kontekście wyróżniamy propagandę horyzontalną – poziomą (odnoszącą się do bieżących wydarzeń i zjawisk), jak również wertykalną – pionową (klasyczny typ propagandy politycznej funkcjonujący w oparciu o występowanie struktur zarządzających oraz środków masowego przekazu)⁵¹³. Ostatnim rodzajem o którym należy wspomnieć jest podział z uwagi na zależność w czasie, między przekazem a wydarzeniami, których przekaz dotyczy. Wyodrębniamy w związku z tym propagandę poprzedzającą (poprzedza wydarzenia, które dopiero nastąpią w niedalekiej przyszłości – najczęściej zaplanowane), następczą (występującą po zajściu określonych zdarzeń) oraz towarzyszącą (działania współistniejące z danymi zdarzeniami, będące następstwem natychmiastowej reakcji dysponenta propagandy na ich zaistnienie)⁵¹⁴.

2.3.1.3. Techniki i metody propagandy

Działalność propagandowa, jak każda działalność celowa, powinna realizować określone funkcje jak i przestrzegać określonych zasad, które umożliwiają jej skuteczne prowadzenie w oparciu o wykorzystywanie metod i technik propagandowych. B. Dobek-Ostrowska za J. Ellulem⁵¹⁵ wyróżniła w powyższym zakresie grupę pięciu funkcji propagandy zaliczając do nich następujące funkcje: integracyjną, adaptacyjną, informacyjno-interpreacyjną, dezinformacyjną i demaskatorską. Pierwsza z nich – funkcja integracyjna – realizuje cel jakim jest zapewnienie stabilizacji istniejącego systemu politycznego oraz społecznego poprzez wzmocnienie już istniejących struktur. Funkcja adaptacyjna, zwana również agitacyjną lub agitatywną, sprowadza się do działania w kierunku motywowania ludzi

⁵¹² S. Kuśmierski, A. Frydrychowicz: *Podstawy wiedzy...*, s. 48.

⁵¹³ B. Dobek-Ostrowska, J. Fras, B. Ociepka: *Teoria i praktyka...*, s. 39-40.

⁵¹⁴ J. Ellul: *Propagandes...*, s. 94-98; H. M. Kula: *Propaganda współczesna...*, s. 95-96.

⁵¹⁵ Zobacz szerzej: J. Ellul: *Propagandes*. Paris 1990.

do podejmowania określonych działań. Jej celem jest uzyskanie akceptacji dla określonych ideologii, nowych struktur władzy czy też wykształcenie nowych wzorów zachowań (przykładem realizacji omawianej funkcji może być rewolucja październikowa w trakcie której była stosowana propaganda leninowska). Trzecia z funkcji określana mianem informacyjno-interpretacyjnej sprowadza się do kreowania określonego przekazu przy wykorzystaniu danej informacji, a następnie dokonywaniu jej interpretacji zgodnie z założeniami dysponenta propagandy. Następną funkcją – dezinformacyjną – odnosi się do oddziaływania na przeciwnika poprzez tworzenie przekazów zawierających fałszywe informacje. Ostatnią funkcją jest funkcja demaskatorska, która polega na wykrywaniu informacji niezgodnych z prawdą, a zatem może być postrzegana jako konsekwencja funkcji dezinformacyjnej⁵¹⁶. Zbliżoną klasyfikację zaproponowali S. Kuśmierski i A. Frydrychowicz, którzy wyróżnili takie funkcje jak: ideowo-wychowawcza, integracyjna, inspiratorska, integracyjno-dezintegracyjna, informacyjno-interpretująca oraz demaskatorska⁵¹⁷.

Skuteczność oddziaływania informacyjnego (stosowania propagandy) zależy nie tylko od realizacji wskazanych wyżej funkcji, ale również od przestrzegania szeregu socjotechnicznych zasad przez każdego jej dysponenta⁵¹⁸. J. Kossecki określa je mianem „współczynników przyswajalności propagandy” oraz sprowadza do grupy następujących dziewięciu zasad: prawdziwości, masowości i długotrwałości działania, informacji pożądanej, emocjonalnego pobudzania, zrozumiałości, specjalizacji, niestawiania kropki nad i, rzekomej oczywistości oraz stopniowania⁵¹⁹. Zasada prawdziwości odwołuje się do zgodności „informacji zawartych w komunikatach propagandowych z informacjami zawartymi w odpowiednich zbiorach oryginałów (o których społeczeństwo przekonuje się głównie poprzez osobiste doświadczenie)”⁵²⁰. Chodzi więc o to, aby dysponent propagandy odwoływał się przede wszystkim do faktów oraz doświadczeń odbiorców, co w konsekwencji ma wytworzyć poczucie zaufania i prawdziwości danego komunikatu. Z kolei propaganda kłamliwa może osiągać krótkotrwałe sukcesy, ponieważ gdy tylko jej odbiorcy zorientują się, że są wprowadzani w błąd, tracą do dysponenta propagandy zaufanie. Propaganda będzie więc skuteczna, jeśli opinia publiczna nie będzie miała możliwości zweryfikowania prawdziwości otrzymywanych informacji⁵²¹. Drugą z zasad jest zasada masowości i długotrwałości działania,

⁵¹⁶ B. Dobek-Ostrowska, J. Fras, B. Ociepka: *Teoria i praktyka...*, s. 29-30.

⁵¹⁷ S. Kuśmierski, A. Frydrychowicz: *Podstawy wiedzy...*, s. 53-57.

⁵¹⁸ J. Kossecki: *Socjotechnika propagandy politycznej*. „Zeszyty poznawcze” 1972, nr 3 (3) R. XIII, s. 15-26.

⁵¹⁹ T. R. Aleksandrowicz: *Podstawy walki informacyjnej...*, s. 86-87; Zobacz szerzej: J. Kossecki: *Cybernetyka społeczna*. Warszawa 1981, s. 434-455.

⁵²⁰ J. Kossecki: *Cybernetyka społeczna...*, s. 435.

⁵²¹ Ibidem, s. 435-438.

która odwołuje się do prawidłowości psychologicznych zgodnie z którymi ludzie dużo chętniej przyjmują, a następnie utożsamiają się z poglądami, które już wcześniej słyszeli z różnych źródeł, bądź też które wpajano im przez długi czas. Ważne jest również, aby taki przekaz nie miał charakteru monotonnego, gdyż może wytworzyć efekt odwrotny od zamierzonego poprzez wytworzenie odczucia znudzenia nieustannie powtarzanym, tym samym bodźcem⁵²². Trzecia zasada – informacji pożądanej – polega na przyjmowaniu przez odbiorców informacji z którymi się utożsamiają oraz które chcieliby, aby zmaterializowały się w rzeczywistości. J. Kossecki zauważa, że na powyższej zasadzie opiera się działanie propagandy demagogicznej, która „stara się wyczuwać wszelkie nastroje i pragnienia społeczeństwa, a potem odpowiednio je preparując, propaguje, podając jako prawdę, nie licząc się przy tym z reguły z rzeczywistością”⁵²³. Zasada emocjonalnego pobudzania z kolei zakłada, że dysponent propagandy powinien podejmować nieustanne działania w celu częstszego stosowania argumentacji nacechowanej emocjonalnie, aniżeli tej odwołującej się do logicznych argumentów zgodnych z zasadami logicznego rozumowania i doświadczenia życiowego. Dysponent powinien zatem odwoływać się przede wszystkim do emocji i uczuć oraz za ich pomocą kontrolować odbiorców. Kolejną z zasad jest zasada zrozumiałości, która polega na używaniu pojęć jasnych (zrozumiałych) dla społeczeństwa czy też po prostu odbiorców. Chodzi o to, aby dostosować używane słowa, znaki i symbole do poziomu wiedzy, inteligencji czy obycia rozmówcy tak, aby móc wywoływać określone skojarzenia pojęciowe w wyniku stosowania danego przekazu propagandowego. Zasada specjalizacji odnosi się do stosowania przekazu informacyjnego zgodnego z poziomem wiedzy oraz pojęć różnych środowisk, do których dociera i na które ma oddziaływać, przede wszystkim uwzględniać aktualny etap historycznego rozwoju danej zbiorowości. Siódma zasada, określona mianem zasady niestawiania kropki nad „i” wskazuje, że skuteczna propaganda musi pozostawiać pewną przestrzeń poznawczą, którą jej odbiorca powinien chcieć uzupełnić. Przekaz informacyjny nie powinien być wyczerpujący względem danego tematu, ale pozostawiać pewne aspekty wymagające wyjaśnienia, które ma uzupełnić odbiorca i w ten sposób wykreować pozytywne odczucie, że to on jest twórcą danych treści, a nie dysponent propagandy⁵²⁴. Przedostatnia, zasada rzekomej oczywistości, jak wskazuje J. Kossecki zakłada, że „udowadnia się inną tezę niż ta, którą chce się propagować, a przy tym tę zasadniczą tezę (którą się rzeczywiście propaguje) podaje jako pewnik niepodlegający dyskusji. Jest to już właściwie propaganda na

⁵²² J. Kossecki: *Socjotechnika propagandy politycznej...*, s. 20-21.

⁵²³ J. Kossecki: *Cybernetyka społeczna...*, s. 440.

⁵²⁴ Ibidem, s. 441-443.

pograniczu tzw. propagandy działającej na podświadomość, gdyż odbiorca, zastanawiając się nad słusnością innej tezy, przyjmuje niepostrzeżenie tezę podaną jako pewnik⁵²⁵. I wreszcie ostania – zasada stopniowania, nakazuje dokonywanie określonych zmian w systemie pojęć danego społeczeństwa poprzez wyjście od układu norm i systemu pojęć już istniejącego i znanego odbiorcy, co ma na celu stopniowe doprowadzenie ich do odpowiednich przekonań oraz twierdzeń, zgodnie z założeniami propagandzisty⁵²⁶.

Powyższy katalog nie ma charakteru enumeratywnego. W związku z tym należy przytoczyć ich podsumowanie sformułowane przez J. Kosseckiego, który stwierdził, że „wskazane powyżej zasady nie wyczerpują tematu, można by podać jeszcze wiele innych zasad skuteczności propagandy; zostały one wybrane jako te, które mają największe znaczenie”⁵²⁷. Propagandysta po zastosowaniu powyższych zasad może rozpocząć oddziaływanie informacyjne przy użyciu wybranych przez niego metod i technik. Termin *metoda* oznacza „celowo dobrany sposób oddziaływania umożliwiający zmianę systemu wartości bądź kierunku lub siły postaw, przekonań i poglądów człowieka bądź jego zachowań”⁵²⁸. Z kolei pod pojęciem *techniki* należy rozumieć „sposoby przemieszczania informacji od nadawcy do odbiorcy, sposoby budowania komunikatu oraz kodowania informacji”⁵²⁹.

Do trzech podstawowych metod propagandowych można zaliczyć takie jak: rzetelna perswazja (nakłanianie odbiorcy do podejmowania lub zaniechania określonych działań przy wykorzystaniu rzeczowych argumentów), sugestia (formułowanie przekazu propagandowego tak aby w konsekwencji wywoływał on u odbiorcy konkretne skutki), manipulacja (kreowanie stanów psychicznych i reakcji odbiorcy przez dysponenta propagandy bez ujawniania swojego celu)⁵³⁰. Następnie w ramach poszczególnych metod można wyróżnić konkretne techniki propagandowe, których w literaturze specjalistycznej można odnaleźć co najmniej kilkadziesiąt. Na potrzeby niniejszej rozprawy zostaną przedstawione wybrane z nich, pośród których znajdują się te najbardziej popularne oraz te które zostaną wykorzystane na dalszym etapie przygotowywania niniejszej rozprawy.

Jedna z najsłynniejszych typologii technik propagandy, stanowiąca załączek współczesnych teorii komunikowania politycznego, została opracowana przez Institute for Propaganda Analysis w 1937 roku⁵³¹. Instytut przedstawił pierwszą naukową klasyfikację

⁵²⁵ Ibidem, s. 443.

⁵²⁶ J. Kossecki: *Socjotechnika propagandy politycznej...*, s. 25.

⁵²⁷ J. Kossecki: *Cybernetyka społeczna...*, s. 445.

⁵²⁸ S. Kuśmierski, A. Frydrychowicz: *Podstawy wiedzy...*, s. 140.

⁵²⁹ Ibidem, s. 141.

⁵³⁰ H. M. Kula: *Propaganda współczesna...*, s. 141-144.

⁵³¹ M. Kolczyński: *Strategie komunikowania...*, s. 74.

technik propagandy wyróżniając spośród nich 7 następujących: *Name-Calling* (etykietowanie), *Glittering Generalities* (błyskotliwe ogólniki), *Transfer* (transfer), *Testimonial* (świadcstwo autorytetu), *Plain Folks* (prostego człowieka), *Card Stacking* (tasowania kart), *Bandwagon* (owczego pędu)⁵³². Pierwsza ze wskazanych technik polega na wywoływaniu u odbiorcy pejoratywnych skojarzeń, bez możliwości dokonania obiektywnej oceny danej treści. Druga sprowadza się do stosowania uproszczonego znaczenia terminów i zestawianiu ich z podstawowymi wartościami społecznymi, czy też używania wieloznacznych pojęć. Trzecia technika to dokonywanie transferu autorytetu z czegoś/kogoś szanowanego, na coś/kogoś innego tak aby to drugie również stało się szanowane. Czwarta z technik polega na tym, że szanowana lub znienawidzona osoba mówi, że coś lub ktoś jest dobre bądź złe. Piąta technika zakłada, że dane idee są przedstawiane jako dobre, ponieważ pochodzą z tej samej społeczności co idee czy wartości występujące w danej zbiorowości. Szósta z technik polega na selekcjonowaniu informacji prawdziwych oraz fałszywych w celu przedstawienia najlepszego lub najgorszego uzasadnienia kogoś lub czegoś. Ostatnia, siódma z technik zakłada wykorzystanie siły owczego pędu, czyli dopasowania przekazu propagandowego do opinii wyrażanych przez większość społeczeństwa (w tym grup bądź grupy)⁵³³. Jak już uprzednio wskazano, można wyróżnić kilkadziesiąt różnych technik propagandowych, jednakże z uwagi na przedmiot niniejszej rozprawy poniżej zostaną omówione jedynie wybrane z nich, które w ocenie autora pozostają najistotniejsze w związku z przedmiotem prowadzonych w niniejszej pracy badań.

Jedną z częściej występujących i stosowanych, nie tylko przez media, ale również przez znaczną część nadawców w życiu codziennym jest technika *argumentum ad personam*. W jej przypadku mamy do czynienia z całkowicie pozamerytoryczną argumentacją w sporze, a jedynie z odwoływaniem się do osoby przeciwnika (w kontekście jego właściwości i warunków osobistych, czy też dokonań, poczynań). Technika ta jest wykorzystywana najczęściej w sytuacji, w której oponent nie posiada już żadnych merytorycznych argumentów na uzasadnienie swoich tez⁵³⁴. Następną techniką jest technika podpowiedzi emocjonalnej, która polega na sugerowaniu odbiorcy danego komunikatu oczekiwanej od propagandysty reakcji na wytworzony przez niego przekaz, przy jednoczesnym użyciu różnego rodzaju środków wyrazu. Można dla przykładu zaliczyć do nich kolorystykę, wielkość czcionek czy

⁵³² G. S. Jowett, V. O'Donnell: *Propaganda and Persuasion...*, s. 237

⁵³³ Ibidem, s. 237; M. Kolczyński: *Strategie komunikowania...*, s. 91.

⁵³⁴ A. Schopenhauer: *Erystyka czyli sztuka prowadzenia sporów*. Warszawa 2010, s. 104-109.

podkład dźwiękowy towarzyszący danej treści⁵³⁵. Kolejną techniką jest wzbudzanie strachu/lęku w odbiorcach, znana również pod nazwą *zarządzania strachem*. Polega ona na odwoływaniu się do emocji takich jak strach, niepokój czy lęk w celu manipulowania odbiorcą. Zarządzanie strachem jest przeprowadzane poprzez tworzenie poczucia zagrożenia z czyjejś (albo czegoś) strony i podsycanie go, a następnie przedstawianie rozwiązania, oczywiście zgodnego z założeniami dysponenta propagandy⁵³⁶. Przedostatnią techniką wartą omówienia jest stosowanie przez propagandzistę metafor i porównań w tworzonych przekazach. Celem takich działań jest wykreowanie u odbiorcy pewnych skojarzeń i stworzenie swego rodzaju połączenia pomiędzy jego świadomością a podświadomością. W konsekwencji powstałe skojarzenia będą wywoływać u odbiorcy emocje pozytywne lub negatywne⁵³⁷. Wreszcie, należy wskazać na technikę przekazu jednostopniowego i dwustopniowego. Pierwszy z nich polega na wysyłaniu danego komunikatu bezpośrednio do odbiorcy. Taka technika może być skuteczna pod warunkiem, że nadawca będzie posiadał u odbiorcy autorytet. Drugi z przekazów (pośredni) zakłada wysyłanie komunikatu do osoby, która posiada w danej zbiorowości (społeczności) autorytet i która to osoba przekaże komunikat wytworzony przez propagandzistę do odbiorców właściwych⁵³⁸.

Uzupełniając w kontekście omawianego problemu badawczego należy również zarysować następujące zagadnienie. W nauce o mediach i komunikowaniu wyróżnia się teorię *agenda-setting*, która została opisana w 1972 roku przez M. McCombsa oraz D. Shawa. Zakłada ona, że media, porozumiewając się z odbiorcą, stosują swego rodzaju hierarchię priorytetów w zakresie przekazywanych wiadomości. Owa klasyfikacja jest dokonywana w odniesieniu do ważności danego komunikatu i która to ważność jest oczywiście ustalana przez jego nadawcę. Informacja taka będzie zatem podawana wyraźnie częściej aniżeli inne wiadomości, jak również eksponowana w sposób wyróżniający się pośród innych. Efektem

⁵³⁵ R. Borecki: *Propaganda i polityka. (Zarys problematyki funkcjonowania środków masowego przekazu w systemach społeczno-politycznych)*. Warszawa 1987, s. 127-139; M. Bartoszewicz: *Walka Propagandowa na Facebooku. Analiza jakościowa zawartości postów opublikowanych przez Prawo i Sprawiedliwość oraz Platformę Obywatelską w okresie tzw. Czarnego Protestu*. W: *Memy czyli życie społeczne w czasach kultury obrazu*. Red. T. Gackowski, K. Brylska, M. Patera. Warszawa 2017, s. 56.

⁵³⁶ A. Pratkanis, E. Aronson: *Wiek propagandy. Używanie i nadużywanie perswazji na co dzień*. Warszawa 2004, s. 182.189. Zobacz szerzej: P. Francuz: *Strach i lęk w reklamie politycznej*. W: *Psychologiczne aspekty komunikacji audiowizualnej*. Red. P. Francuz. Lublin 2007.

⁵³⁷ P. Znyk: *Propaganda. Współczesne oblicza. Technologia zabójstwa medialnego*. Łódź 2011, s. 156; M. Bartoszewicz: *Walka Propagandowa na Facebooku. Analiza jakościowa zawartości postów opublikowanych przez Prawo i Sprawiedliwość oraz Platformę Obywatelską w okresie tzw. Czarnego Protestu*. W: *Memy czyli życie społeczne...*, s. 57.

⁵³⁸ S. Kuśmierski, A. Frydrychowicz: *Podstawy wiedzy...*, s. 160-161.

takiego działania ma być wytworzenie u odbiorcy przekonania, że dana treść jest ważniejsza, aniżeli inne i to na niej powinien skupić swoją uwagę⁵³⁹.

2.3.2. Cyberataki jako instrument prowadzenia wojny informacyjnej

Jak już wielokrotnie wskazywano w niniejszej pracy, wojna informacyjna jest definiowana nie tylko jako oddziaływanie informacyjne przez dysponenta propagandy na odbiorców, ale również jako dokonywanie cyberataków w cyberprzestrzeni. Tym samym konieczne jest omówienie podstawowych pojęć związanych z tym zagadnieniem, takich jak termin *cyberprzestrzeń* (wraz z jej cechami), pojęcie *cyberataków* oraz metody i techniki cyberataków. K. Liedel pisał, że prowadzenie efektywnych działań w dziedzinie bezpieczeństwa wymaga ich wszechstronności, a zatem konieczne jest posiadanie przez państwo zarówno zdolności ofensywnych jak i defensywnych w cyberprzestrzeni. Wskazał również, że „ataki cybernetyczne stają się coraz częstsze, lepiej zorganizowane i bardziej kosztowne, biorąc pod uwagę szkody, jakie wyrządzają administracjom rządowym, biznesowi, gospodarce, a potencjalnie także transportowi, sieciom dostaw i innej infrastrukturze krytycznej; mogą one osiągnąć poziom, którego przekroczenie zagraża narodowemu i euroatlantyckiemu dobrobytowi, bezpieczeństwu i stabilności. Źródłem takich ataków mogą być obce siły wojskowe i służby wywiadowcze, zorganizowane grupy przestępcze, terrorystyczne i/lub grupy ekstremistyczne”⁵⁴⁰.

Wobec tego należy stwierdzić, że zagadnienia związane z cyberatakami stały się domeną nie tylko działalności państw, ale również innych podmiotów i w związku z czym zapewnienie odpowiedniego poziomu krajowego cyberbezpieczeństwa powinno być dla rządów priorytetowe⁵⁴¹. Ponadto można zauważyć, że cyberprzestrzeń nie jest jedynie sferą, w której dokonywane są cyberataki na poszczególne podmioty, ale również bardzo istotnym elementem systemu komunikacji masowej, przede wszystkim dzięki funkcjonowaniu sieci Internet. To w jej ramach funkcjonuje znaczna część mediów, które są jednym z ważniejszych uczestników (realizatorów) działań z zakresu propagandy – wojny informacyjnej.

⁵³⁹ M. E. McCombs, L. Guo: *Agenda-setting Influence of the Media in the Public Sphere*. W: *The Handbook of Media and Mass Communication Theory*. Red. R. S. Fortner, P. M. Fackler. New York 2014, s. 251-265.

⁵⁴⁰ K. Liedel: *Zdolność prowadzenia działań ofensywnych w cyberprzestrzeni warunkiem bezpieczeństwa państwa*. W: *Nie-bezpieczny świat. Systemy Informacja Bezpieczeństwo*. Red. P. Sienkiewicz, H. Świeboda, E. Szczepaniuk. Warszawa 2015, s. 175.

⁵⁴¹ Ibidem, s. 176.

2.3.2.1. Pojęcie i cechy cyberprzestrzeni

Skutkiem rewolucji informacyjnej (teleinformatycznej) było powstanie nowej płaszczyzny ludzkiej aktywności, którą określamy *cyberprzestrzenią*. Wskazany termin spopularyzował W. Gibson, choć, jak wskazuje M. Lakomy, błędnie jest on uważany za jego twórcę, gdyż pojęcie to pojawiło się już w powieściach V. Vinge oraz J. M. Forda. Terminu cyberprzestrzeń W. Gibson po raz pierwszy użył w powieściach „Burning Chrome”, a następnie w „Neuromancer”⁵⁴². Mimo, że powyższy termin nie wywodzi się bezpośrednio z rozważań naukowych i mógłby stać się raczej przedmiotem rozważań literaturoznawców, to jednak przeniknął do literatury specjalistycznej w zakresie teleinformatycznej działalności człowieka, jak i wszelkich innych z nią związanych. Podobnie jak w przypadku omawianych dotychczas terminów, nie ma pośród badaczy jednoznacznego stanowiska co do rozumienia omawianego pojęcia, dlatego też warto przytoczyć szereg jego definicji.

Rozpoczynając rozważania definicyjne cyberprzestrzeni można rozpocząć od potocznego rozumienia tego terminu i tak na przykład „Encyclopedia Britannica” określa go jako „świat stworzony przez łącza między komputerami, urządzeniami z dostępem do Internetu, serwerami, routerami i innymi elementami infrastruktury internetowej”⁵⁴³. Podobną definicję zawiera „Encyklopedia PWN”, gdzie cyberprzestrzeń to „przestrzeń wirtualna, w której odbywa się komunikacja między komputerami połączonymi siecią internetową”⁵⁴⁴. O wiele bardziej rozbudowane definicje można z kolei odnaleźć w literaturze specjalistycznej. T. R. Aleksandrowicz przytacza definicję D. T. Kuehla dla którego cyberprzestrzeń stanowi „globalną domenę w ramach środowiska informacyjnego, której wyróżniający i wyjątkowy charakter jest określony możliwościami wykorzystania elektroniki i spektrum elektromagnetycznego w celu tworzenia, przechowywania, modyfikowania oraz wykorzystywania informacji poprzez współzależne i połączone ze sobą sieci, które bazują na technologiach teleinformatycznych”⁵⁴⁵. Inna definicja prezentowana przez R. Tadeusiewicza wskazuje, że cyberprzestrzeń to „ogół narzędzi sprzętowych i programowych związanych z technikami gromadzenia, przetwarzania, przesyłania i udostępniania informacji, wykorzystywanych przez ludzi do pozyskiwania wiedzy oraz do komunikacji z innymi

⁵⁴² M. Lakomy: *Cyberprzestrzeń jako nowy wymiar...*, s. 71-72.

⁵⁴³ Encyclopedia Britannica: *cyberspace*. <https://www.britannica.com/topic/cyberspace> (dostęp: 30.12.2021).

⁵⁴⁴ Encyklopedia PWN: *cyberprzestrzeń*. <https://sjp.pwn.pl/sjp/cyberprzestrze%C5%84;2553915> (dostęp: 31.12.2021).

⁵⁴⁵ T. R. Aleksandrowicz: *Podstawy walki informacyjnej...*, s. 175.

ludźmi”⁵⁴⁶. M. Madej z kolei proponuje zdefiniowanie pojęcia cyberprzestrzeni jako „ogółu powiązań o charakterze wirtualnym („nieprzestrzennym” w sensie fizycznym, niematerialnym i ageograficznym), powstałych i funkcjonujących dzięki ich fizycznym manifestacjom (komputery, infrastruktura telekomunikacyjna)”⁵⁴⁷. D. Clark z kolei pisze, że jest to zbiór urządzeń komputerowych, które są połączone sieciami oraz w których są przechowywane i wykorzystywane informacje, jak również gdzie odbywa się komunikacja między nimi⁵⁴⁸. M. Lakomy zdefiniował cyberprzestrzeń jako „domenę przetwarzania, przechowywania i przesyłania informacji w formie cyfrowej, funkcjonującą w oparciu o transmisję sygnałów cyfrowych oraz promieniowanie elektromagnetyczne. Jest przestrzenią w swojej istocie niematerialną, ale funkcjonującą dzięki infrastrukturze teleinformatycznej, która te sygnały wytwarza i przesyła”⁵⁴⁹. M. Lakomy za E. Lichockim przytacza również definicję cyberprzestrzeni stającej się w „XXI wieku „układem nerwowym” państwa. Jest to system sterowania krajem, złożony z tysięcy połączonych ze sobą systemów teleinformatycznych, które pozwalają działać państwowym podsektorom infrastruktury”⁵⁵⁰.

Pojęcie cyberprzestrzeni występuje również w terminologii wojskowej i tak na przykład w amerykańskim dokumencie DOD Dictionary of Military and Associated Terms wskazano, że cyberprzestrzeń to „globalna domena w ramach środowiska informacyjnego składająca się ze współzależnych sieci infrastruktury technologii informacyjnych i danych krajowych, w tym Internetu, sieci telekomunikacyjnych, systemów komputerowych oraz wbudowanych procesorów i kontrolerów”⁵⁵¹. Z kolei w brytyjskiej The UK Cyber Security Strategy Protecting and promoting the UK in a digital world wskazano, że jest ona „interaktywną dziedziną składającą się z sieci cyfrowych, która jest wykorzystywana do przechowywania, modyfikowania i przekazywania informacji”⁵⁵². Kolejną definicją – sformułowaną tym razem w ramach działalności państw w organizacji międzynarodowej – jest definicja cyberprzestrzeni zaproponowana przez Komisję Europejską, która wskazuje, że jest to „wirtualna przestrzeń,

⁵⁴⁶ R. Tadeusiewicz: *Zagrożenia w cyberprzestrzeni*. „Nauka” 2010, nr 4/2010, s. 32.

⁵⁴⁷ M. Madej: *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państwa i systemu międzynarodowego*. W: *Bezpieczeństwo Teleinformatyczne...*, s. 32.

⁵⁴⁸ D. Clark: *Characterizing cyberspace: past, present and future*. „ECIR Working Paper” 2010, No. 2010-3, s. 1.

⁵⁴⁹ M. Lakomy: *Cyberprzestrzeń jako nowy...*, s. 83.

⁵⁵⁰ Ibidem, s. 78.

⁵⁵¹ United States Department of Defense: *DOD Dictionary of Military and Associated Terms*. November 2021, s. 55. Tłumaczenie własne. Tekst w oryginale: “A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers”.

⁵⁵² Cabinet Office: *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world*. November 2011, s. 11. Tłumaczenie własne. Tekst w oryginale: „Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information”.

w której krążą elektroniczne dane przetwarzane przez komputery PC z całego świata”⁵⁵³. W polskim porządku prawnym wprowadzona została definicja legalna cyberprzestrzeni, którą zamieszczono między innymi w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024. Strategia definiuje omawiany termin jako „przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2019 r. poz. 700, 730, 848 i 1590), wraz z powiązaniami między nimi oraz relacjami z użytkownikami”⁵⁵⁴. Systemy teleinformatyczne o których mowa w art. 3 pkt 3 pierwszej ze wskazanych ustaw to „zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz.U. z 2021 r. poz. 576)”⁵⁵⁵. W innym polskim dokumencie rządowym będącym „Słownikiem kluczowych pojęć z zakresu cyberbezpieczeństwa”, cyberprzestrzeń jest definiowana jako „globalna publiczna przestrzeń w środowisku informacyjnym składającym się z sieci niezależnych infrastruktur systemów informatycznych, włączając w to Internet, sieci telekomunikacyjne, systemy komputerowe oraz komputery i sterowniki o zastosowaniach wbudowanych”⁵⁵⁶.

Wobec omawianych wyżej rozważań należy podkreślić, że cyberprzestrzeń nie może być utożsamiana wyłącznie z siecią internetową. Jak wskazano bowiem w dokumencie Allied Joint Publication-3.20 Allied Joint Doctrine for Cyberspace Operations, „cyberprzestrzeń to znacznie więcej niż tylko Internet. Wszystkie urządzenia dostępne przez cyberprzestrzeń mogą być potencjalnymi celami i potencjalnymi zagrożeniami. Obejmuje to sieci i urządzenia połączone za pomocą połączeń przewodowych, bezprzewodowych i tych, które wydają się w ogóle nie być połączone. dopełnieniem tej stale rosnącej domeny jest wykorzystanie takiej technologii w rosnącej liczbie dóbr domowych, znanej również jako Internet rzeczy”⁵⁵⁷.

⁵⁵³ J. Wasilewski: *Zarys definicyjny cyberprzestrzeni*. „Przegląd Bezpieczeństwa Wewnętrznego” 2013, nr 9/19, s. 229.

⁵⁵⁴ *Uchwała Nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*. (M.P. z 2019 r. poz. 1037) wraz z załącznikiem do uchwały: *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*.

⁵⁵⁵ *Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne*. (Dz.U. z 2021 r. poz. 2070), art. 3.

⁵⁵⁶ Pełnomocnik Rządu ds. Cyberbezpieczeństwa: *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*. Warszawa 2021. <https://www.gov.pl/attachment/48226cb6-29d4-49f9-860f-acd703072e60> (dostęp: 30.12.2021), s. 88.

⁵⁵⁷ Biuro Standaryzacji NATO: *Allied Joint Publication-3.20 Allied Joint Doctrine for Cyberspace Operations*. Styczeń 2020, s. 1.

W odniesieniu do omawianego w pracy problemu badawczego warto również przytoczyć spostrzeżenie P. Sienkiewicza, który wskazał, że „cyberprzestrzeń jest przestrzenią komunikowania społecznego, lecz nie tylko transinformowania (informowania wiernego), bowiem zachodzą tu procesy świadomego parainformowania, pseudoinformowania i dezinformowania”⁵⁵⁸. Dalej pisał, że „cyberprzestrzeń jest przestrzenią realizacji podstawowych wartości ludzkich we wszystkich sferach działań społecznych. Jest swoistą zapowiedzią nowej cywilizacji informacyjnej, której obecnym przejawem jest rozwój społeczeństwa informacyjnego”⁵⁵⁹. W odniesieniu do powyższych definicji cyberprzestrzeni należy zauważyć, że większość z nich nie odnosi się do jakichkolwiek elementów ludzkich czy społecznych, choć przecież to człowiek jest jej głównym użytkownikiem.

Następnie można wyróżnić szereg cech charakterystycznych cyberprzestrzeni. Jedną z częściej przytaczanych typologii sformułował T. R. Aleksandrowicz wyróżniając takie cechy jak: niezależność od miejsca, niezależność od odległości, niezależność od czasu, niezależność od granic, względna anonimowość oraz możliwość ustalenia sprzętu, nie osoby⁵⁶⁰. T. Hoffmann z kolei wyróżnia katalog podstawowych cech cyberprzestrzeni do których zalicza globalny zasięg, wydajność, uniwersalności oraz taniość w dostępie⁵⁶¹. Inny badacz M. Górka wskazuje na brak granic, dynamiczne procesy i zjawiska oraz anonimowość użytkowników⁵⁶². P. Sienkiewicz, pisząc o cyberprzestrzeni, traktował to pojęcie w sposób szczególnie kompleksowy. Wskazywał na różnego rodzaju cechy posiadane przez cyberprzestrzeń, jednakże przypisywał je do poszczególnych dziedzin życia społecznego. W jego ocenie do cech konstytutywnych cyberprzestrzeni powinno się zaliczać sieciowość, natomiast do cech potencjalnych wirtualność. I tak na przykład w odniesieniu do współczesnych mediów pisał, że uwzględniając ich walory komunikacyjne „nie można pominąć takich cech jak: interaktywność, hipertekstowość i multimedialność. Jedną z przyczyn wyłonienia się tych cech była konwergencja systemów informatycznych, systemów telekomunikacyjnych i mediów elektronicznych”⁵⁶³. Z kolei biorąc pod uwagę obszar w jakim znajduje się cyberprzestrzeń, do jej cech trzeba zaliczyć „brak granic przestrzennych, brak granic politycznych, brak granic

⁵⁵⁸ P. Sienkiewicz: *Bezpieczeństwo cyberprzestrzeni państwa*. „Ekonomiczne Problemy Usług” 2012, nr 88, s. 807.

⁵⁵⁹ Ibidem, s. 808.

⁵⁶⁰ T. R. Aleksandrowicz: *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*. „Przegląd Bezpieczeństwa Wewnętrznego” 2016, nr 15/16, s. 12.

⁵⁶¹ T. Hoffmann: *Główni aktorzy cyberprzestrzeni i ich działalność*. W: *Cyberbezpieczeństwo wyzwaniem XXI wieku*. Red. T. Dębowski. Łódź – Wrocław 2018, s. 12.

⁵⁶² M. Górka: *Cyberbezpieczeństwo jako wyzwanie dla współczesnego państwa i społeczeństwa*. W: *Cyberbezpieczeństwo wyzwaniem XXI wieku*. Red. T. Dębowski. Łódź – Wrocław 2018, s. 34.

⁵⁶³ P. Sienkiewicz: *Bezpieczeństwo cyberprzestrzeni państwa...*, s. 805.

geograficznych oraz brak granic doraźnych”⁵⁶⁴. Z uwagi na zagrożenia, wyróżniamy takie cechy jak: „prosta, ogólnie dostępna technologia, anonimowość sprawcy, wielość form cyberataków, „efekt domina” jako skutek cechy „broni masowej dezorganizacji”, niewielkie koszty ataków”⁵⁶⁵. I wreszcie z uwagi na bezpieczeństwo rozróżniamy: „brak szybkich i skutecznych rozwiązań zabezpieczających mnogość obiektów zagrożeń (ataków), wysokie koszty zabezpieczeń, zróżnicowana podatność obiektów, nieprzewidywalność źródeł zagrożeń, bardzo wysokie koszty”⁵⁶⁶. Wymienione wyżej cechy charakterystyczne dla cyberprzestrzeni ukazują w sposób jednoznaczny jak złożone oraz silnie uwarunkowane jest omawiane pojęcie. D. Clark pisząc o charakterystyce cyberprzestrzeni sformułował hierarchiczną koncepcję czterech warstw wskazując, że pierwszą z nich jest warstwa fizyczna, czyli ogół urządzeń z których zbudowana jest cyberprzestrzeń. Następnie wyróżnił poziom logiczny, czyli wszystko to, co składa się na procesy decyzyjne podejmowane w sieci. Określa go jako swego rodzaju platformy na których są budowane nowe platformy dla kolejnych innowacji. Wreszcie wyróżnia warstwę informacyjną, czyli wszystko to, co znajduje się wewnątrz sieci, jak na przykład muzyka, filmy, dane firm czy strony *web*. Ostatnia z warstw to warstwa ludzka, czyli wszyscy użytkownicy tworzący cyberprzestrzeń oraz kształtują jej złożony charakter⁵⁶⁷.

Na potrzeby niniejszej pracy przyjęto, że cyberprzestrzeń to przestrzeń, w której następuje przyjmowanie, przetwarzanie, przechowywanie i przesyłanie informacji w formie cyfrowej. Cyberprzestrzeń to również sieć sieci współzależnych ze sobą oraz stanowiąca swego rodzaju układ nerwowy każdego państwa. Ponadto omawiana przestrzeń, pomimo że ma wymiar niematerialny, to jednak funkcjonuje w infrastrukturze teleinformatycznej będącej wytworem materialnym człowieka. Cyberprzestrzeń to nie tylko domena sieci Internet, gdyż występuje również w urządzeniach do niej niepodłączonych.

2.3.2.2. Pojęcie cyberataków

Nie ulega wątpliwości, że cyberataki (już chociażby z samego potocznego rozumienia wskazanego terminu) są wrogą działalnością podejmowaną przeciwko innym państwom lub podmiotom w cyberprzestrzeni. W związku z tym w pierwszej kolejności zasadnym wydaje się omówienie szeroko rozumianego terminu *cyberbezpieczeństwo*, który pozostaje

⁵⁶⁴ Ibidem, s. 806.

⁵⁶⁵ Ibidem, s. 806.

⁵⁶⁶ Ibidem, s. 806.

⁵⁶⁷ D. Clark: *Characterizing cyberspace: past, present...*, s. 2-4.

w bezpośrednim związku z powyższą działalnością. Bezpieczeństwo to stan, który daje poczucie pewności i gwarancję jego zachowania, stan spokoju i zabezpieczenia, czyli braku zagrożenia oraz ochrony przed niebezpieczeństwami⁵⁶⁸. W odniesieniu do cyberprzestrzeni można z kolei mówić o bezpieczeństwie teleinformatycznym, a więc działalności polegającej na podejmowaniu „przedsięwzięć obejmujących ochronę z informatyzowanych działów strategicznych, do których można dotrzeć przy pomocy połączeń sieciowych”⁵⁶⁹. Należy również zaznaczyć, że „bezpieczeństwo teleinformatyczne to inaczej bezpieczeństwo informacji i systemów teleinformatycznych rozpatrywane w odniesieniu do instytucji wykorzystującej lub udostępniającej infrastrukturę teleinformatyczną, aby osiągnąć wyznaczone cele”⁵⁷⁰. W odniesieniu do bezpieczeństwa informacji⁵⁷¹ trzeba zauważyć, że jest ono nieustannie narażone na występowanie różnego rodzaju zagrożeń. K. Liderman przyjął szeroki katalog źródeł zagrożeń dla bezpieczeństwa informacji przyjmując, że są to „katastrofy naturalne; błędy ludzi wykorzystujących lub obsługujących systemy informacyjne; błędy w organizacji pracy i procedurach; celowe, szkodliwe działania ludzi skierowane na systemy informacyjne; awarie sprzętu (elementów i podzespołów mechanicznych, elektronicznych, elektromechanicznych) i wady oprogramowania”⁵⁷². J. Kowalewski i M. Kowalewski zaproponowali podstawowy katalog, do którego zaliczyli siłę wyższą, uchybienia organizacyjne, błędy ludzkie, błędy techniczne oraz działania rozmyślne⁵⁷³.

W odniesieniu do konieczności zapewniania odpowiedniego poziomu bezpieczeństwa M. Adamczak i K. Liedel wskazali, że istnieje potrzeba „bezpiecznego i prawidłowego funkcjonowania cyberprzestrzeni, która wymaga od każdego państwa, aby obszar ten był priorytetem w krajowej polityce bezpieczeństwa, z kolei państwo podejmowało działania w zakresie efektywnego tworzenia systemów przeciwdziałania zagrożeniom na poziomach strategicznym, prawnym i instytucjonalnym”⁵⁷⁴. P. Sienkiewicz pisał, że „problem bezpieczeństwa informacyjnego obejmuje zarówno zabezpieczenia zasobów informacyjnych przed niedozwolonymi formami ingerencji obiektów (osób) niepożądanych, w tym ochronę informacji wrażliwych i danych osobowych, jak i różne formy zabezpieczenia systemów

⁵⁶⁸ J. Kaczmarek, W. Łepkowski, B. Zdrodowski (Red.): *Słownik terminów...*, s. 14.

⁵⁶⁹ Ibidem, s. 21.

⁵⁷⁰ Ibidem, s. 21.

⁵⁷¹ W odniesieniu do pojęcia bezpieczeństwa informacji K. Liderman pisze, że „nie ma dotąd jednoznacznej wykładni pojęcia „bezpieczeństwo informacyjne” i związanego z nim pojęcia „bezpieczeństwo informacji”. Oba są często używane w różnych znaczeniach”. Źródło: K. Liderman: *Bezpieczeństwo informacyjne...*, s. 13.

⁵⁷² Ibidem, s. 33.

⁵⁷³ J. Kowalewski, M. Kowalewski: *Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm*. Warszawa 2017, s. 36.

⁵⁷⁴ M. Adamczuk, K. Liedel: *Doktryna cyberbezpieczeństwa*. „Przegląd Bezpieczeństwa Wewnętrznego” 2015, nr 12/7, s. 281.

informatycznych (teleinformatycznych) przed rozpoznanymi destrukcyjnymi działaniami zewnętrznymi i wewnętrznymi obiektów”⁵⁷⁵. Podsumowując rozważania dotyczące zagadnienia cyberbezpieczeństwa trudno nie zgodzić się z poglądem jaki sformułował P. Sienkiewicz pisząc, że „jest także „ciemna strona” cyberprzestrzeni, jako źródła zagrożeń dla bezpieczeństwa międzynarodowego i narodowego. Musi być zatem przedmiotem racjonalnej polityki państwa, gdyż „cyberbezpieczeństwo” stanowi współcześnie jeden z podstawowych filarów (segmentów) systemów bezpieczeństwa narodowego (regionalnego, globalnego). Istnieją bowiem systemy „cyberbroni” (*cyberweapons*), które w charakterze „broni masowej dezorganizacji” mogą być efektywnym środkiem „cyberwojny” (*cyberwar, netwar*)”⁵⁷⁶.

Termin *cyberatak* w powszechnym rozumieniu tego słowa jest definiowany jako „nielegalna próba uszkodzenia cudzego systemu komputerowego lub znajdujących się na nim informacji z wykorzystaniem sieci Internet”⁵⁷⁷. Z taką definicją nie można się w pełni zgodzić, gdyż dokonywanie cyberataków nie jest możliwe wyłącznie z wykorzystaniem Internetu oraz wyłącznie w Internecie. Z uwagi na fakt, że zjawisko cyberataków stanowi przede wszystkim domenę szkodliwego oddziaływania na określoną infrastrukturę w cyberprzestrzeni danego państwa, właściwym jest przytoczenie przede wszystkim definicji tego pojęcia o charakterze militarnym (wojskowym). W „Słowniku terminów i definicji NATO” nie występuje jednoznaczna definicja cyberataku, jednakże odwołanie do tego terminu można odnaleźć w pojęciu *atak na sieć teleinformatyczną*, gdzie wskazuje się, że są to „działania podejmowane w celu zniekształcenia, uniemożliwienia wykorzystania, degradacji lub zniszczenia informacji przechowywanej w komputerze i/lub sieci komputerowej, albo komputera i/lub sieci komputerowej. Uwaga: atak na sieć informatyczną jest rodzajem ataku cybernetycznego”⁵⁷⁸. Z kolei w „Słowniku kluczowych pojęć z zakresu bezpieczeństwa” z 2021 roku, stanowiącym zbiór rekomendacji standaryzujących rozwiązania zabezpieczające w sieciach i systemach informatycznych, cyberatak jest definiowany jako „atak dokonany przez cyberprzestrzeń, którego celem są podmioty wykorzystujące cyberprzestrzeń, z zamiarem uszkodzenia, zablokowania dostępu, zniszczenia lub złośliwego przejęcia środowiska obliczeniowego albo naruszenia integralności danych lub przechwycenia informacji”⁵⁷⁹. Definicja tego pojęcia

⁵⁷⁵ P. Sienkiewicz: *Bezpieczeństwo cyberprzestrzeni państwa...*, s. 807.

⁵⁷⁶ Ibidem, s. 808.

⁵⁷⁷ Cambridge Dictionary: *cyberattack*. <https://dictionary.cambridge.org/dictionary/english/cyberattack> (dostęp: 03.01.2022). Tłumaczenie własne. Tekst w oryginale: „an illegal attempt to harm someone's computer system or the information on it, using the internet”.

⁵⁷⁸ Biuro Standaryzacji NATO: *Słownik terminów...*, s. 118.

⁵⁷⁹ Pełnomocnik Rządu ds. Cyberbezpieczeństwa: *Słownik kluczowych pojęć...*, s. 85.

w amerykańskiej terminologii wojskowej stwierdza, że cyberataki to „wrogie działanie wykorzystujące sieci lub systemy komputerowe lub pokrewne, oraz mające na celu zakłócenie i/lub zniszczenie krytycznych systemów, zasobów lub funkcji cybernetycznych przeciwnika”⁵⁸⁰. W dokumencie Tallinn Manual on the International Law Applicable to Cyber Warfare⁵⁸¹ cyberatak zdefiniowano jako operację cybernetyczną „zarówno ofensywną, jak i defensywną, w przypadku której istnieje uzasadnione przypuszczenie, że spowoduje obrażenia lub śmierć osób lub uszkodzenie lub zniszczenie obiektów”⁵⁸². Z kolei O. Hathaway proponuje jak sama pisze stosunkowo wąską definicję cyberataku stwierdzając, że jest to „każde działanie podjęte w celu osłabienia funkcji sieci komputerowej dla celów politycznych lub bezpieczeństwa narodowego”⁵⁸³. Inna definicja wskazuje, że cyberatak to „wrogi akt przy wykorzystaniu komputera lub związanych z nim sieci lub systemów, zmierzający do zakłócenia i/lub zniszczenia krytycznych cybersystemów przeciwnika, zasobów lub funkcji”⁵⁸⁴. Według M. Lakomego jest to natomiast „wrogie wykorzystanie komputerów, ich sieci oraz innych, pokrewnych technologii i urządzeń (tele)informatycznych, którego celem jest zablokowanie, zakłócenie, zniszczenie lub uzyskanie informacji znajdujących się w sieciach i systemach teleinformatycznych bądź w innych urządzeniach wykorzystujących ICT; zablokowanie, zakłócenie, przejęcie kontroli lub zniszczenie samych sieci i systemów teleinformatycznych bądź innych urządzeń wykorzystujących te technologie”⁵⁸⁵.

Na potrzeby przedmiotowej rozprawy przyjęto ostatnią z zaprezentowanych definicji. Jak bowiem wskazuje sam autor, odnosi się ona również do pozyskiwania określonych informacji, a nie tylko do dokonywania zniszczeń czy też zakłóceń, co jest szczególnie istotne na gruncie prezentowanego w pracy problemu badawczego⁵⁸⁶. W tym miejscu należy przypomnieć, że w ramach niniejszej rozprawy zjawisko wojny informacyjnej jest postrzegane

⁵⁸⁰ The Vice Chairman of the Joint Chiefs of Staff: *Joint Terminology for Cyberspace Operations*. Washington D.C. 2010, s. 5. Tłumaczenie własne. Tekst w oryginale: „a hostile act using computer or related networks or systems, and intended to disrupt and/ or destroy an adversary's critical cyber systems, assets, or functions”.

⁵⁸¹ *Tallinn Manual on the International Law Applicable to Cyber Warfare* jest wydany w 2013 roku opracowaniem przygotowanym przez międzynarodową grupę naukowców pod kierunkiem M. N. Schmitt’a, której przedmiotem są relacje prawa międzynarodowego publicznego z konfliktami w cyberprzestrzeni. W 2017 roku wydano drugą edycję publikacji rozszerzając zakres wersji z 2013 roku.

⁵⁸² M. N. Schmitt (Red.): *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge 2013, s. 92. Tłumaczenie własne. Tekst w oryginale: „whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects”.

⁵⁸³ O. Hathaway: *The Law of Cyber-Attack*. „California Law Review” 2011, Vol 100:817, s. 826. Tłumaczenie własne. Tekst w oryginale: „any action taken to undermine the functions of a computer network for a political or national security purpose”.

⁵⁸⁴ M. Lakomy: *Cyberprzestrzeń jako nowy...*, s. 122.

⁵⁸⁵ Ibidem, s. 122.

⁵⁸⁶ M. Lakomy pisze, że „takie rozumienie tego terminu pozwala dostrzec, iż celem cyberataków nie musi być dokonanie określonych zniszczeń lub zakłóceń w wymiarze materialnym czy niematerialnym, ale także zdobycie określonych informacji w formie cyfrowej, na co często nie zwraca się uwagi”. Źródło: Ibidem, s. 122.

zarówno jako dokonywanie ataków w cyberprzestrzeni, jak i jako prowadzenie kampanii oddziaływania informacyjnego na odbiorców w Internecie, przy czym działania te są wobec siebie komplementarne.

2.3.2.3. Metody i techniki cyberataków

Cyberataki stanowią zagrożenie dla bezpieczeństwa teleinformatycznego państw oraz innych podmiotów. Metody ich przeprowadzania stanowią niezwykle złożone zagadnienie, z kolei mnogość ich typów powoduje, że omówione zostaną jedynie wybrane z nich. Wobec powyższego wyróżniono takie metody jak: stosowanie złośliwego oprogramowania (wirusy komputerowe, robaki, trojany), ataki DoS, ataki DDoS, ataki DRDoS, *social engineering*, *phishing*, *spoofing* oraz *botnet*.

Pierwszym typem ataków wymagającym omówienia są ataki przeprowadzane z wykorzystaniem złośliwego oprogramowania (ang. *malware*). Termin ten należy rozumieć jako oprogramowanie służące do naruszenia systemów bezpieczeństwa w celu naruszenia jego poufności, integralności oraz dostępności. Można wyróżnić szereg ich rodzajów jak na przykład wirusy, robaki, konie trojańskie, bomby logiczne, *rabbit*, *backdoor*⁵⁸⁷. Na potrzeby rozprawy zostaną omówione pierwsze trzy ze wskazanych rodzajów *malware*. Wirus komputerowy to program zaprojektowany tak, aby kopiować i rozprzestrzeniać się z jednego pliku do drugiego, zazwyczaj poprzez dołączanie się do plików danego programu⁵⁸⁸. Wirus jest prawdopodobnie pierwszym typem złośliwego oprogramowania, które zostało stworzone przez człowieka. Warto zaznaczyć, że wraz z ich rozwojem wirusy komputerowe zaczęły stawać się coraz doskonalsze, między innymi poprzez atakowanie wybranych plików, trudność w wykryciu czy sposób rozprzestrzeniania się. Drugim rodzajem szkodliwego oprogramowania są robaki, które posiadają zdolność do samodzielnego transmitowania się w sieciach komputerowych⁵⁸⁹. Co istotne, w „przeciwieństwie do wirusów nie muszą się podłączać do istniejących plików i nie wymagają żadnej działalności użytkownika (np. włączenia określonej aplikacji). Ich celem jest raczej zarażenie całej infrastruktury sieciowej, a nie pojedynczych plików”⁵⁹⁰. Ostatnim wyróżnionym typem złośliwego oprogramowania są trojany. Koń trojański⁵⁹¹ to program który,

⁵⁸⁷ R. Sharp: *An Introduction to Malware*. <http://winntbg.bg.aghhttps://backend.orbit.dtu.dk/ws/portalfiles/portal/139067614/malware.pdf> (dostęp: 15.10.2022), s. 2-3.

⁵⁸⁸ S. Gupta: *Types of Malware and its Analysis*. „International Journal of Scientific & Engineering Research” 2013, Vol. 4, Issue 1, s. 6.

⁵⁸⁹ Pełnomocnik Rządu ds. Cyberbezpieczeństwa: *Słownik kluczowych pojęć...*, s. 255.

⁵⁹⁰ M. Lakomy: *Cyberprzestrzeń jako nowy...*, s. 125.

⁵⁹¹ Nazwa tego typu oprogramowania pochodzi od mitologicznego konia trojańskiego.

jak piszą A. B. Brzezińska oraz M. F. Gawrycki, „nadużywa praw dostępu w domenie użytkownika korzystającego z jego usług. Np. edytor tekstu mógłby zawierać kod, który po wyszukaniu w redagowanym pliku pewnych słów kluczowych skopiowałby cały plik do specjalnego obszaru dostępnego dla twórcy edytora (bez zgody i wiedzy użytkownika tego programu)”⁵⁹². Istotą funkcjonowania tego typu złośliwego oprogramowania jest zatem wykonywanie określonych szkodliwych działań bez zgody i wiedzy użytkownika oraz pod przykryciem prawidłowo funkcjonującego programu.

Kolejnym rodzajem ataków są ataki typu DoS czyli *Denial of Service*. Są one jedną z najprostszych form wykonywania ataków na sieci oraz systemy teleinformatyczne, a jednocześnie jedną z najgroźniejszych. Skutkiem ataku jest utrudnianie lub uniemożliwianie dostępu do danych usług sieciowych poprzez zajęcie dostępnej przepustowości łącza i w konsekwencji odcięcie atakowanego celu od zasobów Internetu⁵⁹³. Odmianą omawianego ataku o której należy wspomnieć jest atak DDos czyli *Distributed Denial Of Service*, którego skutkiem jest „uniemożliwienie lub znaczne spowolnienie dostępu do zasobów uprawnionym podmiotom, prowadzonego przy jednoczesnym wykorzystaniu wielu źródeł ataku – komputerów połączonych w sieć, zwykle w postaci *botnet*”⁵⁹⁴. Różnica pomiędzy powyższymi atakami sprowadza się zatem do dokonywaniu ataków DoS za pomocą jednego urządzenia, z kolei ataków DDoS za pomocą wielu z nich – najczęściej *botnetu*, czyli grupy zainfekowanych komputerów, których liczba może być w zasadzie nieograniczona⁵⁹⁵. Warto również zaznaczyć, że ataki typu DoS i DDoS przeprowadzane są w warstwie sieciowej, a więc z wykorzystaniem infrastruktury sieci, nie zaś bezpośrednio na urządzeniu użytkownika jak ma to miejsce w przypadku złośliwego oprogramowania⁵⁹⁶. Przez pojęcie ataków sieciowych (ang. *network attack*) należy rozumieć przede wszystkim „działania podejmowane z wykorzystaniem sieci komputerowych w celu zakłócenia działania, uniemożliwienia dostępu, uszkodzenia lub zniszczenia informacji znajdujących się w systemach informatycznych lub zakłócenia działania samych sieci”⁵⁹⁷. Poza atakami typu DoS i DDoS można wyróżnić również ataki DRDoS (ang.

⁵⁹² A. B. Brzezińska, M. F. Gawrycki: *Cyberterroryzm jako nowe zagrożenie dla bezpieczeństwa międzynarodowego w dobie globalizacji*. Warszawa 2003, s. 332-333.

⁵⁹³ Q. Gu, P. Liu: *Denial of Service Attacks*. <https://s2.ist.psu.edu/paper/ddos-chap-gu-june-07.pdf> (dostęp: 15.10.2022).

⁵⁹⁴ Pełnomocnik Rządu ds. Cyberbezpieczeństwa: *Słownik kluczowych pojęć...*, s. 94.

⁵⁹⁵ M. Krysiński, P. Miller, A. Pamuła: *Zagrożenia typu Distributed Denial of Service jako przykład ryzyka związanego z prowadzeniem działalności gospodarczej w Internecie*. „Ekonomiczne Problemy Usług” 2017, nr 1/2017, T.2, s. 208.

⁵⁹⁶ J. M. Chmielewski, K. Waćkowski: *Technologie teleinformatyczne – podstawy, rozwój i bezpieczeństwo systemów teleinformatycznych*. W: *Cyberbezpieczeństwo: zarys wykładu*. Red. C. Banasiński. Warszawa 2018, s. 85-91.

⁵⁹⁷ Pełnomocnik Rządu ds. Cyberbezpieczeństwa: *Słownik kluczowych pojęć...*, s. 71.

Distributed Reflective Denial of Service). Polegają one na wykorzystaniu tzw. wzmocnionego odbicia, tzn. atakujący podszywa się pod IP celu a następnie wysyła żądania w konsekwencji czego cel odpowiada na żądanie (wysyła odpowiedź), co jest właśnie tzw. odbiciem. Skutkiem stosowania tego typu ataku jest zwielokrotnienie liczby odpowiedzi, a w konsekwencji zablokowanie łączu w sieci⁵⁹⁸.

Następnym typem cyberataków jaki można wyróżnić jest *social engineering*, czyli dokonywanie ataków socjotechnicznych. Działania takie sprowadzają się przede wszystkim do wywierania określonego wpływu i manipulowania ludźmi w celu ujawnienia poufnych informacji. Jest to również pozyskiwanie wrażliwych informacji przez podmioty (osoby) z zewnątrz⁵⁹⁹. Można je zdefiniować również jako „uzyskanie nieuprawnionego dostępu do informacji poprzez obserwację i oddziaływanie (głównie psychologiczne) na użytkownika(ów) systemu teleinformatycznego oraz przeszukiwanie środowiska pracy atakowanego użytkownika”⁶⁰⁰. Specyfika powyższego rodzaju ataków polega na jego aspekcie fizycznym, przez co należy rozumieć, że nie można go powstrzymać przy użyciu jakichkolwiek zabezpieczeń komputerowych, gdyż bazuje on na psychologii oraz relacjach międzyludzkich. Szczególnie istotne jest to, że „włamania tego typu mogą więc obejmować spreparowane wiadomości e-mail, które mają skłonić użytkownika do ujawnienia wrażliwych danych lub otworzenia pliku zawierającego złośliwy kod, mogą też polegać na przekierowaniu na zainfekowaną stronę internetową”⁶⁰¹. Cyberataki typu *social engineering* można określić zatem jako „działanie zmierzające do uzyskania pożądanego zachowania jednostek i grup społecznych”⁶⁰².

Kolejnym typem cyberataków jest *phishing*. Choć z tym zjawiskiem mamy do czynienia od lat dziewięćdziesiątych XX wieku, to nie traci ono na aktualności, a wręcz przeciwnie. Współcześnie *phishing* nie ogranicza się tylko do poczty e-mail, ale może być przeprowadzany za pośrednictwem wiadomości głosowych, SMS-ów, komunikatorów internetowych, serwisów społecznościowych, a nawet gier wieloosobowych. Jego celem jest nakłonienie użytkownika Internetu do odwiedzenia danej witryny, która jest sfałszowana, choć z pozoru wygląda na identyczną (oryginalną), jak ta na którą w rzeczywistości zamierzał dostać się użytkownik. Tworzenie witryn ma na celu przede wszystkim pozyskiwanie haseł użytkowników, numerów

⁵⁹⁸ T. Lukaseder, K. Stölzle, S. Kleber, B. Erb, F. Kargl: *An SDN-based Approach For Defending Against Reflective DDoS Attacks*. „2018 IEEE 43rd Conference on Local Computer Networks (LCN)” 2019, s. 1-4.

⁵⁹⁹ M. N. O. Sadiku, A. E. Shadare, S. M. Musa: *Social Engineering: An Introduction*. „The Journal of Scientific and Engineering Research” 2016, No 3(3), s. 64-66.

⁶⁰⁰ M. Lakomy: *Cyberprzestrzeń jako nowy...*, s. 130-131.

⁶⁰¹ Ibidem, s. 131.

⁶⁰² Pełnomocnik Rządu ds. Cyberbezpieczeństwa: *Słownik kluczowych pojęć...*, s. 225.

kont bankowych, numerów PIN, czy też po prostu ich danych osobowych⁶⁰³. Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) szacuje na podstawie danych za okres od stycznia 2019 roku do kwietnia 2020 roku, że 34% wszystkich cyberataków dotyczyło wyłudzenia danych przy użyciu poczty elektronicznej (wiadomości email), w przypadku 22% ataków celem były instytucje finansowe, a w odniesieniu do 22% płatności⁶⁰⁴.

Podobnym działaniem do wyżej omówionego jest *spoofing*. Jest to podszywanie się pod legalnego użytkownika (lub zasób) w celu dokonania nieautoryzowanego dostępu do systemu teleinformatycznego, bądź też sprawienie, aby wydawało się, że dana osoba lub organizacja zainicjowała jakąś działalność cybernetyczną⁶⁰⁵. Innymi słowy jest to technika działania polegająca na uzyskaniu nieautoryzowanego dostępu do komputerów, dzięki czemu intruz wysyła wiadomości do komputera z adresem IP wskazującym, że dany przekaz pochodzi od zaufanego nadawcy (hosta)⁶⁰⁶. Do rodzajów *spoofingu* zaliczamy *random spoofing*, *subnet spoofing* i *fixed spoofing*⁶⁰⁷. Jednym z częstszych sposobów stosowania *spoofingu* jest wykorzystywanie połączeń telefonicznych (*Caller ID Spoofing*), poprzez podszywanie się danej osoby pod wybrany numer telefonu w taki sposób, że odbiorca połączenia myśli, że rozmawia np. z pracownikiem banku czy też innej instytucji⁶⁰⁸.

Wreszcie wskazać należy na cyberataki dokonywane z wykorzystaniem sieci *botnet*. Geneza ich istnienia sięga roku 1988, kiedy to został uruchomiony robak Morris Worm, a w wyniku jego działalności powstała sieć składająca się z 6.000 komputerów⁶⁰⁹. *Botnet* można zdefiniować jako sieć zainfekowanych urządzeń, czyli *botów*, które są zdalnie kontrolowane przez inną osobę i wykorzystywane do przeprowadzania operacji lub przestępstw w cyberprzestrzeni. Co istotne nie istnieje jakakolwiek liczba graniczna urządzeń, które mogą zostać zwerbowane do *botnetu*⁶¹⁰. Dla przykładu, jeden z największych *botnetów* na świecie, powstały w 2009 roku i zniszczony w 2010 roku o nazwie BredoLab skupiał około 30 milionów komputerów, z kolei *botnet* Mariposa funkcjonujący w latach 2008-2009 łączył około 12

⁶⁰³ J. A. Chaudhry, S. Chaudhry, R. G. Rittenhouse: *Phishing Attacks and Defenses*. „International Journal of Security and its Applications” 2016, No 10(1), s. 247-255.

⁶⁰⁴ European Union Agency for Cybersecurity: *Wyłudzenie informacji (phishing)*. <https://www.enisa.europa.eu/publications/report-files/ETL-translations/pl/etl2020-phishing-ebook-en-pl.pdf> (dostęp: 14.10.2022).

⁶⁰⁵ M. N. Schmitt (Red.): *Tallinn Manual on the International...*, s. 214.

⁶⁰⁶ S. Gupta: *Types of Malware and its Analysis...*, s. 5.

⁶⁰⁷ Q. Gu, P. Liu: *Denial of Service Attacks*. <https://s2.ist.psu.edu/paper/ddos-chap-gu-june-07.pdf> (dostęp: 15.10.2022).

⁶⁰⁸ Federal Communications Commission: *Consumer Guide. Caller ID Spoofing*. https://www.fcc.gov/sites/default/files/caller_id_spoofing.pdf (dostęp: 14.10.2022).

⁶⁰⁹ T. Eisenberg, D. Gries, J. Hartmanis, D. Holcomb, M. S. Lynn, T. Santoro: *The Cornell Commission: On Morris and the Worm*. „Communications of the ACM” 1989, Vol. 32, Number 6, s. 706-707.

⁶¹⁰ M. N. Schmitt (Red.): *Tallinn Manual on the International...*, s. 210.

milionów komputerów⁶¹¹. Celem działalności *botnetów* jest przede wszystkim dokonywanie ataków DDoS czy też rozsyłanie spamu poprzez przejęcie kontroli nad danym komputerem, oczywiście bez wiedzy użytkownika⁶¹².

⁶¹¹ J. Kowalewski, M. Kowalewski: *Zagrożenia informacji w cyberprzestrzeni...*, s. 56.

⁶¹² European Union Agency for Cybersecurity: *Botnet*. <https://www.enisa.europa.eu/publications/report-files/ETL-translations/pl/etl2020-botnet-ebook-en-pl.pdf> (dostęp: 14.10.2022).

Rozdział 3. Założenia metodologiczne badań

3.1. Problem badawczy

Problem badawczy rozprawy koncentruje się na zagadnieniach dotyczących wojny informacyjnej jako instrumentu polityki zagranicznej realizowanej przez Federację Rosyjską wobec Polski w latach od 2010 do 2022 roku. Praca zmierza do odpowiedzi na pytanie, czy działania podejmowane przez Kreml w cyberprzestrzeni wobec Polski mogą zostać uznane za środek polityki zagranicznej, realizujący interesy narodowe państwa – Rosji. Jest to więc również postawienie pytania, jak elementy składające się na zjawisko wojny informacyjnej mogą być wykorzystywane przez państwa oraz na jakich płaszczyznach i wektorach. Następnie wykazanie czy, a jeśli tak to jak i w jakim zakresie, na powyższym gruncie operuje Federacja Rosyjska. W kontekście stosunków polsko-rosyjskich zagadnieniem badawczym pozostaje próba udzielenia odpowiedzi na pytanie jak powyższe kwestie implikują stosunki polsko-rosyjskie, a w konsekwencji wskazanie, czy Moskwa korzysta z instrumentów wojny informacyjnej do prowadzenia polityki zagranicznej wobec Polski. Wojna informacyjna jest zjawiskiem niezwykle złożonym, dlatego też mając na względzie różne jej płaszczyzny definicyjne oraz sfery występowania przyjęto, że może ona polegać zarówno na dokonywaniu ataków w cyberprzestrzeni, jak i na oddziaływaniu informacyjnym na odbiorców w Internecie. Powstają więc pytania, po pierwsze, w jaki sposób Federacja Rosyjska wykorzystywała cyberprzestrzeń do nieprzyjaznych działań wobec Polski oraz jaki charakter miały związane z tym incydenty teleinformatyczne, będące skutkiem działalności Kremla. Po drugie, w jaki sposób Rosja korzystała z drugiego wektora wojen informacyjnych, a więc działalności propagandowej w Internecie (względem polskich odbiorców), jak również jakie implikacje dla stosunków polsko-rosyjskich wystąpiły w kontekście przedmiotowych działań.

3.2. Cele badawcze

Głównym celem badawczym niniejszej rozprawy jest określenie uwarunkowań, charakteru oraz implikacji rosyjskiej wojny informacyjnej wobec Polski w latach 2010-2022. Praca zmierza przede wszystkim do określenia i scharakteryzowania jej uwarunkowań oraz celów pośrednich i bezpośrednich, jakie dzięki niej realizuje Federacja Rosyjska. Ponadto, rozprawa dąży do określenia instrumentów jakie do tego wykorzystuje, a także do wskazania najważniejszych implikacji powyższych działań. Należy również zaznaczyć, że w ramach

niniejszej rozprawy rosyjska wojna informacyjna jest postrzegana zarówno jako oddziaływanie propagandowe na odbiorców w Internecie, jak i jako działania prowadzone w cyberprzestrzeni poprzez dokonywanie cyberataków. W związku z tym, celem pracy jest omówienie narzędzi i technik propagandowych jakie są wykorzystywane w prorosyjskich kanałach informacyjnych w Internecie, w przekazach dotyczących polski i relacji polsko-rosyjskich, jak również przedstawienie cech charakterystycznych rosyjskich ataków w cyberprzestrzeni wobec Polski.

Przyjęto następujące szczegółowe cele badawcze (CS):

CS 1) Przedstawienie stanu badań w zakresie pojęcia wojny informacyjnej jako instrumentu polityki zagranicznej oraz definicji wojny informacyjnej, jej cech, uwarunkowań oraz celów w odniesieniu zarówno do oddziaływania informacyjnego na odbiorcę w Internecie oraz cyberataków w cyberprzestrzeni. Przedstawienie zjawiska wojny informacyjnej na gruncie stosunków międzynarodowych oraz jako instrumentu realizowanej przez państwa polityki zagranicznej (oddziaływania na środowisko międzynarodowe).

CS 2) Omówienie uwarunkowań wykorzystania wojny informacyjnej jako instrumentu polityki zagranicznej Federacji Rosyjskiej. Określenie jej potencjału w zakresie prowadzenia wojny informacyjnej w cyberprzestrzeni. Ponadto dokonanie omówienia rosyjskich koncepcji wojny informacyjnej oraz ich zestawienia z koncepcjami formułowanymi przez badaczy zachodnich. Wskazanie podstawowych różnic w zakresie cech, instrumentów oraz celów jakie wiążą się z rozumieniem omawianego zjawiska w Rosji oraz na Zachodzie.

CS 3) Określenie uwarunkowań i celów rosyjskiej polityki zagranicznej Federacji Rosyjskiej wobec Polski w latach 2010-2022 oraz zidentyfikowanie i omówienie głównych kwestii spornych występujących w stosunkach polsko-rosyjskich w ramach których Rosja prowadzi wojnę informacyjną wobec Polski. Ponadto wskazanie najważniejszych implikacji głównych kwestii spornych i ich oddziaływania na stosunki bilateralne na linii Warszawa-Moskwa. Wreszcie, omówienie najważniejszych instrumentów jakie wykorzystuje Federacja Rosyjska do prowadzenia wojny informacyjnej wobec Polski.

CS 4) Określenie podatności Polski w cyberprzestrzeni na prowadzoną przez Rosję wojnę informacyjną, jak również potencjału państwa polskiego w zakresie zapewnienia cyberbezpieczeństwa oraz wykrywania i zwalczania cyberataków. Następnie wskazanie ich głównych celów oraz scharakteryzowanie narzędzi i technik wykorzystywanych przez Rosję do prowadzenia operacji w cyberprzestrzeni wobec Polski, jak również wskazanie ich najważniejszych implikacji. Wreszcie skorelowanie podejmowanych działań z realizowaną przez Kreml polityką zagraniczną wobec Polski oraz z kampaniami oddziaływania informacyjnego na odbiorców w Internecie przy wykorzystaniu propagandowych portali

informacyjnych. Po przeprowadzeniu badań w przedmiotowym zakresie nastąpiło wskazanie czy, jakie oraz jak często atakowane są poszczególne podmioty w Polsce. Nastąpi również zidentyfikowanie częstotliwości pojawiania się incydentów teleinformatycznych oraz ich korelacji z występującymi w stosunkach polsko-rosyjskich kwestiami spornymi. Możliwe stanie się ustalenie charakteru i implikacji działalności cyberprzestępczej w kontekście szpiegostwa gospodarczego, działalności wywiadowczej oraz cyberataków wobec infrastruktury krytycznej.

CS 5) Zidentyfikowanie głównych kanałów oddziaływania propagandowego, które są wykorzystywane w Internecie przez Federację Rosyjską wobec Polski oraz określenie technik propagandowych, które są w tym zakresie stosowane. Następnie zestawienie ich z kwestiami spornymi występującymi w stosunkach polsko-rosyjskich oraz ukazanie najważniejszych implikacji z tym związanych. Zrealizowanie celu stało się możliwe dzięki omówieniu uwarunkowań wykorzystania wojny informacyjnej jako instrumentu polityki zagranicznej Rosji. Ponadto określeniu uwarunkowań i celów polityki zagranicznej Kremla wobec Polski w latach 2010-2022. Wreszcie zidentyfikowaniu i omówieniu kwestii spornych w stosunkach polsko-rosyjskich w ramach których Kreml prowadzi wojnę informacyjną.

3.3. Hipotezy badawcze

Hipoteza główna przedmiotowej rozprawy zawiera się w następującym stwierdzeniu: Wojna informacyjna jako instrument polityki zagranicznej prowadzonej przez Federację Rosyjską stale zyskuje na znaczeniu, co należy odnieść również do stosunków polsko-rosyjskich. Rosja w ramach prowadzonej wojny informacyjnej wobec Polski wykorzystuje techniki i narzędzia propagandowe, które służą oddziaływaniu informacyjnemu na odbiorcę. Działania te podejmowane są za pośrednictwem rosyjskich portali informacyjnych. Wojna informacyjna Federacji Rosyjskiej wobec Polski przejawia się również przeprowadzaniem ataków w cyberprzestrzeni wobec Polski. Działania podejmowane w ramach wskazanych wymiarów są komplementarne względem siebie. Celem podejmowanych przez Rosję operacji jest przede wszystkim osłabianie struktur wewnątrzpaństwowych, pogłębianie podziałów społecznych, marginalizowanie pozycji Polski na arenie międzynarodowej, kreowanie jej negatywnego wizerunku na arenie międzynarodowej, a przede wszystkim realizowanie własnych interesów. **Przyjęto następujące szczegółowe hipotezy badawcze (HS):**

HS 1) Rewolucja informatyczna oraz przemiany technologiczne spowodowały, że wojna informacyjna może być wykorzystywana przez państwa na niespotykaną dotąd skalę globalną,

a jej celem jest realizacja własnych interesów na arenie międzynarodowej. Prowadzenie wojny informacyjnej jest możliwe poprzez dokonywanie cyberataków oraz oddziaływanie informacyjne na odbiorcę w Internecie. Powstanie na przełomie XX i XXI wieku społeczeństwa informacyjnego miało swój związek z postępującymi procesami informatyzacji oraz digitalizacji życia społecznego. Spowodowało to powstanie nowych zagrożeń dla bezpieczeństwa teleinformatycznego w wymiarze narodowym oraz międzynarodowym.

HS 2) Rosja zaadaptowała się do przemian technologicznych związanych z postępującą rewolucją informatyczną, które wykorzystuje do prowadzenia wojny informacyjnej. Ponadto posiada infrastrukturę zdolną do prowadzenia operacji informacyjnych w skali globalnej oraz zaplecze defensywne, umożliwiające przeciwdziałanie operacjom informacyjnym. Rosja postrzega wojnę informacyjną jako instrument realizacji własnej polityki zagranicznej. Postrzeganie informacji jako broni jest głęboko zakorzenione w rosyjskiej kulturze strategicznej, a geneza związanych z tym koncepcji ma swój początek w okresie istnienia Związku Socjalistycznych Republik Radzieckich.

HS 3) Polska, ze względu na swoje geostrategiczne położenie, znajduje się w obszarze zainteresowania decydentów politycznych w Rosji. W ramach stosunków polsko-rosyjskich można wyróżnić główne kwestie sporne, na podstawie których Rosja prowadzi wojnę informacyjną wobec Polski. Są to: polityka historyczna, dywersyfikacja źródeł energii, polityka bezpieczeństwa w Europie Środkowo-Wschodniej, polityka bezpieczeństwa NATO, katastrofa samolotu rządowego z Prezydentem Rzeczypospolitej Polskiej w Smoleńsku, aneksja Półwyspu Krymskiego i wojna w Ukrainie oraz program Partnerstwa Wschodniego.

HS 4) Rosja posiada zasoby i zdolności, które wykorzystuje do przeprowadzania ataków w cyberprzestrzeni wobec Polski. Cyberataki dokonywane są na sektor publiczny i prywatny. W sektorze publicznym ich celem jest prowadzenie operacji wywiadowczych oraz atakowanie polskiej infrastruktury krytycznej. Ponadto jest to wspieranie kampanii oddziaływania informacyjnego na odbiorców w Internecie poprzez dostarczanie materiałów źródłowych oraz wspomaganie bieżącej działalności. W stosunku do sektora prywatnego jest to działalność przestępcza polegająca na cyberszpiegostwie gospodarczym oraz na naruszaniu infrastruktury teleinformatycznej poszczególnych podmiotów. Przeprowadzane operacje są komplementarne w stosunku do oddziaływania informacyjnego prowadzonego w ramach funkcjonowania rosyjskich portali informacyjnych. Takie ujęcie zagadnienia wojny informacyjnej wpisuje się w rosyjskie koncepcje tego zjawiska i znajduje swoje odzwierciedlenie w środkach jakie Kreml wykorzystuje do prowadzenia polityki zagranicznej. Cyberataki realizowane przez Moskwę w cyberprzestrzeni wobec Polski mają na celu nie tylko paraliżowanie infrastruktury

teleinformatycznej państwa, ale również dostarczanie informacji na potrzeby prowadzenia kampanii oddziaływania informacyjnego, przy wykorzystaniu rosyjskich portali informacyjnych.

HS 5) Federacja Rosyjska prowadzi wojnę informacyjną wykorzystującą między innymi portal informacyjny Sputnik News International oraz portal internetowy agencji informacyjnej TASS. Narracja publikowanych przez nie treści jest zbieżna z celami rosyjskiej polityki zagranicznej wobec Polski oraz realizowana w oparciu o występujące kwestie sporne w stosunkach bilateralnych. W ramach oddziaływania propagandowego (informacyjnego) Kreml stosuje większość standardowych technik propagandowych. Publikowane przez Rosjan treści charakteryzują się różnorodną tematyką, a do najczęstszych jej kategorii z uwagi na typ zalicza się: polityczne, militarne, gospodarcze, społeczne, technologiczne, ideologiczne oraz religijne. Do głównych celów rosyjskich kampanii oddziaływania informacyjnego należy zaliczyć: „oczernianie Warszawy na arenie międzynarodowej; osłabianie relacji Polski z państwami sąsiednimi i partnerami; destabilizacja współpracy wojskowej Polski w ramach NATO; wzniecanie działań wojennych między Polską a USA; atak na polską politykę energetyczną; ośmieszanie i poniżanie Sił Zbrojnych RP; piętnowanie Polski jako przesiąkniętej nastrojami antyrosyjskimi; obwinianie Polski za pogorszenie stosunków między Rosją a Zachodem”⁶¹³. Należy podkreślić, że w prezentowanym ujęciu rosyjska wojna informacyjna jest postrzegana dwuwektorowo. Po pierwsze jako działalność sprowadzająca się do prowadzenia kampanii oddziaływania informacyjnego wobec odbiorców w Internecie, oraz przy wykorzystaniu określonych technik propagandowych, *framingu*, jak również poruszania zagadnień odnoszących się do występujących w stosunkach polsko-rosyjskich kwestii spornych. Po drugie poprzez dokonywanie ataków w cyberprzestrzeni wobec Polski. Należy szczególnie podkreślić, że działania te są wobec siebie komplementarne, realizując tym samym funkcję wspierającą i uzupełniającą.

3.4. Cezura czasowa badań

Dolną granicą cezury czasowej badań jest 2010 rok. Przyjęcie tej daty wynikało z niezwykle istotnego wydarzenia dla stosunków polsko-rosyjskich, jakim była katastrofa polskiego samolotu Tu-154 w Smoleńsku w wyniku której śmierć ponieśli wszyscy obecni na pokładzie pasażerowie, w tym ówczesny Prezydent RP L. Kaczyński. Wydarzenie to wywarło

⁶¹³ gov.pl: *Disinformation against Poland in 2020 – special services’ view*. <https://www.gov.pl/web/sluzby-specjalne/disinformation-against-poland-in-2020--special-services-view> (dostęp: 25.05.2023).

zasadniczy wpływ na stosunki polsko-rosyjskie w drugiej dekadzie XXI wieku, nadając im zupełnie nowy wymiar. W początkowym okresie wydawało się, że tragedia jakiejś doświadczył polski naród i związana z nią reakcja rosyjska, staną się punktem zwrotnym, w konsekwencji którego dojdzie do pojednania odwiecznie zwaśnionych państw. Katastrofę smoleńską można więc nazwać swego rodzaju resetem w stosunkach polsko-rosyjskich. Pomimo tego do pojednania ostatecznie nie doszło, a omawiane wydarzenia stały się nowym pretekstem do wzajemnych oskarżeń, pomówień i napięć⁶¹⁴.

Cezurę czasową badań przyjęto również w oparciu o etapy oraz zmiany jakie następowały w stosunkach polsko-rosyjskich na przestrzeni lat. Powstały w związku z katastrofą smoleńską impas w relacjach bilateralnych trwał w latach 2011-2013, a główną osią sporu stało się wyjaśnienie jej przyczyn⁶¹⁵. W następnym okresie kluczową kwestią sporną była nielegalna z punktu widzenia prawa międzynarodowego publicznego aneksja Półwyspu Krymskiego (2014) oraz dążenia Ukrainy do większej integracji z Unią Europejską (co wiązało się ze sprzeciwem Kremla)⁶¹⁶. Problemowe pozostawały również kwestie energetyczne, przez co należy rozumieć prowadzoną przez Polskę politykę dywersyfikacji źródeł energii i uniezależnianie się od Rosji⁶¹⁷. W 2015 roku władzę w Polsce objął prawicowy rząd Prawa i Sprawiedliwości, co przełożyło się na zaostrzenie realizowanej przez Warszawę polityki wschodniej⁶¹⁸. W kolejnych latach doszło do zacieśnienia współpracy z Ukrainą na rzecz jej integracji ze strukturami UE oraz NATO, czemu nadal sprzeciwiała się Rosja⁶¹⁹. Wciąż żywe pozostawały koncepcje dywersyfikacji źródeł energii, ale również zwiększanie obecności militarnej Sojuszu Północnoatlantyckiego na tzw. flance wschodniej, a więc również

⁶¹⁴ M. Stolarczyk: *Rosja w polityce zagranicznej Polski w latach 1992-2015*. Katowice 2016, s. 219-225; K. Fedorowicz: *Polska w polityce zagranicznej Rosji w latach 1991-2001*. W: *Polska w Rosji – Rosja w Polsce. Stosunki Polityczne*. Red. R. Paradowski, Sz. Ossowski. Poznań 2003, s. 156-160.

⁶¹⁵ Zobacz szerzej: Ibidem.

⁶¹⁶ M. Banasik: *Bezpieczeństwo Europy Środkowo-Wschodniej w aspekcie zagrożeń płynących z Federacji Rosyjskiej*. „Środkoeuropejskie Studia Polityczne” 2020, nr (2), s. 5; A. Rogozińska: *Analiza zagrożeń kreowanych w cyberprzestrzeni*. W: *Rosja wobec państw Europy Środkowej i Wschodniej: zagrożenia pozamilitarne*. Red. T. Stępniewski. Lublin 2020, s. 69.

⁶¹⁷ *Obwieszczenie Ministra Gospodarki i Pracy z dnia 1 lipca 2005 r. w sprawie polityki energetycznej państwa do 2025 r.* (Monitor Polski 2005 nr 42 poz. 562); *Obwieszczenie Ministra Klimatu i Środowiska z dnia 2 marca 2021 r. w sprawie polityki energetycznej państwa do 2040 r.* (Monitor Polski 2021 r. poz. 264); M. Stolarczyk: *Rosja w polityce zagranicznej Polski...*, s. 248.

⁶¹⁸ Zobacz szerzej: R. Zięba: *Główne problemy w stosunkach polsko-rosyjskich*. „Stosunki Międzynarodowe – International Relations” 2018, nr 3 (T. 54).

⁶¹⁹ Zobacz szerzej: M. Stolarczyk: *Kontrowersje wokół koncepcji i praktyki polityki wschodniej Polski na przełomie pierwszej i drugiej dekady XXI wieku*. W: *Śląsk - Polska - Europa - świat: pamięci Profesora Jana Przewłockiego*. Red. K. Miroszewski, M. Stolarczyk. Katowice 2013; M. Raś: *Cele oddziaływań politycznych Federacji Rosyjskiej*. W: *Rosja wobec państw Europy Środkowej i Wschodniej: zagrożenia pozamilitarne*. Red. T. Stępniewski. Lublin 2020.

w Polsce⁶²⁰. W zasadzie przez cały okres, tj. w latach 2010-2022 niezmienną kwestią sporną pozostawała polityka historyczna, w szczególności wizja roli obu państw jaką odegrały one podczas II wojny światowej⁶²¹.

Ostatecznie pełnowymiarowa rosyjska agresja na Ukrainę w 2022 roku doprowadziła do niespotykanego po zakończeniu zimnej wojny impasu w stosunkach polsko-rosyjskich, co legło u podstaw przyjęcia tej daty rocznej, jako krańcowego punktu prowadzonych badań. Ponadto bezprecedensowe wsparcie jakie zostało udzielone względem Kijowa przez Warszawę (militarne, humanitarne oraz polityczne na arenie międzynarodowej) pozostawało w sprzeczności z interesami rosyjskimi. Choć na koniec 2022 roku implikacje wskazanego konfliktu dla relacji na linii Moskwa-Warszawa są niezwykle trudne do przewidzenia, to z całkowitą pewnością będą one kluczowe w przyszłości. Wynika to z ich dotychczasowego kształtu, jak również zarysowanych wyżej głównych kwestii spornych⁶²².

Wskazać również należy, że przez cały okres, tj. od 2010 do 2022 roku stosunki polsko-rosyjskie pozostawały niezwykle napięte, co sprowadza się do ich z roku na rok nieustannego antagonizowania. Do najważniejszych kwestii spornych w stosunkach bilateralnych które rzutowały na kształt przyjętej cezury czasowej, ale również które stały się przedmiotem badań w rozprawie, można zaliczyć: politykę historyczną, dywersyfikację źródeł energii, politykę bezpieczeństwa w Europie Środkowo-Wschodniej, politykę bezpieczeństwa NATO, katastrofę samolotu rządowego z Prezydentem Rzeczypospolitej Polskiej w Smoleńsku, aneksję Półwyspu Krymskiego i wojnę w Ukrainie oraz program Partnerstwa Wschodniego⁶²³.

3.5. Metodologia badań

Przedmiotem niniejszego podrozdziału są założenia metodologiczne badań w zakresie przyjętych trzech wektorów analizy. Pierwszy stanowią założenia badań nad wojną

⁶²⁰ A. Bodrov: *Bezpieczeństwo europejskie – wizja Rosji*. W: *Polska i Rosja w zmieniającej się Europie*. Red. K. A. Wojtaszczyk, I. N. Novikova. Warszawa 2022, s. 269-270; S. Koziej, P. Pietrzak: *Szczyt NATO w Newport*. „Bezpieczeństwo Narodowe” 2014, nr 2014/III, s. 11-29.

⁶²¹ M. Stolarczyk: *Rosja w polityce zagranicznej Polski...*, s. 68-69; K. Fedorowicz: *Polska w polityce zagranicznej Rosji...*, s. 154.

⁶²² Rada Europejska, Rada Unii Europejskiej: *Reakcja UE wobec rosyjskiej inwazji na Ukrainę*. <https://www.consilium.europa.eu/pl/policies/eu-response-ukraine-invasion/> (dostęp: 28.06.2023); U.S. Department of the Treasury: *Ukraine-/Russia-related Sanctions*. <https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/ukraine-russia-related-sanctions> (dostęp: 28.06.2023); U.S. Department of State: *U.S. Security Cooperation with Ukraine*. <https://www.state.gov/u-s-security-cooperation-with-ukraine/> (dostęp: 28.06.2023).

⁶²³ Każda ze wskazanych głównych kwestii spornych w stosunkach polsko-rosyjskich została szczegółowo omówiona w dalszej części pracy, dlatego też w tym miejscu wyłącznie je zarysowano.

informacyjną jako instrumentem polityki zagranicznej Federacji Rosyjskiej oraz polityką zagraniczną Federacji Rosyjskiej wobec Polski w latach 2010-2022. Drugi odnosi się do badań nad rosyjskimi atakami teleinformatycznymi w cyberprzestrzeni wobec Polski w latach 2010-2022, natomiast trzeci do badań nad rosyjskimi portalami informacyjnymi jako instrumentami wojny informacyjnej Federacji Rosyjskiej wobec Polski w latach 2010-2022.

Każdy z przyjętych trzech wektorów analizy znalazł swoje odzwierciedlenie w danym podrozdziale. Obejmują one założenia metodologiczne, które posłużyły autorowi rozprawy do przeprowadzenia badań będących jej przedmiotem. Ponadto każdy z trzech wektorów analizy został dedykowany i przyporządkowany do poszczególnych szczegółowych celów badawczych pracy, które wskazano w treści każdego z opracowanych podrozdziałów.

3.5.1. Założenia metodologiczne badań nad wojną informacyjną jako instrumentem polityki zagranicznej Federacji Rosyjskiej oraz polityką zagraniczną Federacji Rosyjskiej wobec Polski w latach 2010-2022

Zanim zostaną przedstawione założenia metodologiczne przedmiotowego wektora analizy, w pierwszej kolejności należy omówić zagadnienie poziomów analizy w nauce o stosunkach międzynarodowych. Jest to zagadnienie niezwykle istotne, gdyż to właśnie od wyboru poziomu analizy zależeć będzie granica obszaru badań, przyjęcie określonych założeń oraz ram teoretycznych. Można więc wyróżnić poziom pierwszy, czyli jednostkowy-indywidualistyczny. Jak wskazał E. Halizak, „Poziom jednostkowy analizy jest ważny ponieważ ludzie odgrywają ważną rolę jako decydenci w polityce zagranicznej państwa a także instytucjach międzynarodowych. Rola jednostki ludzkiej w konstruowaniu dziedziny stosunków międzynarodowych (polityki międzynarodowej jest szczególnie doceniana w konstruktywistycznej teorii stosunków międzynarodowych, gdzie przypisuje się jej wręcz centralna rolę w tym procesie”⁶²⁴. Następnie ten sam autor wyróżnił poziom państwa, czyli podmiotu będącego pierwotnym uczestnikiem stosunków międzynarodowych. W dalszej kolejności poziom bilateralny, a więc odnoszący się do relacji dwustronnych poszczególnych państw. Ponadto wskazał na trilateralizm, będący specyficzną formą wielobiegunowości, a więc analizy z perspektywy relacji zachodzących pomiędzy trzema podmiotami na arenie międzynarodowej. Następnie wyróżnił poziom regionalny (kontynentalny), dotyczących

⁶²⁴ E. Halizak: *Poziomy analizy w nauce o stosunkach międzynarodowych*. <https://ptsm.edu.pl/wp-content/uploads/publikacje/poziomy-analizy-stosunkow-miedzynarodowych/Halizak2.pdf> (dostęp: 14.06.2023), s. 6.

analizy regionalnej integracji ekonomicznej czy politycznej. Wreszcie, wskazał na globalny-systemowy poziom analizy, który koncentruje się na bazie dwóch założeń zgodnie z którymi stosunki międzynarodowe to system państw oraz społeczność międzynarodowa identyfikowana w oparciu o kryteria kulturowo-cywilizacyjne⁶²⁵.

Przeprowadzone badania dotyczące rosyjskiej wojny informacyjnej posłużą przede wszystkim zrozumieniu prowadzonej przez Kreml polityki zagranicznej wobec Polski. Należy bowiem zaznaczyć, że to właśnie polityka zagraniczna i wynikające z niej cele stanowią punkt wyjścia do podejmowanych przez Rosję działań w wymiarze transnarodowym, między innymi tych będących przedmiotem niniejszej rozprawy. W. Kostecki wyróżnił w tym kontekście trzy poziomy analizy polityki zagranicznej wskazując na: „a) poziom międzynarodowy (...); b) poziom państwowy (...); c) poziom decyzji”⁶²⁶. Na gruncie przedmiotowej rozprawy analiza polityki zagranicznej została przeprowadzona na poziomie państwowym, czyli w odniesieniu do państwa jako podmiotu będącego pierwotnym i najistotniejszym z uczestników stosunków międzynarodowych (postrzeganie polityki zagranicznej państwa jako wyniku splotu uwarunkowań wewnętrznych). Ponadto na poziomie bilateralnym odnoszącym się do areny międzynarodowej (rozumieć przez to należy reakcję państwa na bodźce, których źródłem jest środowisko zewnętrzne) oraz w kontekście stosunków polsko-rosyjskich. Wreszcie na poziomie decyzji, czyli określania celów i środków, za pomocą których zostaną one zrealizowane – na podstawie przyjętego przez decydentów politycznych modelu procesu decyzyjnego⁶²⁷. Zauważyć przy tym należy, że „dążąc do holistycznego (całościowego) poznania polityki zagranicznej, należy – naturalnie – przyjąć kompleksową strategię postępowania badawczego, opierając się na założeniu, że wyjaśnienia budowane na poszczególnych poziomach nie mogą być traktowane jako zupełne, ani jedyne”⁶²⁸.

Na gruncie niniejszej rozprawy, badania w zakresie stosunków polsko-rosyjskich oparto na teorii neorealizmu⁶²⁹ oraz zastosowano międzynarodowy poziom analizy⁶³⁰. Realizm

⁶²⁵ Ibidem, s. 6-7.

⁶²⁶ W. Kostecki: *Poziomy analizy polityki zagranicznej*. <https://ptsm.edu.pl/wp-content/uploads/publikacje/poziomy-analizy-stosunkow-miedzynarodowych/Kostecki.pdf> (dostęp: 08.06.2023), s. 45; Zobacz szerzej: E. Haliżak, M. Pietraś (Red.): *Poziomy analizy stosunków międzynarodowych*. Warszawa 2013. <https://ptsm.edu.pl/poziomy-analizy-stosunkow-miedzynarodowych/> (dostęp: 08.06.2023).

⁶²⁷ W. Kostecki: *Poziomy analizy polityki...*, s. 45-50.

⁶²⁸ Ibidem, s. 50.

⁶²⁹ Zobacz szerzej: K. Waltz: *Theory of International Politics*. Reading, Massachusetts 1979; J. Czaputowicz: *Mapa współczesnego realizmu: realizm klasyczny, neorealizm, realizm neoklasyczny*. <https://ptsm.edu.pl/wp-content/uploads/publikacje/teoria-realizmu-w-naucze-o-stosunkach-miedzynarodowych/J.Czaputowicz.pdf> (dostęp: 22.06.2023).

⁶³⁰ Zobacz szerzej: W. Kostecki: *Poziomy analizy polityki zagranicznej*. <https://ptsm.edu.pl/wp-content/uploads/publikacje/poziomy-analizy-stosunkow-miedzynarodowych/Kostecki.pdf> (dostęp: 08.06.2023)

w ujęciu klasycznym dąży do stworzenia teorii polityki zagranicznej jako takiej, tak z kolei neorealizm ujmuje to zagadnienie zdecydowanie szerzej, dążąc do utworzenia teorii polityki międzynarodowej. W odróżnieniu od klasycznego realizmu, który skupia się na ludzkiej naturze jako źródle konfliktów, neorealizm kładzie nacisk na strukturę systemu międzynarodowego jako główny czynnik determinujący zachowanie państw. Kluczowym założeniem jest anarchiczny charakter tego systemu, co oznacza brak nadrzędnej władzy nad suwerennymi państwami. W takim środowisku państwa dążą przede wszystkim do zapewnienia sobie bezpieczeństwa i przetrwania, co prowadzi do rywalizacji i balansowania sił na arenie międzynarodowej. Neorealizm podkreśla, że to nie cechy wewnętrzne państw, ale ich pozycja w strukturze międzynarodowej oraz rozkład siły w systemie determinują ich politykę zagraniczną. Realisci uważają, że zmienną niezależną są państwa i ich interesy, natomiast zmienną zależną polityka zagraniczna państw. Neorealiści jako zmienną niezależną postrzegają strukturę systemu międzynarodowego, z kolei jako zmienną zależną rezultaty działań na arenie międzynarodowej⁶³¹. Dlatego też w ocenie autora przyjęcie na gruncie niniejszej rozprawy perspektywy neorealistycznej pozwoli na ujęcie w sposób zupełny oraz kompleksowy badanych zagadnień. Wynika to z faktu, iż skala oraz zasięg obecnych powiązań międzynarodowych (co sprowadza się do rozwoju systemu międzynarodowego) nie pozwala na wyjaśnianie zachodzących zjawisk wyłącznie poprzez interpretację jednostkowych interesów poszczególnych państw.

Badania przeprowadzono przy użyciu takich metod badawczych jak: analiza historyczna, analiza decyzyjna, analiza instytucjonalno-prawna, analiza i krytyka piśmiennictwa oraz synteza i opis. Z kolei główną metodą badawczą zastosowaną w rozprawie była analiza treści. Wszystkie metody badawcze zastosowano do zrealizowania następujących celów szczegółowych: CS1, CS2, CS3, CS4 i CS5.

Analiza treści jest dobrze znaną oraz ugruntowaną metodą w naukach społecznych i humanistycznych, a jej zastosowanie można sprowadzić do czterech elementów takich jak: (1) przygotowanie materiału badawczego, (2) kategoryzacja i kodowanie, (3) analiza i interpretacja, (4) prezentacja wyników z badań. Metoda analizy treści koncentruje się przede wszystkim na sieci pojęć oraz znaczeniu słów w warstwie jawnej treści, nie odnosząc się jednak

⁶³¹ J. Czaputowicz: *Mapa współczesnego realizmu: realizm klasyczny, neorealizm, realizm neoklasyczny*. <https://pts.edu.pl/wp-content/uploads/publikacje/teoria-realizmu-w-nauce-o-stosunkach-miedzynarodowych/J.Czaputowicz.pdf> (dostęp: 22.06.2023), s. 29, 35.

do jej kontekstu⁶³². Jest również często wykorzystywana w badaniu przekazów medialnych (artykułów/wiadomości) pod kątem występujących w nich zjawisk i procesów. Analiza treści stanowi więc badanie zarejestrowanych ludzkich przekazów, do których przykładów można zaliczyć książki, czasopisma, strony internetowe (portale), piosenki, obrazy, listy, prawa i konstytucje⁶³³. E. Babbie wskazał, że „jest szczególnie dobrze dostosowana do badania przekazów i do udzielania odpowiedzi na klasyczne pytanie w badaniach przekazów: kto mówi, co, do kogo, dlaczego, jak i z jakim skutkiem?”⁶³⁴. Analiza treści może zatem odnosić się do analizy przekazów takich jak wypowiedzi ludzi (decydentów politycznych), teksty, dokumenty, zapisy, obrazy, itp.

Do zalet zastosowanej metody należy z pewnością zaliczyć brak oddziaływania badacza na badany obszar, tzn. badacz nie wpływa na analizowane przekazy medialne (artykuły/indywidualne wiadomości), gdyż są one stałe i niezmiennie. Sprowadza się to do możliwości powtarzania badań przy uwzględnianiu innych założeń i zmiennych, jak również weryfikacji poprawności dokonanych ustaleń. W zakresie ograniczeń i ryzyk związanych z zastosowaniem omawianej metody należy z całkowitą pewnością wspomnieć o trudności przy badaniu niektórych zjawisk, które ze swej istoty mogą podlegać ciągłym przeobrażeniom. Z kolei po stronie osoby badacza zachodzi obawa zastosowania różnych wskaźników do stworzenia narzędzia badawczego, w związku z czym niezbędne przy analizie treści pozostaje precyzyjne określenie metodologii przeprowadzanego badania. Analiza treści nie jest bowiem metodą łatwą do zastosowania w badaniach, lecz wymagającą dużego nakładu pracy⁶³⁵.

Analiza treści została wykorzystana do realizacji szczegółowych celów badawczych CS1, CS2, CS3, CS4 i CS5. Jej przedmiotem były główne materiały źródłowe. Przyjęty katalog źródeł jest niezwykle szeroki, co sprowadza się do oparcia badań na licznych dokumentach rządowych (strategiach, koncepcjach, doktrynach, raportach), przede wszystkim tych opublikowanych przez Federację Rosyjską. Do najważniejszych zaliczono takie dokumenty jak: Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej zatwierdzona 9 września 2000 roku, Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej zatwierdzona 5 grudnia 2016 roku, Strategia Bezpieczeństwa Narodowego Federacji Rosyjskiej

⁶³² R. Bäcker, L. Czechowska, G. Gadomska, J. Gajda, K. Gawron-Tabor, M. Giedz, D. Kaspruwicz, M. Mateja, B. Płotka, J. Rak, A. Seklecka, W. Szewczak, M. Winławska, J. Wojciechowska: *Metodologia badań politologicznych*. Warszawa 2016, s. 84.

⁶³³ E. Babbie: *Badania społeczne w praktyce*. Warszawa 2004, s. 342.

⁶³⁴ Ibidem, s. 342.

⁶³⁵ R. Bäcker, L. Czechowska, G. Gadomska, J. Gajda, K. Gawron-Tabor, M. Giedz, D. Kaspruwicz, M. Mateja, B. Płotka, J. Rak, A. Seklecka, W. Szewczak, M. Winławska, J. Wojciechowska: *Metodologia badań...*, s. 167-168.

zatwierdzona 2 lipca 2021 roku, Koncepcja polityki zagranicznej Federacji Rosyjskiej
zatwierdzona 28 czerwca 2000 roku, Koncepcja polityki zagranicznej Federacji Rosyjskiej
zatwierdzona 15 lipca 2008 roku, Koncepcja polityki zagranicznej Federacji Rosyjskiej
zatwierdzona 12 lutego 2013 roku, Koncepcja polityki zagranicznej Federacji Rosyjskiej
zatwierdzona 30 listopada 2016 roku. Ponadto badania przeprowadzono na dokumentach
organizacji międzynarodowych (przede wszystkim Organizacji Narodów Zjednoczonych,
Sojuszu Północnoatlantyckiego oraz Unii Europejskiej) oraz publikacjach krajowych
i międzynarodowych ośrodków badawczych. W niezbędnym zakresie korzystano również
z doniesień medialnych, tj. artykułów prasowych zamieszczanych na portalach informacyjnych
przez portale specjalistyczne, gazety oraz telewizje o zasięgu krajowym i międzynarodowym.
Wreszcie wskazać należy na wykorzystanie wypowiedzi polskich oraz rosyjskich decydentów
politycznych dotyczących omawianych zagadnień, jak również na dorobek badaczy
specjalizujących się w stosunkach polsko-rosyjskich. Kodowanie w ramach analizy treści
objęło wszystkie informacje na temat rosyjskiej wojny informacyjnej, ze szczególnym
uwzględnieniem występowania tego zjawiska w Polsce, ale również w Europie Środkowo-
Wschodniej.

W ramach analizy historycznej omówiona została geneza wojny informacyjnej oraz jej
wykorzystanie jako instrumentu w ramach realizowanej przez państwa polityki zagranicznej.
Ponadto wskazane zostało w jaki sposób wojna informacyjna ewoluowała na przestrzeni lat.
Następnie analiza historyczna została zastosowana do przeprowadzenia badań w zakresie
polityki zagranicznej Federacji Rosyjskiej wobec Polski oraz stosunków polsko-rosyjskich
przed 2010 rokiem. Dzięki temu było możliwe scharakteryzowanie uwarunkowań i wpływów
minionych wydarzeń na stosunki bilateralne od 2010 do 2022 roku⁶³⁶.

Z punktu widzenia badań politologicznych, konieczne było zastosowanie analizy
decyzyjnej oraz analizy instytucjonalno-prawnej. Za ich pomocą zostały zbadane poszczególne
decyzje polityczne grup rządzących w Polsce i w Rosji, po czym wpisano je w stosunki
bilateralne. Następnie omówiono związki przyczynowo-skutkowe pomiędzy poszczególnymi
decyzjami politycznymi, a podejmowanymi działaniami przez decydentów politycznych
w ramach stosunków polsko-rosyjskich. Dzięki temu było możliwe określenie czy istniała
korelacja pomiędzy działaniami podejmowanym przez Rosję w ramach prowadzonej polityki
zagranicznej, a działaniami z zakresu rosyjskiej wojny informacyjnej wobec Polski. Wreszcie
stało się możliwe wyjaśnienie zjawisk na arenie międzynarodowej i ich wpływu na kształt

⁶³⁶ Zobacz szerzej: J. Topolski: *Metodologia Historii*. Warszawa 1968; J. Pomorski (Red.): *Historia, metodologia, współczesność*. Lublin 1998.

podejmowanych przez decydentów politycznych decyzji. Przy zastosowaniu drugiej ze wskazanych metod została przeprowadzona analiza aktów normatywnych dotyczących relacji bilateralnych na linii Moskwa-Warszawa. Były to przede wszystkim zawarte umowy międzynarodowe, dwustronne oraz wielostronne⁶³⁷.

Kolejną zastosowaną metodą była analiza porównawcza (komparatystyka). Pozwoliła ona na zestawienie wybranych kwestii spornych występujących w stosunkach polsko-rosyjskich (na przestrzeni lat 2010-2022), z wynikami badań w zakresie rosyjskiej działalności wobec Polski w cyberprzestrzeni oraz działaniami z zakresu oddziaływania informacyjnego na odbiorców w Internecie. Dzięki temu możliwe było ukazanie czy otrzymane wyniki badań korelowała z aktualnym stanem stosunków polsko-rosyjskich.

Za pomocą analizy i krytyki piśmiennictwa, analizy i krytyki źródeł oraz syntezy i opisu, zbadany został dotychczasowy dorobek badaczy w zakresie polityki zagranicznej Federacji Rosyjskiej wobec Polski oraz jej implikacji dla stosunków polsko-rosyjskich. Ponadto były to uwarunkowania oraz główne kwestie sporne, ale również kwestie związane z zagadnieniem wojny informacyjnej w polityce zagranicznej Kremla⁶³⁸. Wskazane metody miały charakter uzupełniający względem wyżej omówionych.

3.5.2. Założenia metodologiczne badań nad rosyjskimi atakami w cyberprzestrzeni wobec Polski w latach 2010-2022

W pierwszej kolejności należy wskazać na trudności związane z analizą rosyjskiej aktywności wobec Polski w cyberprzestrzeni, co wynika ze stosunkowo niskiej dostępności materiałów źródłowych. Aktywność podmiotów w cyberprzestrzeni danego państwa w dobie informatyzacji oraz digitalizacji, stanowi kluczowy przedmiot jego zainteresowania z punktu widzenia zapewnienia bezpieczeństwa, zarówno w wymiarze narodowym, jak i międzynarodowym. Z tego też względu znaczna część materiałów pozostaje niejawna, co z kolei może potencjalnie utrudniać zidentyfikowanie sprawców danego cyberataku. Następnie należy zauważyć, że przedmiot niniejszych badań pozostaje nie tylko w obszarze zainteresowania nauk społecznych, ale również nauk ścisłych i technicznych. Analogicznie, powyższy stan rzeczy ma również miejsce w przypadku badań nad konsekwencjami

⁶³⁷ Zobacz szerzej: D. Marsh, G. Stoker (Red.): *Teorie i metody w naukach politycznych*. Kraków 2006.

⁶³⁸ Zobacz szerzej: E. Babbie: *Badania społeczne w praktyce...*; R. Bäcker, L. Czechowska, G. Gadomska, J. Gajda, K. Gawron-Tabor, M. Giedz, D. Kasprowicz, M. Mateja, B. Płotka, J. Rak, A. Seklecka, W. Szewczak, M. Winławska, J. Wojciechowska: *Metodologia badań...*

incydentów teleinformatycznych w cyberprzestrzeni. Ponadto każda z nauk wykształciła w tym zakresie własny – odpowiedni dla danej dziedziny – aparat pojęciowy, co do którego niejednokrotnie występują spory terminologiczne. Tym samym w rozprawie bazując na dotychczasowych osiągnięciach powyższych dziedzin zrealizowano badania przede wszystkim z perspektywy stosunków międzynarodowych.

W celu sprostania opisanym wyżej wyzwaniom oraz problemom, w pracy zostały przeprowadzone badania dotyczące rosyjskiej aktywności wobec Polski w cyberprzestrzeni, przy użyciu następujących metod badawczych: analizy treści, analizy decyzyjnej, analizy instytucjonalno-prawnej, metody komparatywnej oraz analizy interwałowej. Analiza zgromadzonego na potrzeby pracy materiału źródłowego miała charakter ilościowy oraz jakościowy. Wybrane metody badawcze pozwoliły na ujęcie omawianych zagadnień w sposób kompleksowy oraz zupełny, przy uwzględnieniu przyjętych szczegółowych celów badawczych.

Podstawową metodą badawczą wykorzystaną w rozprawie była analiza treści⁶³⁹. W badaniach oparto się przede wszystkim na raportach rocznych dwóch kluczowych podmiotów w Polsce, które zajmują się omawianymi zagadnieniami, tj. Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV działającego przy Agencji Bezpieczeństwa Wewnętrznego (ABW)⁶⁴⁰ oraz Zespołu CERT Polska działającego w strukturach Naukowej i Akademickiej Sieci Komputerowej (NASK)⁶⁴¹. Wskazane instytucje z uwagi na rolę oraz zadania jakie wypełniają w ramach funkcjonującego w Polsce Krajowego Systemu Cyberbezpieczeństwa⁶⁴², posiadają w ocenie autora najpełniejszą wiedzę w zakresie omawianych zagadnień. Publikowane przez nie raporty roczne stanowią stosunkowo szeroką analizę incydentów teleinformatycznych do których dochodziło względem Polski w cyberprzestrzeni.

W uzupełnieniu pozyskanych z tych źródeł danych odwołano się również do raportów prywatnych przedsiębiorstw, które zajmują się tematyką dotyczącą cyberbezpieczeństwa oraz incydentami teleinformatycznymi na świecie. Są to przede wszystkim Symantec, FireEye, RAND Corporation, F-Secure, Kaspersky Lab czy Microsoft. W ramach badań posłużono

⁶³⁹ E. Babbie: *Badania społeczne w praktyce...*, s. 342.

⁶⁴⁰ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raporty o stanie bezpieczeństwa cyberprzestrzeni RP*. <https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi> (dostęp: 29.05.2023); Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raporty z działalności zespołu CERT.GOV.PL*. <https://csirt.gov.pl/cer/publikacje/raporty-z-dzialalnosci> (dostęp: 29.05.2023).

⁶⁴¹ CERT Polska: *Publikacje CERT Polska*. <https://cert.pl/publikacje/> (dostęp: 29.05.2023).

⁶⁴² Zobacz szerzej: *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (Dz.U. 2018 poz. 1560).

się również raportami i dokumentami publikowanymi przez rządy państw (w tym Polski) oraz raportami organizacji międzynarodowych, jak chociażby działającej w ramach Unii Europejskiej, Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)⁶⁴³. Wreszcie dokonano analizy pozostałych źródeł badawczych do których zaliczono publikacje ekspertów w dziedzinie cyberbezpieczeństwa oraz treści zawarte na portalach internetowych zajmujących się omawianą tematyką. Odwołanie się do licznych źródeł pozwoliło zatem nie tylko na szersze spojrzenie na przedmiot realizowanych badań oraz pozyskanie niezbędnych w tym celu materiałów, ale umożliwiło również weryfikację w kilku niezależnych źródłach pozyskanych informacji.

Przy użyciu analizy decyzyjnej oraz instytucjonalno-prawnej badaniom poddano polskie dokumenty rządowe dotyczące Polski w cyberprzestrzeni, celem wykazania relacji pomiędzy poszczególnymi założeniami teoretycznymi, a ich faktyczną realizacją i skutkami z tym związanymi. Szczególnie istotne okazały się polskie dokumenty rządowe w zakresie strategii i doktryn dotyczących cyberprzestrzeni oraz zwalczania występujących w niej zagrożeń. Możliwe stało się również scharakteryzowanie zainteresowania polskich decydentów politycznych zagadnieniami związanymi z cyberprzestrzenią oraz cyberobronnością na przestrzeni lat 2010-2022. Niewątpliwie istotne w tym zakresie pozostawało prawodawstwo Unii Europejskiej, które wymusiło na wszystkich państwach członkowskich dokonanie implementacji dyrektywy NIS⁶⁴⁴, a w konsekwencji gruntowego przemodelowania funkcjonujących systemów zapewnienia cyberbezpieczeństwa⁶⁴⁵.

Przy zastosowaniu metody komparatywnej wykazano stopień w jakim Federacja Rosyjska była w badanym okresie zainteresowana Polską w cyberprzestrzeni w ramach realizowanej polityki zagranicznej. Zauważyć należy, że poszczególne rodzaje cyberincydentów, jak również poszczególne sektory w cyberprzestrzeni mogą znajdować się w zainteresowaniu Kremla, w mniejszym albo większym stopniu. W zależności o aktualnych relacji dwustronnych, czy też dominującej w nich kwestii bądź kwestiach spornych, cyberataki mogą przybierać odmiennych charakter oraz cel. Niezbędne pozostaje zatem zestawienie rosyjskiej aktywności wobec Polski w cyberprzestrzeni oraz ujęcie jej kompleksowo, poprzez analizę komparatywną danych pozyskanych w tym zakresie. Przeprowadzono więc kodowanie

⁶⁴³ European Union Agency for Cybersecurity: *Publications ENISA*. <https://www.enisa.europa.eu/publications> (dostęp: 29.05.2023).

⁶⁴⁴ Zobacz szerzej: Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. <https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A32016L1148> (dostęp: 08.06.2023).

⁶⁴⁵ Zagadnienie to zostało szczegółowo omówione w dalszej części pracy.

zgodnie z którym chronologicznie z raportów rocznych Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV⁶⁴⁶ (CSIRT GOV) oraz Zespołu CERT Polska pozyskano wybrane dane roczne (za lata 2010-2022) do których zaliczono rozkład procentowy ataków z Federacji Rosyjskiej na sieci monitorowane przez system ARAKIS, ponadto rozkład przepływów w tej sieci oraz liczbę zarejestrowanych alarmów z podziałem na priorytety. Następnie uwzględniono w ramach analizy komparatywnej liczbę zgłoszonych, faktycznych oraz obsługowanych incydentów, zarejestrowanych przez Zespoły CSIRT GOV oraz CERT Polska, jak również liczbę serwerów C&C zlokalizowanych na terytorium Federacji Rosyjskiej.

Ponadto w badaniach zastosowano analizę interwałową (skalę interwałową), która daje możliwość wyrażenia różnic występujących pomiędzy zmiennymi⁶⁴⁷. W rozprawie do zmiennych tych zaliczono przede wszystkim:

1. Rozkład procentowy ataków z Federacji Rosyjskiej na monitorowane przez system ARAKIS sieci, pod kątem liczby generowanych przepływów w latach 2010-2022.
2. Rozkład przepływów w sieciach teleinformatycznych uczestniczących w projekcie ARAKIS w latach 2010-2022.
3. Liczba zarejestrowanych alarmów (z podziałem na priorytety⁶⁴⁸) przez system ARAKIS w latach 2010-2022.
4. Liczba zgłoszonych oraz faktycznych incydentów teleinformatycznych odnotowanych przez Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV w latach 2020-2022.
5. Liczba incydentów teleinformatycznych obsługowanych ręcznie⁶⁴⁹ przez Zespół CERT Polska w latach 2020-2022.
6. Liczba incydentów teleinformatycznych z uwzględnieniem ich typów, obsługowanych przez Zespół CERT Polska w latach 2010-2022.

⁶⁴⁶ W odniesieniu do raportów rocznych opublikowanych przez Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV należy zaznaczyć, że autor w pracy posługuje się nazwą podmiotu obowiązującą na dzień 31 grudnia 2022 roku (koniec cezury czasowej badań). Uwzględnić jednak należy, że do wejścia w życie w 2018 roku ustawy o krajowym systemie cyberbezpieczeństwa, instytucja działała pod nazwą: Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL. Dlatego też w raportach rocznych za lata 2010-2017 występuje nazwa CERT GOV (CERT.GOV.PL), z kolei za lata 2018-2022 nazwa CSIRT GOV.

⁶⁴⁷ E. Babbie: *Badania społeczne w praktyce...*, s. 157-158.

⁶⁴⁸ Raporty roczne Zespołu CSIRT GOV w zakresie analizy alarmów w sieci Internet na podstawie danych z systemu ARAKIS obejmują podział ich priorytetów na: niski, średni, wysoki, pilny.

⁶⁴⁹ Incydenty obsługiwane ręcznie to incydenty, które zostały zarejestrowane oraz wymagają bezpośredniego działania przez członka Zespołu.

7. Liczba serwerów C&C⁶⁵⁰ na świecie, które były zlokalizowane na terytorium Federacji Rosyjskiej.

Wreszcie wskazać należy, że uzyskane wyniki badań wpisano w analizę celów polityki zagranicznej Federacji Rosyjskiej realizowanej wobec Polski. Zostało to przeprowadzone ze szczególnym uwzględnieniem zidentyfikowanych głównych kwestii spornych w relacjach bilateralnych oraz celem ukazania ich implikacji dla stosunków polsko-rosyjskich. Do najważniejszych głównych kwestii spornych w stosunkach polsko-rosyjskich w latach 2010-2022 zaliczono: politykę historyczną, dywersyfikację źródeł energii, politykę bezpieczeństwa w Europie Środkowo-Wschodniej, politykę bezpieczeństwa NATO, katastrofę samolotu rządowego z Prezydentem Rzeczypospolitej Polskiej w Smoleńsku, aneksję Półwyspu Krymskiego i wojnę w Ukrainie oraz program Partnerstwa Wschodniego⁶⁵¹.

3.5.3. Założenia metodologiczne badań nad rosyjskimi portalami informacyjnymi jako instrumentami wojny informacyjnej Federacji Rosyjskiej wobec Polski w latach 2010-2022

Badania zostały przeprowadzone przy wykorzystaniu analizy treści oraz metod statystycznych. Metody te posłużyły do realizacji przyjętych celów badawczych. Jako **jednostki analizy**, stanowiące obiekty, spośród których zostaną wyodrębnione poszczególne **jednostki obserwacji**, przyjęto rosyjski portal informacyjny **Sputnik News International**⁶⁵², oraz portal internetowy agencji informacyjnej **TASS**⁶⁵³. Badaniom zostaną poddane wyłącznie anglojęzyczne witryny internetowe powyższych podmiotów.

Uzasadnieniem wyboru powyższych podmiotów są ich silne związki z ugrupowaniami rządzącymi w Rosji oraz finansowanie ze środków Kremla, co wpływa na typ oraz charakter publikowanych treści⁶⁵⁴. Pierwotnym założeniem metodologicznym było umieszczenie

⁶⁵⁰ Serwery C&C (ang. *Command & Control*) można zdefiniować jako centra każdej operacji wykorzystującej złośliwe oprogramowanie. To za ich pomocą atakujący kontroluje oprogramowanie, które zainfekowało dany system. Chodzi więc o wydawanie komend np. blokujących zainfekowane urządzenie, wprowadzających zmiany do takiego urządzenia, czy też wykradających z niego dane.

⁶⁵¹ Każda ze wskazanych głównych kwestii spornych w stosunkach polsko-rosyjskich została szczegółowo omówiona w dalszej części pracy, dlatego też w tym miejscu nastąpiło wyłącznie ich zarysowanie.

⁶⁵² Sputnik News International. <https://sputnikglobe.com/>; <https://sputniknews.com/> (dostęp: 26.05.2023).

⁶⁵³ TASS. <https://tass.com> (dostęp: 21.07.2024).

⁶⁵⁴ Zobacz szerzej: Przedstawicielstwo Komisji Europejskiej w Polsce: *Russia Today i Sputnik wyłączone w UE*. https://poland.representation.ec.europa.eu/news/russia-today-i-sputnik-wylaczone-w-ue-2022-03-02_pl (dostęp: 11.03.2023); U.S. Department of State: *Report: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem*. <https://www.state.gov/report-rt-and-sputniks-role-in-russias-disinformation-and-propaganda-ecosystem/> (dostęp: 11.03.2023); European Council, Council of the European Union: *EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU*.

w powyższej grupie portalu informacyjnego Sputnik News Polska, czyli polskojęzycznej wersji portalu Sputnik News International. Ostatecznie stało się to niemożliwe, gdyż od końca 2023 roku następowało stopniowe ograniczanie jego dostępności, i to bez względu na państwo, z którego następowało łączenie z portalem. Ostatecznie na początku 2024 roku domena internetowa Sputnik News Polska stała się całkowicie niedostępna. Po kilku miesiącach stan ten utrzymywał się, dlatego też autor podjął decyzję o ograniczeniu badań do dwóch wskazanych wyżej rosyjskich portali informacyjnych.

Założeniem pracy było również przeprowadzenie badań w zakresie portalu informacyjnego RT (dawniej Russia Today). Początkowo do badań wyodrębniono około 900 artykułów, jednakże w związku ze zmianami w strukturze witryny (dostępności artykułów), ostatecznie możliwe było wytypowanie zaledwie 102 indywidualnych wiadomości⁶⁵⁵. Wobec tego przeprowadzenie badań w oparciu o większą liczbę jednostek obserwacji okazało się niemożliwe i z tego też powodu zrezygnowano z nich.

W ramach poszczególnych jednostek analizy wyróżniono **jednostki obserwacji**. Są nimi wyodrębnione do badań pojedyncze materiały prasowe publikowane na wskazanych wyżej portalach w formie artykułu. Analizie zostały poddane artykuły opublikowane w okresie od dnia 1 stycznia 2010 roku do dnia 31 grudnia 2022 roku w których poruszono kwestie związane z Polską. Badania były przeprowadzone w języku angielskim.

Artykuły (wiadomości) zostały wyodrębnione spośród wszystkich materiałów opublikowanych przez przyjęte do badań portale informacyjne, za pomocą analizy zawartości tematycznej strony internetowej⁶⁵⁶. Przyjętym słowem kluczowym jest wyraz *Poland*. Uzasadnieniem jego wyboru jest fakt, iż wysoce nieprawdopodobnym jest, aby w indywidualnej wiadomości dotyczącej Polski nie użyto tego wyrazu, bądź aby użyto

<https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rt-russia-today-and-sputnik-s-broadcasting-in-the-eu/> (dostęp: 11.03.2023).

⁶⁵⁵ W odniesieniu do portalu RT przeprowadzono następujące czynności. W pierwszej kolejności przy użyciu wyszukiwarki dostępnej na witrynie oraz przy zastosowaniu słowa *Poland* wyodrębniono ponad 300 artykułów, przy czym brak było możliwości, aby wczytać na stronie wyniki powyżej trzysetnego. W związku z tym wykorzystano następującą metodę. W oparciu o *tag* o nazwie *Poland* zamieszczony pod artykułami znajdującymi się na stronie ustalono, że łączna liczba indywidualnych wiadomości w badanym okresie wynosi 0. Następnie zastosowano drugi dostępny na stronie *tag* dotyczący Polski *Poland news* i na tej podstawie otrzymano za badany okres łącznie 102 artykuły (indywidualne wiadomości), przy czym pierwszy z nich został opublikowany dnia 27 lutego 2010 roku, a ostatni dnia 15 stycznia 2022 roku. Następnie wobec braku dostatecznej liczby artykułów do badań, skorzystano z podstrony *Trends Poland-news-eu-europe*, na której znajduje się kilkaset artykułów dotyczących Polski, przy czym pierwszy z nich został opublikowany w 2021 roku. Z uwagi na fakt, że czas publikacji artykułów (od 2021 roku) nie pokrywa się z cezurą badań (lata 2010-2022), odstąpiono od ich wykorzystania. Wobec tego na portalu RT możliwe do wyodrębnienia i zbadania, w oparciu o przyjęte w pracy kryteria, były zaledwie 102 artykuły.

⁶⁵⁶ Wykorzystane zostały do tego wyszukiwarki i filtry wyszukiwania na stronie portalu informacyjnego oraz *tagi* zamieszczone pod danymi artykułami.

wyłącznie jego synonimu. Identyfikacja jednostek obserwacji w ramach poszczególnych jednostek analizy, została przeprowadzona przy wykorzystaniu metody OSINT⁶⁵⁷ w sposób opisany poniżej.

W zakresie Sputnik News International w wyszukiwarce znajdującej się na stronie internetowej witryny w polu *Search* wpisany został wyraz *Poland*. Następnie ograniczono wyszukiwanie artykułów opublikowanych na portalu do okresu od dnia 1 stycznia 2010 roku do dnia 31 grudnia 2022 roku. Z tak przeprowadzonego wyodrębnienia otrzymano łącznie **10.734 artykuły** (indywidualne wiadomości). Pierwszy z artykułów został opublikowany dnia 2 stycznia 2010 roku, a ostatni dnia 31 grudnia 2022 roku⁶⁵⁸. Należy zasygnalizować, że autor planował zastosować do wyodrębniania jednostek obserwacji, dostępny na witrynie *tag* o nazwie *Poland*. Jednakże jego wykorzystanie okazało się niemożliwe wobec faktu, że pierwszy artykuł, który został nim opatrzony, opublikowano dopiero w 2013 roku, a więc 3 lata po dacie początkowej cenzury badań⁶⁵⁹.

W przypadku drugiego z podmiotów, tj. agencji informacyjnej TASS, autor zdecydował się na wykorzystanie do wyodrębniania jednostek obserwacji *tagu* o nazwie *Poland*. Powodem tego jest fakt, że artykuły uzyskane w wyniku przeprowadzenia procesu wyodrębniania, czy to w oparciu o *tag*⁶⁶⁰, czy to przy zastosowaniu wyszukiwarki⁶⁶¹, nie pokrywały się datą publikacji z przyjętą cenzurą badań. Mając na względzie konieczność wyboru metody wyodrębniania artykułów w opisanej powyżej sytuacji, autor uznał, że wykorzystanie *tagów* będzie właściwsze. Dzięki temu badania będą skoncentrowane na artykułach, które zostały skalsyfikowane przez ich autorów, jako te dotyczące Polski. Tak zidentyfikowane jednostki obserwacji będą stanowić bardziej wartościowy materiał do badań, odpowiadający przyjętym w pracy celom badawczym. W ten sposób zidentyfikowano **545 artykułów**, przy czym pierwszy z nich został opublikowany dnia 25 kwietnia 2014 roku, a ostatni dnia 15 grudnia 2022 roku⁶⁶².

Podczas omówionego wyżej procesu identyfikacji poszczególnych artykułów (wiadomości) nie zastosowano wyszukiwarki Google i dostępnych w niej komend wyszukiwania. Pomimo iż jest to relatywnie dobre narzędzie, to skorzystanie z niego okazało się niemożliwe. Wynika to z faktu, że podczas próby dokonania procesu identyfikacji artykułów

⁶⁵⁷ Open Source Intelligence.

⁶⁵⁸ Sputnik News International: *Search*. <https://sputniknews.com/search/?query=> (dostęp: 07.06.2024).

⁶⁵⁹ Sputnik News International: *Tag Poland*. https://sputnikglobe.com/geo_Poland/ (dostęp: 07.08.2024).

⁶⁶⁰ TASS: *Poland*. <https://tass.com/tag/poland> (dostęp: 07.08.2024).

⁶⁶¹ TASS: *Search*. <https://tass.com/search?searchStr=Poland&sort=date> (dostęp: 07.08.2024).

⁶⁶² TASS: *Poland*. <https://tass.com/tag/poland> (dostęp: 24.07.2024).

przy użyciu komendy *site*: otrzymywane wyniki wyszukiwania były niepełne bądź rozbieżne. Należy przez to rozumieć, że otrzymywano wyniki, które nie uwzględniały wszystkich artykułów, które można było znaleźć bezpośrednio na portalu – na przykład przy ręcznym wyszukiwaniu. Ponadto przy zastosowaniu tych samych zmiennych wyszukiwania otrzymywano wyniki różne w zależności od lokalizacji geograficznej z której następowało połączenie z siecią Internet (wysłanie zapytania do wyszukiwarki Google). Wreszcie otrzymywano wyniki, które były diametralnie rozbieżne w zależności dnia, w którym przeprowadzono identyfikację. Przykładowo w dniu X otrzymano łącznie 40 artykułów, podczas gdy przy użyciu tych samych zmiennych wyszukiwania w dniu Y otrzymano łącznie 76 artykułów. Tym samym zastosowanie narzędzia Google okazało się niemożliwe, gdyż jego wykorzystanie zaburzyłoby proces badawczy.

Z uwagi na znaczną liczbę artykułów wyodrębnionych do badań, na potrzeby ich przeprowadzenia został zastosowany **systematyczny dobór próby badawczej**. Łączna liczba wyodrębnionych artykułów wynosi **11.279** i stanowi przyjęty **operat losowania**⁶⁶³. **Wielkość frakcji** ustalono na poziomie 0,5⁶⁶⁴, **poziom ufności** na poziomie 95%⁶⁶⁵, natomiast przyjęty **błąd maksymalny** to 5%⁶⁶⁶. Ustalono, że aby próba badawcza była reprezentatywna w oparciu o powyższe zmienne musi zawierać co najmniej **371 artykułów** stanowiących jednostki obserwacji. W celu wyeliminowania potencjalnych błędów ludzkich – na opisanym niżej etapie – zwiększono próbę badawczą do **376 artykułów**⁶⁶⁷.

W związku z tym, że liczba artykułów na poszczególnych portalach (jednostkach analizy) nie jest jednakowa, podjęto następujące działania. Ustalono, że spośród **11.279 artykułów (100%)**, artykuły na portalu Sputnik News International stanowią **95,16801%** tej liczby, natomiast na witrynie TASS **4,83199%**. Na tej podstawie na portalu Sputnik News International poddanych analizie zostało **358 artykułów (zaokrąglono w górę z 357,83171⁶⁶⁸)**, z kolei na witrynie TASS **18 artykułów (zaokrąglono w dół z 18,16828⁶⁶⁹)** – łącznie **376 artykułów**. W związku z tym, że liczba przyjętych do badań artykułów znajdujących się na witrynie TASS jest relatywnie niska, autor w celu zwiększenia reprezentatywności dokonał

⁶⁶³ Operat losowania stanowi określony zbiór artykułów/indywidualnych wiadomości, spośród których jest wyodrębniana próba badawcza (jednostki obserwacji), przy zastosowaniu określonej metody.

⁶⁶⁴ Wielkość frakcji stanowi odsetek elementów danej populacji do których odnosi się dana cecha. W sytuacji, gdy odsetek ten nie jest znany – jak w niniejszym przypadku – wielkość frakcji jest określana na poziomie 0,5.

⁶⁶⁵ Poziom ufności to wskaźnik, który określa pewność, że wynik danego pomiaru odpowiada rzeczywistości występującej wartości.

⁶⁶⁶ Błąd maksymalny stanowi wielkość o jaką wartość rzeczywista może różnić się od wartości otrzymanej w wynikach badań. Jest to zatem wskaźnik określający górną granicę błędu jaki może wystąpić podczas badań.

⁶⁶⁷ E. Babbie: *Badania społeczne w praktyce...*, s. 201-227.

⁶⁶⁸ Podana wartość stanowi 95,16801% przyjętej próby badawczej.

⁶⁶⁹ Podana wartość stanowi 4,83199% przyjętej próby badawczej.

zmiany wielkości próby badawczej, poprzez zwiększenie jednostek obserwacji **z 18 do 91**. Zwiększenie próby badawczej doprowadzi do poprawy wartości statystycznej badania oraz lepiej odzwierciedli różnorodność badanej populacji. W związku z tym pobrana z ogólnej populacji jednostek obserwacji **próba badawcza wynosi 449 artykułów – jednostek obserwacji**.

W tym miejscu należy wyjaśnić, że powyższe wartości nie stanowią próby badawczej o charakterze reprezentatywnym dla poszczególnych podmiotów. Niemniej jednak celem rozprawy nie jest zbadanie artykułów w sposób reprezentatywny dla każdego z przyjętych do badania podmiotów oddzielnie, ale ujęcie publikowanych przez nie treści w sposób łączny i na tej podstawie zrealizowanie celów badawczych pracy. Racjonalnie trudno jest przyjąć założenie, że badane portale, sklasyfikowane przez badaczy oraz rządy wielu państw na świecie jako media propagandowe Kremla⁶⁷⁰, publikując poszczególne treści robią to w sposób rozbieżny względem siebie.

Łączna liczba artykułów wynosi **11.279 (operat losowania)**, a całkowita liczba przyjętych do badania – **449 (próba badawcza)**. W związku z tym zbadano, zgodnie z systematycznym doбором próby z losowym punktem startowym, co **30. artykuł (interwał losowania)** w przypadku portalu Sputnik News International (10.734 artykuły) oraz co **30. artykuł** na witrynie TASS (545 artykułów). Punkt startowy ustalono losowo w celu wyeliminowania możliwych obciążeń, spowodowanych działaniem czynnika ludzkiego. W przypadku portalu Sputnik News International w wyniku procesu losowania otrzymano **liczbę 3**, a w zakresie witryny TASS **liczbę 1**⁶⁷¹. Badania rozpoczęto od ostatnich artykułów opublikowanych w grudniu 2022 roku, co wynika z faktu, iż podczas procesu wyodrębniania jednostek analizy, artykuły z tego czasu pokazywały się na witrynach jako pierwsze.

Kluczową niereaktywną metodą badawczą zastosowaną w pracy jest analiza treści o charakterze jakościowym. Została ona wykorzystana do zbadania zidentyfikowanych jednostek obserwacji, pod kątem występowania w nich wybranych cech, przyjętych

⁶⁷⁰ Zobacz szerzej: A. Aleshka: *Sputnik Polska. Propaganda Narratives and Cases*. <https://east-center.org/wp-content/uploads/2020/09/Sputnik-Polska-Propaganda.pdf> (dostęp: 11.03.2023); DW: *Der Spiegel: RT – instrument rosyjskiej propagandy*. <https://www.dw.com/pl/der-spiegel-rt-instrument-rosyjskiej-propagandy/a-56724016> (dostęp: 11.03.2023); Przedstawicielstwo Komisji Europejskiej w Polsce: *Russia Today i Sputnik wyłączone w UE*. https://poland.representation.ec.europa.eu/news/russia-today-i-sputnik-wylaczone-w-ue-2022-03-02_pl (dostęp: 11.03.2023); U.S. Department of State: *Report: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem*. <https://www.state.gov/report-rt-and-sputniks-role-in-russias-disinformation-and-propaganda-ecosystem/> (dostęp: 11.03.2023); European Council, Council of the European Union: *EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU*. <https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rt-russia-today-and-sputnik-s-broadcasting-in-the-eu/> (dostęp: 11.03.2023).

⁶⁷¹ E. Babbie: *Badania społeczne w praktyce...*, s. 201-227.

w opracowanym kluczu kategoryzacyjnym. Kodowanie poszczególnych jednostek obserwacji zawartych w dobranej próbie badawczej wykonane było przy użyciu programu Microsoft Excel. Proces ten polegał na przypisaniu do każdej jednostki obserwacji, zgodnie z jej charakterem i właściwościami, określonego kodu (K), według poniższego klucza kategoryzacyjnego:

K1) Typy treści, w kategoriach: polityczne (K1A), militarne (K1B), gospodarcze (K1C), społeczne (K1D), technologiczne (K1E), ideologiczne (K1F), religijne (K1G) oraz inne (K1H). Poszczególne jednostki obserwacji zostały przyporządkowywane maksymalnie do pięciu kategorii kodowych w zależności od tematyki poruszonej w ich treści. Pierwsza grupa kodów została przyporządkowana do jednostek obserwacji (artykułów/indywidualnych wiadomości) w wyniku przeprowadzanej analizy treści. Poniżej wskazano przyjęte typy treści oraz ich ogólne definicje:

1. Polityczne (K1A) – treści dotyczące polityki zagranicznej, systemu politycznego oraz pozostałych wydarzeń politycznych. Odnoszą się zatem do działań, decyzji oraz dyskusji w przedmiocie spraw rządzenia oraz organizacji państwa,

2. Militarne (K1B) – treści dotyczące programów zbrojeniowych, ćwiczeń, prowadzonych manewrów wojskowych oraz pozostałych wydarzeń o charakterze wojskowym. Są to również zagadnienia w zakresie strategii, taktyk, konfliktów, zagrożeń oraz obronności,

3. Gospodarcze (K1C) – treści dotyczące przemysłu, jego potencjału oraz ekonomii. Ponadto odnoszące się do handlu, finansów, inwestycji, rynku pracy, polityki podatkowej, rozwoju gospodarczego, przedsiębiorczości oraz regulacji prawnych w tym zakresie,

4. Społeczne (K1D) – treści dotyczące tożsamości kulturowej oraz stosunków społecznych, ale również kwestie równości, praw człowieka, edukacji, zdrowia, migracji, kultury, różnorodności społecznej czy opieki społecznej,

5. Technologiczne (K1E) – treści dotyczące rozwoju technologicznego, sposobów wytwarzania i przetwarzania danego dobra/zasobu. Odnoszące się więc do postępu technologicznego, innowacji, informatyzacji i digitalizacji, sztucznej inteligencji, cyberbezpieczeństwa, telekomunikacji oraz rozwoju technologicznego społeczeństwa,

6. Ideologiczne (K1F) – treści dotyczące kwestii światopoglądowych oraz ideologicznych. Są to zatem systemy ideologiczne, zbiory przekonań politycznych, filozoficznych, światopoglądowych, wartości, doktryn i ideologii wpływających na sposób myślenia, działania oraz politykę w społeczeństwie,

7. Religijne (K1G) – treści dotyczące wyznania oraz systemu wierzeń i praktyk religijnych. Ponadto odnoszące się do duchowości, wartości moralnych i etycznych w tym kontekście, instytucji religijnych oraz ich wpływu na inne dziedziny życia społecznego,

8. Inne (K1H) – treści niezawierające się w żadnej ze wskazanych kategorii.

K2) Kwestie sporne w stosunkach polsko-rosyjskich: polityka historyczna (K2A), dywersyfikacja źródeł energii (K2B), polityka bezpieczeństwa w Europie Środkowo-Wschodniej (K2C), polityka bezpieczeństwa NATO (K2D), katastrofa samolotu rządowego z Prezydentem Rzeczypospolitej Polskiej w Smoleńsku (K2E), aneksja Półwyspu Krymskiego i wojna w Ukrainie (K2F) oraz program Partnerstwa Wschodniego (K2G). Poszczególne jednostki obserwacji zostały przyporządkowywane maksymalnie do pięciu kategorii kodowych (kwestii spornych) w zależności od tematyki poruszonej w ich treści. Powyższy katalog nie ma oczywiście charakteru enumeratywnego, a na stosunki polsko-rosyjskie wpływał szereg innych czynników i uwarunkowań. Mimo to w ocenie autora pracy przytoczone wyżej kwestie były najistotniejsze dla kształtowania relacji bilateralnych stron w okresie od początku 2010 roku do końca 2022 roku⁶⁷².

K3) Typ *framingu*. *Framing* polega na wybieraniu w ramach danego komunikatu pewnych aspektów rzeczywistości i nadawaniu im konkretnego brzmienia oraz ładunku emocjonalnego w zależności od woli dysponenta propagandy. W analizie jego wykorzystania przewidziano trzy kategorie *framingu*: **pozytywny (K3A), neutralny (K3B) i negatywny (K3C).** Kategorie te odnoszą się do wydźwięku jaki został nadany danemu komunikatowi, który może mieć charakter pozytywny, neutralny lub negatywny. Do każdej jednostki obserwacji została przyporządkowana maksymalnie jedna kategoria kodowa.

Pojęcie *framingu* wraz z terminem *frames* pojawiło się po raz pierwszy w latach siedemdziesiątych XX wieku w pracy amerykańskiego socjologa E. Goffmana zatytułowanej *Frame analysis. An essay on the organization of experience*. Jego rozważania stanowią podstawę teoretyczną *framing'u* dlatego też to właśnie na nich naukowcy opierają swoje badania związane z tym zagadnieniem. E. Goffman w ramach *framingu* wyróżnił *frames* czyli ramy interpretacyjne, które mają umożliwić określenie *schematów interpretacji*, co z kolei pozwala na dostrzeżenie, umiejscowienie i nazwanie konkretnych wydarzeń⁶⁷³. T. Gitlin określił *framing* jako „trwałe wzorce poznania, interpretacji i prezentacji, wyboru, podkreślania i wykluczania, za pomocą których osoby posługujące się symbolami regularnie organizują

⁶⁷² Zobacz szerzej: 5.5. Stosunki polsko-rosyjskie w kontekście występujących głównych kwestii spornych w latach 2010-2022.

⁶⁷³ Zobacz szerzej: E. Goffman: *Frame analysis. An essay on the organization of experience*. New York 1974.

dyskurs”⁶⁷⁴. Z kolei R. Entman stwierdził, że jest to „wybranie niektórych aspektów postrzeganej rzeczywistości i uwypuklenie jej w komunikowanym tekście w taki sposób, aby promować określoną definicję problemu, interpretację przyczynową, ocenę moralną i/lub zalecenia dotyczące postępowania”⁶⁷⁵. W badaniach dotyczących *framingu* można wskazać na kilka klasyfikacji stosowanych *frames* (ram). R. Neuman wyróżnił: *human impact* (wpływ człowieka), *conflict* (konflikt), *powerlessness* (bezsilność/bezradność), *economics* (ekonomia), *moral values* (wartości moralne)⁶⁷⁶. H. Semetko i P. Valkenburg sformułowali z kolei następujący podział na ramy takie jak: *conflict* (konflikt), *human interest* (interes ludzki), *attribution of responsibility* (przypisanie odpowiedzialności), *morality* (moralność) i *economic consequences* (konsekwencje ekonomiczne)⁶⁷⁷. Z kolei J. Cappella i K. Jamieson wyróżnili ramy: *horse race* (wyścig konny), *strategic* (strategię), *game* (grę), *personality* (osobowość), *issue* (wydanie), *episodic* (epizodyczny)⁶⁷⁸. Na potrzeby pracy autor przyjął prostą klasyfikację ram wyróżniając *framing*: pozytywny (K3A), neutralny (K3B) oraz negatywny (K3C). Poszczególne rama została przyporządkowana do danej jednostki obserwacji w zależności od tego w jakim charakterze (wydźwięku) jest przedstawiana Polska, bądź też z jakimi wydarzeniami została zestawiona. Autor skupił się zatem na występowaniu słów kluczowych wartościowych pozytywnie, neutralnie bądź negatywnie oraz związany z tym kontekst.

Badania zostały zatem przeprowadzone nie tylko poprzez zidentyfikowanie kontekstu znaczeniowego danego artykułu, ale również poprzez analizę treści poszczególnych jednostek obserwacji (artykułów/wiadomości). Miało to na celu zweryfikowanie czy występowały w nich wyrażenia (słowa) o określonych konotacjach znaczeniowych. Można tutaj przykładowo wskazać na wartościowanie pozytywne i negatywne, a więc wartościowanie przy pomocy słów dobry i zły, przy czym jeśli coś nie jest ani dobre ani złe to jest neutralne⁶⁷⁹. Należy zaznaczyć, że wartościowanie może być przeprowadzane w sposób bezpośredni lub pośredni. Sposób bezpośredni to wskazanie, że coś jest złe albo dobre, ładne albo brzydkie, mądre albo głupie.

⁶⁷⁴ T. Gitlin: *The Whole World is Watching: Mass Media in the Making and the Unmaking of the New Left*. Berkeley 1980, s. 7. Tłumaczenie własne. Tekst w oryginale: “a persistent patterns of cognition, interpretation, and presentation, selection, emphasis and exclusion by which symbol-handlers routinely organizes discourse”.

⁶⁷⁵ R. M. Entman: *Framing: Toward Clarification of a Fractured Paradigm*. „Journal of Communication” 1993, nr 43 (4), s. 52-53. Tłumaczenie własne. Tekst w oryginale: “select some aspects of a perceived reality and make them more salient in a communicating text, in such a way as to promote a particular problem definition, causal interpretation, moral evaluation, and/or treatment recommendation”.

⁶⁷⁶ Zobacz szerzej: W. R. Neuman, M. Just, A. N. Crigler: *Common knowledge. News and the construction of political meaning*. Chicago 1992.

⁶⁷⁷ H. A. Semetko, P. M. Valkenburg: *Framing European politics: a content analysis of press and television news*. „Journal of Communication” 2000, Vol. 50, No. 2, s. 93-109.

⁶⁷⁸ Zobacz szerzej: J. N. Cappella, K. H. Jamieson: *Spiral of cynicism. The press and the public good*. New York 1997.

⁶⁷⁹ Zobacz szerzej: E. Laskowska: *Wartościowanie w języku potocznym*. Bydgoszcz 1993.

Z kolei wartościowanie w sposób pośredni to stosowanie słów, które nadają wyrażeniu kontekst w znaczeniu metaforycznym, a więc na przykład (z punktu widzenia polityki zagranicznej): jesteśmy strażnikami pokoju i stabilności w regionie; nasza polityka zagraniczna to fundament mostu, który umożliwia współpracę i dialog; nasze relacje bilateralne to pole minowe⁶⁸⁰. *Framing* w niniejszej rozprawie ma charakter uzupełniający oraz pomocniczy względem badań prowadzonych w zakresie stosowanych technik propagandowych.

K4) Techniki propagandowe. Kodowanie zastosowanej techniki propagandowej przeprowadzono na podstawie klasyfikacji stworzonej przez The Institute for Propaganda Analysis w której wyróżniono: **Name-Calling** (etykietowanie) (K4A), **Glittering Generalities** (błyskotliwe ogólniki) (K4B), **Transfer** (transfer) (K4C), **Testimonial** (świadcstwo autorytetu) (K4D), **Plain Folks** (prosty człowiek) (K4E), **Card Stacking** (tasowanie kart) (K4F), **Bandwagon** (owczy pęd) (K4G)⁶⁸¹. Instytut został założony w 1937 roku, a jednym z wyników prowadzonych przez niego badań było opracowanie pierwszej naukowej (wskazanej wyżej) klasyfikacji technik propagandy⁶⁸². Jednostki obserwacji na podstawie ich treści, zostały przyporządkowane do maksymalnie pięciu kategorii kodowych. Każda z nich była zastosowana w procesie kodowania oraz zdefiniowana w sposób następujący:

1. Name-Calling (etykietowanie) (K4A) – nadawanie informacji negatywnej etykiety w celu jej potępienia, bez wcześniejszego zbadania/przedstawienia dowodów w tym zakresie. Głównym celem jest dyskredytacja osób, rzeczy lub idei poprzez wzbudzanie wobec nich pejoratywnych skojarzeń, bez dopuszczenia do ich subiektywnej oceny;

2. Glittering Generalities (błyskotliwe ogólniki) (K4B) – wykorzystanie uproszczonego lub stereotypowego myślenia w odniesieniu do określonych zjawisk i terminów oraz połączenie ich z podstawowymi wartościami społecznymi. Jest to również stosowanie pojęć wieloznacznych do interpretacji określonych działań lub problemów społecznych;

3. Transfer (transfer) (K4C) – transfer autorytetu z czegoś szanowanego na coś innego, tak by to drugie również stało się szanowane i akceptowalne. Przebiega również odwrotnie, tzn. poprzez transfer z czegoś nieszanowanego na coś innego, tak by to drugie zostało odrzucone;

4. Testimonial (świadcstwo autorytetu) (K4D) – wykorzystanie autorytetu innych osób, znanych i szanowanych, do propagowania określonych idei. Polega na tym, że osoba szanowana lub nieszanowana mówi, że dana osoba lub rzecz jest dobra bądź zła;

⁶⁸⁰ Zobacz szerzej: R. Tokarski: *Światy za słowami. Wykłady z semantyki leksykalnej*. Lublin 2013.

⁶⁸¹ G. S. Jowett, V. O'Donnell: *Propaganda and Persuasion*. Thousand Oaks 2012, s. 237

⁶⁸² M. Kolczyński: *Strategie komunikowania politycznego*. Katowice 2008, s. 74.

5. **Plain Folks** (prostego człowieka) (K4E) – nadawca takiego komunikatu próbuje identyfikować się z grupą społeczną, utożsamiać z odbiorcami, podkreślając, że wyznają wspólne wartości oraz mają jednakowe przekonania. Jest to również pokazanie, że dane idee są dobre, ponieważ pochodzą od zwykłych ludzi (społeczeństwa);

6. **Card Stacking** (tasowania kart) (K4F) – sprowadza się do odpowiedniego wykorzystywania faktów lub fałszu w celu przedstawienia w określony sposób (pozytywny bądź negatywny) danej idei, osoby, zjawiska czy rzeczy. Chodzi więc o wspieranie bieżącego oddziaływania propagandy przez odpowiednią selekcję używanych argumentów – prawdziwych bądź fałszywych;

7. **Bandwagon** (owczego pędu) (K4G) – polega na wykorzystaniu powszechnie występującej w danej grupie lub społeczeństwie opinii (faktycznie bądź rzekomo), wyrażanej przez większość jednostek. Sprowadza się do przekonywania odbiorcy, że skoro większość tak robi to on też powinien, aby nie zostać wykluczonym⁶⁸³.

⁶⁸³ G. S. Jowett, V. O'Donnell: *Propaganda and Persuasion...*, s. 237; Ibidem, s. 91; Zobacz szerzej: M. Bartosiewicz: *Teorie propagandy w obliczu algorytmizacji internetowego komunikowania społecznego*. „Kultura Współczesna” 2019, nr 1(104); J. M. Sproule: *Authorship and Origins of the Seven Propaganda Devices: A Research Note*. „Rhetoric and Public Affairs” 2001, Vol 4, No. 1; S. Kuśmierski, A. Frydrychowicz: *Podstawy wiedzy o propagandzie*. Warszawa 1980.

Rozdział 4. Wojna informacyjna w polityce zagranicznej Federacji Rosyjskiej

4.1. Polityka zagraniczna Federacji Rosyjskiej w XXI wieku

W. Churchill zdefiniował niegdyś Rosję jako „zagadkę, owianą tajemnicą, wewnątrz zagadki”⁶⁸⁴ i trudno się z tym stwierdzeniem nie zgodzić. To państwo o powierzchni ponad 17.000.000 km², co stanowi około 11% wszystkich terenów lądowych na świecie. To państwo tak ogromne, że zostało podzielone aż na 11 stref czasowych, co sprawia, że gdy w Moskwie obserwuje się zachód słońca, we Władywostoku widzi się jego wschód. Geografia Rosji ma ogromne znaczenie z punktu widzenia jej rozwoju cywilizacyjnego na przestrzeni dziejów. Stosunkowo niewielkie Księstwo Moskiewskie o powierzchni około 10 tysięcy km² w przeciągu kilku wieków przekształciło się w państwo, które w szczycie swojej potęgi (okresu istnienia Związku Socjalistycznych Republik Radzieckich) obejmowało obszar ponad 22.400.000 km², czyli około 15% powierzchni lądowej kuli ziemskiej⁶⁸⁵. Rosja to przede wszystkim państwo nizinne, co z pewnością ułatwiało ekspansję z uwagi na małą liczbę przeszkód naturalnych. Umożliwiło to dotarcie aż nad Pacyfik, a nawet Alaskę czy do Kalifornii. Jednocześnie pojawił się problem związany z administrowaniem zajętymi terenami, co stanowiło wyzwanie dla każdego przywódcy, który sprawował władzę w Rosji. Choć państwo to kulturowo jest silnie złączone z Zachodem, to jednak zajmując bardzo rozległe tereny Azji Północnej doświadczyło obcych inwazji, względnej izolacji oraz zacofania, co z kolei doprowadziło do militaryzacji rosyjskiego społeczeństwa⁶⁸⁶. Ponadto uwzględniając powyższe czynniki, jak i biorąc pod uwagę pozycję Rosji na arenie międzynarodowej, w szczególności trwającą kilka wieków ekspansję imperialną i mocarstwową, jak również fakt posiadania znacznych bogactw naturalnych oraz znacznego potencjału jądrowego, można poczynić stwierdzenie, że jest państwem w pewien sposób unikalnym⁶⁸⁷. Nie mogą więc zatem dziwić posiadane przez Kreml, ale i zwykłych Rosjan aspiracje o mocarstwowej wielkości swojego państwa. Społeczeństwo rosyjskie wobec upokorzenia jakiego doznało po upadku

⁶⁸⁴ The New York Times: *Churchill's definition of Russia still rings true*. <https://www.nytimes.com/2008/08/01/world/europe/01iht-letter.1.14939466.html> (dostęp: 01.10.2022). Tłumaczenie własne. Tekst w oryginale: „Russia is a mystery, shrouded in mystery, inside an enigma”.

⁶⁸⁵ J. Potulski: *Rola i znaczenie tradycji w funkcjonowaniu współczesnych instytucji politycznych w Rosji*. Toruń 2005, s. 18.

⁶⁸⁶ N. V. Riasanovsky, M. D. Steinberg: *Historia Rosji*. Kraków 2009, s. 3-10.

⁶⁸⁷ S. Bieleń, A. Skrzypek: *Wstęp W: Rosja. Rozważania imperiologiczne*. Red. S. Bieleń, A. Skrzypek. Warszawa 2015, s. 7.

w 1991 roku Związku Socjalistycznych Republik Radzieckich⁶⁸⁸ wydaje się być niezwykle podatne na wszelkiego rodzaju projekty zakładające odbudowę utraconego imperium, z kolei decydenci polityczni na Kremlu z chęcią i ogromnym zaangażowaniem podejmują się ich realizacji, na wielu starych jak i nowych płaszczyznach prowadzonej przez Rosję polityki zagranicznej. W tym podrozdziale przedstawiona została geneza rosyjskiej polityki zagranicznej od początku jej państwowości, ze szczególnym uwzględnieniem okresu istnienia ZSRR oraz współcześnie Federacji Rosyjskiej. Ponadto zostaną określone i scharakteryzowane najważniejsze uwarunkowania prowadzonej polityki zagranicznej jak i cele której w jej ramach są realizowane przez Kreml.

4.1.1. Geneza polityki zagranicznej Federacji Rosyjskiej

Aby zrozumieć istotę prowadzonej przez Federację Rosyjską polityki zagranicznej należy rozpocząć od omówienia jej genezy, która sięga o wiele dalej niż do czasów Związku Socjalistycznych Republik Radzieckich i jego upadku w 1991 roku. S. Bieleń trafnie stwierdził, że „jednym z najważniejszych czynników tożsamości międzynarodowej współczesnej Rosji jest jej tradycja mocarstwowa i imperialna”⁶⁸⁹. Należy tutaj zauważyć, że tożsamość ta będzie jednym z najważniejszych uwarunkowań które determinowały, determinują i będą determinować prowadzoną przez Kreml politykę zagraniczną.

Aby w sposób precyzyjny dokonać omówienia rosyjskich tradycji mocarstwowych i imperialnych, należy w pierwszej kolejności odnieść się w sposób ogólny do genezy rosyjskiej państwowości. Historia Rosji nie jest jednoznaczna, jak próbowało i próbuje się to wielokrotnie przedstawiać. W kontekście etnicznym to przede wszystkim historia ludów wywodzących się

⁶⁸⁸ W tym miejscu należy przytoczyć genezę stosowania przymiotnika *radziecki* używanego w Polsce w oficjalnej nazwie omawianego państwa. W nomenklaturze zachodniej jak i samego ZSRR stosowano przymiotnik *sowiecki*, jednakże z uwagi na negatywne konotacje tego pojęcia, które występowały w Polsce po II wojnie światowej, zdecydowano o jego zastąpieniu przymiotnikiem *radziecki*, nawiązującym tym samym do Rad, które funkcjonowały w ZSRR jako organy przedstawicielskie. W wielu umowach międzynarodowych zawieranych pomiędzy PRL i ZSRR odnaleźć można sformułowanie Związek Socjalistycznych Republik Rad, nie z kolei Związek Socjalistycznych Republik Sowieckich, która to nazwa była rzeczywiście właściwa. W kwestii terminologicznej należy również zaznaczyć, że kalką semantyczną jest „polski przymiotnik *radziecki* użyty jako odpowiednik odpowiadającym rosyjskiego *советский* (*sowiecki*), natomiast słowo *sowiecki* jest zapożyczeniem właściwym (leksykalnym)”. Choć pośród językoznawców występują w tej materii spory, to jednak w przeważającej mierze stosowany częściej pozostaje przymiotnik *radziecki*. Trzeba również zauważyć, że współcześnie przymiotnik *sowiecki* ma charakter raczej deprecjonujący. Źródło cytatu: K. Kłosińska: *Sowiecki a radziecki*. <https://sjp.pwn.pl/poradnia/haslo/Sowiecki-a-radziecki;18706.html> (dostęp: 03.03.2023); B. Burska-Ratajczyk: *Postsowiecki i poradziecki*. Uniwersytet Łódzki. Poradnia językowa. <https://poradnia-jezykowa.uni.lodz.pl/faq/postsowiecki-i-poradziecki/> (dostęp: 16.07.2022); M. Bańko: *Sowiecki czy radziecki?* *Słownik Języka Polskiego PWN*. <https://sjp.pwn.pl/poradnia/haslo/sowiecki-czy-radziecki;3265.html> (dostęp: 16.07.2022).

⁶⁸⁹ S. Bieleń: *Tożsamość międzynarodowa Federacji Rosyjskiej*. Warszawa 2006, s. 91.

z plemion wschodniosłowiańskich. Za jej początek uznać należy powstanie Rusi Kijowskiej⁶⁹⁰, w wyniku objęcia w 862 roku władzy przez wareskiego przywódcę Ruryka, pierwszego władcy z dynastii Rurykowiczów⁶⁹¹. Następnie, w 988 roku za sprawą Włodzimierza I Wielkiego (zwanego również Świętym), chrześcijaństwo stało się oficjalną religią obowiązującą w państwie⁶⁹². W ciągu niecałych 200 lat Ruś Kijowska obejmowała ziemie Europy Wschodniej od Morza Bałtyckiego po Morze Czarne. Następne wieki to okres rozbiecia dzielnicowego, podległości Złotej Ordzie (zachodniej części imperium Czyngis-chana) i wreszcie budowy Wielkiego Księstwa Moskiewskiego⁶⁹³. Ten okres w historii Rosji rozpoczyna erę podbojów, które miały służyć zebraniu wszystkich ziem ruskich, co z kolei współcześnie ma bardziej walor ideologiczny, aniżeli historyczno-geograficzny⁶⁹⁴.

Władcą, który na kartach historii zapisał się jako pierwszy który uczynił Rosję wielką był Iwan IV Groźny, a jego koronacja na pierwszego cara Rosji w 1547 roku rozpoczęła okres moskiewskiego absolutyzmu. Jego panowanie to czas niezwykle brutalnych rządów, podczas których tytuł cara zyskał miano samowładztwa niezależnego i suwerennego monarchy, władcy wszystkiego i wszystkich. Iwan IV Groźny odmienił Rosję przeprowadzając szereg reform armii oraz powiększając jej terytorium poprzez między innymi rozpoczęcie eksploracji Syberii. Nie powinno zatem dziwić, że jest on postrzegany jako car, który stworzył potęgę Rosji opartej na silnej władzy i strachu, tworząc wizerunek władcy, który obowiązywał w państwie przez kolejne wieki⁶⁹⁵. Następnym z carów, który zapisał się na kartach rosyjskiej historii był Piotr I Wielki. Otworzył on Rosję na Zachód dążąc do zwiększania jej wpływów oraz modernizacji państwa (przede wszystkim utworzenia nowoczesnej armii), które w okresie jego panowania opierało się w znacznej mierze na rolnictwie. W tym czasie Rosja brała również udział w wielu wojnach, których skutkiem było powiększenie jej terytorium oraz uzyskanie dostępu do Morza Bałtyckiego, nad brzegiem którego Piotr I Wielki założył nową (na wzór zachodni) stolicę, Sankt Petersburg⁶⁹⁶. Niewątpliwie otworzył przed Rosją epokę imperialną, wnosząc do polityki zagranicznej dwa wzorce postępowania, takie jak dominacja sił zbrojnych i celów militarnych oraz otwarcie na świat poprzez przełamanie tradycyjnego moskiewskiego wzorca

⁶⁹⁰ Istnieje wiele sporów co do genezy powstania narodu i państwa rosyjskiego. Najpowszechniejszą z nich oraz uznawaną pod względem naukowym jest teoria normańska, zgodnie z którą pochodzenie państwa staroruskiego należy przypisać silnym wpływom Waregów. Źródło: L. Bazylow: *Historia Rosji*. Wrocław 2005, s. 20-22.

⁶⁹¹ Ibidem, s. 22.

⁶⁹² Ibidem, s. 26.

⁶⁹³ J. Diec: *Geostrategiczny wybór Rosji u zarania trzeciego tysiąclecia. Tom I Doktryna rosyjskiej polityki zagranicznej. Partnerzy najbliżsi i najdalsi*. Kraków 2015, s. 31-38; N. V. Riasanovsky, M. D. Steinberg: *Historia Rosji...*, s. 23-136 (Część: II i III).

⁶⁹⁴ S. Bieleń: *Tożsamość międzynarodowa...*, s. 93.

⁶⁹⁵ L. Bazylow: *Historia Rosji...*, s. 73-88.

⁶⁹⁶ N. V. Riasanovsky, M. D. Steinberg: *Historia Rosji...*, s. 219, 226-249.

izolacjonizmu⁶⁹⁷. W 1721 roku Piotr I zaczął używać tytułu imperatora, z kolei samo określenie *imperium* zostało wpisane w oficjalną nazwę państwa, co miało wskazywać na jego ambicje co do roli jaką Rosja ma odgrywać na świecie. Tutaj podnieść należy, że poza Rosją, sformułowanie *imperium* występowało w nazwach jeszcze dwóch innych państw, Imperium Rzymskiego oraz Imperium Brytyjskiego⁶⁹⁸. Następnym z przywódców, który przyczynił się do budowy mocarstwowej pozycji Rosji była caryca Katarzyna II, która kontynuowała politykę Piotra I Wielkiego zwiększając zaangażowanie Rosji na arenie międzynarodowej, w szczególności w Europie. Rosyjski pisarz N. M. Karamzin napisał, że „Piotr zadziwił zwycięstwami. Katarzyna sprawiła, iż przywykliśmy do nich”⁶⁹⁹. Działania Katarzyny II sprowadzały się również do rozwoju poddaństwa i umacniania pozycji oraz przywilejów szlachty⁷⁰⁰. Co więcej, budowa silnego państwa – Imperium Rosyjskiego i jego ekspansja zewnętrzna nie następowała jak w wielu państwach zachodnich po sobie, ale jednocześnie⁷⁰¹. Ostatnim z rosyjskich carów był Mikołaj II, który objął tron w 1894 roku i to w dość młodym wieku, nie będąc dostatecznie dobrze przygotowanym do funkcji jaką przyszło mu pełnić. Miało to swoje konsekwencje w prowadzonej przez niego polityce wewnętrznej i przejawiało się często zbyt spóźnionymi reakcjami na zaistniałe wydarzenia i tendencje społeczne, które doprowadziły ostatecznie do upadku caratu w Rosji. W okresie panowania Mikołaja II w państwie intensywnie rozwijały się ruchy robotnicze, a zgłaszane przez nie postulaty były na kursie kolizyjnym z obecną władzą. Klęska Rosji w wojnie z Japonią (1904-1905) oraz porażki ponoszone na froncie I wojny światowej (1914-1918) doprowadziły w konsekwencji powyższego do jednego z największych wydarzeń XX wieku⁷⁰².

N. V. Riasanowski napisał, że „mówi się, iż rewolucje nie wybuchają wcale wtedy, gdy ludzie uciskani są ponad wszelką miarę i zupełnie pozbawieni nadziei i środków do życia (warunki takie popychają jedynie do ślepych i bezowocnych buntów), lecz wówczas, gdy występuje pewien rozwój, postęp i wzrost oczekiwań, hamowany jednakże przez archaiczny i surowy porządek panujący w państwie. Na początku XX wieku tak właśnie wyglądała sytuacja w Rosji i to nie tylko w sferze polityki, lecz także w sprawach gospodarczych i społecznych”⁷⁰³. W Rosji istniały warunki konieczne do wybuchu rewolucji, takie jak niechęć

⁶⁹⁷ J. Diec: *Geostrategiczny wybór...*, s. 39-40.

⁶⁹⁸ S. Bieleń: *Identyfikacja Rosji w stosunkach międzynarodowych*. W: *Polityka zagraniczna Rosji*. Red. S. Bieleń, M. Raś. Warszawa 2008, s. 34-36.

⁶⁹⁹ M. A. Geller: *Historia Imperium Rosyjskiego*. Warszawa 2005, s. 442.

⁷⁰⁰ N. V. Riasanovsky, M. D. Steinberg: *Historia Rosji...* s. 280-282; M. A. Geller: *Historia Imperium Rosyjskiego...*, s. 442., s. 442-467.

⁷⁰¹ S. Bieleń: *Tożsamość międzynarodowa...*, s. 93.

⁷⁰² L. Bazyłow: *Historia Rosji...*, s. 312-347, 367-375.

⁷⁰³ N. V. Riasanovsky, M. D. Steinberg: *Historia Rosji...*, s. 458.

do udziału w trwającej I wojnie światowej, rozkład wewnętrzny dworu carskiego, wzrost znaczenia proletariatu oraz skali ich żądań, czy brak reform ustrojowych. Wszystko to doprowadziło do upadku Imperium Rosyjskiego, co miało miejsce po abdykacji cara Mikołaja II w 1917 roku⁷⁰⁴. Po okresie walk wewnętrznych władzę przejęli bolszewicy, a skutkiem ich polityki było proklamowanie w 1922 roku Związku Socjalistycznych Republik Radzieckich⁷⁰⁵. W ciągu kolejnych dziesięcioleci dokonywała się rewolucja w wymiarze politycznym jak i społecznym w wyniku której społeczeństwo rosyjskie stało się sowieckim⁷⁰⁶. Politykę zagraniczną ZSRR z tego okresu należy postrzegać dwutorowo, po pierwsze poprzez podejmowane działań mających na celu doprowadzenie do uznania nowego tworu państwowego na arenie międzynarodowej przez inne państwa oraz po drugie poprzez podsycanie antagonizmów i niepokojów społecznych w innych państwach na świecie (przede wszystkim w Europie), celem wywołania przewrotów rewolucyjnych (czym zajmował się Komintern)⁷⁰⁷. Śmierć W. I. Lenina, twórcy rewolucji bolszewickiej, spowodowała kolejne walki wewnętrzne o władzę z których zwycięsko wyszedł kolejny przywódca ZSRR, J. Stalin. Wprowadził on rządy silnej ręki, brutalnie rozprawiając się ze swoimi przeciwnikami⁷⁰⁸. Kontynuował również agresywną politykę zagraniczną, której czołowym założeniem była nieuchronność rewolucji, która zniszczy system kapitalistyczny⁷⁰⁹. ZSRR coraz bardziej stawał się krajem totalitarnym, aniżeli krajem rad⁷¹⁰.

Polityka J. Stalina odcisnęła niezwykle silne piętno na współczesnej tożsamości narodowej i tradycji mocarstwowej Federacji Rosyjskiej, a zasadniczą rolę w prowadzonej przez niego polityce wewnętrznej jak i zagranicznej odegrały wydarzenia, których początek miał miejsce 22 czerwca 1941 roku. Tego dnia rozpoczęła się operacja Barbarossa, czyli wojna pomiędzy III Rzeszą a ZSRR, znana również w tym państwie pod nazwą Wielkiej wojny ojczyźnianej⁷¹¹. Pomimo początkowych znaczących sukcesów wojsk niemieckich, II wojna światowa ostatecznie zakończyła się zwycięstwem państw alianckich. Niewątpliwie ogromny

⁷⁰⁴ M. A. Geller: *Historia Imperium Rosyjskiego...*, s. 728.

⁷⁰⁵ L. Bazyłow: *Historia Rosji...*, s. 411.

⁷⁰⁶ N. V. Riasanovsky, M. D. Steinberg: *Historia Rosji...*, s. 602-603.

⁷⁰⁷ L. Bazyłow: *Historia Rosji...*, s. 411-414; N. V. Riasanovsky, M. D. Steinberg: *Historia Rosji...*, s. 544-562.

⁷⁰⁸ J. Diec: *Geostrategiczny wybór...*, s. 51-55.

⁷⁰⁹ L. Bazyłow: *Historia Rosji...*, s. 414-417.

⁷¹⁰ Wizja W. I. Lenina na ustrój oraz system polityczny ZSRR sprowadzała się do postrzegania go jako kraju rad, a więc państwa w którym decyzje podejmują zbiorowe organy przedstawicielskie. Tak też W. I. Lenin wypowiedział się formułując słynny *List do Zjazdu*, w którym w sposób niezwykle dosadny skrytykował wszystkich swoich potencjalnych następców, postulując jednocześnie istotę kolektywnego kierownictwa partii oraz dążąc do wprowadzenia jak największej reprezentacji robotników do Komitetu Centralnego, aby ograniczyć w ten sposób rolę aparatu partyjnego. Źródło: L. Bazyłow: *Historia Rosji...*, s. 415.

⁷¹¹ D. R. Marples: *Historia ZSRR: od rewolucji do rozpadu*. Wrocław 2006, s. 169-175.

ciężar wojny wziął na siebie ZSRR, czego skutkiem było zakorzenienie w rosyjskim narodzie przekonania o ogromnym poświęceniu jakie Rosjanie oddali światu. Tym samym to Dzień Zwycięstwa, a nie Wielka Rewolucja Październikowa został uznany za najważniejsze wydarzenie w historii Związku Radzieckiego, a obecnie Federacji Rosyjskiej⁷¹². Rosja, mimo ogromu strat, wyszła z wojny zwycięsko jako supermocarstwo (wraz z USA), łamiąc tym samym dotychczasową potęgę i dyktat Francji oraz Wielkiej Brytanii na arenie międzynarodowej. Rosja nigdy dotąd w historii nie znaczyła tak wiele i nie posiadała tak znaczących wpływów na świecie. Związek Radziecki, będąc ówczesnie u szczytu swojej potęgi, rozpoczął działania zmierzające do światowej ekspansji. W stosunkach międzynarodowych wytworzył się układ bipolarny w ramach którego zaistniały dwa supermocarstwa rywalizujące o hegemonię na arenie międzynarodowej, USA i ZSRR⁷¹³. Początek owej rywalizacji będący początkiem zimnej wojny zwiastował W. Churchill, który w 1946 roku w Fulton wygłosił przemówienie, w którym stwierdził, że Europa została podzielona *żelazną kurtyną*⁷¹⁴.

Pozycja międzynarodowa Związku Radzieckiego nieustannie wzrastała, na co składało się wiele czynników. Najważniejszym z nich była popularyzacja ideologii komunistycznej, nie tylko w obrębie państw związkowych ZSRR oraz państw satelickich, ale również w przestrzeni globalnej poprzez propagowanie radzieckich idei i wartości, systemu gospodarczego czy też stylu życia. Kolejnym przykładem może być stałe członkostwo w Radzie Bezpieczeństwa Organizacji Narodów Zjednoczonych, które umożliwiało efektywne wpływanie na kształt ładu międzynarodowego, również dzięki posiadanemu prawu *weta*⁷¹⁵. Innym z kolei było opanowanie technologii produkcji broni nuklearnej, która stała się istotnym elementem zimnowojennej rywalizacji. Ponadto posiadanie znacznych zasobów broni masowego rażenia przez ZSRR gwarantowało mu utrzymanie statusu supermocarstwa⁷¹⁶. Czynnik ten nadal pozostaje niezwykle istotny w kontaktach z Rosją. Śmierć J. Stalina w 1953 roku rozpoczęła w ZSRR okres odwilży, czego symbolem było wygłoszenie przez jego następcę N. Chruszczowa referatu „O kulcie jednostki i jego następstwach”⁷¹⁷. Nie zwiastowało to jednak obniżenia napięć na arenie międzynarodowej pomiędzy blokiem wschodnim pod przywództwem Kremla i zachodnim pod przywództwem Waszyngtonu. Okres zimnej wojny

⁷¹² Ibidem, s. 194-196.

⁷¹³ R. Kuźniar: *Bezpieczeństwo międzynarodowe*. Warszawa 2012, s. 28-37.

⁷¹⁴ J. Krasuski: *Europa Zachodnia po II wojnie światowej: dzieje polityczne*. Poznań 1990, s. 86-89.

⁷¹⁵ *Karta Narodów Zjednoczonych, Statut Międzynarodowego Trybunału Sprawiedliwości i Porozumienie ustanawiające Komisję Przygotowawczą Narodów Zjednoczonych* (Dz.U. 1947 nr 23 poz. 90), art. 23 i następne.

⁷¹⁶ R. Kuźniar: *Bezpieczeństwo międzynarodowe...*, s. 29-31.

⁷¹⁷ N. V. Riasanovsky, M. D. Steinberg: *Historia Rosji...*, s. 575-578 i 590-593.

to nieustanna rywalizacja na wielu płaszczyznach: militarnej, technologicznej, politycznej, ideologicznej czy społecznej, a ich przejawem stały się konflikty i kryzysy na arenie międzynarodowej. Wydaje się zatem trafnym stwierdzenie, że imperializm rosyjski, a później radziecki nie był jedynie programem politycznych działań, ale swego rodzaju typem mentalności, czy też systemem wartości⁷¹⁸. Przez setki lat trwania Imperium Rosyjskiego, a następnie dziesiątki lat trwania Związku Radzieckiego, społeczeństwo rosyjskie utrzymywało w sobie przekonanie o ogromnej potędze swojego państwa, która jednak została utracona w 1991 roku, kiedy to rozpadł się ZSRR⁷¹⁹. Tym samym w XX wieku Rosjanie dwukrotnie utracili swoje imperium. Państwo, które panicznie boi się upokorzenia, zostało upokorzone. Utrata pozycji supermocarstwa spowodowała nie tylko utratę wpływów na świecie, ale również kryzys tożsamości narodowej Rosjan, budowanej przez dziesiątki, a nawet setki lat⁷²⁰. Załamanie się systemu socjalistycznego skutkowało również niespotykanym dotąd w historii Rosji kryzysem gospodarczym. Utrzymanie dotychczasowego modelu ekonomicznego nie było możliwe, wobec czego otwarto społeczeństwo i gospodarkę, wprowadzając elementy kapitalistyczne z którymi dotychczas walczono. Rosja odrzuciła system totalitarny rozpoczynając budowę państwa demokratycznego, nadal jednak pozostając obciążona swoim dziedzictwem cywilizacyjnym⁷²¹. W tym kontekście trafnie zauważył J. Potulski pisząc, że „upadek ZSRR przyniósł nie tylko rezygnację z tradycji marksistowsko-leninowskiej, ale także odrzucenie dotychczasowego systemu wartości, idei, zwyczajów. Ta pokojowa zmiana postawiła przed Rosją problem ‘jak odbudować państwo?’”⁷²². Niemniej jednak mimo słabości i mankamentów jakie przez cały okres swojego istnienia ciążyły na ZSRR, można zauważyć, że w wielu badaniach i sondażach przeprowadzanych wśród Rosjan współcześnie znaczna ich część, a nawet większość podziela pogląd, że rozpad Związku Radzieckiego był błędem. Nie dziwi zatem fakt, że kolejni Prezydenci Federacji Rosyjskiej, a wskazać tutaj należy szczególnie na W. Putina, starali się tą społeczną potrzebę podsycać i zaspokajać⁷²³.

⁷¹⁸ S. Bieleń: *Tożsamość międzynarodowa...*, s. 94.

⁷¹⁹ 26 grudnia 1991 roku na skutek samorozwiązania Związek Socjalistycznych Republik Radzieckich przestał istnieć. W wyniku tego wydarzenia powstało 15 niepodległych państw z których największym była Federacja Rosyjska. Stała się ona faktycznym i prawnym sukcesorem ZSRR. Rozwiązanie Związku Radzieckiego położyło również kres jego zwierzchności nad państwami satelickimi w Europie Środkowo-Wschodniej. Od ZSRR uniezależniły się takie państwa jak Polska, Czechosłowacja, Rumunia, Bułgaria czy Węgry. Źródło: D. R. Marples: *Historia ZSRR...*, s. 319-323.

⁷²⁰ S. Bieleń: *Tożsamość międzynarodowa...*, s. 94-96.

⁷²¹ J. Potulski: *Rola i znaczenie tradycji w funkcjonowaniu...*, s. 147.

⁷²² Ibidem, s. 147.

⁷²³ A. Jach: *Rosyjska nostalgia imperialna*. W: *Rosja. Rozważania imperiologiczne*. Red. S. Bieleń, A. Skrzypek. Warszawa 2015, s. 87-88.

Choć Federacja Rosyjska jest sukcesorem Związku Socjalistycznych Republik Radzieckich to wydaje się, że status ten dzierży jedynie formalnie⁷²⁴. Wiąże się to z faktem, że Rosja nie posiada takiego potencjału jaki posiadał ZSRR, a w konsekwencji utraciła zdolność do występowania na arenie międzynarodowej w roli supermocarstwa, będąc współcześnie postrzegana raczej w kategoriach mocarstwa regionalnego⁷²⁵. Okres pierwszej dekady po upadku ZSRR to czas hegemonii USA na świecie, z kolei w samej Rosji procesów zmierzających do przewartościowania swojego zaangażowania w sprawy międzynarodowe oraz próby określenia roli jaką nowe państwo, sukcesor dotychczasowego supermocarstwa, będzie pełnić⁷²⁶. Jednocześnie mogłoby się wydawać, że Rosja nie do końca pojęła ogrom klęski jaką poniosła, podobnie zresztą jak szeroko rozumiany Zachód⁷²⁷. Pierwsza dekada od upadku ZSRR to również okres nadziei jaką żywiono w związku z zachodzącymi w Rosji procesami (przemianami) demokratycznymi. W tym kontekście wyrażano często oczekiwanie, że będzie ona partnerem Zachodu na arenie międzynarodowej. Takie wnioski wyprowadzano między innymi na podstawie działań podejmowanych przez Kreml, takich jak wycofanie wojsk radzieckich z państw Europy Środkowej i Wschodniej, zgoda na przystąpienie byłych państw satelickich ZSRR do Sojuszu Północnoatlantyckiego, poparcie przez Rosję USA w walce z terroryzmem po 11 września 2001 roku czy też wreszcie utworzenie Rady NATO-Rosja⁷²⁸. W kontekście prowadzonej przez Kreml polityki zagranicznej w XXI wieku na szczególne uwzględnienie zasługuje ta realizowana przez W. Putina. Początek jego prezydentury to okres nadziei na pogłębianie procesów demokratycznych w Rosji. W. Putin kładł duży nacisk na zacieśnianie współpracy z państwami europejskimi, z kolei w stosunku do byłych państw ZSRR postulował integrację postsowiecką, kładąc nacisk na wspólne wartości i interesy⁷²⁹. Z czasem, w sytuacji spadku znaczenia i możliwości oddziaływania Rosji w skali globalnej, podjął on

⁷²⁴ Po upadku Związku Socjalistycznych Republik Radzieckich jego prawnopolitycznym sukcesorem, który przejął ogół przysługujących ZSRR praw i obowiązków na arenie międzynarodowej, stała się Federacja Rosyjska. Tym samym doszło do zmiany w zakresie układu sił na świecie, w wyniku której zniknął jeden z biegunów zimnowojennej rywalizacji. USA stały się jedynym dominującym supermocarstwem, z kolei Federacja Rosyjska, będąc jednym z piętnastu nowopowstałych państw po rozpadzie Związku Radzieckiego, nie miała rzeczywistych zdolności, aby stać się w pełni kontynuatorem ZSRR. Wynika to przede wszystkim z faktu, że Federacja Rosyjska nie dysponowała zarówno potencjałem, jak i możliwościami w zakresie oddziaływania na arenie międzynarodowej, w takim wymiarze w jakim robił to Związek Radziecki. Tym samym o ile formalna sukcesja nie budzi wątpliwości, to sukcesja rzeczywista może być dyskusyjna. Źródło: A. Bryc: *Rosja w XXI wieku. Gracz światowy czy koniec ery?* Warszawa 2009, s. 13-15.

⁷²⁵ Ibidem, s. 13-15.

⁷²⁶ S. Bieleń, A. Skrzypek: *Wstęp W: Rosja. Rozważania imperiologiczne...*, s. 8-9.

⁷²⁷ A. Czajkowski: *Federacja Rosyjska: przywracanie utraconej wielkości*. W: *Polityka zagraniczna: aktorzy, potencjały, strategię*. Red. T. Łoś-Nowak. Warszawa 2011, s. 81-83.

⁷²⁸ S. Bieleń: *Polityka w stosunkach międzynarodowych*. Warszawa 2010, s. 64.

⁷²⁹ B. Ło: *Russian Foreign Policy in the Post-Soviet Era Reality, Illusion and Mythmaking*. New York 2002, s. 159-160.

działania które zmierzały i zmierzają do zmiany tego stanu. Choć takie cele posiadają zasadniczo wszystkie państwa na świecie które prowadzą samodzielną politykę zagraniczną, to w odniesieniu do polityki W. Putina jest to coś więcej – to podejmowanie działań zmierzających do odbudowy potęgi supermocarstwa jakim było ZSRR⁷³⁰. S. Bieleń wskazał, że „reżim Putina okazał się skuteczną drogą między demokracją a autorytaryzmem, na tyle sprawny i popierany przez społeczeństwo, aby nie tylko sprostać zjawiskom kryzysowym, ale także obronić stabilność geopolityczną Rosji i pokusić się o odbudowę statusu mocarstwowego”⁷³¹.

W. Putin oferuje Rosjanom projekt, w którym zobowiązał się przywrócić Rosji wielkość, jaką znaczna część z nich pamięta jeszcze z czasów ZSRR. Przywraca dumę narodową snując wizję budowy wielkiego imperium o należnej mu pozycji na świecie. Koncepcje rosyjskiej polityki zagranicznej w ciągu ostatnich 30 lat znacznie ewoluowały. Obecnie są one skoncentrowane na rewizji ładu międzynarodowego, który wykształcił się po zakończeniu zimnej wojny, a ponadto na odbudowie strefy wpływów na obszarach byłych państw związkowych ZSRR. Z kolei NATO oraz USA nie są już traktowane jako sojusznicy, ale jako jedno z podstawowych zagrożeń dla bezpieczeństwa oraz interesów Federacji Rosyjskiej⁷³². Takie założenia wydają się nawiązywać do rywalizacji z okresu zimnej wojny, co z kolei potwierdza prowadzona przez Kreml polityka wewnętrzna, gdzie Rosja jest przedstawiana jako twierdza⁷³³ oblężona przez państwa zachodnie⁷³⁴. Ponadto jak wskazali S. Bieleń i A. Skrzypek „destabilizacja na obszarze postradzieckim, nostalgia za utraconym imperium, a także silne sprzężenia gospodarcze i w dziedzinie bezpieczeństwa spowodowały, że Rosja przyznała sobie prawo do odgrywania ról arbitra i gwaranta stabilności tzw. bliskiej zagranicy”⁷³⁵. Stwierdzili oni również, że „przywracając Rosji odpowiedzialność za wielką przestrzeń poimperialną, Rosjanie kompensują sobie różne niedogodności i historyczne upokorzenia. Pragną „narodowej wielkości” oraz przywrócenia „dawnej chwały Rosji”. W tym sensie w ideologii państwowej Rosji pobrzmiewają nuty rewanżyzmu i rewizjonizmu geopolitycznego”⁷³⁶.

⁷³⁰ S. Bieleń: *Polityka w stosunkach międzynarodowych...*, s. 64.

⁷³¹ Ibidem, s. 64-65.

⁷³² M. Banasik: *Interesy i cele strategiczne Federacji Rosyjskiej oraz ich konsekwencje dla bezpieczeństwa międzynarodowego*. W: *Polityka Federacji Rosyjskiej i jej konsekwencje dla bezpieczeństwa międzynarodowego*. Red. M. Banasik. Warszawa 2019, s. 116-118.

⁷³³ Charakterystyka syndromu oblężonej twierdzy została przedstawiona w dalszej części pracy.

⁷³⁴ Z. Modrzejewski: *Dezinformacja w służbie walki informacyjnej*. W: *Bezpieczeństwo informacyjne w dobie postprawdy*. Red. T. W. Grabowski, M. Lakomy, K. Oświecimski. Kraków 2018, s. 105-114.

⁷³⁵ S. Bieleń, A. Skrzypek: *Wstęp W: Rosja. Rozważania imperiologiczne...*, s. 8.

⁷³⁶ Ibidem, s. 10.

Z pewnością można stwierdzić, że Federacja Rosyjska nie odcięła się od spuścizny politycznej ZSRR⁷³⁷. Dokonując porównania obu podmiotów można wskazać na elementy wspólne takie jak chociażby istnienie elementów ideologii państwowej, idei mocarstwowości na arenie międzynarodowej, istotną rolę struktur siłowych w państwie oraz fasadowe instytucje demokratyczne⁷³⁸ (które w rzeczywistości pozostają fikcją wobec powszechnej kontroli obywateli). Nie można oczywiście całkowicie postrzegać Federacji Rosyjskiej jako ZSRR ze zmienioną nazwą. Można bowiem wskazać na różnice jakie pomiędzy nimi występują, jak gospodarka rynkowa powiązana z gospodarką światową czy też zmniejszenie roli aparatu partyjnego. Mimo to, reasumując powyższe rozważania, ale jak również w obliczu konfliktu rosyjsko-ukraińskiego, który rozpoczął się 24 lutego 2022 roku, należy spodziewać się dalszego podważania przez Kreml *status quo* na arenie międzynarodowej, a w konsekwencji licznych sporów w stosunkach międzynarodowych, których przedmiotem będzie rewizja pozimnowojennego ładu międzynarodowego, w szczególności w przestrzeni granicznej Federacji Rosyjskiej (tzw. bliskiej zagranicy), a więc głównie wobec byłych państw członkowskich ZSRR.

4.1.2. Uwarunkowania polityki zagranicznej Federacji Rosyjskiej

Uwarunkowania polityki zagranicznej nie tylko Federacji Rosyjskiej, ale wszystkich państw na świecie stanowią niezwykle złożone zagadnienie. Ilość czynników, które wpływają na działania podejmowane przez decydentów politycznych na arenie międzynarodowej jest ogromna, a ponadto część z ich niejawna. Na potrzeby niniejszej pracy wyróżniono szereg uwarunkowań prowadzonej przez Kreml polityki zagranicznej, które w ocenie autora w sposób

⁷³⁷ W przestrzeni publicznej Federacji Rosyjskiej nadal można odnaleźć niezwykle żywą symbolikę Związku Radzieckiego pochodzącą z okresu jego istnienia. Przykłady takiej symboliki znajdują się na Placu Czerwonym i to nie tylko podczas corocznej defilady z okazji *Dnia Zwycięstwa* organizowanej 9-ego maja. Okazałe baszty Kremla nadal pozostają zwieńczone czerwoną gwiazdą, a w centrum placu odnajdziemy wyraźnie wyeksponowane Mauzoleum Lenina, ojca rewolucji bolszewickiej. Symbole ZSRR występują również w Siłach Zbrojnych Federacji Rosyjskiej na umundurowaniu żołnierzy, czy też stanowią oznaczenie konkretnego rodzaju sił zbrojnych (np. czerwona gwiazda znajduje się na samolotach sił powietrznych jako znak identyfikacyjny).

⁷³⁸ Zgodnie z obowiązującą Konstytucją Federacja Rosyjska jest państwem federalnym o republikańskiej formie rządów (art. 1), w którym władza państwowa jest sprawowana na zasadzie trójpodziału władzy, tj. przez władzę ustawodawczą, wykonawczą i sądowniczą (art. 10). Do najważniejszych organów władzy w Rosji należy zaliczyć Prezydenta Federacji Rosyjskiej (rozdział 4), Zgromadzenie Federalne (rozdział 5), Rząd Federacji Rosyjskiej (rozdział 6), władzę sądowniczą (rozdział 7) oraz Samorząd terytorialny (rozdział 8). Jednakże dokonując analizy poszczególnych zapisów ustawy zasadniczej można zauważyć, że niezwykle silną pozycję w systemie politycznym państwa posiada Prezydent Federacji, którego prerogatywy pozostają w jawnej dysproporcji z innymi występującymi w państwie organami władzy publicznej, co nie jest cechą systemów demokratycznych. Źródło: *Konstytucja Federacji Rosyjskiej przyjęta w ogólnonarodowym referendum w dniu 12 grudnia 1993 roku*. <http://libr.sejm.gov.pl/tek01/txt/konst/rosja.html> (dostęp: 22.10.2022).

największy wpływają na działania podejmowane w wymiarze zewnętrznym przez Rosję. Zaliczono do nich takie uwarunkowania jak: geografia państwa, potencjał ludnościowy, potencjał surowcowy, system gospodarczy, system polityczny, potencjał militarny, spuścizna ideologiczna po upadku ZSRR, trendy ewolucji najbliższego środowiska międzynarodowego oraz pozycja w systemie stosunków i ról międzynarodowych.

Pierwszym a jednocześnie jednym z podstawowych uwarunkowań polityki zagranicznej każdego państwa jest jego geografia. W przypadku Rosji, jak już wspomniano wyżej, jest to czynnik, który w sposób szczególnie determinował jej rozwój cywilizacyjny, w tym prowadzoną politykę zagraniczną. Powierzchnia Federacji Rosyjskiej, największego państwa na świecie, wynosi około 17 milionów km²⁷³⁹. Znajduje się na kontynencie europejskim oraz azjatyckim, granicząc z takimi państwami jak Norwegia, Finlandia, Estonia, Łotwa, Litwa, Polska, Białoruś, Ukraina, Gruzja, Azerbejdżan, Kazachstan, Chiny, Mongolia oraz Korea Północna. Łączna długość granic lądowych to w przybliżeniu około 22.400 km⁷⁴⁰. Ponadto Rosja posiada granice morskie, a do najważniejszych z nich należy zaliczyć granicę z Japonią (Morze Ochockie) oraz USA (Cieśnina Beringa). Co również ważne, państwo to posiada bardzo rozbudowaną linię brzegową której długość wynosi około 37.600 km i przebiega przede wszystkim w północnej (Ocean Arktyczny) i wschodniej (Ocean Spokojny) jego części⁷⁴¹. Wobec tak rozbudowanej i zróżnicowanej granicy państwowej Federacja Rosyjska zyskuje ogromne zdolności do prowadzenia działań zewnętrznych w wymiarze globalnym (w tym ekspansywnych, co jest szczególnie widoczne w kontekście rosyjskiej historii), a jednocześnie jest zobligowana do posiadania znacznych sił zbrojnych w celu jej obrony.

Rosja jest państwem bardzo zróżnicowanym pod względem rzeźby powierzchni terenu. W przeważającej mierze występują tutaj tereny nizinne, lecz wyróżniamy również pasma górskie (np. Kaukaz, Ural). Pod kątem występującego klimatu można mówić o jeszcze większej różnorodności, gdyż odnajdziemy tutaj na klimat subpolarny na północy, umiarkowany chłodny w środkowej części państwa oraz umiarkowany ciepły i podzwrotnikowy śródziemnomorski w południowej. Występują tutaj między innymi półpustynie, stepy, tajgi, tundry czy wieczne zmarzliny. Rozciągłość terytorium ze wschodu na zachód wynosi około 10

⁷³⁹ Dokładna powierzchnia Federacji Rosyjskiej wynosi 17.098.242 km², przy czym powierzchnia lądowa to 16.377.742 km², a powierzchnia morska to 720.500 km². Źródło: World Atlas. Maps of Russia. <https://www.worldatlas.com/maps/russia> (dostęp: 21.03.2023). Na dzień 31 grudnia 2022 roku powierzchnia całkowita Rosji pozostaje kwestią sporną, co wiąże się z uwzględnianiem w jej granicach Półwyspu Krymskiego oraz terenów zajętych we wschodniej Ukrainie.

⁷⁴⁰ Central Intelligence Agency: *The World Factbook. Russia. Geography*. <https://www.cia.gov/the-world-factbook/countries/russia/#geography> (dostęp: 23.07.2022).

⁷⁴¹ Ministerstwo Spraw Zagranicznych: *Informator Ekonomiczny. Informacje ogólne*. <https://www.gov.pl/web/rosja/informator-ekonomiczny> (dostęp: 23.07.2022).

tysięcy kilometrów, z kolei z północy na południe około 5 tysięcy kilometrów⁷⁴². Wielkość obszaru zajmowanego na przestrzeni wieków przez Rosję wywarła ogromny wpływ na świadomość narodu, co do jego roli jaką ma odgrywać na świecie oraz na kształtowanie koncepcji polityki zagranicznej. J. Potulski wskazał, że „rosyjska ciągłość polityczno-państwowa pozostaje w związku z czynnikiem przestrzennym. Duża w przeszłości łatwość rozciągania obszaru władczego na wschód i południe spowodowała efekt terytorialny z którego wielu Rosjan jest dumnych do tej pory”⁷⁴³. Analizując uwarunkowania geograficzne prowadzonej przez Rosję polityki zagranicznej, a których zarys został przedstawiony powyżej należy wskazać, że Kreml posiada duże możliwości (niekoniecznie zdolności) w zakresie operowania w skali globalnej. Należy przez to rozumieć dostęp do najważniejszych akwenów jakimi są Ocean Spokojny i Atlantycki. Ponadto Rosja graniczy z państwami o statusie mocarstwa, przede wszystkim USA i Chinami, jak i z państwami będącymi członkami NATO, co z kolei może prowadzić do konfrontacji, ale również do rozwoju bilateralnej współpracy w różnych dziedzinach.

Kolejnym z uwarunkowań jest potencjał ludnościowy państwa. W przypadku Federacji Rosyjskiej wielkość terytorium nie koresponduje z potencjałem ludzkim. Rosję zamieszkuje w przybliżeniu około 142 milionów⁷⁴⁴ obywateli, co plasuje ją na 9. miejscu na świecie⁷⁴⁵. Należy jednak zaznaczyć, że około $\frac{3}{4}$ z nich żyje w części zachodniej państwa, europejskiej, gdzie znajduje się najwięcej największych miast. Pod względem miejsca zamieszkania państwo jest silnie skoncentrowane na ośrodkach miejskich, gdyż około 74% ludności zamieszkuje miasta, z kolei pozostałe 26% tereny wiejskie. Gęstość zaludnienia stanowi niespełna 8,4 osoby na 1 km²⁷⁴⁶. Stolicą jest Moskwa, pozostająca największym miastem w Europie, zamieszkiwanym przez ponad 12 milionów mieszkańców, co stanowi ponad 8,3% ludności całego państwa⁷⁴⁷. Dane dotyczące liczby ludności zamieszkującej Rosję należy odnieść do

⁷⁴² WorldAtlas: *Maps of Russia*. <https://www.worldatlas.com/maps/russia> (dostęp: 23.07.2022).

⁷⁴³ J. Potulski: *Rola i znaczenie tradycji w funkcjonowaniu...*, s. 23.

⁷⁴⁴ Z kolei według Międzynarodowego Funduszu Walutowego Federację Rosyjską zamieszkiwało w 2021 roku około 145 milionów obywateli a według prognoz liczba ta ulegnie zmniejszeniu do około 144 milionów w 2027 roku. Źródło: International Monetary Fund: *World Economic Outlook Database. April 2022 Edition*. <https://www.imf.org/en/Publications/WEO/weo-database/2022/April> (dostęp: 30.07.2022).

⁷⁴⁵ Central Intelligence Agency: *The World Factbook. Russia. People and Society*. <https://www.cia.gov/the-world-factbook/countries/russia/#people-and-society> (dostęp: 23.07.2022).

⁷⁴⁶ Dla porównania można wskazać, że gęstość zaludnienia w Polsce według danych Głównego Urzędu Statystycznego wynosi niecałe 124 osoby na km², a w całej Unii Europejskiej według Komisji Europejskiej (Eurostat) około 109 osób na km². Z kolei w Chinach są to 153 osoby na km². Tym samym Federacja Rosyjska jest jednym z najmniej zaludnionych państw na świecie przy uwzględnieniu wielkości posiadanego terytorium.

⁷⁴⁷ Ministerstwo Spraw Zagranicznych: *Informator Ekonomiczny. Informacje ogólne*. <https://www.gov.pl/web/rosja/informator-ekonomiczny> (dostęp: 23.07.2022).

innych państw na świecie. Najludniejszym państwem globu są Chiny⁷⁴⁸ z liczbą ludności sięgającą ponad 1,4 miliarda, co stanowi wartość prawie 10 razy większą niż liczba ludności w Rosji. Potencjał demograficzny nie wypada również najlepiej na tle USA, gdzie zamieszkuje ponad 329 milionów⁷⁴⁹ ludzi czy Unii Europejskiej, w której łączna liczba mieszkańców państw członkowskich wynosi niecałe 447 milionów⁷⁵⁰. Ponadto w najbliższych latach należy spodziewać się spadku liczby ludności w Rosji. Według szacunków, w 2050 roku może wynieść ona około 134 milionów⁷⁵¹.

Zdecydowaną większość obywateli Federacji Rosyjskiej stanowią Rosjanie, tj. około 77,7%. Pozostała część to Tatarzy (3,7%), Ukraińcy (1,4%), Baszkirze (1,1%), Czuwasze (1%), Czeczeni (1%). 10,2% stanowią pozostałe narodowości, a 3,9% jest nieokreślona. W rosyjskim spisie ludności wyróżnić można również około 200 innych grup narodowościowych i etnicznych⁷⁵². Należy zatem stwierdzić, że Rosja jest państwem zróżnicowanym etnicznie, co wynika między innymi z wielowiekowych podbojów innych nacji i narodów. Głównym językiem urzędowym jest język rosyjski, choć poszczególne republiki mogą ustanawiać dodatkowe, własne języki urzędowe. Obecnie około 85,7% ludności zamieszkującej Federację Rosyjską mówi w języku urzędowym, około 3,2% w języku tatarskim, 1% czeczeńskim oraz około 10,1% w innych językach⁷⁵³. W odniesieniu do powyższych liczb należy wskazać, że pochodzą one ze spisu przeprowadzonego w 2010 roku, z kolei w 2021 roku został przeprowadzony nowy spis powszechny. W nowym spisie populację oszacowano na 144,7 mln (łącznie z zaanektowanym Półwyspem Krymskim), natomiast struktura narodowościowa i etniczna co do zasady nie uległa większym zmianom względem 2010 roku⁷⁵⁴. Co istotne, wielonarodowa struktura państwa wymaga jej ustabilizowania oraz uporządkowania. Występowanie w Rosji wielu mniejszości etnicznych oraz narodowościowych implikuje powstawanie problemów wewnętrznych, związanych z utrzymaniem integralności terytorialnej⁷⁵⁵. Należy w tym kontekście zauważyć, że w skład Federacji zgodnie z jej

⁷⁴⁸ W tym miejscu należy zaznaczyć, że Chiny w 2023 roku utraciły status najludniejszego państwa świata na rzecz Indii.

⁷⁴⁹ United States Census Bureau: *U.S. and World Population Clock*. <https://www.census.gov/popclock/> (dostęp: 23.07.2022).

⁷⁵⁰ European Commission. Eurostat: *Population and population change statistics*. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Population_and_population_change_statistics (dostęp: 23.07.2022).

⁷⁵¹ S. Gardocki: *Polityka zagraniczna Rosji. Determinanty, interesy i środki*. „Studia Orientalne” 2020, nr 2 (18), s. 10.

⁷⁵² Central Intelligence Agency: *The World Factbook. Russia. People and Society*. <https://www.cia.gov/the-world-factbook/countries/russia/#people-and-society> (dostęp: 23.07.2022).

⁷⁵³ Ibidem.

⁷⁵⁴ Russia.Post: *Russia's changing ethnic landscape: Three takeaways from the 2021 census*. https://russiapost.info/society/ethnic_landscape (dostęp: 11.03.2024).

⁷⁵⁵ J. Potulski: *Rola i znaczenie tradycji w funkcjonowaniu...*, s. 50.

Konstytucją wchodzi ponad 20 autonomicznych republik⁷⁵⁶. Jednakże z drugiej strony rozpad ZSRR pozostawił poza granicami obecnej Federacji Rosyjskiej około ¼ terytorium, a wraz z nim ponad 40% ówczesnej ludności, w znacznej części rosyjskojęzycznej⁷⁵⁷. Mniejszości rosyjskojęzyczne występujące w wielu państwach byłego ZSRR pozwalają Kremlowi na ich wykorzystywanie jako nośnika kulturowego, ale również w charakterze politycznym⁷⁵⁸. Jednocześnie niejednokrotnie stanowią dla Rosji pretekst i uzasadnienie dla podejmowanych działań na arenie międzynarodowej⁷⁵⁹.

Następnym z uwarunkowań polityki zagranicznej Kremla jest potencjał surowcowy państwa. Rosja, między innymi z uwagi na obszar zajmowanego terytorium, posiada znaczące zasoby surowców naturalnych, przede wszystkim surowców energetycznych. Surowce te są również bardzo istotnym środkiem prowadzonej przez Kreml polityki zagranicznej w ramach której wykształciło się zjawisko tzw. *szantażu energetycznego*. Wyjaśnianie go nie wydaje się wymagać szerszego omówienia z uwagi na jego stosunkowo częste występowanie w obliczu kryzysów w relacjach Rosji z innymi państwami. Szantaż energetyczny jest możliwy nie tylko dzięki posiadaniu ogromnych zasobów surowców, przede wszystkim ropy naftowej⁷⁶⁰ i gazu ziemnego, ale również dzięki uzależnieniu wielu państw od importu tych surowców z Rosji⁷⁶¹. Według danych za 2021 rok jest ona trzecim największym na świecie producentem pierwszego ze wskazanych surowców, wydobywając dziennie 10,78 milionów baryłek, co stanowi około 11% całej światowej produkcji. Ustępuje tylko USA z produkcją na poziomie dziennym wynoszącym 18,88 milionów baryłek oraz Arabii Saudyjskiej produkującej z kolei 10,84 miliona baryłek dziennie⁷⁶². Jednocześnie wskazać należy, że w ujęciu globalnym Rosja zużywa około 4% tego surowca, a więc pozostała jego część jest eksportowana do innych

⁷⁵⁶ *Konstytucja Federacji Rosyjskiej przyjęta w ogólnonarodowym referendum w dniu 12 grudnia 1993 roku.* <http://libr.sejm.gov.pl/tek01/txt/konst/rosja.html> (dostęp: 22.10.2022).

⁷⁵⁷ S. Bieleń: *Polityka zagraniczna Rosji*. W: *Federacja Rosyjska 1991-2001*. Red. J. Adamowski, A. Skrzypek, Warszawa 2002, s. 257.

⁷⁵⁸ J. Olędzka: *Russian Language as a Tool of Geopolitical Influence*. „Yearbook of the Institute of East-Central Europe” 2017, Vol. 15. No. 3, s. 135-158; K. Baraniuk: *Mniejszości rosyjskojęzyczne w polityce zagranicznej Federacji Rosyjskiej – przykład Estonii*. „Wschodnioznawstwo” 2016, nr 10, s. 289-297.

⁷⁵⁹ G. Pawlikowski: *Mniejszość rosyjska jak instrument polityki zagranicznej Federacji Rosyjskiej po 1991 roku. Wybrane aspekty*. „Przegląd Geopolityczny” 2016, nr 15, s. 123-134.

⁷⁶⁰ Kategoria ropy naftowa obejmuje w zestawieniu ropę naftową oraz wszystkie inne płyny ropopochodne oraz biopaliwa.

⁷⁶¹ Przykładowo można wskazać, że w 2021 roku gaz ziemny importowany z Federacji Rosyjskiej do krajów Unii Europejskiej stanowił średnio 40% ich zapotrzebowania. W przypadku ropy naftowej wskaźnik ten wynosił 27%, z kolei w zakresie węgla 46%. Energia stanowiła 62% całkowitego importu Unii Europejskiej z Rosji, a wartość wymiany wyniosła około 99 miliardów euro. Źródło: International Energy Agency: *Russia*. <https://www.iea.org/countries/russia> (dostęp: 28.07.2022); European Commission: *In focus: Reducing the EU's dependence on imported fossil fuels*. https://ec.europa.eu/info/news/focus-reducing-eus-dependence-imported-fossil-fuels-2022-apr-20_en (dostęp: 28.07.2022).

⁷⁶² Energy Information Administration: *What countries are the top producers and consumers of oil?* <https://www.eia.gov/tools/faqs/faq.php?id=709&t=6> (dostęp: 28.07.2022).

państw (w mniejszym stopniu magazynowana)⁷⁶³. W odniesieniu do światowego wydobycia drugiego ze wskazanych surowców tj. gazu ziemnego, Rosja również pozostaje jednym z liderów, notując w 2020 roku wydobycie roczne na poziomie ponad 638 miliardów m³ i zajmując pod tym względem drugą pozycję, zaraz za USA z wydobyciem na poziomie ponad 914 miliardów m³⁷⁶⁴. Co również istotne, Rosja posiada najprawdopodobniej największe na świecie rezerwy gazu ziemnego i ropy naftowej. Według szacunków rosyjskiej administracji, przy obecnej eksploatacji wystarczą one nawet na 103 lata, z kolei rezerwy samej ropy naftowej na 59 lat⁷⁶⁵. Niewykluczone, że liczby te ulegną zwiększeniu wobec odkrycia nowych złóż surowców na przykład na obszarze Arktyki, która w ostatnich kilkunastu latach pozostaje przedmiotem zainteresowania wielu państw⁷⁶⁶. W 2020 roku przyjęta została Strategia energetyczna Federacji Rosyjskiej do 2035 roku. Dokument zakłada między innymi zwiększanie wydobycia ropy naftowej i gazu ziemnego oraz prowadzenie polityki dostosowującej rosyjski przemysł wydobywczy do nieprzyjaznych działań podejmowanych przez Zachód oraz dynamicznej sytuacji na światowych rynkach energetycznych⁷⁶⁷. Eksport omawianych surowców pozostaje jednym z ważniejszych elementów polityki Kremla, będąc narzędziem do dyscyplinowania państw prowadzących politykę zagraniczną wbrew koncepcjom rosyjskim, ale również wobec państw nieprzyjaznych. Z drugiej strony oparcie rosyjskiej gospodarki o przychody z eksportu surowców może w przypadku wstrzymania ich sprzedaży powodować mniejsze bądź większe kryzysy na rynku wewnętrznym (powstanie deficytu budżetowego).

Wreszcie wskazać należy na uwarunkowanie dotyczące systemu gospodarczego państwa, który jest powiązany z poprzednio omówionym potencjałem surowcowym. Potencjał gospodarczy Rosji budzi ogromne kontrowersje, co jest wynikiem faktu, że po rozpadzie Związku Radzieckiego reformy gospodarcze nie doprowadziły do wprowadzenia w państwie w pełni systemu gospodarki wolnorynkowej. W tym kontekście S. Gardocki przytacza poglądy

⁷⁶³ Ibidem.

⁷⁶⁴ BP, Centre for Energy Economics Research and Policy, Heriot-Watt University: *Statistical Review of World Energy 2021 70th edition*. <https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/energy-economics/statistical-review/bp-stats-review-2021-full-report.pdf> (dostęp: 28.07.2022); World Population Review: *Natural Gas by Country 2022*. <https://worldpopulationreview.com/country-rankings/natural-gas-by-country> (dostęp: 28.07.2022).

⁷⁶⁵ Warsaw Institute: *How Long Russian Oil and Gas Reserves Are Enough to Last?* <https://warsawinstitute.org/long-russian-oil-gas-reserves-enough-last/> (dostęp: 28.07.2022).

⁷⁶⁶ Zobacz szerzej: O. R. Young, J. Yand, A. Zagorski: *The "New" Arctic as a Zone of Peaceful Competition*. „Polar Perspectives” 2022, No. 11.

⁷⁶⁷ *Strategia energetyczna Federacji Rosyjskiej do 2035 roku zatwierdzona dekretem rządowym z dnia 9 czerwca 2020 roku numer 1523*. Moskwa 2020. <https://www.climate-laws.org/geographies/russia/policies/energy-strategy-2035-approved-by-government-decree-1523-r-2020> (dostęp: 28.07.2022).

rosyjskiego badacza A. V. Tonkonogowa który wskazał, że jednym z istotniejszych zagrożeń dla systemu ekonomicznego Federacji Rosyjskiej jest wykształcanie się od lat dziewięćdziesiątych oligarchicznego kapitalizmu⁷⁶⁸. Gospodarka Rosji, biorąc pod uwagę zasięg terytorialny państwa oraz zamieszkującą w nim ludność nie należy do najsilniejszych, pomimo iż według Międzynarodowego Funduszu Walutowego w 2021 roku znajdowała się wśród 20 państw z największą nominalną wartością Produktu Krajowego Brutto (PKB)⁷⁶⁹. Wartość gospodarki Rosji według nominalnego PKB⁷⁷⁰ plasuje się na poziomie 1,775 biliona dolarów i zapewnia jej 11. miejsce w rankingu⁷⁷¹. Jednocześnie wskazaną wartość można porównać do innych państw takich jak Francja (PKB 2,935 biliona dolarów, około 65 milionów obywateli), Niemcy (PKB 4,225 biliona dolarów, około 83 milionów obywateli), Włochy (PKB 2,101 biliona dolarów, około 59 milionów obywateli), Japonia (PKB 4,937 biliona dolarów, około 125 milionów obywateli), Korea Południowa (PKB 1,798 biliona dolarów, około 51 milionów obywateli), Hiszpania (PKB 1,426 biliona dolarów, około 47 milionów obywateli), Wielka Brytania (PKB 3,187 biliona dolarów, około 67 milionów obywateli) czy USA (PKB 22,997 biliona dolarów, około 322 milionów obywateli). Dokonując analizy powyższych danych można wyprowadzić wnioski, że od państwa o tak rozległym terytorium, posiadającym znaczne zasoby ludzkie oraz znaczne ilości zasobów naturalnych, przede wszystkim surowców energetycznych, należałoby oczekiwać o wiele większego nominalnego Produktu Krajowego Brutto. Porównując wielkość gospodarki rosyjskiej do gospodarki polskiej można z kolei wskazać, że państwo które jest około 53 razy mniejsze pod względem powierzchni terytorium oraz posiadające niecałe 4 razy mniej obywateli posiada nominalne PKB na poziomie 0,674 biliona dolarów, czyli o około 2,6 razy mniej niż Federacja Rosyjska⁷⁷².

Sytuacja gospodarcza Federacji Rosyjskiej wygląda jeszcze gorzej, gdy porównamy wskaźniki nominalnego Produktu Krajowego Brutto *per capita*, który w przypadku Rosji wynosi około 12 tysięcy dolarów. Z kolei we Francji jest to wartość około 65 tysięcy dolarów, w Niemczech około 50 tysięcy dolarów, we Włoszech około 35 tysięcy dolarów, w Japonii około 40 tysięcy dolarów, w Korei Południowej około 34 tysięcy dolarów, w Hiszpanii około

⁷⁶⁸ S. Gardocki: *Polityka zagraniczna Rosji. Determinanty...*, s. 8-9.

⁷⁶⁹ International Monetary Fund: *World Economic Outlook Database. April 2022 Edition*. <https://www.imf.org/en/Publications/WEO/weo-database/2022/April> (dostęp: 30.07.2022).

⁷⁷⁰ Nominalny Produkt Krajowy Brutto to wskaźnik pozwalający ustalić łączną wartość dóbr i usług wytworzonych w danym państwie, w oparciu o aktualną wartość pieniądza. Najczęściej do roli pieniądza przyjmuje się dolara międzynarodowego, który jest umowną walutą opartą na dolarze amerykańskim i służącą do wyrażania realnego poziomu PKB wraz z jego częściami składowymi. Celem takiego działania jest wyeliminowanie różnic w poziomach cen występujących w poszczególnych państwach.

⁷⁷¹ International Monetary Fund: *World Economic Outlook Database. April 2022 Edition*. <https://www.imf.org/en/Publications/WEO/weo-database/2022/April> (dostęp: 30.07.2022).

⁷⁷² Ibidem.

30 tysięcy dolarów, w Wielkiej Brytanii około 47 tysięcy dolarów, a w USA około 69 tysięcy dolarów. W zestawieniu tym Rosja jest zdeklasowana również przez Polskę, której PKB *per capita* kształtuje się na poziomie zbliżonym do prawie 18 tysięcy dolarów. Tym samym w powyższym ujęciu gospodarka Federacji plasuje się na 63. pozycji (tuż za Chinami)⁷⁷³. Poziom życia obywateli w państwie znajduje się wobec tego na bardzo niskim poziomie, całkowicie nieodpowiadającym potencjałowi z jakim mamy do czynienia w innych sferach.

Choć przemysł Federacji Rosyjskiej nie należy do największych na świecie, to jednak dzięki osiągnięciom Związku Radzieckiego (które Rosja odziedziczyła) jest w stanie wytwarzać produkty zaawansowane technologicznie (na przykład sprzęt i pojazdy kosmiczne czy też nowoczesne środki uzbrojenia)⁷⁷⁴. Rosja w latach 2017-2021 była drugim na świecie (zaraz po USA) eksporterem broni konwencjonalnej z udziałem w rynku wynoszącym 18,6%, a do największych odbiorców zaliczały się Indie oraz Chiny⁷⁷⁵. Gospodarka Rosji jest oparta na wydobyciu (produkcji) i eksporcie surowców energetycznych, jak również innych kopalin. Najważniejszymi produktami eksportowymi są: ropa naftowa, rafinowana ropa naftowa, gaz ziemny, węgiel, pszenica i żelazo⁷⁷⁶. Państwo to posiada również rozbudowany przemysł metalurgiczny oraz sektor usług. Do najważniejszych z gałęzi gospodarki zaliczyć należy: handel (15,9%), przemysł wytwórczy (13,7%), górnictwo (9,4%), budownictwo (6,2%) oraz sektor rolniczy (4,8%)⁷⁷⁷. Biorąc pod uwagę potencjał surowcowy Federacji Rosyjskiej oraz jej pozycję jako producenta i jednocześnie eksportera surowców energetycznych na świecie, nie sposób nie wspomnieć o konsekwencjach jakie wywołuje ten fakt w jej gospodarce narodowej, przede wszystkim w budżecie. W tym kontekście nie bez znaczenia pozostaje cena za baryłkę ropy oraz metru sześciennego gazu ziemnego na giełdach światowych. W przypadku ropy naftowej, w latach dziewięćdziesiątych pozostawała ona względnie stabilna i utrzymywała się na poziomie około 21-23 dolarów, z kolei od 2001 roku odnotowaliśmy wzrost kursu do szczytowego poziomu, który został osiągnięty w 2008 roku i wyniósł ponad 140 dolarów. Średnia cena baryłki do 2021 roku wynosiła około 75 dolarów, z kolei w 2022 roku dochodziła momentami do niecałych 130 dolarów⁷⁷⁸. W przypadku gazu ziemnego w ostatnich latach

⁷⁷³ Ibidem.

⁷⁷⁴ Central Intelligence Agency: *The World Factbook. Russia. Economy*. <https://www.cia.gov/the-world-factbook/countries/russia/#economy> (dostęp: 30.07.2022).

⁷⁷⁵ Stockholm International Peace Research Institute: *Trends in international arms transfers 2021*. Stockholm 2022. https://www.sipri.org/sites/default/files/2022-03/fs_2203_at_2021.pdf (dostęp: 30.07.2022), s. 2-4.

⁷⁷⁶ Ibidem.

⁷⁷⁷ Ministerstwo Spraw Zagranicznych: *Informator Ekonomiczny. Gospodarka*. <https://www.gov.pl/web/rosja/informator-ekonomiczny> (dostęp: 30.07.2022).

⁷⁷⁸ Trading Economics: *Crude oil*. <https://tradingeconomics.com/commodity/crude-oil> (dostęp: 28.07.2022).

również można było zaobserwować podobną tendencję na rynkach światowych, gdzie cena wynosiła od poziomu około 2 dolarów za m³ do ponad 8 dolarów za m³ w pierwszej połowie 2022 roku⁷⁷⁹. W tym miejscu podnieść należy, że powyższe produkty stanowiły w 2021 roku około 54% rosyjskiego eksportu, z czego ropa i gaz 49%. Z kolei wpływy do budżetu z tego tytułu wyniosły w 2021 roku około 36% łącznych dochodów, a w latach ubiegłych 28% w 2020 roku (początek pandemii COVID-19), w 2019 roku około 39% w 2018 roku i około 46%⁷⁸⁰. Uwzględniając fakt, że ceny surowców są uzależnione od ich kursów na rynkach światowych, należy stwierdzić, że mają one olbrzymie znaczenie dla rosyjskiego budżetu. Wzrost cen surowców wpływa stymulująco na jej gospodarkę zapewniając środki na realizację zaplanowanych zadań, z kolei ich spadek może spowodować konieczność redukcji wydatków, a w konsekwencji spowolnienie gospodarcze, w najgorszym wypadku kryzys.

Kolejnym uwarunkowaniem jest system polityczny. Federacja Rosyjska jest federalnym państwem demokratycznym z systemem prezydenckim opierającym się na trójpodziale władzy. Zakłada on istnienie władzy ustawodawczej, parlamentu tj. Zgromadzenia Federalnego (izba niższa – Duma Państwowa, izba wyższa – Rada Federacji), władzy wykonawczej tj. prezydenta i rządu z premierem na czele oraz władzy sądowniczej⁷⁸¹. Z uwagi na przedmiot badań, charakterystyka omawianego uwarunkowania została poświęcona przede wszystkim urzędowi i roli Prezydenta Federacji Rosyjskiej, który ma największy i ostateczny wpływ na kształt realizowanej polityki wewnętrznej, a przede wszystkim polityki zagranicznej. Jego instytucja pojawiła się po raz pierwszy w ustawie o prezydencie RFSRR⁷⁸² z 1991 roku, która określiła jego rolę jako najwyższej osoby urzędowej oraz głowy władzy wykonawczej, przyznając mu również rolę egzekutywy. Następnie, w uchwalonej w 1993 roku Konstytucji, prezydentowi przyznano większość uprawnień zawartych we wskazanej ustawie, z tym, że postawiono prezydenta poza tradycyjnym trójpodziałem władzy w ten sposób, że stał się on organem dominującym⁷⁸³. Tutaj zauważyć należy, że wiele opracowań naukowych definiuje system polityczny Rosji jako system superprezydencki (lub też system prezydencki wschodni), który tym różni się od systemu prezydenckiego, że zakłada istnienie głowy państwa, która posiada bardzo szerokie prerogatywy w porównaniu z innymi organami władzy⁷⁸⁴. Specyfika ustroju

⁷⁷⁹ Trading Economics: *Natural gas*. <https://tradingeconomics.com/commodity/natural-gas> (dostęp: 28.07.2022).

⁷⁸⁰ Demagog: *Jaki jest udział sektora energetycznego w eksporcie i PKB Rosji?* <https://demagog.org.pl/wypowiedzi/jaki-jest-udzial-sektora-energetycznego-w-eksporcie-i-pkb-rosji/> (dostęp: 30.07.2022).

⁷⁸¹ *Konstytucja Federacji Rosyjskiej przyjęta w ogólnonarodowym referendum w dniu 12 grudnia 1993 roku*. <http://libr.sejm.gov.pl/tek01/txt/konst/rosja.html> (dostęp: 30.07.2022).

⁷⁸² Rosyjska Federacyjna Socjalistyczna Republika Radziecka.

⁷⁸³ J. Potulski: *Rola i znaczenie tradycji w funkcjonowaniu...*, s. 348-349.

⁷⁸⁴ A. K. Pushkov: *Constitutional Reform as a Struggle for Power*. „East European Constitutional Review” 1998, Vol. 7 No. 4, s. 77-79.

superprezydenckiego to swego rodzaju występowanie systemu prezydenckiego przy jednoczesnym marginalizowaniu w państwie innych założeń właściwych dla demokratycznych rozwiązań (przede wszystkim zasady trójpodziału władzy)⁷⁸⁵. Niektórzy badacze wskazują wręcz, że system superprezydencki może być traktowany jako system autorytarny i prowadzić do wielu nadużyć⁷⁸⁶. W Rosji Prezydenta Federacji zaliczono do organów wykonawczych, choć przyznano mu uprawnienia znacząco wykraczające poza tę władzę⁷⁸⁷. W stosunkach międzynarodowych rola głowy państwa nie ogranicza się wyłącznie do jego reprezentacji, ale przede wszystkim zgodnie z art. 80. Konstytucji Federacji Rosyjskiej „Prezydent Federacji Rosyjskiej, zgodnie z Konstytucją Federacji Rosyjskiej i ustawami federalnymi, określa podstawowe kierunki wewnętrznej i zagranicznej polityki państwa”⁷⁸⁸, z kolei art. 86. wskazuje, że prezydent kieruje polityką zagraniczną Federacji Rosyjskiej, a art. 90. umożliwia mu wydawanie dekretów i rozporządzeń⁷⁸⁹. Postrzeganie roli Prezydenta Federacji jako przewodniej w państwie nie wynika wyłącznie z zapisów zawartych w Konstytucji, ale również z faktu, że rozdział mu poświęcony znajduje się przed rozdziałami poświęconymi parlamentowi, rządowi, samorządowi oraz sądownictwu. Można wręcz wskazać, że pomimo przyjęcia w Konstytucji zasady trójpodziału władzy, Prezent Federacji znajduje się niejako poza systemem składającym się z innych organów władzy⁷⁹⁰. Zmiany wprowadzone do Konstytucji Federacji Rosyjskiej, ostatnie w lipcu 2020 roku, umocniły scentralizowany system superprezydencki sprawiając, że trójpodział władzy coraz bardziej staje się jedynie sformułowaniem zawartym w ustawie zasadniczej, aniżeli faktycznie respektowaną zasadą⁷⁹¹. W Związku Radzieckim funkcjonował system jednopartyjny, z kolei na czele partii (Komunistycznej Partii Związku Radzieckiego) stał Generalny Sekretarz Komitetu Centralnego. Twórcy Konstytucji Federacji Rosyjskiej odeszli w tym zakresie od spuścizny pozostawionej przez ZSRR cedując najważniejsze uprawnienia w państwie właśnie na Prezydenta Federacji. W Rosji funkcjonuje 31 partii politycznych (stan na wrzesień 2021

⁷⁸⁵ J. Szymanek: *Legislatura i egzekutywa w prezydenckich i półprezydenckich systemach rządów*. „Przegląd Sejmowy” 2017, nr 1(138)/2017, s. 104.

⁷⁸⁶ J. Ishiyama, R. Kennedy: *Superpresidentialism and Political Party Development in Russia, Ukraine, Armenia and Kyrgyzstan*. „Europe-Asia Studies” 2001, Vol. 53, No. 8, s. 1178.

⁷⁸⁷ M. Raś: *Aktywność międzynarodowa regionów Federacji Rosyjskiej*. Warszawa 2018, s. 144.

⁷⁸⁸ *Konstytucja Federacji Rosyjskiej przyjęta w ogólnonarodowym referendum w dniu 12 grudnia 1993 roku*. <http://libr.sejm.gov.pl/tek01/txt/konst/rosja.html> (dostęp: 30.07.2022).

⁷⁸⁹ Ibidem.

⁷⁹⁰ B. Dziemidok-Olszewska: *Pozycja ustrojowa prezydentów Polski i Rosji*. „Wschód Europy” 2019, Vol. 5, No. 1/2019, s. 34-37.

⁷⁹¹ M. Domańska, M. Menkiszak, J. Rogoża, I. Wiśniewska: *Rosja u progu 2021 roku. Sytuacja polityczna, społeczna i gospodarcza*. „Komentarze OSW” 2021, nr 371. https://www.osw.waw.pl/sites/default/files/komentarze_371_0.pdf (dostęp: 30.07.2022), s. 2.

roku)⁷⁹², a największą z nich jest partia Jedna Rosja, która od 2001 roku stanowi zaplecze polityczne W. Putina. Posiada również większość w obu izbach parlamentu Federacji oraz pośród radnych administracji samorządowej⁷⁹³. Tym samym można zauważyć, że w Rosji doszło w pewien sposób do zmiany organu wykonawczego z Sekretarza Generalnego KC KPZR na Prezydenta Federacji. Co również ważne – jak wskazała A. Bryc – mechanizm polityki zagranicznej Rosji stanowi odzwierciedlenie jej systemu politycznego, którego jak wskazano wyżej, specyficzną cechą pozostaje uwarunkowana tradycjami historycznymi centralizacja władzy⁷⁹⁴. Warto również zasygnalizować kwestie związane z kolejnymi generacjami rosyjskich elit władzy (między innymi tzw. dzieci Kremla). W tym kontekście wskazuje się, że odgrywają one niezwykle ważną rolę w systemie polityczno-biznesowym Rosji. Ponadto uprzywilejowane miejsce dzieci i krewnych członków elit politycznych Kremla dowodzi, że prawdziwa jest teza o mafijno-klanowym charakterze władzy Rosji. Analitycy zauważają jednak, że znaczenie tych układów dowodzi, iż system władzy na Kremlu nie przeobrazi się wraz z postępującą zmianą pokoleniową⁷⁹⁵.

Wreszcie omówić należy uwarunkowanie jakim jest potencjał militarny Federacji Rosyjskiej. Jest on o tyle istotny, że stanowi przede wszystkim spuściznę po ZSRR pozostając elementem, który w ogromnym stopniu kształtuje pozycję Kremla na arenie międzynarodowej, przede wszystkim z uwagi na posiadany największy na świecie arsenał nuklearny⁷⁹⁶. W skład Sił Zbrojnych Federacji Rosyjskiej wchodzi siły lądowe, marynarka wojenna, siły powietrzno-kosmiczne, wojska powietrznodesantowe oraz wojska rakietowe strategicznego przeznaczenia⁷⁹⁷. Według CIA (Central Intelligence Agency) Rosja posiada armię liczącą około 850 tysięcy żołnierzy w służbie czynnej⁷⁹⁸ oraz 200-250 tysięcy żołnierzy Federalnej Gwardii

⁷⁹² Central Intelligence Agency: *The World Factbook. Russia. Government*. <https://www.cia.gov/the-world-factbook/countries/russia/#government> (dostęp: 30.07.2022).

⁷⁹³ TASS: *Russia's 2021 Parliamentary Elections*. <https://tass.com/russias-2021-parliamentary-elections> (dostęp: 31.07.2022); Ośrodek Studiów Wschodnich: *Rosja: wybory bez wyboru*. <https://www.osw.waw.pl/pl/publikacje/analizy/2021-09-20/rosja-wybory-bez-wyboru> (dostęp: 31.07.2022).

⁷⁹⁴ A. Bryc: *Mechanizm polityki zagranicznej Federacji Rosyjskiej*. W: *Polityka zagraniczna Federacji Rosyjskiej. Wybrane aspekty stosunków z Polską, Ukrainą i Białorusią*. Red. L. Zyblikiewicz, M. Czajkowski, P. Bajor. Kraków 2010 s. 43-54.

⁷⁹⁵ B. Bielszczuk, A. Legucka: *Raport. Druga generacja elity władzy w Rosji*. Warszawa 2018, s. 5-7.

⁷⁹⁶ Stockholm International Peace Research Institute: *SIPRI Yearbook 2022. Armaments, Disarmament and International Security. Summary*. Solna 2022, s. 15.

⁷⁹⁷ Central Intelligence Agency: *The World Factbook. Russia. Military and Security*. <https://www.cia.gov/the-world-factbook/countries/russia/#military-and-security> (dostęp: 22.10.2022).

⁷⁹⁸ Ibidem. Według danych CIA na liczbę 850 tysięcy żołnierzy w służbie czynnej składa się co najmniej „300 tys. wojsk lądowych; 40 tys. wojsk powietrznych; 150 tys. marynarki wojennej; 160 tys. sił powietrznych; 70 tys. strategicznych sił rakietowych; ok. 20 tys. sił operacji specjalnych; ok. 100 tys. innego personelu mundurowego (dowództwo i kontrola, cybernetyka, wsparcie, logistyka, ochrona itp.)”. Tłumaczenie własne. Tekst w oryginale: „300,000 Ground Troops; 40,000 Airborne Troops; 150,000 Navy; 160,000 Aerospace Forces; 70,000 Strategic Rocket Forces; approximately 20,000 special operations forces; approximately 100,000 other uniformed personnel (command and control, cyber, support, logistics, security, etc.)”.

Narodowej. Ponadto we wrześniu 2022 roku w związku z trwającą wojną w Ukrainie powołano do czynnej służby wojskowej 300 tysięcy rezerwistów oraz zaplanowano zwiększenie ogólnej liczby personelu sił zbrojnych o 137 tysięcy⁷⁹⁹. Na wyposażeniu posiada ponad 12.400 czołgów i 30.000 pojazdów opancerzonych. Ponad 6.500 jednostek artylerii samobieżnej, 7.500 jednostek artylerii holowanej oraz prawie 3.400 wyrzutni rakiet. Ponadto w skład Rosyjskiej Floty wchodzi około 600 jednostek, w tym jeden lotniskowiec (wybudowany w czasach ZSRR), z kolei w wojskach powietrznych prawie 4.200 statków różnego rodzaju i przeznaczenia. Większość posiadanego sprzętu została wyprodukowana bądź bazuje na konstrukcjach powstałych w ZSRR, chociaż w ostatnich latach Rosyjskie Siły Zbrojne przechodzą proces modernizacji. Powyższe liczby będą w przyszłości weryfikowane w związku z trwającą wojną rosyjsko-ukraińską⁸⁰⁰. Federacja posiada największy na świecie arsenał nuklearny liczący niecałe 6.000 głowic, z czego ponad 1.500 pozostaje rozmieszczonych na pozycjach bojowych (gotowych do użycia). Drugi największy arsenał posiadają USA z liczbą całkowitą głowic wynoszącą około 5.400 sztuk. Aby ukazać siłę posiadanego przez Kreml arsenału nuklearnego należy zestawić ją z kolejnymi państwami w rankingu, które mają na wyposażeniu Sił Zbrojnych broń jądrową tj. Wielką Brytanią, Francją oraz Chinami, gdzie wielkość arsenału w przypadku każdego z nich nie przekracza 350 sztuk głowic⁸⁰¹.

Pod względem wydatków ponoszonych na obronność Federacja Rosyjska zajmuje stosunkowo wysokie miejsce przeznaczając na ten cel około 4% PKB w 2020 roku (wyprzedzając USA, które przeznaczają na zbrojenia 3,73% PKB w 2020 roku)⁸⁰². Jednakże w tym kontekście warto przytoczyć raport przygotowany przez Stockholm International Peace Research Institute, gdzie wartość PKB przeznaczaną na zbrojenia ujęto kwotowo i tak w 2021 roku w przypadku Federacji Rosyjskiej było to około 66 miliardów dolarów. Więcej funduszy na zbrojenia przeznaczyły z kolei takie państwa jak Wielka Brytania (około 68 miliardów dolarów), Indie (około 76 miliardów dolarów), Chiny (około 293 miliarda dolarów) oraz USA, które deklasując wszystkich rywali przeznaczyły na nie około 801 miliardów dolarów, co stanowi prawie tyle samo, ile na zbrojenia przeznacza 10 kolejnych państw w rankingu łącznie⁸⁰³. W 2022 roku wydatki na zbrojenia w Rosji zostały znacznie zwiększone i wyniosły

⁷⁹⁹ Ibidem.

⁸⁰⁰ Forces Net: *Russia vs Britain: How do their militaries stack up?* <https://www.forces.net/news/russia-vs-britain-how-do-militaries-stack> (dostęp: 24.10.2022).

⁸⁰¹ Stockholm International Peace Research Institute: *SIPRI Yearbook 2022. Armaments...*, s. 14-15.

⁸⁰² Central Intelligence Agency: *The World Factbook. Russia. Military and Security*. <https://www.cia.gov/the-world-factbook/countries/russia/#military-and-security> (dostęp: 31.07.2022).

⁸⁰³ Stockholm International Peace Research Institute: *Trends in World Military Expenditure 2021*. Stockholm 2022. https://www.sipri.org/sites/default/files/2022-04/fs_2204_milex_2021_0.pdf (dostęp: 24.10.2022).

154 miliardy dolarów⁸⁰⁴, co jest jednak związane przede wszystkim z konfliktem rosyjsko-ukraińskim (2022), przed którego rozpoczęciem wydatki na zbrojenia wynosiły średniorocznie w latach 2017-2021 około 64 miliardów dolarów⁸⁰⁵. Warto zasygnalizować, że do 2025 roku Federacja Rosyjska zamierza wydać na zbrojenia łącznie około 600 miliardów dolarów⁸⁰⁶. Ponadto, względna słabość gospodarcza państwa determinuje również ograniczone fundusze na zbrojenia, co nie pozwala na utrzymanie tak licznej i dobrze wyposażonej armii jak miało to miejsce w czasach zimnej wojny. Dodatkowo, rozpoczęta 24 lutego 2022 roku rosyjska inwazja na terytorium Ukrainy dobitnie unaoczniała problemy z jakimi mierzą się siły zbrojne Kremla. Państwo będące z punktu widzenia strategicznego znaczącą potęgą wojskową na świecie do końca 2022 roku nie osiągnęło podstawowego celu jakim było zajęcie całego, o wiele słabszego od siebie państwa. Niedobory w nowoczesnym uzbrojeniu, wszechobecna korupcja i nepotyzm w armii oraz bardzo niskie morale żołnierzy to tylko niektóre z problemów jakie można zaobserwować w rosyjskiej armii. Nakazuje to zrewidować poglądy w przedmiocie znaczącej potęgi Sił Zbrojnych Federacji Rosyjskiej, co z pewnością będzie przedmiotem szerszych rozważań badaczy i specjalistów w ciągu najbliższych lat.

Ostatnim z uwarunkowań, a jednocześnie właściwym wyłącznie dla Federacji Rosyjskiej (nie licząc innych państw powstałych po rozpadzie ZSRR), jest spuścizna ideologiczna państwa po upadku Związku Socjalistycznych Republik Radzieckich. Historia Rosji pokazuje, że państwo to na przestrzeni setek lat swojego istnienia oraz bez względu na rządzące nią elity wykazywało bardzo silne przywiązanie do idei mocarstwowych i imperialnych. W przypadku Rosji powyższe uwarunkowanie jest również o tyle istotne, że nigdy nie zerwała ona więzów formalnych z poprzednią formacją państwową, a będąc właściwie faktycznym i prawnym jej sukcesorem. Rozpad ZSRR był na arenie międzynarodowej o tyle istotnym wydarzeniem, że ukształtował możliwości działania Federacji Rosyjskiej na świecie⁸⁰⁷. S. Bieleń trafnie w tym kontekście wskazał, że Rosja „nigdy bowiem nie ogłosiła niepodległości i nie skorzysta z prawa do wystąpienia z ZSRR. Przyjęcie deklaracji suwerenności państwowej 12 czerwca 1990 roku było podyktowane przede wszystkim koniecznością uporządkowania relacji między największą z republik radzieckich

⁸⁰⁴ TASS: *Russia's national defense budget to total \$154 bln through 2022*. <https://tass.com/defense/1080646> (dostęp: 31.07.2022).

⁸⁰⁵ Statista: *Military spending in Russia from 1993 to 2021*. <https://www.statista.com/statistics/1203160/military-expenditure-russia/> (dostęp: 31.07.2022).

⁸⁰⁶ Reuters: *Russia to spend \$600 billion on defence and security by 2025*. <https://www.reuters.com/business/aerospace-defense/russia-spend-600-bln-defence-security-by-2025-source-2022-09-23/> (dostęp: 19.01.2025).

⁸⁰⁷ A. Bryc: *Rosja w XXI wieku. Światowy...*, s. 13-15.

a władzami centralnymi przed podpisaniem nowej umowy związkowej, nie zaś chęcią demontażu komunistycznego imperium”⁸⁰⁸.

Jednocześnie rozpad ZSRR spowodował pośród elit politycznych swego rodzaju utratę, czy też kryzys tożsamości w ramach realizowanej polityki zagranicznej. Początek lat dziewięćdziesiątych XX wieku to dominacja poczucia porażki i klęski oraz problem braku poczucia nowej tożsamości narodowo-państwowej⁸⁰⁹. B. Lo pisał o wystąpieniu tzw. syndromu imperium, swego rodzaju poczucia utraconej mocarstwowości, ale również poczucia przyszłej imperialnej misji. Syndrom ten w jego ocenie miał również ogromny wpływ na kształt prowadzonej polityki zagranicznej, przede wszystkim względem byłych państw związkowych ZSRR⁸¹⁰. Obserwując kształt prowadzonej przez Rosję na przestrzeni lat polityki, czy też drobnych gestów jak utrzymanie jako obowiązującego hymnu państwowego z okresu istnienia ZSRR (z wprowadzonymi zmianami), jak również utrzymaniu w przestrzeni publicznej symboliki Związku Radzieckiego, trudno takim wnioskom nie nadać waloru trafności. Podobnie zresztą należy zgodzić się z tym, że „rosyjska droga do nieodległości polegała w istocie na ustanowieniu wyższości własnego ustawodawstwa nad związkowym oraz na przyjęciu w następstwie sierpniowego puczu 1991 roku przez rosyjskie elity rządzące znacznej części kompetencji władz centralnych i kontroli nad majątkiem państwowym ZSRR”⁸¹¹. J. Diec w swoich rozważaniach poszedł jeszcze dalej pisząc, że Rosja jako podmiot zachowała „swoją tożsamość, zmieniając jedynie nazwę: była początkowo Imperium Rosyjskim, następnie Związkiem Socjalistycznych Republik Radzieckich, aby od pewnego momentu kontynuować swoje istnienie jako Federacja Rosyjska”⁸¹². W jego opinii taka koncepcja stanowi nie tylko uzasadnienie dla funkcjonowania Rosji w przestrzeni międzynarodowej, ale i uzasadnienie dla samych Rosjan, pośród których istnieje ogromne przywiązanie do ZSRR oraz tęsknota za utraconym imperium. Liczne badania przeprowadzane w tym zakresie dowodzą temu twierdzeniu⁸¹³. Rozpad ZSRR był nie tylko szokiem w sensie psychologicznym, ale i jak stwierdził sam W. Putin – największą katastrofą geopolityczną XX wieku⁸¹⁴.

Kolejnym z uwarunkowań są trendy ewolucji najbliższego środowiska międzynarodowego, które można określić również jako ewolucję otoczenia zewnętrznego. Federacja Rosyjska jako uczestnik stosunków międzynarodowych, będący jednocześnie

⁸⁰⁸ S. Bieleń: *Tożsamość międzynarodowa Federacji...*, s. 91.

⁸⁰⁹ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych stosunków międzynarodowych*. Warszawa 2004, s. 307.

⁸¹⁰ B. Lo: *Russian Foreign Policy in the Post-Soviet...*, s. 48-49.

⁸¹¹ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych stosunków...*, s. 307.

⁸¹² J. Diec: *Geostrategiczny wybór...*, s. 86.

⁸¹³ *Ibidem*, s. 86-87.

⁸¹⁴ S. Bieleń: *Identyfikacja Rosji w stosunkach międzynarodowych*. W: *Polityka zagraniczna...*, s. 35.

sukcesorem Związku Radzieckiego, posiada bardzo duże zdolności w zakresie oddziaływania na inne podmioty na świecie. Koniec zimnej wojny wiązał się z upadkiem ładu bipolarnego na arenie międzynarodowej, a w konsekwencji zaistnieniem konieczności przewartościowania obecnych interesów narodowych, a więc założeń realizowanej przez Moskwę polityki zagranicznej⁸¹⁵. Współcześnie największy wpływ na politykę zagraniczną Kremla mają takie zmiany w otoczeniu międzynarodowym jak wzrost gospodarczo-polityczny w Chinach, zmiany w światowym systemie gospodarczym, aneksja Półwyspu Krymskiego oraz wojna w Ukrainie⁸¹⁶. Zagadnienia te były stosunkowo szeroko omawiane przed badaczami, dlatego też w tym miejscu warto omówić inne obszary i państwa pozostające w kręgu zainteresowania Rosji. W ostatnich latach był to przede wszystkim Bliski Wschód, Iran, Indie oraz Afryka. Zaangażowanie Kremla na Bliskim Wschodzie wynika przede wszystkim z próby wykreowania ładu międzynarodowego, który chroniłby interesy Federacji przed ingerencją Zachodu, głównie USA. Moskwa tym samym wychodzi poza obszar państw tzw. bliskiej zagranicy, tworząc dla siebie nowe strefy wpływów. Należy również zauważyć, że „odbudowa wielkomocarstwowej pozycji Rosji na Bliskim Wschodzie stała się ważnym środkiem legitymizacji reżimu Putina, zarówno w oczach szeroko pojętej rosyjskiej elity, jak i rosyjskiego społeczeństwa”⁸¹⁷. W odniesieniu do Iranu, Rosja poszukuje silnego partnera w tamtejszym rejonie Azji, który mógłby wzmocnić blok antyamerykański (w konsekwencji wytworzyć bufor u jej południowych granic), co pozostaje również w zgodzie z interesami Teheranu. Współpraca rosyjsko-irańska była bardzo dobrze widoczna podczas rosyjskiej interwencji w Syrii w 2015 roku⁸¹⁸, a współcześnie w związku z wojną w Ukrainie (2022)⁸¹⁹. Wreszcie należy zauważyć istotną rolę Indii w prowadzonej przez Kreml polityce zagranicznej, gdyż rząd w Delhi pozostaje jednym z największych na świecie odbiorców rosyjskiego uzbrojenia. Współpraca obu państw obejmuje również kwestie pokojowego wykorzystania energii atomowej, tworzenia korytarzy transportowych czy sprzedaży surowców energetycznych. Dla Kremla Indie to nie tylko rynek zbytu, ale również państwo stanowiące przeciwwagę dla nieustannie wzrastającej pozycji Chin w regionie (i na świecie)⁸²⁰. Ostatnim z obszarów jest Afryka, która już od czasów

⁸¹⁵ S. Bieleń: *Tożsamość międzynarodowa Federacji...*, s. 43-50.

⁸¹⁶ S. Gardocki: *Polityka zagraniczna Rosji. Determinanty...*, s. 15.

⁸¹⁷ W. Rodkiewicz: *Bliskowschodnia polityka Rosji regionalne ambicje, globalne cele*. „Prace Ośrodka Studiów Wschodnich” 2017, nr 71. https://www.osw.waw.pl/sites/default/files/prace_71_bliskowschodnia_polityka_rosji_net_0.pdf (dostęp: 22.10.2022), s. 5.

⁸¹⁸ W. Rodkiewicz: *Wbrew Ameryce. Polityka Rosji wobec Iranu*. „Komentarze OSW” 2020, nr 319. https://www.osw.waw.pl/sites/default/files/komentarze_319_0.pdf (dostęp: 22.10.2022), s. 1-9.

⁸¹⁹ U.S. Department of State: *On Russia's Acquisition of UAVs from Iran*. <https://www.state.gov/on-russias-acquisition-of-uavs-from-iran/> (dostęp: 22.10.2022).

⁸²⁰ J. Diec: *Geostrategiczny wybór...*, s. 248-253.

istnienia ZSRR pozostaje w zainteresowaniu Kremla. Jest to spowodowane przede wszystkim bogatymi złożami surowców, którymi jest zainteresowana Moskwa. Ponadto państwa afrykańskie stanowią ogromny rynek zbytu dla rosyjskich towarów oraz technologii⁸²¹.

Ostatnim z uwarunkowań jest pozycja Rosji w systemie stosunków i ról międzynarodowych. W przypadku tego uwarunkowania, jak i omawianego powyżej, niezwykle istotnym pozostaje fakt, że Federacja Rosyjska jest sukcesorem Związku Radzieckiego. Wskutek tego Kreml odziedziczył przede wszystkim mandat stałego członka (z prawem weta) w Radzie Bezpieczeństwa Organizacji Narodów Zjednoczonych⁸²² czy też największy na świecie arsenał nuklearny⁸²³. Co do ważniejszych organizacji międzynarodowych, Rosja pozostaje członkiem Organizacji Bezpieczeństwa i Współpracy w Europie⁸²⁴, jednakże działania podejmowane przez Kreml na świecie, a zmierzające do odbudowy swojej dawnej strefy wpływów, skutkowały wykluczeniem Federacji Rosyjskiej z różnych organizacji międzynarodowych oraz grup. I tak na przykład w 2008 roku Rosja została czasowo zawieszona w Radzie NATO-Rosja w związku z konfliktem gruzińsko-rosyjskim, następnie w 2014 roku zawieszono Rosję w ramach spotkań grupy G8 (obecnie G7) po dokonaniu przez nią aneksji Krymu, aby wreszcie w 2022 roku wykluczyć ją z Rady Europy w związku z dokonaną inwazją w Ukrainie. Należy również zauważyć, że w kontekście wojny rosyjsko-ukraińskiej określenie obecnej pozycji Rosji oraz jej roli w systemie międzynarodowym, jest zadaniem niezwykle trudnym. Przed dokonaniem inwazji Rosja na świecie była postrzegana raczej jako silny partner polityczno-militarny, posiadający ogromne zasoby surowców energetycznych, zdolny do oddziaływania na innych uczestników stosunków międzynarodowych w skali globalnej⁸²⁵. Z kolei po dokonaniu inwazji pozycja Rosji została przez wiele państw w znacznym stopniu zmarginalizowana, co miało swój bezpośredni związek z nałożonymi na nią sankcjami i związanymi z tym konsekwencjami.

Z powyższych rozważań należy wyprowadzić wniosek, że omówione uwarunkowania nie pozostają bez istotnego znaczenia dla kształtu realizowanej przez Kreml polityki zagranicznej. Rosja nie posiada już tak dużych zdolności w zakresie oddziaływania na arenie międzynarodowej jak ZSRR, jednakże prowadzi politykę prowadzącą do ich odbudowy. Celem elit politycznych Rosji jest również zaspokajanie mocarstwowych ambicji Rosjan,

⁸²¹ Ibidem, s. 255-259.

⁸²² *Karta Narodów Zjednoczonych, Statut Międzynarodowego Trybunału Sprawiedliwości i Porozumienie ustanawiające Komisję Przygotowawczą Narodów Zjednoczonych* (Dz.U. 1947 nr 23 poz. 90), art. 23 i następne.

⁸²³ Stockholm International Peace Research Institute: *SIPRI Yearbook 2022. Armaments...*, s. 14-15.

⁸²⁴ A. Bryc: *Rosja w XXI wieku. Światowy...*, s. 143-146.

⁸²⁵ S. Gardocki: *Polityka zagraniczna Rosji. Determinanty...*, s. 15.

sprowadzających się do chęci odzyskania poczucia dumy i potęgi własnego państwa. Rosja nie zrezygnowała z narracji występującej również w czasach Związku Radzieckiego, propagujących poglądy o rywalizacji Zachodu (agresora) ze Wschodem oraz konieczności podjęcia działań obronnych. Symbolika radziecka jest nadal widoczna w przestrzeni publicznej, co z kolei dowodzi jej istotnego znaczenia w polityce wewnętrznej, a w konsekwencji zagranicznej. Coroczne defilady zwycięstwa organizowane w Moskwie 9 maja swoim rozmachem i charakterem dorównują tym z okresu istnienia ZSRR, z kolei na frontowej części siedziby Ministerstwa Spraw Zagranicznych Federacji Rosyjskiej nadal można dostrzec skrzyżowany sierp i młot na tle kuli ziemskiej (godło Związku Socjalistycznych Republik Radzieckich). W związku z tym, twierdzenie o kluczowym wpływie spuścizny ideologicznej ZSRR na kształt polityki zagranicznej prowadzonej przez elity rządzące Kremla jest w pełni uzasadnione. Oczywiście nie można jednoznacznie stwierdzić czy polityka zagraniczna prowadzona przez Moskwę zmierza do rywalizacji z Zachodem, którą z kolei znamy z okresu zimnowojennego (Rosja nie posiada do tego wystarczających zdolności), jednakże można z całą pewnością wyprowadzić wniosek, że działania podejmowane przez Kreml zmierzają do odizolowania się od wpływów zewnętrznych na państwo, obrony „rosyjskości” czy też „rosyjskiego świata”, nie tylko w wymiarze wewnętrznym ale i zewnętrznym, przede wszystkim na obszarach byłego Związku Socjalistycznych Republik Radzieckich.

4.1.3. Cele polityki zagranicznej Federacji Rosyjskiej

Upadek Związku Socjalistycznych Republik Radzieckich spowodował konieczność przewartościowania celów realizowanej przez Federację Rosyjską polityki zagranicznej. Pierwsze lata istnienia Federacji to okres w którym występował pośród elit politycznych proces zmierzający do określenia swojej tożsamości, a w odniesieniu do stosunków międzynarodowych i polityki zagranicznej, określenia roli Rosji na arenie międzynarodowej. Do połowy lat dziewięćdziesiątych w kręgach politycznych Kremla wykształciły się cztery zasadnicze koncepcje prowadzenia polityki, które jak pisze E. Cziomer „w większym lub mniejszym stopniu wpływały na kształtowanie i praktyczną realizację polityki zagranicznej bezpieczeństwa zewnętrznego Rosji”⁸²⁶. Pierwsza z nich, koncepcja geopolitycznego realizmu, zakładała wykorzystanie wszystkich możliwych narzędzi do odtworzenia mocarstwowej pozycji Rosji na świecie. Druga – koncepcja imperialna, sprowadzała się również do odbudowy

⁸²⁶ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych stosunków...*, s. 309.

moceństwowej pozycji Rosji, jednakże w dwóch odmianach, nacjonalistycznej (odbudowa na wzór Rosji Carskiej) i komunistycznej (odbudowa na wzór Związku Socjalistycznych Republik Radzieckich). Trzecia koncepcja, euroazjatycka, przewidywała utrzymanie pozycji moceństwowej Federacji w Europie oraz Azji z jednoczesną negacją wzorców pochodzących z zachodniego modelu politycznego oraz społeczno-gospodarczego. Ostatnia, koncepcja prozachodnia i proeuropejska, postulowała konieczność przeprowadzenia reform w państwie i zbliżenia do wzorców zachodnich poprzez wprowadzenie gospodarki wolnorynkowej oraz demokracji, a w konsekwencji doprowadzenie do wzmocnienia pozycji Federacji na arenie międzynarodowej. Priorytetem miała być więc współpraca z USA oraz Unią Europejską, w szczególności z Niemcami i Francją⁸²⁷.

Ostatnia z wymienionych koncepcji była szczególnie widoczna w okresie prezydentury B. Jelcyna (1991-1999), który postulował zacieśnianie relacji z Zachodem, a będącego przecież dotychczas głównym rywalem nieistniejącego już Związku Radzieckiego⁸²⁸. Koncepcja prozachodnia opierała się na przekonaniu o przynależności cywilizacji rosyjskiej do Zachodu, z kolei w tym zakresie wyrażano nadzieje na wsparcie z jego strony w dokonywaniu demokratycznego przeobrażenia w państwie⁸²⁹. Kreml nie pozostał również obojętny w zakresie byłych państw ZSRR. W 1993 roku w Podstawowych założeniach polityki zagranicznej Federacji Rosyjskiej oraz Podstawowych założeniach doktryny obronnej Federacji Rosyjskiej dokonano podziału otoczenia zewnętrznego Rosji na zagranicę *dalszą* i *bliższą*. Zagranicę bliższą stanowiły przede wszystkim państwa obszaru poradzieckiego, z kolei zagranica dalsza to reszta świata⁸³⁰. Druga połowa lat dziewięćdziesiątych XX wieku to okres kolejnego przewartościowania celów polityki zagranicznej Kremla. Nastąpiło ochłodzenie w relacjach ze światem Zachodnim, w szczególności z USA, co ówczesny Minister Spraw Zagranicznych Rosji A. Kozyriew nazwał zakończeniem „miesiąca miodowego”⁸³¹. Przyczyną tych wydarzeń były wydarzenia w polityce wewnętrznej Rosji, w ramach której elity rządzące zaczęły dostrzegać potrzebę zakwestionowania hegemonii USA na świecie. W ocenie Kremla jednobiegunowy ład międzynarodowy był niemożliwy do zaakceptowania wobec faktu istnienia na świecie wielu równouprawnionych państw o różnych interesach. Jednocześnie

⁸²⁷ M. Jedliński: *Polityka zagraniczna Federacji Rosyjskiej w latach 90-tych. Kontekst historyczno-ideowy*. „Środkowoeuropejskie studia polityczne” 2009, nr 3, s. 1-18; Ibidem, s. 309.

⁸²⁸ A. Czajkowski: *Federacja Rosyjska: przywracanie utraconej wielkości*. W: *Polityka zagraniczna: aktorzy...*, s. 83-84.

⁸²⁹ A. Bryc: *Cele polityki zagranicznej Federacji Rosyjskiej*. Toruń 2004, s. 23-24.

⁸³⁰ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych stosunków...*, s. 309-310.

⁸³¹ S. Bieleń: *Polityka Federacji Rosyjskiej wobec Stanów Zjednoczonych Ameryki*. W: *Polityka zagraniczna Rosji*. Red. S. Bieleń, M. Raś. Warszawa 2008, s. 34-36.

Rosja zagwarantowała sobie prawo do ich obrony, w tym przy użyciu sił zbrojnych za granicą oraz użycia broni masowego rażenia (arsenału nuklearnego). Ponadto celem Rosji miało być aktywne uczestnictwo w rozwiązywaniu problemów globalizującego się świata jak i mocne zaznaczenie swojej obecności na świecie⁸³². Koniec XX wieku to również podejmowanie przez Rosję działań zapobiegawczych względem rozszerzania NATO oraz przyjmowania nowych państw do Unii Europejskiej, szczególnie byłych państw satelickich⁸³³. H. C. d'Encausse, francuska badaczka specjalizująca się w zagadnieniach związanych z Rosją, na zadane jej w 1999 roku pytanie: „Czy Rosja jest jeszcze mocarstwem?”⁸³⁴, odpowiedziała: „Dziś nie, ale jutro będzie”⁸³⁵.

Zaktualizowana i przyjęta w 2000 roku Koncepcja polityki zagranicznej Federacji Rosyjskiej zakładała, że istniejący ład międzynarodowy wymaga analizy w odniesieniu do pozycji Federacji na świecie, a w konsekwencji zmiany jej priorytetów w prowadzonej polityce zagranicznej⁸³⁶. Szczególnie zauważalne w nowej koncepcji było wzmocnienie zapisów o obronie rosyjskich obywateli i rodaków za granicą, konieczności kreowania wielobiegunowego ładu międzynarodowego, wzmocnienia współdziałania na arenie międzynarodowej (zabieg przeciwko hegemonii USA) oraz zmiana kierunków priorytetowych, gdzie po Wspólnocie Niepodległych Państw⁸³⁷ znalazła się Europa zamiast USA (ukazywało to dążenie Rosji do wzmocnienia relacji z partnerami postrzeganymi w mniejszym stopniu jako konkurent militarny)⁸³⁸. Ponowne ocieplenie relacji Rosji z Zachodem nastąpiło stosunkowo szybko, co było związane z zamachami z 11 września 2001 roku, a jednocześnie objęciem urzędu Prezydenta Federacji przez W. Putina. Zaoferował on USA pomoc, telefonując po atakach terrorystycznych jako pierwszy do ówczesnego amerykańskiego prezydenta

⁸³² A. Czajkowski: *Federacja Rosyjska: przywracanie utraconej wielkości*. W: *Polityka zagraniczna: aktorzy...*, s. 85.

⁸³³ E. Cziomer, L. W. Zyblikiewicz: *Zarys współczesnych stosunków...*, s. 315.

⁸³⁴ T. A. Kisielewski: *Schylek Rosji*. Poznań 2007, s. 5.

⁸³⁵ Ibidem, s. 5.

⁸³⁶ *Koncepcja polityki zagranicznej Federacji Rosyjskiej zatwierdzona 28 czerwca 2000 roku*. Moskwa 2000. <https://www.bits.de/EURA/russia052800.pdf> (dostęp: 24.10.2022).

⁸³⁷ Wspólnota Niepodległych Państw została utworzona w 1991 roku jako częściowy sukcesor Związku Socjalistycznych Republik Radzieckich. Jako sukcesora należy tutaj rozumieć podmiot, który zrzeszałby państwa (wcześniej republiki) tak jak czynił to ZSRR. Początkowo w skład Wspólnoty wchodziła Rosja, Białoruś i Ukraina (do 2018 roku), a następnie Armenia, Azerbejdżan, Kazachstan, Kirgistan, Mołdawia, Tadżykistan, Turkmenistan, Uzbekistan i Gruzja (do 2008 roku). Państwa nadbałtyckie (Litwa, Łotwa, Estonia) nie wstąpiły do Wspólnoty. Celem jej istnienia było utworzenie związku niepodległych i suwerennych państw prowadzących własną politykę zagraniczną, należących do Organizacji Narodów Zjednoczonych oraz posiadających własną armię i rządy. Współpraca pomiędzy państwami członkowskimi miała dotyczyć przede wszystkim polityki bezpieczeństwa, gospodarki, nauki, kultury, oświaty i wymiany informacji. Źródło: R. Bierzanek, J. Symonides: *Prawo Międzynarodowe Publiczne*. Warszawa 2005, s. 129-130.

⁸³⁸ J. Diec: *Geostrategiczny wybór...*, s. 178-179; A. Bryc: *Cele polityki zagranicznej...*, s. 34-36.

G. W. Busha⁸³⁹. Rządy W. Putina zbiegły się z ożywieniem rosyjskiej gospodarki, co było spowodowane wzrostem cen surowców energetycznych (ropa naftowa i gaz ziemny) na rynkach światowych, tym samym zmniejszając zależność Rosji od zagranicznych czynników gospodarczych. Jednocześnie postrzeganie przez decydentów politycznych czasu lat dziewięćdziesiątych XX wieku jako okresu podległości Zachodowi, w trakcie którego rosyjskie interesy były lekceważone, doprowadziło do bardziej asertywnych i agresywnych działań Kremla na arenie międzynarodowej w pierwszej dekadzie XXI wieku. W. Putin chciał w wyniku prowadzonej polityki zagranicznej ukształtować i zaznaczyć status państwa rosyjskiego, jako wielkiego mocarstwa. Kulminacją tych działań była z kolei wojna gruzińsko-rosyjska z 2008 roku. Tym samym postawa Rosji wobec Zachodu stawała się coraz bardziej konfrontacyjna⁸⁴⁰. Jednocześnie umiejętne wywarzenie przez W. Putina rządów w państwie, zgodnie z tradycyjnym modelem sprawowania władzy, oscylującym pomiędzy demokracją a autorytaryzmem, zapewniało mu ogromne poparcie społeczne⁸⁴¹.

Rok 2008 przyniósł nie tylko zmianę na stanowisku Prezydenta Federacji w osobie D. Miedwiediewa, jednego z najbliższych współpracowników W. Putina, ale również nową Koncepcję polityki zagranicznej Federacji Rosyjskiej⁸⁴². J. Diec zauważa, że koncepcja była „owocem innych doświadczeń Rosji, nade wszystko jej rosnącej pozycji międzynarodowej jako ‘mocarstwa energetycznego’. Nominalnie jednak stanowiła tylko modyfikację poprzedniczki. Mocnym akcentem tej wersji jest kolejne, tym razem bardziej dobitne zwrócenie uwagi na konieczność wsparcia i popularyzacji języka rosyjskiego i kultury narodów Rosji”⁸⁴³. Główne założenia dokumentu ponownie nadają prymat relacjom z państwami obszaru poradzieckiego, postulując walkę ze zjawiskami neofaszystowskimi oraz próbom przeinaczania historii w celu wykorzystania jej do konfrontacji w polityce światowej, jak i tworzeniu równoprawnego partnerstwa z Unią Europejską oraz NATO⁸⁴⁴. Rok 2012 przyniósł ponowną zmianę na stanowisku Prezydenta Rosji, a właściwie powrót na to miejsce W. Putina. Rok później została

⁸³⁹ S. Bieleń: *Polityka Federacji Rosyjskiej wobec Stanów Zjednoczonych Ameryki*. W: *Polityka zagraniczna...*, s. 54.

⁸⁴⁰ CIDOB Barcelona Centre for International Affairs: *CIDOB International Yearbook 2010. Country profile, Russian Federation*. <https://www.cidob.org/sites/default/files/2025-01/ANUARIO%202010%20ANGLES.pdf> (dostęp: 12.08.2022).

⁸⁴¹ A. Bryc: *Putinizm jako doktryna odbudowy imperium?* W: *Rosja. Rozważania imperiologiczne*. Red. S. Bieleń, A. Skrzypek. Warszawa 2015, s. 99-100.

⁸⁴² *Koncepcja polityki zagranicznej Federacji Rosyjskiej zatwierdzona 15 lipca 2008 roku*. Moskwa 2008. <http://kremlin.ru/acts/news/785> (dostęp: 24.10.2022).

⁸⁴³ J. Diec: *Geostrategiczny wybór...*, s. 179.

⁸⁴⁴ A. Czajkowski: *Federacja Rosyjska: przywracanie utraconej wielkości*. W: *Polityka zagraniczna: aktorzy...*, s. 98-102; Ibidem, s. 179-181.

przyjęta kolejna Koncepcja polityki zagranicznej Federacji Rosyjskiej⁸⁴⁵. Dokument, będąc czwartym przyjętym w poradzieckiej historii Rosji utrzymał wiele typowych założeń, które pojawiały się w poprzednich jego wersjach⁸⁴⁶, jednakże został wzbogacony o nowe elementy występującego ówczesnie ładu międzynarodowy takie jak: „1) fundamentalna zmiana układu sił na arenie międzynarodowej polegająca na osłabieniu świata zachodniego i rosnącej potęgę Azji; 2) ogólna destabilizacja systemu międzynarodowego, spowodowana przez kryzys gospodarczy i finansowy oraz nowe jakościowo zjawisko, jakim jest agresywny radykalizm islamski; 3) intensyfikacja ‘konkurencji’ na arenie międzynarodowej, w której rosnącą rolę odgrywa czynnik tożsamości kulturowej i cywilizacyjnej; 4) wzrost nieprzewidywalności sytuacji międzynarodowej”⁸⁴⁷. Wskazać również należy, że w dokumencie Zachód jest postrzegany jako główne źródło problemów związanych z erozją systemu międzynarodowego. Jego działania prowadzą do pogłębiania kryzysu gospodarczo-finansowego oraz podejmowania jednostronnych decyzji bez właściwej konsultacji i zgody Organizacji Narodów Zjednoczonych⁸⁴⁸.

W roku 2014 doszło do wydarzenia, które przewartościowało znaczenie Federacji Rosyjskiej w skali globalnej. Nielegalna z punktu widzenia prawa międzynarodowego publicznego, a faktycznie dokonana aneksja Półwyspu Krymskiego udowodniła, że Kreml jest gotów do obrony swoich interesów, a jednocześnie jest w stanie ponieść koszty międzynarodowe podejmowanych działań. Niewątpliwie w rosyjskiej polityce wewnętrznej aneksja Półwyspu Krymskiego była ogromnym sukcesem propagandowym, co spowodowało wzrost poparcia dla prowadzonej przez W. Putina polityki⁸⁴⁹. Taki model działań Kremla został wpisany w kolejną Koncepcję polityki zagranicznej Federacji Rosyjskiej z 2016 roku⁸⁵⁰.

⁸⁴⁵ *Koncepcja polityki zagranicznej Federacji Rosyjskiej zatwierdzona 12 lutego 2013 roku*. Moskwa 2013. <http://www.pircenter.org/media/content/files/9/13617765900.pdf> (dostęp: 24.10.2022).

⁸⁴⁶ J. Diec pisze, że do stałych elementów wszystkich wersji *Koncepcji polityki zagranicznej Federacji Rosyjskiej* można zaliczyć: (1) priorytetowe traktowanie obszaru obejmującego Wspólnotę Niepodległych Państw, (2) dążenie do ukształtowania pozytywnych stosunków z państwami europejskimi (przede wszystkim Unią Europejską) w zakresie wymiany handlowej, (3) uznanie USA i NATO jako istotnych graczy w polityce międzynarodowej, (4) dążenie do tworzenia świata pozbawionego tradycyjnych podziałów politycznych i gospodarczych, (5) podtrzymywanie deklaracji pozostawania przy zasadzie suwerenności i nieingerencji w sprawy wewnętrzne innych państw, (6) dążenie do niwelowania konfliktów na Bliskim Wschodzie, (7) marginalizacja znaczenia partnerów latynoamerykańskich i afrykańskich. Źródło: J. Diec: *Geostrategiczny wybór...*, s. 183-184.

⁸⁴⁷ Ośrodek Studiów Wschodnich: *Koncepcja polityki zagranicznej Federacji Rosyjskiej*. <https://www.osw.waw.pl/pl/publikacje/analizy/2013-02-20/koncepcja-polityki-zagranicznej-federacji-rosyjskiej> (dostęp: 12.08.2022).

⁸⁴⁸ Ibidem.

⁸⁴⁹ Ośrodek Studiów Wschodnich: *Konsekwencje aneksji Krymu*. <https://www.osw.waw.pl/pl/publikacje/analizy/2014-03-19/konsekwencje-aneksji-krymu> (dostęp: 12.08.2022).

⁸⁵⁰ *Koncepcja polityki zagranicznej Federacji Rosyjskiej zatwierdzona 30 listopada 2016 roku*. Moskwa 2016. <http://static.kremlin.ru/media/acts/files/0001201612010045.pdf> (dostęp: 24.10.2022).

Podkreślono w niej znaczenie ideologii rosyjskiego świata (*ruskij mir*⁸⁵¹), która ma stanowić trzon prowadzonej przez Federację polityki w wymiarze zewnętrznym. Kluczowym dla Kremla pozostało utrzymanie swojej strefy wpływów (przede wszystkim obszaru byłych państw ZSRR, tzw. bliskiej zagranicy), jak również umacnianie swojej pozycji na świecie. W tym celu należy dokonać rozbudowy potencjału militarnego, zwiększając jednocześnie zaangażowanie w konflikty regionalne (np. wschodnia Ukraina, walka z Państwem Islamskim na Bliskim Wschodzie). Istotne pozostało również kreowanie pozytywnego wizerunku państwa na świecie, wobec czego zwiększeniu miało ulec finansowanie mediów funkcjonujących w zasięgu globalnym. W wymiarze wewnętrznym Kreml nadal będzie postrzegał prowadzoną politykę zagraniczną jako kluczowe narzędzie w kreowaniu pośród społeczeństwa rosyjskiego obrazu państwa jako globalnego mocarstwa⁸⁵². W dokumencie wskazano również wprost, że koniecznym jest „wzmocnienie pozycji rosyjskich środków masowego przekazu i masowej komunikacji w globalnej przestrzeni informacyjnej oraz dotarcie do szerokich kręgów społeczności międzynarodowej z rosyjskim punktem widzenia na procesy międzynarodowe”⁸⁵³. Przytoczony zapis należy rozumieć jako chęć Kremla do wzmocnienia swoich zdolności w zakresie obrony przed oddziaływaniem informacyjnym z zewnątrz, ale przede wszystkim kontynuowanie działań agresywnych w globalnej przestrzeni informacyjnej poprzez propagowanie i narzucanie swojego punktu widzenia na sprawy międzynarodowe innym uczestnikom.

Zmiany w koncepcji polityki zagranicznej prowadzonej przez Rosję przyniósł rok 2021, kiedy to w listopadzie podczas rozszerzonego kolegium Ministerstwa Spraw Zagranicznych Rosji na którym obecny był W. Putin wyznaczono najważniejsze cele dla rosyjskiej dyplomacji.

⁸⁵¹ Koncepcja *ruskiego miru* nie jest wytworem współczesnych elit politycznych i rządzących w Rosji, a jej genezę można odnaleźć już w czasach Carskiej Rosji. Co jednak istotne, jak pisze A. Wierzbicki, jego celem „nie jest tyle restauracja realnego (terytorialnego) imperium, ile restauracja świadomości mocarstwowej, wyobrażenia o dawnej, świetnej przeszłości, łączącej różne narody wokół kultury rosyjskiej i więzi z Rosją (...), *ruski mir* ma zasadniczo obronny charakter, zmierzający do ochrony rosyjskiego interesu narodowego, nieodłącznie związanego przede wszystkim z „bliską granicą” (...), pozostając koncepcją zorientowaną na obronę rosyjskiego interesu narodowego od czasu do czasu *ruski mir* przyjmuje charakter bardziej ekspansywny (odpowiedź na atak Gruzji w 2008 r., aneksja Krymu, zaangażowanie w konflikt na wschodzie Ukrainy), będąc reakcją na sytuację międzynarodową w najbliższym środowisku geopolitycznym Federacji Rosyjskiej. W rosyjskim rozumieniu jest to wtedy również obrona, ale staje się ona jedynie bardziej aktywna niż ekspansywna”. Źródło: A. Wierzbicki: *Russkij mir jako projekt restauracyjny imperium*. W: *Rosja. Rozważania imperiologiczne*. Red. S. Bieleń, A. Skrzypek. Warszawa 2015, s. 135-136.

⁸⁵² *Koncepcja polityki zagranicznej Federacji Rosyjskiej zatwierdzona 30 listopada 2016 roku*. Moskwa 2016. <http://static.kremlin.ru/media/acts/files/0001201612010045.pdf> (dostęp: 24.10.2022); A. M. Dyner: *Nowa Koncepcja rosyjskiej polityki zagranicznej*. „Biuletyn Polskiego Instytutu Spraw Międzynarodowych” 2017, nr 1 (1443) <https://pism.pl/upload/images/artykuly/legacy/files/22686.pdf> (dostęp: 12.08.2022); A. Daniluk: *Nowa koncepcja polityki zagranicznej Federacji Rosyjskiej z 2016 roku – analiza dokumentu w kontekście wydarzeń na arenie międzynarodowej*. „Studia Wschodnioeuropejskie” 2017, nr 7/2017, s. 55-72.

⁸⁵³ *Koncepcja polityki zagranicznej Federacji Rosyjskiej zatwierdzona 30 listopada 2016 roku*. Moskwa 2016. <http://static.kremlin.ru/media/acts/files/0001201612010045.pdf> (dostęp: 24.10.2022).

Skrytykowano działania podejmowane przez NATO, tj. militaryzację wschodniej flanki oraz wyrażono nadzieje na otrzymanie od Sojuszu gwarancji bezpieczeństwa. W istocie było to swego rodzaju ultimatum, w ramach którego zażądano wycofania się z podjętych działań, albo zagrożono nieuchronną eskalacją napięcia. Ponadto podkreślono konieczność wzmocnienia realizowanej koncepcji *ruskiego miru*, między innymi poprzez udzielanie pomocy Rosjanom żyjącym poza Federacją. Zapowiedziano podejmowanie działań mających na celu rozwiązywanie konfliktów na terenach byłego Związku Socjalistycznych Republik Radzieckich, na Bliskim Wschodzie oraz w Afryce Północnej⁸⁵⁴. Rosja dała zatem jasny sygnał Zachodowi, że zamierza bronić swoich interesów na arenie międzynarodowej oraz oczekuje z jego strony (w ocenie Rosji Zachód wszedł na ścieżkę konfrontacji) jasnych deklaracji oraz podjęcia działań deeskalacyjnych.

W 2021 roku dokonano również zaktualizowania Strategii bezpieczeństwa narodowego Federacji Rosyjskiej. Ponownie jak w poprzedniej jej wersji z 2015 roku podkreślono, że głównym zagrożeniem dla interesów narodowych Federacji jest polityka prowadzona przez Zachód, przede wszystkim USA. Można zaobserwować również wzrost znaczenia siły militarnej jako elementu osiągania celów polityki zagranicznej. Co więcej, położono nacisk na kwestie związane z bezpieczeństwem informacyjnym wskazując, że globalna przestrzeń informacyjna jest aktywnie zagospodarowywana jako nowa sfera działań wojennych, jak również, że „dywersje informacyjne i psychologiczne oraz ‘westernizacja’ kultury zwiększają zagrożenie utraty przez Federację Rosyjską suwerenności kulturowej”⁸⁵⁵. Nie ulega zatem wątpliwości, że treść strategii sprowadza się do stwierdzenia istnienia permanentnego zagrożenia jakim jest konfrontacja z Zachodem oraz przez Zachód wywołana. Z kolei Rosja wedle tych dokumentów podejmuje wyłącznie działania niezbędne do ochrony swoich interesów narodowych, gdyż wskutek działalności innych państw została do tego zmuszona. Tutaj należy również zauważyć, że dokładnie w takim samym tonie władze Kremla uzasadniały dokonaną inwazję w Ukrainie (2022), wskazując, że są to działania będące wyłącznie odpowiedzią na agresywną politykę Zachodu, przede wszystkim NATO pod przewodnictwem USA.

W odniesieniu do przeprowadzonych wyżej rozważań, należy w roli uzupełniającej zarysować cele polityki zagranicznej Federacji Rosyjskiej, realizowane wobec innych państw

⁸⁵⁴ A. M. Dyner: *Zaktualizowane kierunki polityki zagranicznej Rosji*. „Komentarz PISM” 2021, nr 88/2021 <https://pism.pl/webroot/upload/files/Komentarz%20PISM%20nr%2088-2021.pdf> (dostęp: 12.08.2022).

⁸⁵⁵ *Strategia Bezpieczeństwa Narodowego Federacji Rosyjskiej zatwierdzona 2 lipca 2021 roku*. Moskwa 2021. https://poland.mid.ru/pl/press-centre/news/strategia_bezpiecze_stwa_narodowego_federacji_rosyjskiej/ (dostęp: 24.10.2022).

oraz części świata na początku trzeciej dekady XXI wieku. W pierwszej kolejności trzeba zauważyć, że stosunki rosyjsko-amerykańskie pozostają niezwykle napięte. Kreml liczył na uzyskanie od USA gwarancji bezpieczeństwa, w tym nierozszerzania NATO na wschód. Ponadto wyrażenie przez Waszyngton gotowości do rozmów z Moskwą ośmieliło Rosjan do formułowania nowych żądań i eskalacji napięcia. Wobec trwającego konfliktu na Ukrainie nie należy spodziewać się w najbliższym czasie poprawy wzajemnych relacji⁸⁵⁶. Z kolei w odniesieniu do stosunków chińsko-rosyjskich można zauważyć, że pierwsze z państw wykorzystuje Kreml do wzmacniania swojej pozycji na świecie, natomiast dla Moskwy Pekin stanowi bardzo atrakcyjny rynek zbytu surowców energetycznych⁸⁵⁷. Co więcej, Rosjanie wobec nałożenia na nich sankcji w 2022 roku będą dążyć do głębszej współpracy w zakresie wymiany technologicznej z Państwem Środka. Należy jednak rozważyć, czy wobec stanu konfliktu rosyjsko-ukraińskiego na koniec 2022 roku Moskwa nadal posiada dostatecznie silną pozycję, aby być dla Pekinu równym partnerem⁸⁵⁸. Drugim niezwykle ważnym państwem na kierunku azjatyckim są od wielu lat dla Federacji Rosyjskiej Indie. Silne partnerstwo rosyjsko-indyjskie opiera się przede wszystkim na podobnej wizji świata oraz zbieżnych interesach strategicznych. Szczególnie ważnym pozostaje czynnik militarny, gdyż oba państwa prowadzą wspólne ćwiczenia wojskowe, a ponadto Indie pozyskują rosyjskie uzbrojenie. Szacuje się, że siły zbrojne tego państwa posiadają na wyposażeniu od około 60% do nawet 90% uzbrojenia dostarczonego przez Moskwę⁸⁵⁹. Wspomnieć również należy, że dla Rosji istotnymi kierunkami prowadzonej przez nią polityki zagranicznej pozostają Bliski Wschód⁸⁶⁰, Afryka⁸⁶¹ oraz Ameryka Łacińska⁸⁶².

⁸⁵⁶ A. Legucka: *Bilans i perspektywy polityki Rosji wobec USA po roku prezydentury Joe Bidena*. „Biuletyn Polskiego Instytutu Spraw Międzynarodowych” 2022, nr 23 (2442). [https://www.pism.pl/webroot/upload/files/Biuletyn/Biuletyn%20PISM%20nr%2023%20\(2442\)%208%20lutego%202022%20r.pdf](https://www.pism.pl/webroot/upload/files/Biuletyn/Biuletyn%20PISM%20nr%2023%20(2442)%208%20lutego%202022%20r.pdf) (dostęp: 03.03.2023), s. 1-2.

⁸⁵⁷ B. Panek: *Polityka Federacji Rosyjskiej w regionie Europy, Azji i Pacyfiku*. Warszawa 2015, s. 108-114.

⁸⁵⁸ J. Jakóbowski: *Chiński dylemat. Rosyjska inwazja na Ukrainę a sytuacja strategiczna Chin*. „Komentarze Ośrodka Studiów Wschodnich” 2022, nr 435. https://www.osw.waw.pl/sites/default/files/Komentarz_OSW_435.pdf (dostęp: 03.03.2023), s. 1-7.

⁸⁵⁹ P. Kugiel: *Słabnące partnerstwo Indii i Rosji - niespodziewany efekt wojny na Ukrainie*. „Biuletyn Polskiego Instytutu Spraw Międzynarodowych” 2022, nr 174 (2593). [https://www.pism.pl/webroot/upload/files/Biuletyn/Biuletyn%20PISM%20nr%20174%20\(2593\)%208%20listopada%202022%20r.pdf](https://www.pism.pl/webroot/upload/files/Biuletyn/Biuletyn%20PISM%20nr%20174%20(2593)%208%20listopada%202022%20r.pdf) (dostęp: 03.03.2023).

⁸⁶⁰ Defence24: *Bliski Wschód wobec wojny na Ukrainie: rosyjska propaganda i biznes*. <https://defence24.pl/geopolityka/bliski-wschod-wobec-wojny-na-ukrainie-rosyjska-propaganda-i-biznes> (dostęp: 03.03.2023).

⁸⁶¹ J. Czerep, A. Legucka: *Wzrost zaangażowania Rosji w Afryce*. „Biuletyn Polskiego Instytutu Spraw Międzynarodowych” 2019, nr 162 (1910). https://www.pism.pl/publikacje/Wzrost_zaanagazowania_Rosji_w_Afryce_ (dostęp: 03.03.2023), s. 1-3.

⁸⁶² B. Znojek: *Kierunki współpracy Rosji z partnerami w Ameryce Łacińskiej*. „Biuletyn Polskiego Instytutu Spraw Międzynarodowych” 2022, nr 83 (2502). <https://pism.pl/publikacje/kierunki-wspolpracy-rosji-z-partnerami-w-ameryce-lacinskiej> (dostęp: 03.03.2023), s. 1-2.

Przeprowadzona wyżej analiza omawiająca koncepcje rosyjskiej polityki zagranicznej wskazuje na kilka elementów stałych, które ulegały ewolucji oraz znaczeniu na przestrzeni ostatnich ponad 30 lat. Po upadku ZSRR w Rosji rozpoczął się proces, który można określić poszukiwaniem swojej tożsamości w pozimnowojennym świecie⁸⁶³. Bez względu na to jak określimy obecną pozycję Rosji, to z pewnością trzeba uznać jako trafne spostrzeżenie, iż od momentu objęcia władzy przez W. Putina prowadzi on politykę zmierzającą do odbudowy wpływów państwa rosyjskiego w skali globalnej. Rosja chce być postrzegana, ale również traktowana jako mocarstwo o zasięgu globalnym, jako godny sukcesor Związku Socjalistycznych Republik Radzieckich. Z oficjalnych dokumentów rządowych takich jak koncepcje, doktryny i strategie można wyprowadzić wnioski, że elity rządzące na Kremlu zdają sobie sprawę z licznych dysproporcji oraz ograniczonego potencjału jakim dysponuje Federacja Rosyjska. Tym samym nie jest ona w stanie aktywnie konkurować z USA na arenie międzynarodowej. Ponadto, rządzący mają świadomość, że pozycja Rosji jest oparta przede wszystkim na posiadanym arsenale nuklearnym (będącym spuścizną po ZSRR), jak również na posiadaniu znacznej ilości zasobów naturalnych, przede wszystkim surowców energetycznych, które często stanowią kartę przetargową w realizowanej polityce zagranicznej. Z kolei użycie sił zbrojnych ma charakter ostateczności i organiczna się (na chwilę obecną) głównie do obszaru poradzieckiego. Co istotne, takie działania w ocenie Moskwy są spowodowane wyłącznie agresywną polityką Zachodu, w związku z czym Rosja jest zmuszona do obrony swoich interesów wszelkimi możliwymi metodami. Co ważne, im częściej Kreml dostrzega procesy zbliżania się państw obszaru byłego ZSRR do Zachodu, tym częściej jest skłonny podejmować działania zmierzające od ich osłabiania za pomocą wszelkich środków. Tym samym Rosja staje się zagrożeniem dla bezpieczeństwa w tych regionach świata⁸⁶⁴. Należy zauważyć, że w ciągu ostatnich kilkunastu lat, Moskwa realizuje politykę zagraniczną w oparciu przede wszystkim o instrumenty z kategorii *soft power* (miękką siłą), rzadziej z *hard power* (twardą siłą)⁸⁶⁵. Często wykorzystywanym instrumentem z kategorii *soft power*, jest propagowanie i realizowanie koncepcji tzw. *ruskiego miru*, co jest możliwe między innymi dzięki zwiększaniu obecności Rosji w globalnej przestrzeni informacyjnej (medialnej)⁸⁶⁶. Drugim instrumentem jest osłabianie przeciwnika poprzez destabilizowanie sytuacji

⁸⁶³ S. Bieleń: *Tożsamość międzynarodowa Federacji...*, s. 43.

⁸⁶⁴ M. Banasik: *Interesy i cele strategiczne Federacji...*, s. 114-117.

⁸⁶⁵ S. Gardocki: *Polityka zagraniczna Rosji. Determinanty...*, s. 24-26.

⁸⁶⁶ Przykładem jest powstanie w 2005 roku rosyjskiej, ogólnopolskiej oraz wielojęzycznej telewizji informacyjnej Russia Today, obecnie RT. Podmiot ten od samego początku swojego istnienia pozostaje silnie związany z decydentami politycznymi na Kremlu.

wewnętrznej państwa, głównie w sferze politycznej, społecznej i gospodarczej, za pomocą kampanii oddziaływania informacyjnego i dokonywanych cyberataków⁸⁶⁷.

4.2. Wojna informacyjna jako instrument polityki zagranicznej Federacji Rosyjskiej

Informacja wykorzystana jako broń, cechuje się niskim kosztem wytworzenia, uniwersalnym charakterem, łatwą dostępnością oraz nieograniczonym zasięgiem. Przede wszystkim nie uznaje ona granic państwowych, a jej kontrola w dzisiejszym społeczeństwie informacyjnym jest w znacznym stopniu utrudniona, aby nie powiedzieć, że niemożliwa⁸⁶⁸. Doskonale zdaje sobie z tego sprawę Kreml, który mając stosunkowo ograniczone możliwości w zakresie oddziaływania na inne państwa, ucieka się do metod proporcjonalnie prostych i tanich, a jednocześnie bardzo skutecznych. Wojna informacyjna nie stanowi już jedynie hipotetycznego zagrożenia, nie jest abstrakcyjnym tworem, który może być omawiany jedynie na płaszczyźnie teoretycznej⁸⁶⁹. Rosyjska wojna informacyjna od lat staje się, a właściwie już się stała praktycznym wymiarem i narzędziem prowadzonej przez Kreml polityki zagranicznej wobec wielu państw na świecie. W niniejszym podrozdziale zostaną przedstawione i scharakteryzowane takie zagadnienia jak: geneza wojny informacyjnej w polityce zagranicznej Rosji, uwarunkowania rosyjskiej wojny informacyjne (doktryny, znaczenie i koncepcje), jak również wybrane jej środki oraz przykłady prowadzonej przez Rosję wojny informacyjnej w Estonii, Gruzji, USA oraz Ukrainie.

4.2.1. Geneza i uwarunkowania wojny informacyjnej w polityce zagranicznej Federacji Rosyjskiej

Historia rosyjskiej wojny informacyjnej rozpoczyna się już w okresie istnienia Związku Radzieckiego, a jej zastosowanie jako narzędzia w prowadzonej polityce zagranicznej zawsze miało jak i ma współcześnie charakter kompleksowy. Ma trwałe cechy wypracowane na przestrzeni dziesiątek lat, które utrwaliły się w systemie politycznym Związku

⁸⁶⁷ S. Gardocki: *Polityka zagraniczna Rosji. Determinanty...*, s. 26-27.

⁸⁶⁸ Zobacz szerzej: J. Darczewska: *Anatomia rosyjskiej wojny informacyjnej Operacja Krymska – studium przypadku*. „Punkt widzenia” 2014, nr 42. https://www.osw.waw.pl/sites/default/files/anatomia_rosyjskiej_wojny_informacyjnej.pdf (dostęp: 05.03.2023); J. Darczewska: *Wojna informacyjna Rosji z Zachodem. Nowe wyzwanie?* „Przegląd Bezpieczeństwa Wewnętrznego” 2015, Wydanie Specjalne; T. R. Aleksandrowicz: *Podstawy walki informacyjnej*. Warszawa 2016.

⁸⁶⁹ M. Wrzosek: *Rosyjska dominacja informacyjna w sferze militarnej*. W: *Informacja czynnikiem warunkującym bezpieczeństwo. Kontekst rosyjski*. Red. M. Banasik. Warszawa 2021, s. 13.

Socjalistycznych Republik Radzieckich, a współcześnie ewoluują w systemie politycznym Federacji Rosyjskiej. Niewiele państw na świecie zajmuje się zjawiskiem wojny informacyjnej na tak szeroką skalę oraz realizuje ją przy użyciu tak znacznych zasobów organizacyjnych i finansowych⁸⁷⁰. Kreowanie, pozyskiwanie, przetwarzanie itp. informacji na potrzeby państwa jest domeną funkcjonujących w jego strukturach służb specjalnych (informacyjnych). Nie inaczej ma się to w przypadku Rosji, gdzie pełnią one specyficzną funkcję będąc jednocześnie podległe jak i zwierzchnie wobec władzy. Sprowadza się to do stwierdzenia, że służby specjale w państwie mają ogromną możliwości wpływania na prowadzoną przez nie politykę wewnętrzną i zagraniczną. Nic więc dziwnego, że Y. Harrel postawił pytanie „czy należy stwierdzić, zapożyczając od Woltera jego *bon mot* o Prusach, iż Rosja to nie państwo, które dysponuje służbami informacyjnymi, lecz służby informacyjne, w których dyspozycji jest państwo?”⁸⁷¹.

Nawiązania do koncepcji rosyjskich wojen informacyjnych można odnaleźć już w dorobku J. Messnera⁸⁷², twórcy teorii wojen buntowniczych, których istotnym orężem są działania w przestrzeni informacyjnej. Wskazywał, że cele wojen buntowniczych muszą podlegać klasyfikacji w związku z czym zaproponował następującą ich hierarchię: „1) zniszczenie morale ludności przeciwnika; 2) pokonanie aktywnych jednostek (wojska, partyzantów, walczących ruchów ludowych); 3) zagarnięcie lub zniszczenie przedmiotów o wartości psychologicznej; 4) zagarnięcie lub zniszczenie przedmiotów o wartości materialnej; 5) osiągnięcie efektów zewnętrznych w celu znalezienia nowych sojuszników i zaszkodzenia duchowi sojuszników przeciwnika”⁸⁷³. Następnie wskazał, że w tym samym

⁸⁷⁰ J. Darczewska: *Anatomia rosyjskiej wojny...*, s. 5-22, 33-36.

⁸⁷¹ Y. Harrel: *Rosyjska cyber-strategia*. Warszawa 2015, s. 63.

⁸⁷² Jewgienij Messner urodzony w 1891 roku w Odessie w Imperium Rosyjskim, zmarły w 1974 roku w Buenos Aires w Argentynie. Był pułkownikiem Armii Imperium Rosyjskiego oraz Białej Armii (zwolennicy caratu w Rosji). Studiował na Noworosyjskim Uniwersytecie Państwowym, gdzie ukończył I kurs na Wydziale Fizyki i Matematyki. Następnie wstąpił do wojska, gdzie w 1912 roku awansował na swój pierwszy stopień oficerski, chorążego artylerii. Po rozpoczęciu rewolucji bolszewickiej w 1917 roku brał udział w walkach z komunistami walcząc w szeregach Białej Armii. W wyniku poniesionej klęski przez zwolenników caratu w Rosji, był zmuszony wyemigrować do Belgradu, gdzie od 1931 roku wykładał w Akademii Wojskowej. Po zajęciu przez III Rzeszę Królestwa Jugosławii i rozpoczęciu wojny z ZSRR, wstąpił do Wehrmachtu, gdzie służył w 1 Rosyjskiej Armii Narodowej (formacja kolaborująca z Niemcami), pełniąc funkcję oficera propagandy. W 1945 roku został internowany w Lichtensteinie, a dwa lata później wyemigrował do Argentyny. Posiadając stopień naukowy doktora tworzył prace z zakresu teorii wojskowości, a do najważniejszych z nich zaliczamy: *Oblicze współczesnej wojny* (1959), *Miatież - nazwa III Wojny światowej* (1960), *Współcześni oficerowie* (1961), *Ogólnoswiatowa matieżewojna* (1971).

⁸⁷³ J. Messner: *Хочешь Мира, Победы Матежевойну!* Москва 2005. http://militera.lib.ru/science/messner_ea01/index.html (dostęp: 21.08.2022), s. 132. Tłumaczenie własne. Tekst w oryginale: „1) развал морали вражеского народа, 2) разгром его активной части (воинства, партизанства, борющихся народных движений), 3) захват или уничтожение объектов психологической ценности, 4) захват или уничтожение объектов материальной ценности, 5) эффекты внешнего порядка ради приобретения новых союзников, потрясения духа союзников врага”.

czasie należy dążyć do „a) zabezpieczenia morale swojego narodu, b) zabezpieczenia swojej aktywnej, wojowniczej siły, c) obrony psychologicznie lub życiowo niezbędnych obiektów oraz d) unikanie wszystkiego, co mogłoby wywołać nieprzychylną reakcję w państwach neutralnych, ale będących przedmiotem naszego zainteresowania”⁸⁷⁴. Zaznaczył również, że „we wszystkich przypadkach należy zwracać uwagę na reakcje nie tylko w sferach decyzyjnych, ale także w szerszych masach, pełnoprawnych uczestnikach wojny czy powstania”⁸⁷⁵. Koncepcje J. Messnera zakładają więc zmianę tradycyjnego postrzegania przeciwnika którym są siły zbrojne innego państwa, a w konsekwencji swego rodzaju jego rozmycie. Przeciwnikiem stało się społeczeństwo (danego państwa), a przestrzeń w której ma miejsce konflikt może również być przestrzenią sfery ludzkiej świadomości⁸⁷⁶. T. Aleksandrowicz pisał, że wskazał on również na konieczność podejmowania działań prowadzących do „rozkładu morale danego narodu i rozbicie aktywnych części państwa (sił zbrojnych, ruchów społecznych). Głównym celem wojny buntowniczej jest „zdobycie duszy wrogiego narodu”, stąd istotną rolę odgrywają w niej dziennikarze, dywersanci, prowokatorzy, propagandyści, a pojęcie linii frontu w takiej wojnie odnosi się do poszczególnych sfer aktywności danego społeczeństwa”⁸⁷⁷. Tym samym wskazać należy, że założenia koncepcji J. Messnera, przekonane o zakończeniu pod koniec XX wieku *clauswitzowskich wojen*⁸⁷⁸ są obecne we współczesnych założeniach rosyjskich wojen informacyjnych i stanowiły dla nich punkt wyjścia⁸⁷⁹.

Geneza współczesnych koncepcji rosyjskich wojen informacyjnych wywodzi się również bezpośrednio z dorobku doktryny Związku Socjalistycznych Republik Radzieckich⁸⁸⁰. Dezinformacja była bowiem elementem realizowanej polityki wewnętrznej, jak i zewnętrznej

⁸⁷⁴ Ibidem, s. 132. Tłumaczenie własne. Tekst w oryginale: „a) к сбережению морали своего народа, б) к сбережению своей активной, воюющей силы, в) к обороне психологически или жизненно необходимых объектов и г) к избежанию всего, что даст неблагоприятный отклик в государствах нейтральных, но для нас интересных”.

⁸⁷⁵ Ibidem, s. 132. Tłumaczenie własne. Tekst w oryginale: „Во всех случаях иметь в виду реакции не только в руководящих сферах, но и в широких массах, полноценных участниках войны или мятежа”.

⁸⁷⁶ J. Kiera: *Implikacje koncepcji wojen buntowniczych Jewgienija Messnera dla doktryny bezpieczeństwa Federacji Rosyjskiej w XXI wieku*. W: *Perspektywy zagrożeń dla bezpieczeństwa międzynarodowego kreowanych przez Federację Rosyjską*. Red. M. Banasik, A. Rogozińska. Warszawa 2019, s. 162-164.

⁸⁷⁷ T. R. Aleksandrowicz: *Zagrożenia dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym. Budowanie zdolności defensywnych i ofensywnych w infosferze*. Warszawa 2021, s. 103.

⁸⁷⁸ M. Banasik: *Rywalizacja presja i agresja Federacji Rosyjskiej. Konsekwencje dla bezpieczeństwa międzynarodowego*. Warszawa 2021, s. 121.

⁸⁷⁹ W tym miejscu należy jednak zauważyć, że swego rodzaju odejście od tego założenia można zaobserwować w związku z trwającym pełnowymiarowym konwencjonalnym konfliktem rosyjsko-ukraińskim, jak również można było obserwować w 2008 roku podczas wojny gruzińsko-rosyjskiej.

⁸⁸⁰ E. Lucas, P. Pomerantsev: *Winning the Information War. Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe. A Report by CEPA's Information Warfare Project in Partnership with the Legatum Institute*. Washington D.C. 2016, s. 6.

od początków jego istnienia. W 1942 roku była nauczana w Rosyjskim Instytucie Wojskowym Języków Obcych, a jej ideologia sięgała korzeniami do koncepcji marksistowsko-leninowskich, gdzie występowała pod nazwą *teorii specpropagandy*⁸⁸¹. Jak pisze M. Banasik, „Kreml od dawna dążył do dominacji informacyjnej wewnątrz i poza swoimi granicami, wpływał na wydarzenia i zachowania w państwach uznawanych zarówno za konkurencyjne, jak i pozostające pod rosyjską strefą wpływu, wykorzystując różnorodne mechanizmy oddziaływania”⁸⁸². Już od początkowego okresu istnienia ZSRR dużą wagę przykładano do kontroli przepływu informacji. Ojciec rewolucji, W. I. Lenin uważał, że międzynarodową burżuazję można pokonać w sposób niekonwencjonalny, tj. poprzez wykorzystywanie istniejących pomiędzy wrogami konfliktów, czy podtrzymywanie pomiędzy sojusznikami sojuszków, nawet jeśli te miałyby być tylko chwilowe⁸⁸³. W tym czasie wykształciło się również pojęcie *agitporpagandy*, a więc połączenia agitacji skierowanej do emocji odbiorcy i propagandy skierowanej do jego umysłu. Stała się więc ona bronią informacyjną, służącą realizowaniu zamierzonych celów politycznych⁸⁸⁴.

Aktywność Związku Radzieckiego w okresie zimnej wojny ulegała stopniowemu rozszerzaniu sprowadzając się do wojny informacyjnej polegającej na oddziaływaniu na ludność ZSRR, jak i ludność za granicą. Kreml finansował przedsięwzięcia, które były krytycznie nastawione do szeroko rozumianego Zachodu oraz promował idee komunizmu. W tym celu wspierano antyzachodnie ruchy pokojowe, czy też zapraszano zachodnich myślicieli i artystów do państwa by wypowiadali się w sposób pozytywny na temat Związku Radzieckiego⁸⁸⁵. Służby specjalne z KGB⁸⁸⁶ na czele prowadziły kampanie oddziaływania informacyjnego, czego przykładem może być operacja Infektion z 1983 roku w ramach której sponsorowana przez rosyjskie służby indyjska gazeta *The Patriot* opublikowała artykuł oskarżający amerykańskie władze o stworzenie wirusa AIDS i wykorzystywanie go jako broni. W 1987 roku wiadomość ukazała się ponad 40 razy w kontrolowanej przez Związek Radziecki

⁸⁸¹ J. Darczewska: *Anatomia rosyjskiej wojny...*, s. 9.

⁸⁸² M. Banasik: *Rywalizacja presja i agresja Federacji...*, s. 109.

⁸⁸³ Ibidem, s. 110.

⁸⁸⁴ K. Brown: *Agitprop in Soviet Russia*. „Constructing the Past” 2013, Vol. 1, Issue 1, 4-2013, s. 5-8.

⁸⁸⁵ M. Banasik: *Rywalizacja presja i agresja Federacji...*, s. 110-110.

⁸⁸⁶ KGB (Komitet Bezpieczeństwa Państwowego przy Radzie Ministrów ZSRR) – jedna z najważniejszych służb specjalnych ZSRR odpowiedzialna za prowadzenie działań wywiadowczych i kontrwywiadowczych w kraju i zagranicą, inwigilację ludności, prowadzenie między innymi działań dezinformacyjnych oraz zwalczanie opozycji politycznej. Rozwiązana w 1991 roku po upadku ZSRR i przekształcona w Federacji Rosyjskiej w służby takie jak: Służba Wywiadu Zagranicznego Federacji Rosyjskiej, Federalna Służba Bezpieczeństwa Federacji Rosyjskiej oraz Federalna Służba Ochrony Federacji Rosyjskiej. W skład KGB wchodził Zarząd V odpowiedzialny między innymi za walkę ideologiczną.

prasie, będąc przedrukowaną lub nadawaną w ponad 80 państwach i 30 językach⁸⁸⁷. Innym przykładem mogą być działania zmierzające do kompromitacji amerykańskiego prezydenta R. Reagana czy papieża Jana Pawła II⁸⁸⁸.

Po upadku ZSRR radziecki aparat propagandowy został przeorganizowany przede wszystkim w ramach służb specjalnych tworzonych w Federacji Rosyjskiej. Jednocześnie postępująca rewolucja technologiczna w świecie cyfrowym zaoferowała wiele nowych możliwości w zakresie prowadzenia kampanii oddziaływania informacyjnego. Działania propagandowe i dezinformacyjne dobrze znane z okresu zimnej wojny nie zostały jednak zakończone, lecz zmodyfikowane i dostosowane do zmian jakie wystąpiły na świecie⁸⁸⁹. Współcześnie stosowana propaganda nie ma już wymiaru lewicowego, gdyż nie odpowiada realiom współczesnego ładu międzynarodowego, jak i jest stosunkowo łatwo identyfikowalna. W związku z tym, współczesne działania Kremla polegają zarówno na popieraniu ideologii lewicowej, jak i ruchów skrajnie prawicowych, a łączącą je cechą jest propagowanie wrogości i nieufności wobec zachodnich systemów społeczeństwa demokratycznego⁸⁹⁰. Można zatem wyprowadzić wniosek, że działania propagandowe Związku Radzieckiego były sprowadzane przede wszystkim do propagandowania ideologii komunistycznej, z kolei współcześnie po rozpadzie ZSRR władze na Kremlu nie mają już takich ograniczeń, a podstawowym ich celem jest dezintegracja społeczna innych państw. Co więcej, nowa propaganda jest przemyślanie ukierunkowana, sprawna oraz pozbawiona faktów, ale również przyjemna dla odbiorcy i angażująca emocjonalnie. Kreowane przekazy są zupełnie pozbawione zimnowojennego stylu, często sztywnego i nudnego⁸⁹¹.

Można zatem wskazać, że choć sposób prowadzenia wojny informacyjnej w ramach realizowanej przez Kreml polityki zagranicznej uległ zmianie (z uwagi na zmiany zachodzące w środowisku międzynarodowym), to niezmiennie jej cele pozostają stałe⁸⁹². Rosja nieustannie dokonuje modyfikacji zarówno technicznej jak i merytorycznej formułowanych przez siebie przekazów w ramach prowadzonych kampanii oddziaływania informacyjnego. Co więcej, są one „dostosowywane do potrzeb państwa i są rozwijane w miarę wprowadzania do użytku nowych technologii informacyjnych. W opinii ekspertów, powiązanie technik dezinformacji z elementami działań psychologicznych przynosi określone rezultaty, których efektem jest

⁸⁸⁷ T. Rid: *Wojna informacyjna...*, s. 369-415; E. Lucas, P. Pomerantsev: *Winning the Information War...*, s. 17.

⁸⁸⁸ T. R. Aleksandrowicz: *Podstawy walki informacyjnej...*, s. 93.

⁸⁸⁹ E. Lucas, P. Pomerantsev: *Winning the Information War...*, s. 5-6.

⁸⁹⁰ M. Banasik: *Rywalizacja presja i agresja Federacji Rosyjskiej...*, s. 111.

⁸⁹¹ E. Lucas, P. Pomerantsev: *Winning the Information War...*, s. 9.

⁸⁹² Ibidem, s. 6.

narzucane w przestrzeni publicznej własnej narracji i sposobu interpretowania zachodzących zdarzeń”⁸⁹³. Działalność Kremla ujęto w sposób systemowy w raporcie Departamentu Stanu z 2020 roku w którym stwierdzono, że „rosyjska dezinformacja i propaganda to ekosystem zbioru oficjalnych, *proxy* i nieautoryzowanych kanałów komunikacyjnych i platform, które Rosja wykorzystuje do tworzenia i wzmacniania fałszywych narracji”⁸⁹⁴. Rosyjska wojna informacyjna to zatem produkt tradycyjny, wykorzystywany od dziesiątek lat, a jednocześnie dostosowany do nowopowstałych narzędzi medialnych, które pojawiły się wraz z rozwojem technologicznym, przede wszystkim sieci Internet.

Wejście Rosji w XXI wieku przyniosło szereg reform związanych z szeroko rozumianą budową zaplecza informacyjnego. Jak pisze J. Darczewska, „rosyjska teoria wojen informacyjnych ma także rys interdyscyplinarnej nauki stosowanej. Odnosi się bowiem do bardzo szerokiego spektrum działań (politycznych, gospodarczych, społecznych, militarnych, wywiadowczych, kontrwywiadowczych, dyplomatycznych, propagandowych, psychologicznych, informatycznych, technologii komunikacyjnych, edukacyjnych i in.)”⁸⁹⁵. Wiązało się to z utworzeniem w 2003 roku przy Uniwersytecie Moskiewskim im. Łomonosowa Instytutu Problemów Bezpieczeństwa Informacyjnego, którego jedną ze specjalizacji jest problematyka współpracy międzynarodowej w zakresie bezpieczeństwa informacyjnego. Z kolei kształceniem kadr zajmuje się utworzone również przy wskazanej uczelni wyższej Informacyjno-Analityczne Centrum Badań Procesów Społeczno-Politycznych na Obszarze Poradzieckim. Jednym z jego priorytetów w zakresie prowadzonych działań są badawcze projekty stosowane, monitoring przestrzeni informacyjnej oraz informacyjne zabezpieczenie działalności struktur państwowych⁸⁹⁶. Tym samym należy stwierdzić, że Rosja pozostaje w pełni świadoma co do znaczenia jak i możliwości wiążących się z prowadzeniem kampanii oddziaływania informacyjnego oraz działań jakie należy podejmować by zwiększać w tym zakresie swój potencjał.

W odniesieniu do oceny zdolności w zakresie wykorzystania wojny informacyjnej jako narzędzia w prowadzonej przez Rosję polityce zagranicznej należy wreszcie wskazać, że jej potencjał nie jest niski, a wręcz przeciwnie. Rosja, zwłaszcza po rozpadzie Związku Radzieckiego, bywa bardzo często kojarzona jako państwo, które jest nieprzystosowane do

⁸⁹³ M. Wrzosek: *Rosyjska dominacja informacyjna w sferze...*, s. 13-14.

⁸⁹⁴ U.S. Department of State: *GEC Special Report. Pillars of Russia's Disinformation and Propaganda Ecosystem*. Washington D.C. 2020, s. 3. Tłumaczenie własne. Tekst w oryginale: „russia's disinformation and propaganda ecosystem is the collection of official, proxy, and unattributed communication channels and platforms that Russia uses to create and amplify false narratives”.

⁸⁹⁵ J. Darczewska: *Anatomia rosyjskiej wojny...*, s. 10.

⁸⁹⁶ Ibidem, s. 10-11.

postępującej rewolucji informatycznej i informacyjnej. Jest to jednak założenie całkowicie błędne. Zmiany zachodzące w ramach wskazanych przemian nie były niezrozumiałe ani pomijane przez rządzących zarówno w Związku Radzieckim, jak i współcześnie w Rosji⁸⁹⁷. Dla przykładu, już w 1961 roku Rada Cybernetyczna Akademii Nauk w Moskwie przedłożyła opracowanie pt. „Cybernetyka na usługach komunizmu”, w którym postulowano stworzenie regionalnych ośrodków informatycznych, umożliwiających używanie komputerów do sporządzania statystyk i planowania zadań oraz zwiększenie szybkości podejmowania decyzji przez kadry kierownicze⁸⁹⁸. Z kolei S. Gerowitch w swoim raporcie pisał, że w latach siedemdziesiątych XX wieku wśród amerykańskiej administracji panował lęk związany z obawą, że Związek Radziecki posiada zaawansowany system zarządzania zbudowany w oparciu o sieć komputerów SOVNET, który miał znacznie wyprzedzać pod kątem technologicznym amerykański ARPANET, współcześnie znany pod nazwą Internet. Tym samym trafny pozostaje wniosek, że prace prowadzone przez ZSRR były postrzegane jako zaawansowane oraz upatrywane jako realne zagrożenie w USA⁸⁹⁹. Rozpad Związku Radzieckiego z oczywistych względów zahamował postępującą w tym państwie rewolucję informatyczną oraz informacyjną. Nie nastąpiło to jednak w takim stopniu, aby nie móc określić Rosji jako współinicjatorce postępujących przemian technologicznych, które współcześnie umożliwiają prowadzenie kampanii oddziaływania informacyjnego w globalnej przestrzeni informacyjnej oraz cyberataków w cyberprzestrzeni.

Analizując genezę rosyjskich wojen informacyjnych nie sposób nie wspomnieć o występującym w rosyjskiej kulturze strategicznej syndromie oblężonej twierdzy, przez który należy rozumieć „optykę sytuacyjną (atmosferę) zakładającą otoczenie, osaczenie danego systemu (w skali mikro i makro) przez wrogie, agresywne podmioty”⁹⁰⁰. Zjawisko to należy rozumieć wielowymiarowo, toteż z „jednej strony to określone dyspozycje psychologiczne oparte na strachu, nienawiści, poczuciu osaczenia przez wrogie siły, na granicy (lub poza nią) paranoi. Jest to jednak także dynamiczne zjawisko społeczno-kulturowe: aksjologia wojny, centralizacja konfliktu z wrogiem otoczeniem, intensyfikacja negatywnych stereotypów”⁹⁰¹. Syndrom ten wykształcił i utrwalił występujące we współczesnej Rosji postrzeganie Zachodu jako wroga, a co za tym idzie zakorzenienie przeświadczenia, że zimna wojna nadal trwa. Takie

⁸⁹⁷ Y. Harrel: *Rosyjska cyber-strategia...*, s. 26.

⁸⁹⁸ Ibidem, s. 70.

⁸⁹⁹ Ibidem, s. 26; Zobacz szerzej: S. Gerovitch: *From Newspeak to Cyberspeak, a history of Soviet Cybernetics*. Cambridge 2002.

⁹⁰⁰ J. Ziółkowski: *Zarządzanie syndromem oblężenia w demokracji liberalnej*. „Studia Politologiczne” 2016, Vol. 41, s. 171; Zobacz szerzej: J. Ziółkowski: *Syndrom oblężonej twierdzy*. Warszawa 2019.

⁹⁰¹ Ibidem, s. 171-172.

ujmowanie otaczającej Rosję rzeczywistości zdecydowanie ułatwia uzasadnianie podejmowanych działań na arenie międzynarodowej przed swoimi obywatelami, a wręcz skutkuje ich całkowitą aprobatą. Syndrom ten obecny już w czasach istnienia ZSRR kreował w społeczeństwie obraz państwa radzieckiego, które będąc nieustannie zagrożone atakiem ze strony USA lub NATO musiało być pod każdym względem samowystarczalne i zdolne do obrony⁹⁰². Taka koncepcja stała się ideologicznym zapleczem rosyjskiej polityki informacyjnej w wymiarze wewnętrznym, co z kolei umożliwia uzasadnianie działań podejmowanych w wymiarze zewnętrznym. Jednocześnie powoduje konsolidację społeczeństwa, które akceptuje prowadzoną przez Kreml politykę twardej władzy⁹⁰³.

Elementem zdecydowanie ułatwiającym prowadzenie kampanii oddziaływania informacyjnego jest diaspora rosyjskojęzyczna występująca w wielu państwach na świecie, przede wszystkim państwach tzw. bliskiej zagranicy. Po upadku Związku Radzieckiego na terytorium obecnej Federacji Rosyjskiej znalazło się tylko 52% dotychczasowej populacji państwa. Z kolei pośród ludności, która nie weszła w skład nowopowstałego tworu można wyróżnić około 25 milionową diasporę rosyjskojęzyczną⁹⁰⁴. Czynnikiem ten jest niezwykle istotnym elementem prowadzonych przez Rosję działań, gdzie występująca diaspora rosyjskojęzyczna zachowała więzi kulturowe i emocjonalne z Rosją, co z kolei stwarza dogodną przestrzeń dla rosyjskiej działalności informacyjnej⁹⁰⁵. Diaspora rosyjskojęzyczna może więc stanowić czynnik dezintegrujący państwa od wewnątrz, w szczególności wobec dużego zainteresowania władz Kremla ochroną interesów wszystkich Rosjan, bez względu na miejsce ich zamieszkania. Okoliczność ta jest również bardzo często podkreślana w dokumentach rządowych takich jak doktryny, strategie i koncepcje⁹⁰⁶. Doskonałym przykładem wykorzystania rosyjskiej diaspory przez Kreml w prowadzonej polityce zagranicznej może być trwający od 2014 roku konflikt we wschodniej Ukrainie, podczas którego ochrona ludności rosyjskojęzycznej była jednym z podstawowych argumentów uzasadniających podejmowane przez Rosję działania⁹⁰⁷. Rosyjska diaspora w ramach

⁹⁰² R. Kłaczyński: *Kultura strategiczna Federacji Rosyjskiej*. „Nowa Polityka Wschodnia” 2012, nr 1 (2), s. 26.

⁹⁰³ Zobacz szerzej: A. Kudors: *Fortress Russia: Political, Economic, and Security Development in Russia Following the Annexation of Crimea and its Consequences for the Baltic States*. Riga 2016.

⁹⁰⁴ A. Bryc: *Rosja w XXI wieku. Światowy...*, s. 13-14.

⁹⁰⁵ J. Darczewska: *Anatomia rosyjskiej wojny...*, s. 34-35.

⁹⁰⁶ M. Delong: „*Ruski mir*” jako narzędzie rosyjskiej ekspansji geopolitycznej na terytorium Ukrainy. „Przegląd Geopolityczny” 2020, nr 33, s. 56.

⁹⁰⁷ I. J. Courter: *Russian Preinvasion Influence Activities in the War with Ukraine*. „Military Review” 2022, July 2022 Online Exclusive Article, s. 1-12.

prowadzonej wojny informacyjnej ma również służyć rywalizacji cywilizacyjnej pomiędzy kulturą euroazjatycką a zachodnią⁹⁰⁸.

Wreszcie należy odnieść się do rosyjskich koncepcji wojny informacyjnej formułowanych przez jej teoretyków. W tym celu wszelkie rozważania należy rozpocząć od ukazania sposobu postrzegania (definiowania) wojny informacyjnej przez nich oraz decydentów politycznych. W pierwszej kolejności trzeba poczynić stwierdzenie, że choć koncepcje te nie są nowe, to jednocześnie nie są statyczne, ulegając nieustannej ewolucji oraz dostosowując się do zmieniającego środowiska międzynarodowego⁹⁰⁹. Następnie należy ponownie podkreślić sformułowania wskazywane w poprzedniej części niniejszej rozprawy, że wojna informacyjna w ujęciu rosyjskim różni się od koncepcji zachodnich. Stosowana przez Kreml szeroko rozumiana dezinformacja różni się od tradycyjnych form propagandy jakie występują w nauce zachodniej, a można wręcz poczynić stwierdzenie, że koncepcje te zbudowano w opozycji do nich⁹¹⁰. E. Lucas i P. Pomerantsew wskazują, że w Rosji takie koncepcje określane są mianem wojny informacyjno-psychologicznej. Piszą, że „jej celem nie jest przekonanie czy perswazja, ale raczej podważenie. Zamiast pobudzać odbiorców do działania, stara się utrzymać ich w stanie zawieszenia i dekoncentracji, pasywności, paranoi. (...) Jest to taktyka stosowana w celu dezorganizacji i zdemoralizowania przeciwnika. Toczy się w sferze percepcji i umysłów ludzi. Trwa zarówno w czasie pokoju, jak i w czasie wojny. Rosyjska dezinformacja jest rozpowszechniana zarówno jawnie – za pośrednictwem obcojęzycznej telewizji (zwłaszcza wielojęzycznej RT) i samowłańczej agencji informacyjnej Sputnik International – jak i potajemnie, przy użyciu pozornie niezależnych dziennikarzy, ekspertów i komentatorów”⁹¹¹. Podnieść również należy, że elementem właściwym dla rosyjskich wojen informacyjnych jest ich prowadzenie przeważnie poniżej granicy otwartego konfliktu zbrojnego. Należy przez to rozumieć, że taka wojna jest swego rodzaju wojną

⁹⁰⁸ M. Banasik: *Teoria i praktyka wojny informacyjnej stosowanej przez Federację Rosyjską*. W: *Informacja czynnikiem warunkującym bezpieczeństwo. Kontekst rosyjski*. Red. M. Banasik. Warszawa 2021, s. 56.

⁹⁰⁹ K. Giles, A. Seaboyer: *The Russian Information Warfare Construct*. Technical Report, Report number: DRDC-RDDC-2019-C241Affiliation: Defence Research and Development Canada 2019, s. 4-5.

⁹¹⁰ J. Darczewska: *Anatomia rosyjskiej wojny...*, s. 7.

⁹¹¹ E. Lucas, P. Pomerantsev: *Winning the Information War. Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe. A Report by CEPA's Information Warfare Project in Partnership with the Legatum Institute*. Washington D.C. 2016, s. 5. Tłumaczenie własne. Tekst w oryginale: „Its aim is not to convince or persuade, but rather to undermine. Instead of agitating audiences into action, it seeks to keep them hooked and distracted, passive and paranoid. (...) It is a tactic used to disorganize and demoralize an opponent. It is fought in the realms of perception and the minds of men. It continues through both official peace and wartime. Russian disinformation is disseminated both overtly through foreign-language television (notably the multilingual RT) and the self-styled news agency Sputnik International and covertly, using notionally independent journalists, experts and commentators”.

niewypowiedzianą, czy nawet nienależącą do wstępnej fazy konfliktu⁹¹². Kremłowska konfrontacja informacyjna w wyniku podjętych działań ma na celu wywieranie wpływu na „sferę mentalną, postawy emocjonalne i behawioralne oraz stan moralny czy psychiczny przeciwnika”⁹¹³.

Definicje wojny informacyjnej zawarte w literaturze rosyjskiej oraz dokumentach rządowych nie powinny być zestawiane z definicjami nowszymi, występującymi na Zachodzie. K. Giles wskazał w tym kontekście, że „hasło ‘wojna informacyjna’ (*informatsionnaya voyna*) w glosariuszu kluczowych terminów z zakresu bezpieczeństwa informacyjnego opracowanym przez Akademię Wojskową Sztabu Generalnego wyraźnie rozróżnia definicję rosyjską – wszechstronną i nieograniczoną do czasu wojny – od zachodniej – ograniczonych, taktycznych operacji informacyjnych prowadzonych podczas działań wojennych”⁹¹⁴. Dalej pisał, że „w niektórych zachodnich definicjach wojskowych istnieje ryzyko, że będą one ograniczone do oszustwa, polegającego na dostarczeniu dowódcy wojskowemu przeciwnika fałszywych informacji operacyjnych, na których może oprzeć swoją decyzję. Zamiast tego rosyjskie podmioty państwowe i niepaństwowe wykorzystują historię, kulturę, język, nacjonalizm i inne czynniki, aby prowadzić wzmocnione cybernetycznie kampanie dezinformacyjne o znacznie szerszych celach”⁹¹⁵. Ponadto, terminologia rosyjska zamiast pojęcia *cyberprzestrzeń* odwołuje się do pojęcia *przestrzeni informacyjnej*. Tym samym obejmuje zjawiskiem wojny informacyjnej nie tylko komputerowe przetwarzanie informacji (na przykład cyberataki), ale również ludzi, przez co należy rozumieć sferę psychologiczną człowieka. Dokonując analizy powyższych rozważań można zauważyć, że rosyjskie wojny informacyjne, w zależności od celu działania, składają się z dwóch rodzajów. Pierwszy to wojna informacyjno-psychologiczna prowadzona stale wobec ludności i sił zbrojnych, drugi z kolei to wojna informacyjno-technologiczna prowadzona w czasie wojny (konfliktu zbrojnego) oraz przeciwko systemom przetwarzającym informacje⁹¹⁶. R. Bebbler natomiast sprowadził prowadzone przez Kreml

⁹¹² P. Antonovich: *Cyberwarfare: Nature and Content*. „Military Thought” 2011, Vol. 20, No. 3, s. 35-43.

⁹¹³ M. Banasik: *Teoria i praktyka wojny informacyjnej...*, s. 58.

⁹¹⁴ K. Giles: *The Next Phase of Russian Information Warfare*. NATO Strategic Communications Centre of Excellence. Riga 2016, s. 2. Tłumaczenie własne. Tekst w oryginale: „The entry for ‘Information war’ (*informatsionnaya voyna*) in a glossary of key information security terms produced by the Military Academy of the General Staff makes a clear distinction between the Russian definition - all-encompassing, and not limited to wartime - and the Western one - limited, tactical information operations carried out during hostilities”.

⁹¹⁵ Ibidem, s. 2. Tłumaczenie własne. Tekst w oryginale: „In some Western military definitions, these risk being effectively limited to deception, providing an adversary military commander with false operational information on which to base his decision.⁴ But the Russian approach is much broader than simply sowing lies and denial, for instance maintaining that Russian troops and equipment are not where they plainly are. Instead, Russian state and non-state actors have exploited history, culture, language, nationalism and more to carry out cyber-enhanced disinformation campaigns with much wider objectives”.

⁹¹⁶ K. Giles, A. Seaboyer: *The Russian Information Warfare Construct...*, s. 9.

operacje w cyberprzestrzeni do trzech elementów takich jak „ukierunkowanie na ludność danego kraju przy użyciu dyplomatów, wynajętych „ekspertów” i naukowców, aby wpływać na postrzeganie i opinie; wykorzystanie operacji informacyjnych, aby kontrolować przekaz; oraz ofensywne operacje cybernetyczne przeciwko komputerom i systemom komunikacyjnym”⁹¹⁷. Ponadto poczynił niezwykle ważne stwierdzenie zauważając, że Rosjanie wykorzystują informacje do „dezorientacji, paraliżu i przewrotu, w przeciwieństwie do amerykańskiego/zachodniego modelu, który wykorzystuje informacje do przekonywania”⁹¹⁸. Powyższe spostrzeżenia w sposób zupełny oddają charakter rosyjskiej wojny informacyjnej, rozumianej zarówno jako oddziaływanie informacyjne na odbiorców oraz dokonywanie cyberataków.

J. Darczewska z kolei pisząc o terminologii rosyjskiej w zakresie wojen informacyjnych stwierdziła, że „nie mieszczą się one w żadnej z definicji terminów przyjętych na Zachodzie. Terminy ‘wojna cybernetyczna’, ‘wojna informacyjna’, czy ‘wojna sieciowa’ mają w Rosji zdecydowanie odmienny zakres pojęciowy. Tylko nieliczni teoretycy rozróżniają ‘cyberwar’ i ‘netwar’, przeciwstawiając technologiczny i społeczny wymiar wojen IV generacji. Dotyczy to jednak z reguły publikacji omawiających zachodnią literaturę przedmiotu; w zdecydowanej większości rosyjscy autorzy pod pojęciem ‘wojna informacyjna’ rozumieją oddziaływanie na masową świadomość w międzypaństwowej rywalizacji systemów cywilizacyjnych w przestrzeni informacyjnej, wykorzystujące szczególne sposoby kontroli nad zasobami informacyjnymi, a używane w charakterze ‘broni informacyjnej’”⁹¹⁹. Takie rozumienie przez Rosjan wojny informacyjnej nie jest zagadnieniem stosunkowo nowym, choć świat zaczął się nim interesować na szerszą skalę dopiero wobec działań podejmowanych w 2014 roku w wyniku których doszło do aneksji Półwyspu Krymskiego. T. L. Thomas napisał, że „podejście Rosji jest odzwierciedleniem jej dialektycznej logiki i procesów historycznych, które ją ukształtowały, a także odzwierciedleniem jej wysiłków na rzecz dostosowania się do nowego środowiska”⁹²⁰. Wskazywał on również, że w Rosji panowało przekonanie (które występuje również współcześnie), że winną rozpadu ZSRR, komunizmu oraz jednoczącej

⁹¹⁷ R. Bebbler: *Information War and Rethinking Phase 0*. „Journal of Information Warfare” 2016, Vol. 15 (Issue 2), s. 44. Tłumaczenie własne. Tekst w oryginale: „the targeting of the domestic population of a country using diplomats, hired ‘experts’ and academics to influence perceptions and opinions; the use of information operations to control the message; and offensive cyber operations against computers and communication systems”.

⁹¹⁸ Ibidem, s. 44. Tłumaczenie własne. Tekst w oryginale: „confuse, paralyze, and subvert, unlike the American/Western model, which uses information to persuade”.

⁹¹⁹ J. Darczewska: *Anatomia rosyjskiej wojny...*, s. 12.

⁹²⁰ T. L. Thomas: *Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations*. „The Journal of Slavic Military Studies” 1998, Vol. 11, No. 1, s. 57. Tłumaczenie własne. Tekst w oryginale: „Russia's approach is a reflection of its dialectical logic and the historical processes that have shaped it, and a reflection of its efforts to adjust to a new environment”.

państwo ideologii była udana zachodnia kampania oddziaływania informacyjnego, prowadzona w skali globalnej⁹²¹. I to właśnie w tym kontekście należy wyprowadzić wniosek, że tak szerokie rozumienie przez Rosję pojęcia wojny informacyjnej jest spowodowane faktem, iż działania przeciwko ZSRR nie były prowadzone wyłącznie za pośrednictwem środków militarnych, a wręcz przeciwnie, głównie za pośrednictwem środków pozamilitarnych. Dlatego zatem Rosja, identyfikując istniejące uprzednio zagrożenia jak i błędy które zostały popełnione, podejmuje współcześnie działania na tak szeroką skalę, aby nauczona doświadczeniem ich ponownie nie popełnić, a wreszcie uzyskując zdolności defensywne przejść do ofensywy – co można było zaobserwować na przykładzie aneksji Półwyspu Krymskiego.

Sposób prowadzenia przez Kreml wojen informacyjnych wynika również z publikowanych dokumentów rządowych, a do najważniejszych z nich należy zaliczyć Doktrynę bezpieczeństwa informacyjnego Federacji Rosyjskiej w wersji z 2000⁹²² i 2016⁹²³ roku. Opublikowanie pierwszego ze wskazanych dokumentów wiązało się ze zmianami w procesie kształcenia funkcjonariuszy resortowych i pozaresortowych, poprzez uzupełnienie ich szkolenia o teorię prowadzenia walki informacyjnej⁹²⁴. Najważniejsze kwestie poruszone w doktrynie odnoszą się do podkreślenia konieczności udoskonalania technicznego, naukowego, prawnego i organizacyjnego krajowej przestrzeni informacyjnej⁹²⁵. Wskazano, że do największych zagrożeń należą „wpływ, jaki poprzez informację mogą wywierać polityczne, ekonomiczne, wojskowe i informacyjne podmioty zagraniczne na kształtowanie i realizację strategii polityki zagranicznej Federacji Rosyjskiej; dezinformacja szerzona w obcych krajach, dotycząca polityki zagranicznej Federacji Rosyjskiej; pogwałcenie praw rosyjskich obywateli i podmiotów w sferze informacji za granicą”⁹²⁶. Rosja dokonała zatem analizy w zakresie zagrożeń dla jej bezpieczeństwa informacyjnego, ale również w zakresie możliwości jej oddziaływania w globalnej przestrzeni informacyjnej. Tym samym należy uznać, że informacja została włączona przez Rosję do ofensywnego oraz defensywnego katalogu zdolności operacyjnych państwa⁹²⁷. Reasumując powyższe rozważania należy uznać, że Rosja weszła

⁹²¹ Ibidem, s. 57-58.

⁹²² *Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej zatwierdzona 9 września 2000 roku*. Moskwa 2000. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf (dostęp: 24.10.2022).

⁹²³ *Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej zatwierdzona 5 grudnia 2016 roku*. Moskwa 2016. <http://kremlin.ru/acts/bank/41460> (dostęp: 24.10.2022).

⁹²⁴ J. Darczewska: *Anatomia rosyjskiej wojny...*, s. 9-10.

⁹²⁵ Y. Harrel: *Rosyjska cyber-strategia...*, s. 103-114.

⁹²⁶ *Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej zatwierdzona 9 września 2000 roku*. Moskwa 2000. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf (dostęp: 24.10.2022).

⁹²⁷ Ibidem.

w XXI wiek z pełną świadomością co do zagrożeń jak i wyzwań związanych z bezpieczeństwem informacyjnym w wymiarze wewnętrznym jak i zewnętrznym.

Drugi dokument to Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej, opublikowana stosunkowo późno, bo w 2016 roku, a więc 16 lat po swojej poprzedniczce. Zasadnicza różnica przyjętej doktryny polega na tym, iż o ile w dokumencie z 2000 roku wskazywano na wzrost znaczenia roli informacji we współczesnym świecie, tak w dokumencie z 2016 roku mowa jest już o jej postrzeganiu w kategorii integralnej części życia politycznego, społecznego czy ekonomicznego. Dokonano zdefiniowania pojęcia bezpieczeństwa informacji Federacji Rosyjskiej jako stanu „ochrony jednostki, społeczeństwa i państwa przed wewnętrznymi i zewnętrznymi zagrożeniami informacyjnymi, pozwalającego na zapewnienie konstytucyjnych praw i wolności człowieka i obywatela, godnej jakości i poziomu życia obywateli, suwerenności, integralności terytorialnej i zrównoważonego rozwoju społeczno-gospodarczego Federacji Rosyjskiej, jak również obronności i bezpieczeństwa państwa”⁹²⁸. Wymieniono ponadto zagrożenia występujące w przestrzeni informacyjnej, które sprowadzają się do stroniczej oceny rosyjskiej polityki zagranicznej dokonywanej przez media zachodnie oraz dyskryminacji mediów rosyjskich i ich pracowników. Wskazano również na procesy skutkujące negatywnym oddziaływaniem informacyjnym na mieszkańców Rosji (przede wszystkim młodzież) w zakresie degeneracji tożsamości narodowej państwa⁹²⁹. Kreml, mając świadomość co do powyższych faktów, będzie prowadził działania w celu zwiększenia swojej obecności w globalnej przestrzeni medialnej⁹³⁰. Dokument ten, podobnie zresztą jak inne nawiązujące do omawianej problematyki, ma charakter interdyscyplinarny, zakładający prowadzenie kampanii oddziaływania informacyjnego w sferze politycznej, ekonomicznej, militarnej, społecznej, cyberprzestrzeni, wywiadu, dyplomacji, psychologicznej, komunikacyjnej oraz edukacyjnej. Jednocześnie sprowadza się do rywalizacji wartości świata rosyjskiego z zachodnim, który dla Rosji stanowi zagrożenie cywilizacyjne⁹³¹.

Wzrost znaczenia informacji w prowadzonej przez Kreml polityce zagranicznej, jest widoczny nie tylko na podstawie zapisów i zmian w przytoczonych doktrynach, ale również

⁹²⁸ *Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej zatwierdzona 5 grudnia 2016 roku*. Moskwa 2016. <http://kremlin.ru/acts/bank/41460> (dostęp: 24.10.2022). Tłumaczenie własne. Tekst w oryginale w wersji angielskiej: „protection of the individual, society and the State against internal and external information threats, allowing to ensure the constitutional human and civil rights and freedoms, the decent quality and standard of living for citizens, the sovereignty, the territorial integrity and sustainable socioeconomic development of the Russian Federation, as well as defence and security of the State”.

⁹²⁹ K. Savranska: *Problematyka walki informacyjnej w relacjach Rosji z wybranymi państwami europejskimi. Perspektywa medioznawcza*. Gdańsk 2020, s. 72-78.

⁹³⁰ *Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej zatwierdzona 5 grudnia 2016 roku*. Moskwa 2016. <http://kremlin.ru/acts/bank/41460> (dostęp: 24.10.2022).

⁹³¹ M. Banasik: *Teoria i praktyka wojny informacyjnej...*, s. 56.

wobec faktu, że już 5 lat po opublikowaniu dokumentu z 2016 roku został wydany nowy pt. *Podstawy polityki państwowej Federacji Rosyjskiej w dziedzinie międzynarodowego bezpieczeństwa informacyjnego*⁹³². Jego postanowienia zawierają „oficjalne poglądy na istotę międzynarodowego bezpieczeństwa informacyjnego, określają główne zagrożenia dla międzynarodowego bezpieczeństwa informacyjnego, cel, zadania polityki państwowej Federacji Rosyjskiej w dziedzinie międzynarodowego bezpieczeństwa informacyjnego”⁹³³. Pierwszym z wymienionych w dokumencie zagrożeń jest „wykorzystanie technologii informacyjnych i komunikacyjnych w sferze wojskowo-politycznej i innej w celu podważania (naruszania) suwerenności, naruszania integralności terytorialnej państw oraz prowadzenia w globalnej przestrzeni informacyjnej innych działań, które uniemożliwiają utrzymanie międzynarodowego pokoju, bezpieczeństwa i stabilności”⁹³⁴. Jednocześnie w celu przeciwdziałania zagrożeniom postuluje się „rozwój współpracy z państwami zagranicznymi w celu zapobiegania (rozwiązywania) konfliktów międzypaństwowych w globalnej przestrzeni informacyjnej”⁹³⁵. Co ciekawe, działania podejmowane przez Kreml stanowią dokładnie takie samo zagrożenie jakie wskazuje się w omawianym dokumencie, choć oczywiście z perspektywy Rosji prowadzone przez nią kampanie oddziaływania informacyjnego są jedynie odpowiedzią na działalność Zachodu. W tym zakresie dokument powiela postanowienia sformułowane w doktrynie z 2016 roku⁹³⁶. Ponadto w dokumencie z 2021 roku zdefiniowano pojęcie międzynarodowego bezpieczeństwa informacyjnego wskazując, że jest to „stan globalnej przestrzeni informacyjnej, przy którym na podstawie powszechnie uznanych zasad i norm prawa międzynarodowego oraz na zasadzie równoprawnego partnerstwa zapewnione jest utrzymanie międzynarodowego pokoju, bezpieczeństwa i stabilności”⁹³⁷.

Omawiając powyższe kwestie nie sposób nie wspomnieć o wybranych teoretykach rosyjskich wojen informacyjnych do których czołówki z pewnością można zaliczyć I. Panarina, A. Dugina oraz S. Rastorgujewa. Pierwszy z nich, I. Panarin podjął próbę dowiedzenia w swojej pracy pt. „Druga światowa wojna informacyjna – wojna przeciwko Rosji”, że wszystkie tzw. Kolorowe rewolucje czy też Arabska Wiosna były wynikiem prowadzonych przez Zachód

⁹³² *Podstawy polityki państwowej Federacji Rosyjskiej w dziedzinie międzynarodowego bezpieczeństwa informacyjnego zatwierdzone 12 kwietnia 2021 roku*. Moskwa 2021. <http://www.kremlin.ru/acts/bank/46614> (dostęp: 24.10.2022).

⁹³³ Ibidem.

⁹³⁴ Ibidem.

⁹³⁵ Ibidem.

⁹³⁶ *Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej zatwierdzona 5 grudnia 2016 roku*. Moskwa 2016. <http://kremlin.ru/acts/bank/41460> (dostęp: 24.10.2022).

⁹³⁷ *Podstawy polityki państwowej Federacji Rosyjskiej w dziedzinie międzynarodowego bezpieczeństwa informacyjnego zatwierdzone 12 kwietnia 2021 roku*. Moskwa 2021. <http://www.kremlin.ru/acts/bank/46614> (dostęp: 24.10.2022).

kampanii oddziaływania informacyjnego, w ramach których główną rolę odegrały USA. J. Darczeńska przytacza sformułowany przez niego pogląd zgodnie z którym, aby im przeciwdziałać „narodowy system walki informacyjnej, polegający na jawnym i tajnym sterowaniu procesami komunikacyjnymi, musi być adekwatny do współczesnych realiów globalnych. Oparty na najlepszych doświadczeniach ZSRR, winien być wzbogacony o doświadczenia USA i Chin”⁹³⁸. Ponadto I. Panarin stwierdził, że w jego ocenie uzyskiwanie pozytywnych rezultatów w podejmowanych działaniach jest nierozdzielnie związane z koniecznością zaistnienia przewagi w ramach prowadzonych wojen informacyjnych⁹³⁹. Pisał również o globalnej konfrontacji informacyjnej w sferze politycznej, która w jego ocenie obejmuje takie elementy jak: strategiczną analizę polityczną (uzyskanie informacji), wpływ informacji (blokowanie, przetwarzanie, wymiana oraz modyfikowanie informacji) i opór informacyjny (obrona przed wrogimi działaniami)⁹⁴⁰.

Drugi z teoretyków, A. Dugin, wyróżnił koncepcję tzw. *wojny sieciowej*, polegającej na zdobywaniu przewagi w konfrontacji informacyjnej, prowadzonej z innymi państwami w skali globalnej. Aby tego dokonać należy, podobnie jak w czasach ZSRR, podejmować działania o charakterze agitacyjno-propagandowym oraz wywiadowczo-organizacyjnym, przy czym będą one prowadzone przede wszystkim przez podmioty niepaństwowe przy jednoczesnym nieoficjalnym wsparciu ze strony służb specjalnych i administracji rządowej Federacji Rosyjskiej⁹⁴¹. Jak pisze M. Wojnowski, działania te polegają „na tworzeniu, finansowaniu i kierowaniu działalnością różnego rodzaju organizacji i nielegalnych grup opozycyjnych w celu uzyskania wpływu na szerokie sfery działalności politycznej i społecznej w innych państwach. Jest to realizowane m.in. przez jawne lub tajne wykupywanie lokalnych mediów, indoktrynowanie ekspertów, dziennikarzy i przedstawicieli różnych środowisk politycznych, a następnie przekształcanie ich w świadomą lub nieświadomą agenturę wpływu, co odbywa się na prestiżowych konferencjach naukowych”⁹⁴².

Kolejny badacz, S. Rastorgujew⁹⁴³ z Instytutu Problemów Bezpieczeństwa Informacyjnego Uniwersytetu Łomonosowa w Moskwie, dokonał z kolei zrównania kategorii

⁹³⁸ J. Darczeńska: *Anatomia rosyjskiej wojny...*, s. 16.

⁹³⁹ Ibidem, s. 17.

⁹⁴⁰ M. Wrzosek, Sz. Markiewicz, Z. Modrzejewski: *Dominacja informacyjna w wojnie hybrydowej*. W: *Informacyjny wymiar wojny hybrydowej*. Red. M. Wrzosek, Sz. Markiewicz, Z. Modrzejewski. Warszawa 2018, s. 109.

⁹⁴¹ M. Wojnowski: *Koncepcja wojny sieciowej Aleksandra Dugina jako narzędzie realizacji celów geopolitycznych Federacji Rosyjskiej*. „Przegląd Bezpieczeństwa Wewnętrznego” 2017, Vol. 9, s. 30.

⁹⁴² Ibidem, s. 30.

⁹⁴³ Siergiej Rastorgujew – rosyjski pułkownik Federalnej Służby Bezpieczeństwa Federacji Rosyjskiej oraz były zastępca Naczelnika Instytutu Naukowo-badawczego Technologii Informacyjnych Federalnej Służby Bezpieczeństwa Federacji Rosyjskiej.

celów jakie są osiągane przy prowadzeniu wojen informacyjnych z celami osiąganymi podczas innych wojen konwencjonalnych. W jego ocenie wojny toczą się o zasoby państw, podczas gdy wojny informacyjne o zasoby społeczne. Jednocześnie wskazuje, że kluczem do nich są elity oraz media przeciwnika, pośród których konieczne jest posiadanie niezbędnej liczby agentów wpływu, z kolei cała strategia wojny informacyjnej łączy ogromną ilość powiązanych wzajemnie taktycznych operacji informacyjnych⁹⁴⁴. Ta koncepcja wydaje się w sposób pełny oddawać istniejące w rosyjskiej teorii wojen informacyjnych przemieszanie porządku militarnego z pozamilitarnym, co do celów jakie realizują Rosjanie, jak i w zakresie różnic pomiędzy wojną informacyjną a wojną konwencjonalną.

Dlatego też należy ponownie podkreślić, że powyższe okoliczności, jak i przytoczone dotychczas w pracy poglądy oraz stanowiska przesądziły o przyjęciu na gruncie niniejszej rozprawy i zastosowaniu terminu wojna informacyjna, nie natomiast walka informacyjna. Jak już zauważono, wojna informacyjna jest bowiem terminem zdecydowanie szerszym, obejmującym wiele form walki. Ponadto stanowi pojęcie przyjęte i ugruntowane w literaturze specjalistycznej, a co najistotniejsze takim terminem posługują się Rosjanie, nie tylko w publikacjach dotyczących wojny informacyjnej, ale w ogóle w działalności z tym związanej. Biorąc pod uwagę problem badawczy prezentowany w pracy, przyjęcie terminu walka, zamiast wojna, nie oddałoby właściwego oraz całościowego znaczenia omawianych zagadnień. Ma to szczególne znaczenie wobec faktu, że przedmiotem rozprawy są nie tylko działania polegające na oddziaływaniu informacyjnym na odbiorcę, ale również dokonywanie ataków w cyberprzestrzeni⁹⁴⁵.

4.2.2. Wybrane środki prowadzenia wojny informacyjnej w polityce zagranicznej Federacji Rosyjskiej

Federacja Rosyjska w ramach prowadzonych wojen informacyjnych stosuje wiele metod oddziaływania informacyjnego zarówno na kierunku wewnętrznym (w Rosji) jak i zewnętrznym (poza Rosją). Ich rodzaj jest uzależniony przede wszystkim od znaczenia danego państwa w rosyjskiej polityce zagranicznej, ale również od możliwości oddziaływania oraz jego skuteczności przy zastosowaniu konkretnego środka. Niemniej jednak należy mieć na uwadze, że Rosja używa „narzędzi z pogranicza absurdu i nierzeczywistości jako broni w wojnie informacyjnej, prawda jest bez znaczenia. Serwisy informacyjne w Rosji dostarczają

⁹⁴⁴ Z. Modrzejewski: *Dezinformacja w służbie walki informacyjnej...*, s. 106.

⁹⁴⁵ Zobacz szerzej: *Rozdział 2. Wojna informacyjna jako instrument prowadzenia polityki zagranicznej*.

wiadomości, w których granice między faktami a fikcją zostały zupełnie zatarte”⁹⁴⁶. Na potrzeby niniejszej rozprawy zostaną przedstawione wybrane ze środków, ze szczególnym uwzględnieniem tych, które będą przedmiotem badań niniejszej rozprawy. Do najważniejszych z nich (na kierunku zewnętrznym) zaliczono (1) działalność tzw. *farm trolli*, (2) działalność portali informacyjnych oraz (3) cyberataki.

Pierwszym ze środków są tzw. farmy trolli. Rozpoczynając omawianie tego zagadnienia należy wspomnieć o Agencji Badań Internetowych z siedzibą w Sankt Petersburgu. Oficjalnie prywatne przedsiębiorstwo, w rzeczywistości silnie powiązane z rosyjskimi strukturami rządowymi. Jest to podmiot zajmujący się najogólniej rzecz ujmując wywieraniem wpływu w Internecie⁹⁴⁷. Zwane również pod nazwą Trolle z Olgino⁹⁴⁸, powstałe w 2013 roku przedsiębiorstwo założone przez J. Prigożyna, bliskiego współpracownika W. Putina. Działanie Agencji polega na wykorzystywaniu fałszywych kont na portalach społecznościowych, witrynach internetowych oraz forach dyskusyjnych, z kolei jej pracownicy publikują treści (najczęściej komentarze i wpisy) zgodne z aktualną polityką oraz instrukcjami z Kremla⁹⁴⁹. Należy również podkreślić, że rosyjski aparat realizujący zadania z zakresu oddziaływania informacyjnego ma bardzo rozbudowaną strukturę przez co można z całą pewnością wnioskować, że Agencja nie jest jedynym podmiotem, czy też farmą, która rozpowszechnia rosyjską propagandę. *Trolling* w Internecie nie ogranicza się wyłącznie do działań podejmowanych przez osoby fizyczne, ale również do wykorzystania tzw. *botów*. Boty to programy, zautomatyzowane procesy, które przeszukując Internet w sposób automatyczny odpowiadają na dane komentarze czy wiadomości na podstawie wykrytych w nich słów kluczowych⁹⁵⁰. Ich działalność to nie tylko reagowanie na pojawiające się treści, ale również ich automatyczne rozpowszechnianie⁹⁵¹. Ponadto uwzględniając działalność powyższych podmiotów nie można zapominać, że ich celem nie jest jedynie dezinformowanie odbiorcy, ale również jak najszerze rozpowszechnianie sfabrykowanych treści. W związku z tym celem działań rosyjskich jest spowodowanie, aby dany przekaz propagandowy był kolportowany również przez jego odbiorców⁹⁵². M. Seddon opisując jak wygląda dzień pracy rosyjskiego

⁹⁴⁶ Ibidem, s. 109.

⁹⁴⁷ T. Rid: *Wojna informacyjna*. Warszawa 2022, s. 529-547.

⁹⁴⁸ Olgino (wieś) – przedmieście Sankt Petersburga gdzie znajduje się siedziba Agencji Badań Internetowych.

⁹⁴⁹ M. Wojnowski: *Wybory prezydenckie jako narzędzie destabilizacji państw w teorii i praktyce rosyjskich operacji informacyjno-psychologicznych w XX i XXI w.* „Przegląd Bezpieczeństwa Wewnętrznego” 2019, Vol. 21, s. 30.

⁹⁵⁰ K. Giles: *Handbook of Russian Information Warfare. Fellowship Monograph Research Division NATO Defense College*. 2016, Vol. 9, s. 54-60.

⁹⁵¹ CyberDefence24: *Strategia rosyjskich botów w sieci – uderzyć w NATO i Polskę*. <https://cyberdefence24.pl/polityka-i-prawo/strategia-rosyjskich-botow-w-sieciuderzyc-w-nato-i-polske> (dostęp: 22.09.2022).

⁹⁵² K. Giles: *Handbook of Russian Information...*, s. 55-60.

trolla wskazał na przykładzie Agencji Badań Internetowych, że ma on za zadanie opublikowanie co najmniej 50 postów dziennie. Ma również obowiązek prowadzić 6 kont na Facebooku publikując minimum 3 posty dziennie oraz dyskutując na grupach minimum 2 razy dziennie. Według założeń, do końca pierwszego miesiąca pracy zdobędzie on około 500 subskrybentów i będzie otrzymywał około 5 komentarzy dziennie. W odniesieniu do Twittera (od lipca 2023 roku portal funkcjonuje pod nazwą X) pracownicy mają zarządzać 10 kontami, posiadać maksymalnie 2 tysiące odbiorców oraz publikować na nich minimum 50 razy dziennie⁹⁵³. Z kolei M. Mindijarow, który był zatrudniony w jednym z działów Agencji od listopada 2014 roku do lutego 2015 roku pracował w 12-godzinnych zmianach oraz był zobowiązany do napisania 135 komentarzy po 200 znaków każdy w trakcie jednego dnia⁹⁵⁴. Co również istotne, omawiane środki oddziaływania nie były dostępne w czasach ZSRR, podczas gdy współcześnie stanowią niezwykle proste i tanie narzędzie wywierania wpływu, ale przede wszystkim narzędzie o ogromnym zasięgu⁹⁵⁵. W tym kontekście nie ulega wątpliwości, że o ile w czasach ZSRR KGB musiało podjąć szereg licznych i karkołomnych działań by wytworzona propaganda przedostała się do zachodnich mediów, o tyle współcześnie przy użyciu Internetu zdolności rosyjskie w tym zakresie są właściwie niczym nieograniczone⁹⁵⁶. Ponadto, badacze z RAND Corp. zauważyli, że media społecznościowe są świetnym instrumentem do zarządzania zbiorowymi emocjami, z uwagi na możliwość ich kontrolowania za pomocą stosunkowo łatwych i tanich narzędzi⁹⁵⁷. Nie jest możliwe precyzyjne określenie liczby zakładanych kont na portalach społecznościowych przez osoby związane z rosyjskimi służbami, jednakże można wskazać na kilka przykładów w tym zakresie. Po rozpoczęciu rosyjskiej inwazji w Ukrainie Facebook poinformował, że w ciągu 48 godzin zlokalizowano i zlikwidowano sieć składającą się z około 40 kont rozsiewających rosyjską propagandę, które miały łącznie około 5 tysięcy osób obserwujących, a na Instagramie około 500⁹⁵⁸. O ile ilość ta może nie zrobić dużego wrażenia, to pojawienie się po kilku kolejnych miesiącach informacji

⁹⁵³ BuzzFeedNews: *Documents Show How Russia's Troll Army Hit America*. <https://www.buzzfeednews.com/article/maxseddon/documents-show-how-russias-troll-army-hit-america> (dostęp: 25.09.2022).

⁹⁵⁴ T. Rid: *Wojna informacyjna...*, s. 534.

⁹⁵⁵ K. Savranska: *Problematyka walki informacyjnej...*, s. 86.

⁹⁵⁶ M. Weiss, P. Pomerantsev: *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money. A Special Report presented by The Interpreter, a project of the Institute of Modern Russia*. New York 2014, s. 17.

⁹⁵⁷ T. R. Aleksandrowicz: *Zagrożenia dla bezpieczeństwa informacyjnego...*, s. 56.

⁹⁵⁸ NBC News: *Facebook, Twitter remove disinformation accounts targeting Ukrainians*. <https://www.nbcnews.com/tech/internet/facebook-twitter-remove-disinformation-accounts-targeting-ukrainians-rcna17880> (dostęp: 26.09.2022); Twitter, Użytkownik Nathaniel Gleicher, Data opublikowania: 28.02.2022 7:17 AM, <https://twitter.com/ngleicher/status/1498180571809280001?s=20&t=PEa6XUCoSC7L6WlyAtwomQ> (dostęp: 26.09.2022).

o zlikwidowaniu przez Państwową Służbę Bezpieczeństwa Ukrainy farmy *botów* liczącej ponad 1 milion kont oraz grup w sieciach społecznościowych z prawie 400 tysiącami odbiorców, ukazuje skalę i możliwości w zakresie prowadzonych przez Kreml kampanii oddziaływania informacyjnego w Internecie⁹⁵⁹. Należy również podkreślić, że istotną rolę w wykorzystywaniu portali społecznościowych takich jak Facebook, Twitter (od lipca 2023 roku portal funkcjonuje pod nazwą X) czy Instagram odgrywa polityka wewnętrzna wskazanych przedsiębiorstw, stosowane algorytmy oraz możliwość wykupywania reklam z opcją *targetowania* grup odbiorców. Czynniki te nie tylko ułatwiają prowadzenie działań rosyjskiemu aparatowi propagandowemu, ale również wpływają w znacznym stopniu na jego ogromną skuteczność⁹⁶⁰.

Drugim ze środków wartym uwagi jest działalność portali informacyjnych, nie tylko rosyjskojęzycznych, ale również anglojęzycznych czy też portali publikujących w języku państwa, do którego obywateli skierowany jest dany przekaz. Rosja bardzo dobrze rozwinęła swój arsenał medialny, tworząc konglomerat zdolny do prowadzenia kampanii oddziaływania informacyjnego w skali globalnej⁹⁶¹. W tym celu tworzone są duże portale informacyjne jak na przykład RT⁹⁶² lub Sputnik News⁹⁶³ oraz portale mniejsze, które co do zasady kopiuje treści z ich większych odpowiedników oraz publikują je w języku jakim posługuje się odbiorca, do którego skierowany jest dany komunikat⁹⁶⁴. Jako przykład można wskazać na dane opublikowane przez portal NewsGuard, którego pracownicy zidentyfikowali 273 portale szerzące dezinformację na temat agresji Rosji w Ukrainie z czego 131 z nich publikuje w języku angielskim, 43 we francuskim, 22 w niemieckim, 30 we włoskim a 47 w innych językach⁹⁶⁵. Jako inny przykład można przytoczyć dane polskiego portalu OKO.press, który zidentyfikował 43 polskojęzyczne podmioty propagujące rosyjską wersję wspomnianego konfliktu z czego 27

⁹⁵⁹ interfax-UKRAINE: *SBU liquidates million-strong bot farm destabilizing situation in Ukraine on order of political force*. <https://interfax.com.ua/news/general/850029.html> (dostęp: 26.09.2022).

⁹⁶⁰ J. Aro: *Trolle Putina. Prawdziwe historie z frontów rosyjskiej wojny informacyjnej*. Kraków 2020, s. 280.

⁹⁶¹ Zobacz szerzej: K. Kaczmarek: *Rosyjska dezinformacja jako element budowania wpływów w Europie: Analiza i perspektywy*. „Roczniki Nauk Społecznych” 2024, nr 1, Tom 16(52); P. Jeż: *Współczesna aktywność dezinformacyjna Federacji Rosyjskiej i przykłady jej neutralizacji*. „Res Politicæ” 2023, T. 15; P. Kmieciak: *Bezpieczeństwo informacyjne Rzeczypospolitej w dobie fake news – przykłady wykorzystania mediów cyfrowych w szerzeniu dezinformacji*. „Bezpieczeństwo Obronność Socjologia” 2019, nr 11/12.

⁹⁶² RT – działająca od 2005 roku ogólnopolska oraz wielojęzyczna rosyjska telewizja informacyjna, prowadząca również portal informacyjny pod tą samą nazwą (do 2009 roku pod nazwą Russia Today).

⁹⁶³ Sputnik News – rosyjska rządowa agencja informacyjna powstała w 2014 roku, prowadząca wielojęzyczny portal informacyjny, w tym w języku polskim (do 2022 roku).

⁹⁶⁴ Zobacz szerzej: O. Jastrzębska: *Prorosyjskie portale internetowe w Polsce i innych krajach Europy środkowej jako istotny element kształtowania prowadzonej przez Rosję wojny informacyjnej*. „Ante Portas – Studia nad Bezpieczeństwem” 2018, nr 2(11).

⁹⁶⁵ NewsGuard: *Russia-Ukraine Disinformation Tracking Center: 273 Websites Spreading War Disinformation And The Top Myths They Publish*. <https://www.newsguardtech.com/special-reports/russian-disinformation-tracking-center/> (dostęp: 25.09.2022).

to portale informacyjne, 11 blogów oraz 5 niszowych platform społecznościowych i serwisów⁹⁶⁶. Stworzona w ten sposób przez Kreml struktura medialna dowodzi, że jego celem jest dotarcie z rosyjskim punktem widzenia do jak najszerzej grupy odbiorców, co natomiast wynika z oficjalnych dokumentów rządowych⁹⁶⁷. Niewątpliwą konsekwencją istnienia tak dużej liczby portali informacyjnych rozpowszechniających rosyjską propagandę będzie wytworzenie u odbiorców komunikatów przekonania o prawdziwości danego podglądu, w myśl tzw. społecznego dowodu słuszności⁹⁶⁸. Ten sam mechanizm będzie również występował w przypadku działalności internetowych *trolli* oraz *botów* w wyniku multiplikowania przekazów propagandowych.

Trzeci, ostatni z omawianych środków stanowią cyberataki. Choć nie sprowadzają się one bezpośrednio do oddziaływania informacyjnego na odbiorcę, to stanowią ważny element uzupełniający prowadzonych przez Kreml kampanii. Rosja do przeprowadzania cyberataków korzysta przede wszystkim z usług profesjonalnych hakerów, pracujących na rzecz służb specjalnych, takich jak GRU (Główny Zarząd Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej), FSB (Federalnej Służby Bezpieczeństwa Federacji Rosyjskiej) oraz SWR (Służby Wywiadu Zagranicznego Federacji Rosyjskiej). Ich działania są realizowane w zgodzie z prowadzoną przez Kreml polityką zagraniczną oraz na zlecenie organów rządowych. Poza podmiotami państwowymi działają również organizacje cyberprzestępcze wobec których Kreml nie wyciąga konsekwencji, o ile prowadzona przez nie działalność jest skierowana wyłącznie wobec państw zachodnich⁹⁶⁹. Co istotne, Kreml zleca również prowadzenie operacji w cyberprzestrzeni podmiotom zewnętrznym o mniej lub bardziej formalnym charakterze, jak na przykład hakerzy czy aktywiści⁹⁷⁰. W tym kontekście warto wspomnieć o grupach APT, czyli Advanced Persistent Threat. Są to grupy hakerów posiadające dostęp do szeregu zasobów, które umożliwiają przełamanie zabezpieczeń sieci teleinformatycznych, a po włamaniu zrealizowanie zakładanych celów o różnorodnym charakterze⁹⁷¹. Takie podmioty pochodzą

⁹⁶⁶ OKO.press: *43 portale nadają codziennie antyukraińską propagandę po polsku [RAPORT Z SIECI]*. <https://oko.press/antyukrainska-propaganda-po-polsku-raport-z-sieci/> (dostęp: 25.09.2022).

⁹⁶⁷ *Koncepcja polityki zagranicznej Federacji Rosyjskiej zatwierdzona 30 listopada 2016 roku*. Moskwa 2016. <http://static.kremlin.ru/media/acts/files/0001201612010045.pdf> (dostęp: 24.10.2022).

⁹⁶⁸ R. Cialdini: *Wywieranie wpływu na ludzi. Teoria i praktyka*. Sopot 2016, s. 133-184.

⁹⁶⁹ A. Kozłowski: *Działalność Rosji w cyberprzestrzeni zagrożeniem dla bezpieczeństwa państw regionu euroatlantyckiego*. W: *Informacja czynnikiem warunkującym bezpieczeństwo. Kontekst rosyjski*. Red. M. Banasik. Warszawa 2021, s. 99.

⁹⁷⁰ S. Gardocki, H. Worona: *Wykorzystanie przez Rosję cyberprzestrzeni w konfliktach hybrydowych a rosyjska polityka cyberbezpieczeństwa*. „Colloquium Pedagogika – Nauki o Polityce i Administracji” 2020, nr 2(38)/2020, s. 39.

⁹⁷¹ A. Rot, B. Olszewski: *Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection*. „Position papers of the Federated Conference on Computer Science and Information Systems” 2017, Vol. 13, s. 113-117.

z Federacji Rosyjskiej i działają na jej rzecz, niejednokrotnie będąc blisko związanymi z jej służbami specjalnymi. Do najbardziej jaskrawych przykładów można zaliczyć APT-28 (prawdopodobna komórka wywiadu wojskowego GRU), APT-29 (powiązana ze służbami specjalnymi Kremla) oraz SandWorm (jednostka militarna podległa GRU). Grupy te stoją za licznymi cyberatakami na całym świecie, a ich działalności poświęcono wiele opracowań przygotowanych przez instytucje zajmujące się cyberbezpieczeństwem⁹⁷². Cyberataki dokonywane przez Rosję w kontekście wojny informacyjnej powinny być traktowane jako jej element uzupełniający, czy też raczej umożliwiający podejmowane konkretnych działań w przestrzeni informacyjnej oraz ich wzmacnianie. Wskutek ataków Kreml może pozyskiwać informacje służące do przeprowadzania kampanii oddziaływania informacyjnego, wykradać dokumenty w celu ich sfabrykowania, kolportować przekazy propagandowe czy też podejmować działania z zakresu cyberszpiegostwa⁹⁷³.

Jak wspomniano na wstępie powyższy katalog środków prowadzenia przez Kreml wojny informacyjnej nie ma charakteru enumeratywnego. Niemniej jednak te wymienione powyżej są nie tylko najczęstszym przedmiotem badań, ale również są przez Rosjan najchętniej wykorzystywane. Nie można jednak wykluczyć, że w przyszłości nie rozwiną się nowe środki dotyczące prowadzenia przez Kreml kampanii z zakresu oddziaływania informacyjnego w globalnej przestrzeni informacyjnej, zarówno w wymiarze propagandowym jak również w wymiarze dokonywanych cyberataków.

4.3. Wybrane przykłady wojny informacyjnej w polityce zagranicznej Federacji Rosyjskiej

Jak już zostało uprzednio wskazane, wojny informacyjne prowadzone przez Rosję nie stanowią jedynie hipotetycznego zagrożenia. Kreml od wielu lat prowadzi zaplanowane oraz zmasowane kampanie oddziaływania informacyjnego, choć w zakresie ich świadomości swego rodzaju przełom nastąpił dopiero w 2014 roku, kiedy to podczas aneksji Półwyspu Krymskiego działania podejmowane przez Rosję doprowadziły do całkowitego paraliżu społeczności międzynarodowej, która nie była w stanie podjąć działań zmierzających do skutecznego powstrzymania Federacji Rosyjskiej. W niniejszym podrozdziale zostaną omówione wybrane

⁹⁷² Zobacz szerzej: 6.2. *Charakterystyka, przebieg i implikacje rosyjskich ataków teleinformatycznych wobec Polski w cyberprzestrzeni w latach 2010-2022.*

⁹⁷³ P. Brangetto, M. A. Veenendaal: *Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations*. 8th International Conference on Cyber Conflict Cyber Power 2016, s. 121-126.

(najbardziej znane) przykłady prowadzonych przez Federację wojen informacyjnych w Estonii, Gruzji, USA oraz Ukrainie.

Pierwszym przykładem rosyjskiej działalności w cyberprzestrzeni o jakim należy wspomnieć jest operacja nazwana Moonlight Maze. Choć nadal występują liczne rozbieżności co do miejsca pochodzenia powyższego cyberataku, to jednak większość znanych śladów prowadzi do Rosji. Operacja została przeprowadzona na bardzo szeroką skalę, a jej celami były między innymi takie instytucje jak NASA, Pentagon, podmioty świadczące usługi dla wojska, naukowcy oraz szereg amerykańskich agencji rządowych. Cyberataki były przeprowadzane przy wykorzystaniu tzw. tylnych drzwi (ang. *backdoor*), dzięki czemu atakujący zyskiwali możliwość w zasadzie nieograniczonej penetracji systemów informatycznych, co przy uwzględnieniu faktu, że ich administratorzy nie przykładali należytej wagi do wykrywania potencjalnych luk bezpieczeństwa, doprowadziło do kradzieży ogromnej ilości danych. Moonlight Maze była pierwszą operacją cyberszpiegowską na świecie, która wywarła ogromny wpływ na zwiększenie świadomości w zakresie zagrożeń w cyberprzestrzeni⁹⁷⁴.

Warto również wspomnieć o szeroko rozpowszechnionym przykładzie dokonanych cyberataków w Estonii w 2007 roku (określonych mianem pierwszej cyberwojny), których autorami byli hakerzy powiązani z rosyjskim rządem. Cyberataki dokonane w Estonii były poprzedzone sporem jaki wystąpił pomiędzy rządem w Tallinie a rosyjską mniejszością, którego przedmiotem były plany usunięcia radzieckiego pomnika z centrum stolicy. Estonia, będąc jednym z najbardziej z informatyzowanych państw na świecie, stała się również podatna na szereg cyberzagrożeń. Dokonane cyberataki zostały wymierzone zarówno w sektor publiczny jak i prywatny, a ich celem były strony rządowe oraz banki. Wskutek tego przez bardzo długi czas cyberprzestrzeń państwa pozostawała w znacznym stopniu sparaliżowana, a instytucje rządowe nie były w stanie opanować zaistniałej sytuacji. Zmasowane rosyjskie cyberataki były dokonywane z wykorzystaniem ataków typu DDoS i SQL injection oraz sieci botnet.⁹⁷⁵

Następnym przykładem jest rosyjska wojna informacyjna w Gruzji, będąca bezpośrednio związana z gruzińsko-rosyjskim konfliktem zbrojnym z 2008 roku. Operacje rosyjskie były prowadzone przede wszystkim w cyberprzestrzeni i rozpoczęły się już kilka tygodni przed rozpoczęciem faktycznych działań zbrojnych. Jak pisze M. Lakomy, podczas

⁹⁷⁴ J. A. Guerrero-Saade, C. Raiu, D. Moore, T. Rid: *Penquin's Moonlit Maze. The Dawn of Nation-State Digital Espionage*. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180251/Penquins_Moonlit_Maze_PDF_eng.pdf (dostęp: 23.10.2022).

⁹⁷⁵ M. Lakomy: *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*. Katowice 2015, s. 184-202.

jednego z pierwszych ataków zablokowana została strona internetowa prezydenta Gruzji Michała Saakaszwilego. Następnie dokonano ataku na strony internetowe agencji informacyjnej OS-Inform oraz OSRadio. W wyniku tych działań treści zamieszczone na tych portalach zostały zastąpione przez materiały skierowane do Osetyńczyków (wobec których Gruzja prowadziła działania zbrojne), a więc materiały zgodne z narracją Kremla. W momencie wybuchu faktycznego konfliktu zbrojnego doszło do zmasowanego cyberataku, w wyniku którego 54 witryny należące zarówno do podmiotów rządowych jak i prywatnych zostały zmodyfikowane w taki sposób, aby rozpowszechniać treści spójne z rosyjskimi działaniami propagandowymi⁹⁷⁶. Powyższe działania dowodzą przede wszystkim zorganizowania, masowości oraz celowości rosyjskich kampanii informacyjnych, a także roli, jaką pełnią one przed rozpoczęciem oraz w trakcie konfliktu zbrojnego. Należy również zauważyć, że wystąpiło wzajemne uzupełnianie w zakresie dokonywanych cyberataków z kampaniami propagandowymi. Pomimo zakończenia konfliktu, Kreml nadal prowadzi kampanie oddziaływania informacyjnych w Gruzji. Prowadzony w ramach Unii Europejskiej program do walki z dezinformacją EUvsDisinfo wykrył ponad 300 przypadków rosyjskich aktywności dezinformacyjnych. Polegały one głównie na rozprzestrzenianiu przez media rosyjskie informacji kwestionujących: demokratyczność Gruzji, jej integralność terytorialną, czy sens proeuropejskiej oraz pronatowskiej polityki. Warto zaznaczyć, że aktywności te stanowiły około 5% wszystkich działań, które zostały zidentyfikowane w 2015 roku w ramach funkcjonowania programu⁹⁷⁷.

Kolejnym, dobrze udokumentowanym przypadkiem rosyjskiej wojny informacyjnej jest trwający od 2014 roku konflikt we wschodniej Ukrainie. Należy podkreślić, że dopiero wydarzenia związane z aneksją Półwyspu Krymskiego uwidoczniły siłę oraz znaczenie rosyjskiej wojny informacyjnej w prowadzonej przez to państwo polityce zagranicznej⁹⁷⁸. Wszelkiego rodzaju działania dezinformacyjne towarzyszyły działaniom bojowym od samego początku konfliktu⁹⁷⁹. Kampania informacyjna prowadzona przez rosyjskie służby specjalne, polityków, dyplomatów, ale przede wszystkim media, uzasadniająca aneksję Półwyspu

⁹⁷⁶ Ibidem, s. 211-228.

⁹⁷⁷ Cyberdefence24.pl: *Zachód produkuje broń biologiczną w Gruzji? Dezinformacyjne macki Kremla dosięgają Kaukazu*. <https://cyberdefence24.pl/bezpieczenstwo-informacyjne/zachod-produkuje-bron-biologiczna-w-gruzji-dezinformacyjne-macki-kremla-dosiegaja-kaukazu> (dostęp: 27.09.2022); Zobacz szerzej: A. Legucka: *Walka z rosyjską dezinformacją w Unii Europejskiej*. „Biuletyn Polskiego Instytutu Spraw Międzynarodowych” 2019, nr 111 (1859). <https://pism.pl/upload/images/artykuly/0414d618-2799-421d-8510-b1130a66303e/1570904090174.pdf> (dostęp: 11.03.2024).

⁹⁷⁸ J. Kowalewski, M. Kowalewski: *Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm*. Warszawa 2017, s. 131-136.

⁹⁷⁹ Z. Modrzejewski: *Dezinformacja w służbie walki informacyjnej...*, s. 110.

Krymskiego oraz wsparcie separatystów we wschodniej Ukrainie skutkowało całkowitym paraliżem społeczności międzynarodowej, która poza sankcjami nałożonymi na Rosję, nie była w stanie podjąć innych kroków w celu neutralizacji powstałego zagrożenia. B. Pacek wskazał wręcz, że „nigdy dotąd nie było tak trudno sprecyzować, kto jest właściwym przeciwnikiem prowadzonych działań”⁹⁸⁰. Podejmowane w jej trakcie działania uzasadniano przede wszystkim ochroną ludności rosyjskiej na terytorium Ukrainy, niestabilnością rządów w Kijowie oraz wrogim działaniem względem Rosji⁹⁸¹. Polska wspierała działania podejmowane przez rząd ukraiński w walce z prorosyjskimi separatystami oraz sprzeciwiała się aneksji Krymu. W wyniku tego Rosja rozpoczęła prowadzenie działań mających na celu podważenie stosunków polsko-ukraińskich, nie tylko w wymiarze politycznym, ale i społecznym⁹⁸². Przykładem może być 2018 rok, kiedy na antenie telewizji Rossija 1 wyemitowano program, w trakcie którego rozważano w jaki sposób można podzielić Ukrainę pomiędzy Polskę i Rosję. Taka narracja była również powielana i lobbowana przez przedstawicieli do Dumy Państwowej Federacji Rosyjskiej⁹⁸³. W 2022 roku rosyjskiej inwazji w Ukrainie towarzyszyły w niespotykanej dotąd skali zmasowane kampanie, których celem było i jest usprawiedliwienie rosyjskiego ataku oraz udowodnienie, że Rosja została do niego zmuszona w wyniku wrogich działań podejmowanych przez Zachód, w szczególności członków NATO, z kolei celem Kremla jest jedynie oswobodzenie Ukrainy spod panowania pronazistowskiego rządu⁹⁸⁴. Narracje rosyjskie zakładają, że Ukraina sama w sobie nie jest antyrosyjska, jednakże stała się taka w wyniku działań podejmowanych przez Zachód (w tym Polskę)⁹⁸⁵.

Kolejnym z przykładów jest ingerencja w wybory prezydenckie w USA z 2016 roku. Przypadek ten jest o tyle istotny, że rosyjskie działania nie były podejmowane względem stosunkowo marginalnego państwa na arenie międzynarodowej, jak np. Gruzja czy Ukraina, w dodatku państwa leżącego w byłej strefie wpływów Związku Radzieckiego, lecz w stosunku do niekwestionowanego światowego mocarstwa, z którym rywalizowała w okresie zimnowojennym. Co więcej, działania te miały na celu ingerencję w wynik wyborów prezydenckich, czyli na wybór osoby mającej realny oraz bezpośredni wpływ na prowadzoną

⁹⁸⁰ B. Pacek: *Wojna hybrydowa na Ukrainie*. Warszawa 2018, s. 229.

⁹⁸¹ J. Darczewska: *Anatomia rosyjskiej wojny...*, s. 5-6.

⁹⁸² T. R. Aleksandrowicz: *Podstawy walki informacyjnej...*, s. 138-139.

⁹⁸³ Rzeczpospolita: *Telewizja Rossija 1, Polsko-rosyjski rozbiór Ukrainy*. <https://www.rp.pl/Konflikt-na-Ukrainie/181009974-Telewizja-Rossija-1-Polsko-rosyjski-rozbiór-Ukrainy.html> (dostęp: 27.09.2022).

⁹⁸⁴ Ośrodek Studiów Wschodnich: *Propaganda masowego rażenia. Rosyjska telewizja w obliczu wojny*. <https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2022-05-06/propaganda-masowego-razenia-rosyjska-telewizja-w-obliczu-wojny> (dostęp: 27.09.2022).

⁹⁸⁵ Ośrodek Studiów Wschodnich: *Putin: Ukraińcy to Rosjanie, Ukraina to „anty-Rosja”*. <https://www.osw.waw.pl/pl/publikacje/analizy/2021-07-13/putin-ukraincy-to-rosjanie-ukraina-to-anty-rosja> (dostęp: 27.09.2022).

przez USA politykę zagraniczną. Zgodnie z opublikowanym ponad 1300-stronicowym raportem przez Senacką Komisję ds. Wywiadu, ingerencja Kremla była ukierunkowana na wspieranie D. Trumpa, a podejmowane działania miały miejsce już w 2014 roku⁹⁸⁶. Wskazano, że Rosjanie mogli wykrywać luki w amerykańskich systemach głosowania celem ich późniejszego wykorzystania oraz podważenia zaufania społeczeństwa do amerykańskiego systemu wyborczego⁹⁸⁷. Podstawą działań Kremla były zaplanowane, długofalowe kampanie oddziaływania informacyjnego, których celem było nie tylko osłabienie amerykańskiego ustroju demokratycznego, ale przede wszystkim Jak pisze M. Wojnowski, „zdestabilizowanie kraju przez wywołanie gwałtownych starć na tle rasowym, etnicznym, religijnym i narodowościowym, a w konsekwencji – doprowadzenie do chaosu i osłabienia międzynarodowej pozycji Stanów Zjednoczonych”⁹⁸⁸. Rosja wykorzystała luki w amerykańskim systemie cyberbezpieczeństwa przeprowadzając ataki na poziomie stanowym oraz lokalnym, co utrudniło zidentyfikowanie zagrożenia przez podmioty federalne, a w konsekwencji ich skuteczne zneutralizowanie. Autorzy raportu wskazują ponadto, że to W. Putin zlecił włamanie się na skrzynki pocztowe osób powiązanych z ówczesną kandydatką na urząd prezydenta, H. Clinton, oraz z Partią Demokratyczną. Istotnym wnioskiem jest stwierdzenie, że jedną z głównych ról w operacjach prowadzonych przez Rosję odegrała działalność portalu WikiLeaks, jak również co szokujące, że osoby pracujące dla tej organizacji zdawały sobie sprawę, iż wspierają w rzeczywistości rosyjski wywiad. Co jednak najważniejsze, dokument podkreśla, że działania Federacji Rosyjskiej były od samego początku trwale ukierunkowane na faworyzowanie (wspieranie) kandydatury D. Trumpa, co w konsekwencji pomogło mu wygrać wybory prezydenckie⁹⁸⁹. W kontekście ingerencji w proces wyborczy badacze wyróżnili cztery podstawowe obszary oddziaływania (wpływu) zaliczając do nich: „kradzież informacji; selektywny przekaz informacji; stosowanie propagandy i dezinformacji; wyprowadzanie z użytku systemu głosowania w całym kraju”⁹⁹⁰.

⁹⁸⁶ Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1: *Russian Efforts Against Election Infrastructure with Additional Views*. <https://www.hsdl.org/?abstract&did=830205> (dostęp: 28.09.2022).

⁹⁸⁷ M. A. Piotrowski: *Amerykańskie oceny dotyczące ingerencji Rosji w przebieg wyborów prezydenckich w USA*. „Biuletyn Polskiego Instytutu Spraw Międzynarodowych” 2017, nr 8 (1450) <https://pism.pl/upload/images/artykuly/legacy/files/22768.pdf> (dostęp: 28.09.2022).

⁹⁸⁸ M. Wojnowski, *Wybory prezydenckie jako narzędzie...*, s. 36.

⁹⁸⁹ Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1: *Russian Efforts Against Election Infrastructure with Additional Views*. <https://www.hsdl.org/?abstract&did=830205> (dostęp: 28.09.2022).

⁹⁹⁰ A. Kruglashov, S. Shvydiuk: *Hybrydowe zagrożenia dla demokracji. Wybrane przykłady zewnętrznej ingerencji Rosji w wybory*. „Wschód Europy” 2020, Vol. 6, No. 2/2020, s. 83; Zobacz szerzej: J. van de Velde: *The Dangers of Forceful Countermeasures as a Response to Cyber Election Interference*. https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3719850_code2431285.pdf?abstractid=3043828&mirid=1 (dostęp: 03.03.2023).

Ponadto w ramach tych wydarzeń można było zaobserwować skoordynowaną kampanię w mediach społecznościowych, które stały się dla Rosjan między innymi narzędziem do publikacji *fake news*, dezinformacji oraz podważania wiarygodności amerykańskiego rządu. Ponadto w odniesieniu do działalności w cyberprzestrzeni w zakresie dokonywanych cyberataków widoczna była znacząca aktywność ze strony grup APT-28 i APT-29, które dokonywały kradzieży dokumentów Partii Demokratycznej⁹⁹¹. Powyższe w sposób niezwykle widoczny wskazuje na schemat działania Kremla, zakładający prowadzenie kampanii oddziaływania Informacyjnego na odbiorców w Internecie z jednoczesnym dokonywaniem cyberataków, przy czym działania te są wobec siebie komplementarne. Wojna informacyjna została więc ujęta przez Rosjan w sposób kompleksowy, wychodzący zdecydowanie poza przestrzeń walki informacyjnej – stąd też na gruncie niniejszej rozprawy autor posługuje się tym pojęciem. Odnotować należy, że z końcem 2022 roku J. Prigożyn (biznesmen powiązany z Kremlem oraz grupą Wagnera, właściciel fabryki *trolli*) zapytany o komentarza na temat ingerencji Moskwy w wybory parlamentarne w USA, które odbyły się w tym samym roku odpowiedział, że Rosja ingerowała, ingeruje oraz nadal będzie ingerować. Zaznaczył, że będzie to następować ostrożnie, dokładnie, chirurgicznie oraz po swojemu, tak jak Rosjanie potrafią to robić⁹⁹². Co jednak niezwykle ważne, Rosyjska ingerencja w wybory prezydenckie w USA w 2016 roku nie może być sprowadzana wyłącznie do sprzyjania jednej bądź drugiej stronie, ale do rozważań jak bardzo wpłynęła na ostateczny wynik wyborów. Tym samym należy zauważyć, że przeprowadzone rosyjskie kampanie oddziaływania informacyjnego istotnie wpłynęły na proces wyborczy największego mocarstwa na świecie, co ma niebagatelne znaczenie dla wagi omawianego problemu badawczego.

⁹⁹¹ A. Kruglashov, S. Shvydiuk: *Hybrydowe zagrożenia dla demokracji...*, s. 83.

⁹⁹² Reuters: *Russia's Prigozhin admits interfering in U.S. elections*. <https://www.reuters.com/world/us/russias-prigozhin-admits-interfering-us-elections-2022-11-07/> (dostęp: 03.03.2023); Rzeczpospolita: *Prigożyn przyznaje: Rosja ingerowała w wybory w USA. I będzie ingerować*. <https://www.rp.pl/konflikty-zbrojne/art37367861-prigozyn-przyznaje-rosja-ingerowala-w-wybory-w-usa-i-bedzie-ingerowac> (dostęp: 03.03.2023).

Rozdział 5. Polska w polityce zagranicznej Federacji Rosyjskiej w latach 2010-2022

5.1. Geneza stosunków polsko-radzieckich oraz polsko-rosyjskich

Jak już zostało stwierdzone w poprzednim rozdziale, stosunki Rosji z innymi państwami były determinowane w znacznej mierze jej dziedzictwem imperialnym oraz mocarstwowym. Nie inaczej wyglądało to w przypadku Polski, z którą przez wiele wieków graniczyła Rosja, a następnie w XX wieku Związek Socjalistycznych Republik Radzieckich. Interesy obu państw wielokrotnie się ścierały prowadząc do licznych sporów, konfliktów i wojen, a ich implikacje można obserwować również współcześnie. W związku z tym niezbędne jest zarysowanie genezy stosunków polsko-rosyjskich oraz polsko-radzieckich ze wskazaniem najważniejszych wydarzeń które im towarzyszyły na przestrzeni wieków, tj. początków państwowości (X wiek), wojen o Inflanty (1558-1583), I wojny północnej (1563-1570), wielkiej smuty (1598-1613), powstania B. Chmielnickiego (1648-1654), II wojny północnej (1655-1660), wojny o sukcesję polską (1733-1735), zaborów ziem polskich (1772, 1793, 1795), wojny polsko-bolszewickiej (1919-1921), II wojny światowej (1939-1945) oraz zimnej wojny (1945/1947-1991)⁹⁹³.

Początek historii Rosji to w zasadzie powstanie pierwszych zrębów jej państwowości, czyli Rusi Kijowskiej, co miało miejsce z końcem IX wieku⁹⁹⁴. Kolejny wiek przyniósł natomiast szereg zasadniczych przemian, które miały w przyszłości wpłynąć na rolę oraz kształt państwa we wschodniej części Europy. Zaliczyć do nich należy przede wszystkim powstanie bardziej sformalizowanych struktur państwowych, rozpoczęcie rozległej ekspansji terytorialnej oraz ustanowienie chrześcijaństwa religią państwową⁹⁹⁵. Nie inaczej sytuacja wyglądała na terenach dzisiejszej Polski, gdzie rodząca się monarchia wczesnopiastowska umacniała swoje wpływy i władzę w tej części świata, a momentem szczególnie istotnym było wydarzenie z 966 roku znane jako chrzest Polski⁹⁹⁶. Rodzące się państwo polskie i ruskie (rosyjskie) dzieliły ze sobą wspólną granicę, czego skutkiem były pierwsze zarzewia wzajemnej rywalizacji o terytoria (począwszy od Grodów Czerwieńskich w X i XI wieku). Jak się okazało, spory te miały determinować przyszłe wzajemne relacje sąsiadów przez najbliższe kilka wieków, choć nie cechowały się one w tym czasie szczególną intensywnością⁹⁹⁷.

⁹⁹³ Geneza stosunków polsko-rosyjskich w latach 1992-2009 została omówiona w dalszej części rozdziału.

⁹⁹⁴ L. Bazyłow: *Historia Rosji*. Wrocław 2005, s. 20-22.

⁹⁹⁵ Ibidem, s. 22-29.

⁹⁹⁶ J. Topolski: *Historia Polski*. Wydanie elektroniczne 2015, s. 49-63.

⁹⁹⁷ S. Szczur: *Historia Polski. Średniowiecze*. Kraków 2002, s. 42-43.

Zmiana w powyższym zakresie nastąpiła wraz nadejściem XVI wieku, który zarówno dla Polski (Rzeczypospolitej Obojga Narodów) jak i Rosji (Carstwa Rosyjskiego) był czasem niezwykle ważnym pod względem kształtującej się pozycji tych państw na arenie międzynarodowej. W Polsce rozpoczynał się właśnie okres tzw. złotego wieku, co wiązało się między innymi z zawarciem unii lubelskiej w 1569 roku i skutkowało powstaniem państwa polsko-litewskiego⁹⁹⁸. Nowopowstały twór, czyli Rzeczypospolita Obojga Narodów, stała się jednym z największych państw w Europie pod względem politycznym, militarnym, kulturalnym i gospodarczym⁹⁹⁹. Z kolei w Rosji to moment powstania Carstwa Rosyjskiego na czele którego stanął pierwszy car Iwan IV Groźny, rozpoczynając nie tylko okres moskiewskiego absolutyzmu, ale również wprowadzając państwo na drogę mocarstwową i imperialną¹⁰⁰⁰. XVI a następnie XVII wiek to jednocześnie czas licznych sporów oraz konfliktów pomiędzy wielowiekowymi sąsiadami. Do najważniejszych z nich zaliczamy: wojny o Inflanty (1558-1583), I wojnę północną (1563-1570), wielką smutę (1598-1613), powstanie B. Chmielnickiego (1648-1654), II wojnę północną (1655-1660) oraz wojnę o sukcesję polską (1733-1735).

Pierwsze ze wskazanych wydarzeń było w zasadzie pierwszą serią poważniejszych konfliktów, które przeniosły rywalizację o terytoria z południowej i środkowej części granicy państw na jej północ. W interesie Rosji było zdobycie dostępu do Morza Bałtyckiego¹⁰⁰¹, gdyż posiadany przez nią fragment wybrzeża nie dawał takich możliwości kontaktów z Zachodem, jakich oczekiwał Iwan IV Groźny¹⁰⁰². Pierwsze lata wojny przebiegały pomyślnie dla cara, jednakże z czasem sytuacja uległa zmianie. Działania zbrojne zakończyły się w 1583 roku, a Inflanty przeszły na własność Polski, Szwecji oraz Danii¹⁰⁰³. Nierozwiązane spory, przede wszystkim trwająca w latach 1563-1570 I wojna północna¹⁰⁰⁴, doprowadziły do dalszego antagonizowania stosunków polsko-rosyjskich oraz konfliktów jakie miały wybuchnąć na tych terenach w przyszłości¹⁰⁰⁵.

Czas świetności Rosji został na chwilę przerwany w latach 1598-1613, a więc przez okres, który w historiografii nazywany jest wielką smutą. Śmierć ostatniego cara z dynastii

⁹⁹⁸ Unia realna Korony Królestwa Polskiego i Wielkiego Księstwa Litewskiego, będąca następstwem unii personalnej z 1385 roku.

⁹⁹⁹ J. Topolski: *Historia Polski...*, s. 110-113, 130-135.

¹⁰⁰⁰ L. Bazylow: *Historia Rosji...*, s. 73-82, 86-88.

¹⁰⁰¹ E. Donnert: *Walka Rosji o dostęp do Morza Bałtyckiego w II połowie XVI wieku*. W: *Polityka zagraniczna Rosji i ZSRR*. Red. W. Materski. Łódź 1994, s. 5-9.

¹⁰⁰² L. Bazylow: *Historia Rosji...*, s. 80.

¹⁰⁰³ M. Smoleń: *Historia Rosji*. W: *Rosjoznawstwo. Wprowadzenie do studiów nad Rosją*. Red. L. Suchanek. Kraków 2004, s. 51-52.

¹⁰⁰⁴ M. Markiewicz: *Historia Polski 1492-1795*. Kraków 2002, s. 379-381.

¹⁰⁰⁵ L. Bazylow: *Historia Rosji...*, s. 87-88.

Rurykowiczów oraz występującą w związku z tym słabość wewnętrzną państwa postanowiła wykorzystać Polska. Król Zygmunt III Waza dążąc do podporządkowania Moskwy osadził na kremlowskim tronie swojego syna, Władysława IV Wazę. Ostatecznie do zrealizowania tych planów nie doszło, gdyż warunkiem bojarów rosyjskich na objęcie władzy przez syna polskiego króla było przejście nowego cara na prawosławie, a na co nie zgodził się Zygmunt III Waza¹⁰⁰⁶. W tym czasie magnaci polscy za zgodą króla organizowali również tzw. *dymitriady*, a celem tych wypraw było osadzenie na tronie moskiewskim pretendentów podających się za zaginionego syna cara Iwana IV Groźnego. Finalnie próby podporządkowania Rosji nie przyniosły oczekiwanych rezultatów. Pomimo iż Polacy jako nieliczni w historii zdobyli Moskwę, to ich rządy nie trwały zbyt długo. W 1612 roku polski garnizon Kremla został zmuszony do kapitulacji¹⁰⁰⁷, a dzień ten jest współcześnie świętowany w Rosji 4 listopada jako Dzień Jedności Narodowej. Ostatecznie niepokoje wewnętrzne w państwie jak i okres największych wpływów polskich w Moskwie zakończył się w 1613 roku wyborem na cara Michała I z dynastii Romanowów, która panowała w Rosji do 1917 roku¹⁰⁰⁸.

Kolejnym istotnym wydarzeniem które w znacznym stopniu wpłynęło na późniejsze stosunki polsko-rosyjskie było powstanie w Ukrainie, którego dowodzącym został B. Chmielnicki (1648-1654). Przywódca kozacki wiedząc, że nie ma szans w bezpośrednim starciu z wojskami koronnymi zwrócił się o pomoc do Rosji. Choć początkowo Moskwa nie była zainteresowana propozycjami powstańców, to z czasem wobec ujawnienia się słabości wewnętrznych Polski oraz sukcesów wojsk zaporoskich wmieszała się w wewnętrzny konflikt¹⁰⁰⁹. W 1653 roku Sobór Ziemski w Ukrainie zdecydował o włączeniu do Rosji tych z ziem które znajdowały się pod kontrolą B. Chmielnickiego, z kolei starszyzna kozacka uznała zwierzchność cara. W 1655 roku w Polsce rozpoczął się potop szwedzki (1655-1660), co ostatecznie uniemożliwiło pokonanie powstańców¹⁰¹⁰. Wydarzenia w Ukrainie w znacznym stopniu osłabiły wewnętrznie Rzeczpospolitą Obojga Narodów, a kwestie historyczno-etniczne związane z tym okresem występują w stosunkach polsko-rosyjskich również współcześnie.

Potop szwedzki, funkcjonujący w historiografii również pod nazwą II wojny północnej (1655-1660)¹⁰¹¹, co prawda nie był konfliktem pomiędzy Polską i Rosją, jednakże doprowadził do przemian wewnątrz państwa polskiego, wyczerpania militarnego, politycznego oraz

¹⁰⁰⁶ Ibidem, s. 103-107.

¹⁰⁰⁷ J. Topolski: *Historia Polski...*, s. 149-150; Ibidem, s. 106-107.

¹⁰⁰⁸ M. Markiewicz: *Historia Polski...*, s. 458; L. Bazyłow: *Historia Rosji...*, s. 108-109.

¹⁰⁰⁹ M. Smoleń: *Historia Rosji. W: Rosjoznawstwo. Wprowadzenie do studiów nad Rosją.* Red. L. Suchanek. Kraków 2004, s. 57-58; M. Markiewicz: *Historia Polski...*, s. 515-519.

¹⁰¹⁰ J. Topolski: *Historia Polski...*, s. 180-181; L. Bazyłow: *Historia Rosji...*, s. 120-122.

¹⁰¹¹ L. Bazyłow: *Historia Rosji...*, s. 122.

gospodarczego, a w konsekwencji przyczynił się do osłabienia potęgi państwa w XVIII wieku. Z kolei w carskiej Rosji XVIII wiek to czas panowania cara Piotra I Wielkiego, reformatora oraz twórcy otwartego na Zachód nowoczesnego państwa rosyjskiego¹⁰¹², jak również carycy Katarzyny II, która kontynuowała jego politykę zwiększając zaangażowanie Rosji na arenie międzynarodowej¹⁰¹³. Warto również odnotować, że rok 1721 to przyjęcie przez Piotra I tytułu imperatora, a zawarty w tym samym roku pokój w Nystad zakończył III wojnę północną i ustanowił rosyjską supremację nad wschodnią częścią kontynentu europejskiego. Kreml wyszedł z wojny jako imperium, Rzeczpospolita z kolei jako państwo osłabione oraz skazane na rosnące rosyjskie wpływy w państwie¹⁰¹⁴.

Niezwykłe ważnym, a często pomijanym wydarzeniem w stosunkach polsko-rosyjskich była wojna o sukcesję polską (1733-1735), podczas której o koronę rywalizował Stanisław Leszczyński oraz August III Sas, wspierany przez Rosję¹⁰¹⁵. Wojna zakończyła się zwycięstwem drugiego z nich, a Rzeczpospolita w znacznym stopniu utraciła swoją suwerenność na arenie międzynarodowej. Kreml w coraz większym stopniu ingerował w wewnętrzne sprawy Polski, niezwykle wyniszczonej i osłabionej w drugiej połowie XVIII wieku¹⁰¹⁶. Kolejne lata istnienia Rzeczypospolitej Obojga Narodów to postępujący rozkład państwa spowodowany czynnikami wewnętrznymi¹⁰¹⁷, jak i zewnętrzną ingerencją państw sąsiednich, przede wszystkim Imperium Rosyjskiego. Kulminacyjnym momentem stosunków polsko-rosyjskich był okres rozbiorów (1772, 1793, 1795), kiedy to w wyniku ostatniego z nich Polska przestała istnieć i zniknęła z map świata na 123 lata¹⁰¹⁸. Czas ten to również postępująca rusyfikacja ziem polskich, która doprowadziła do kolejnych wzajemnych antagonizmów w szczególności w warstwie społecznej państwa polskiego.

Odzyskanie przez Polskę niepodległości w 1918 roku nie sprzyjało rozwijaniu przyjaznych stosunków polsko-radzieckich¹⁰¹⁹. Zaszłości historyczne, szczególnie lata

¹⁰¹² N. V. Riasanovsky, M. D. Steinberg: *Historia Rosji*. Kraków 2009, s. 219, 226-249; J. Diec: *Geostrategiczny wybór Rosji u zarania trzeciego tysiąclecia. Tom I Doktryna rosyjskiej polityki zagranicznej. Partnerzy najbliżsi i najdalsi*. Kraków 2015, s. 39-40; S. Bieleń: *Identyfikacja Rosji w stosunkach międzynarodowych*. W: *Polityka zagraniczna Rosji*. Red. S. Bieleń, M. Raś. Warszawa 2008, s. 34-36.

¹⁰¹³ N. V. Riasanovsky, M. D. Steinberg: *Historia Rosji...*, s. 280-282; S. Bieleń: *Tożsamość międzynarodowa Federacji Rosyjskiej*. Warszawa 2006, s. 93.

¹⁰¹⁴ A. Nowak: *Jak rozbić rosyjskie imperium? Idee polskiej polityki wschodniej (1733-1921)*. Kraków 1999, s. 11.

¹⁰¹⁵ J. Topolski: *Historia Polski...*, s. 202-208.

¹⁰¹⁶ M. Markiewicz: *Historia Polski...*, s. 623-629.

¹⁰¹⁷ Do podstawowych czynników wewnętrznych działających destrukcyjnie na Rzeczpospolitą Obojga Narodów należy zaliczyć przede wszystkim słabą władzę elekcyjnego monarchy, słabą armię, jak i dbanie przez magnatów szlacheckich o ich partykularne interesy, stojące często w sprzeczności z interesami państwa.

¹⁰¹⁸ L. Bazyłow: *Historia Rosji...*, s. 169-180; M. Markiewicz: *Historia Polski...*, s. 716-719.

¹⁰¹⁹ W związku z powstaniem w 1917 roku Rosyjskiej Federacyjnej Socjalistycznej Republiki Radzieckiej formalnie należy mówić o stosunkach polsko-radzieckich, nie natomiast o stosunkach polsko-rosyjskich. Trzeba również zauważyć, że od roku 1918 do roku 1922, a więc do czasu utworzenia ZSRR, wszystkie republiki

zaborów, podsycaly napięcia, spory i konflikty w relacjach obu państw. Istotne pozostawały również kwestie przemian w zakresie istniejącego ładu międzynarodowego po I wojnie światowej oraz przejęcie władzy w Rosji przez bolszewików w 1917 roku po obaleniu cara Mikołaja II. Następstwem powyższego było rozpoczęcie trwającej w latach 1919-1921 wojny polsko-bolszewickiej. Kierunek zachodni był dla bolszewików szczególnie istotny, co było związane z planami W. I. Lenina dotyczącymi ekspansji rewolucji robotniczej do innych państw Europy. Pomimo początkowych sukcesów strony polskiej wynikających z przeprowadzenia uderzenia prewencyjnego, bolszewicy stosunkowo szybko odzyskali inicjatywę, której nowopowstałe i słabe państwo polskie nie było w stanie się przeciwstawić. Do decydującego starcia doszło w 1920 roku podczas bitwy warszawskiej podczas której wojsko polskie odrzuciło natarcie wojsk bolszewickich¹⁰²⁰. W 1921 roku zawarto traktat brzeski, który ustanowił granicę w sposób kompromisowy, co miało również na celu ustabilizowanie sytuacji wewnętrznej w obu państwach¹⁰²¹ oraz poprawienie stosunków radzieckich z Zachodem wobec oficjalnie kreowanej w kolejnych latach przez Kreml polityki utrzymywania międzynarodowego pokoju i bezpieczeństwa¹⁰²².

Względna normalizacja stosunków polsko-radzieckich nie trwała jednak długo. Polska znalazła się bowiem w bardzo trudnym położeniu politycznym i geograficznym, z jednej strony pomiędzy Rzeszą Niemiecką (III Rzeszą) A. Hitlera oraz z drugiej strony Związkiem Socjalistycznych Republik Radzieckich¹⁰²³ (ZSRR) J. Stalina. Polityka konfrontacyjna obydwu przywódców stanowiła zagrożenie dla bezpieczeństwa państwa polskiego, a jej kulminacją było podpisanie przez nich w 1939 roku paktu Ribbentrop-Mołotow¹⁰²⁴, którego jednym z tajnych załączników był plan podziału Polski po zbliżającej się wojnie¹⁰²⁵. W tym samym roku rozpoczęła się II wojna światowa (1939-1945) w wyniku której Związek Radziecki dokonał inwazji na terytorium Polski, zajmując jej wschodnią część. Tym samym Polska ponownie

radzieckie prowadziły formalnie samodzielną politykę zagraniczną, co wymagało w tym okresie ich ścisłej współpracy w celu wypracowania wspólnego stanowiska prezentowanego na arenie międzynarodowej. Oczywiście należy podkreślić, że w kształtowaniu i realizacji polityki zagranicznej dominowały organy Federacyjnej Rosyjskiej Socjalistycznej Republiki Radzieckiej. Zobacz szerzej: V. Gonć: *Kwestia koordynacji polityki zagranicznej republik radzieckich w okresie do utworzenia ZSRR*. W: *Polityka zagraniczna Rosji i ZSRR*. Red. W. Materski. Łódź 1994, s. 79-85.

¹⁰²⁰ J. Topolski: *Historia Polski...*, s. 282-295.

¹⁰²¹ L. Bazyłow: *Historia Rosji...*, s. 401-402.

¹⁰²² P. Chmielewski: *Polityka zagraniczna Związku Radzieckiego na rzecz utrzymania pokoju i bezpieczeństwa międzynarodowego do II wojny światowej*. W: *Polityka zagraniczna Rosji i ZSRR*. Red. W. Materski. Łódź 1994, s. 87-97.

¹⁰²³ 30 grudnia 1922 roku powstał Związek Socjalistycznych Republik Radzieckich w skład którego weszła Rosyjska Federacyjna Socjalistyczna Republika Radziecka.

¹⁰²⁴ A. Taras: *Anatomia nienawiści. Stosunki polsko-rosyjskie XVIII-XX w.* Warszawa 2015, s. 596-604.

¹⁰²⁵ J. Topolski: *Historia Polski...*, s. 311-312; L. Bazyłow: *Historia Rosji...*, s. 445.

utraciła niepodległość, a stosunki polsko-radzieckie uległy znacznemu pogorszeniu po względnej normalizacji jaka miała miejsce w 1921 roku. Mimo deklaracji ZSRR o poszanowaniu zasad współistnienia państw o odmiennych systemach społecznych, Kreml nie wyrzekł się wojny jak i możliwości użycia siły, co pokazał rok 1939 i przyłączenie się do agresji niemieckiej na Polskę¹⁰²⁶. J. Stalin mając pewność, iż Zachód nie stanie w obronie Polski, zdecydował się na atak argumentując go bankructwem państwa polskiego oraz rozkładem rządu polskiego¹⁰²⁷, co z kolei miało uzasadniać wygaśnięcie wzajemnych układów o nieagresji¹⁰²⁸. Po ataku III Rzeszy na ZSRR i porażkach na froncie wschodnim doszło do oficjalnej zmiany stanowiska radzieckiego w kwestii polskiej, czego przykładem może być zawarcie układu Sikorski-Majski w 1941 roku. Na jego mocy przywrócono stosunki dyplomatyczne oraz ustalono warunki wspólnej walki przeciwko III Rzeszy¹⁰²⁹. Ponowny kryzys w stosunkach polsko-radzieckich nastąpił w 1943 roku w wyniku ujawnienia przez Niemców zbrodni katyńskiej, za co strona polska obwiniła ZSRR. Dało to J. Stalinowi pretekst do ponownego zerwania stosunków dyplomatycznych z polskim rządem na uchodźctwie i możliwość utworzenia konkurencyjnego Związku Patriotów Polskich, stanowiącego załóżkę nowego proradzieckiego rządu w Polsce¹⁰³⁰. Oczywiście należy zauważyć, że krok ten był możliwy wobec zmian jakie miały miejsce na froncie wschodnim i przejścia Niemców do defensywy. Schyłek II wojny światowej przyniósł ostateczne przesądzenie losów powojennej Polski oraz stosunków polsko-radzieckich. W 1944 roku na ziemiach polskich ogłoszono bowiem Manifest Polskiego Komitetu Wyzwolenia Narodowego, który stał się namiastką nowego prokremlowskiego rządu w Warszawie. Z kolei w 1945 roku powstał Tymczasowy Rząd Jedności Narodowej¹⁰³¹, który został zaaprobowany przez mocarstwa zachodnie podczas konferencji jałtańskiej (1945) wraz z nowymi granicami państwa polskiego narzuconymi przez J. Stalina¹⁰³².

Ostatnim z wydarzeń kształtujących genezę stosunków polsko-rosyjskich był okres zimnej wojny (1945/1947-1991), który zakończył się upadkiem ZSRR oraz powstaniem Federacji Rosyjskiej (1991). Zwycięstwo aliantów podczas II wojny światowej doprowadziło do zmian funkcjonującego na świecie ładu międzynarodowego w ramach którego powstały dwa

¹⁰²⁶ M. Smoleń: *Historia Rosji*. W: *Rosjoznawstwo. Wprowadzenie do studiów nad Rosją*. Red. L. Suchanek. Kraków 2004, s. 82-84.

¹⁰²⁷ A. Taras: *Anatomia nienawiści...*, s. 612-613, 648-650.

¹⁰²⁸ L. Bazyłow: *Historia Rosji...*, s. 445.

¹⁰²⁹ E. Duraczyński: *Układ Sikorski-Majski*. „Dzieje najnowsze” 1987, Rocznik XIX/1987, s. 91-112.

¹⁰³⁰ L. Bazyłow: *Historia Rosji...*, s. 465-466.

¹⁰³¹ A. Taras: *Anatomia nienawiści...*, s. 832-834; J. Topolski: *Historia Polski...*, s. 342-350.

¹⁰³² L. Pastusiak: *Teheran, Jałta, Poczdam: Wielka Trójka o zachodniej granicy Polski*. „Niepodległość i Pamięć” 2017, nr 24/1 (57), s. 79-100; Ibidem, s. 345-347.

nowe mocarstwa dominujące – USA i ZSRR. Europa Wschodnia, w tym Polska, znalazła się pod bezpośrednim wpływem decyzyjnym Kremla, a stan ten trwał do rozpadu Związku Radzieckiego w 1991 roku¹⁰³³. W okresie zimnej wojny dotychczasowi sojusznicy stanęli przeciwko sobie tworząc blok państw zachodnich oraz blok państw wschodnich, z kolei Europę rozdzieliła żelazna kurtyna¹⁰³⁴. Interesy narodowe państw bloku wschodniego zostały podporządkowane Moskwie, a zatem w tym kontekście nie można mówić o równoprawnych stosunkach polsko-radzieckich. Stopniowa odwilż w relacjach obydwu państw nastąpiła dopiero w latach pięćdziesiątych XX wieku co miało swój bezpośredni związek ze śmiercią J. Stalina¹⁰³⁵ jak i dojściem do władzy W. Gomułki. W kolejnych latach stało się możliwe stopniowe ożywienie kontaktów rządu w Warszawie z Zachodem, co jednak nie wiązało się ze zmniejszeniem wpływów ZSRR w Polsce¹⁰³⁶. Ponadto w 1949 roku w ramach grupy państwach socjalistycznych powołano do życia Radę Wzajemnej Pomocy Gospodarczej, która miała być odpowiedzią na niepowodzenia radzieckiego odpowiednika planu Marshalla. Celem organizacji było wzajemne wspieranie w zakresie rozwoju gospodarek centralnie planowanych, wzrostu wydajności pracy czy dobrobytu państw członkowskich. W istocie była ona mechanizmem umożliwiającym sprawowanie większej kontroli przez ZSRR nad gospodarkami państw satelickich oraz wymianę gospodarczą na preferencyjnych dla Kremla warunkach¹⁰³⁷. Z kolei w 1955 roku utworzono Układ Warszawski, czyli organizację polityczno-wojskową, która miała być przeciwwagą dla państw zrzeszonych w ramach NATO. Dowództwo Układu znajdowało się w rękach radzieckich, wobec czego stanowił on narzędzie władzy Kremla nad siłami zbrojnymi państw członkowskich. Postanowienia układu nie tylko umożliwiały stacjonowanie wojsk ZSRR w państwach będących jego stroną, ale również gwarantowały w tym zakresie hegemonię radziecką, zarówno w czasie pokoju jak i ewentualnych działań zbrojnych¹⁰³⁸. W latach osiemdziesiątych XX wieku w Polsce powstała Solidarność, co z kolei przełożyło się na niezadowolenie ze strony radzieckiej i skutkowało wprowadzeniem w stan wojenny, który trwał w latach 1981-1983. W 1985 roku władzę w ZSRR przejął M. Gorbaczow, który rozpoczął okres przemian w Związku Radzieckim nazwany *pierestrojką*. Wprowadzane reformy w państwie nie uchroniły go przed rozpadem, co miało miejsce w 1991

¹⁰³³ S. Weremiuk: *Specyfika stosunków polsko-radzieckich w latach 1944-1991*. „Przegląd Bezpieczeństwa Wewnętrznego” 2014, nr 11/14, s. 43-44.

¹⁰³⁴ J. Krasuski: *Europa Zachodnia po II wojnie światowej: dzieje polityczne*. Poznań 1990, s. 86-89.

¹⁰³⁵ N. V. Riasanovsky, M. D. Steinberg: *Historia Rosji...*, s. 575-578, 590-593.

¹⁰³⁶ J. Topolski: *Historia Polski...*, s. 369-370.

¹⁰³⁷ E. Cziomer: *Przesłanki i istota kształtowania się konfliktu Wschód-Zachód*. W: *Międzynarodowe Stosunki Polityczne*. Red. E. Cziomer. Kraków 2008, s. 140-144.

¹⁰³⁸ R. Bierzanek, J. Symonides: *Prawo Międzynarodowe Publiczne*. Warszawa 2005, s. 324-325.

roku i wymusiło konieczność nowego uregulowania wzajemnych stosunków, jednak nie polsko-radzieckich, a już polsko-rosyjskich¹⁰³⁹.

Reasumując powyższe rozważania można zauważyć, że konflikty i spory w relacjach polsko-rosyjskich, a następnie polsko-radzieckich cechowały się nieustanną rywalizacją, a nie bez znaczenia pozostawał tutaj czynnik geograficzny, gdyż oba państwa przez setki lat dzieliły ze sobą wspólną granicę. Polska i Rosja rywalizowały na wielu płaszczyznach a do najważniejszych należy zaliczyć spory o charakterze politycznym, militarnym, religijnym oraz kulturowym. Wzajemne animozje mają charakter trwały oraz powracają w większym lub mniejszym stopniu wraz ze zmianami pojawiającymi się w prowadzonej przez Kreml i Warszawę polityce zagranicznej.

5.2. Uwarunkowania polityki zagranicznej Federacji Rosyjskiej wobec Polski

W poprzednim rozdziale wskazano oraz scharakteryzowano najważniejsze uwarunkowania polityki zagranicznej Federacji Rosyjskiej. W tej części pracy powyższe zagadnienia zostaną omówione na kanwie stosunków polsko-rosyjskich, ze szczególnym uwzględnieniem polityki zagranicznej Kremla wobec Warszawy. Powyższe kwestie są niezwykle złożone oraz uwarunkowane nie tylko bieżącymi wydarzeniami na arenie międzynarodowej, ale również zaszłościami historycznymi, które występowały pomiędzy wielowiekowymi sąsiadami. Dlatego też zostaną przedstawione, w ocenie autora, najważniejsze z uwarunkowań występujących w relacjach dwustronnych. W związku z tym wyróżniono uwarunkowania wewnętrzne o charakterze obiektywnym takie jak: geografia, demografia, gospodarka, siły zbrojne, ustrój polityczny. Z kolei do uwarunkowań wewnętrznych o charakterze subiektywnym zaliczono: koncepcje polityki zagranicznej Federacji Rosyjskiej wobec Polski, obraz Polski w społeczeństwie Rosyjskim oraz aktywność rosyjskiej służby zagranicznej i dyplomacji w Polsce. Następnie do uwarunkowań zewnętrznych o charakterze obiektywnym zaklasyfikowano: wiążące umowy międzynarodowe zawarte przez Polskę i Rosję oraz członkostwo w najważniejszych organizacjach międzynarodowych. Wreszcie do uwarunkowań zewnętrznych o charakterze subiektywnym zaliczono: koncepcje polityki zagranicznej Polski wobec Rosji, obraz Rosji w polskim społeczeństwie oraz aktywność polskiej służby zagranicznej i dyplomacji w Federacji Rosyjskiej. Jak wspomniano powyższe uwarunkowania nie mają charakteru enumeratywnego

¹⁰³⁹ M. Smoleń: *Historia Rosji. W: Rosjoznawstwo. Wprowadzenie do studiów nad Rosją*. Red. L. Suchanek. Kraków 2004, s. 89-91.

niemniej jednak oddziałują one w największym stopniu na kształtowanie relacji bilateralnych i w związku z tym konieczne jest ich zarysowanie. Należy również nadmienić, że w dalszej części pracy w osobnym podrozdziale zostaną omówione najważniejsze kwestie sporne występujące w stosunkach polsko-rosyjskich w latach 2010-2022, dlatego też w tym miejscu zostaną one pominięte.

5.2.1. Uwarunkowania wewnętrzne polityki zagranicznej Federacji Rosyjskiej wobec Polski

Uwarunkowania wewnętrzne o charakterze obiektywnym polityki zagranicznej Federacji Rosyjskiej zostały omówione w poprzednim podrozdziale, toteż w tej części pracy zostaną one przedstawione wyłącznie na tle porównawczym na kanwie stosunków polsko-rosyjskich w drugiej i na początku trzeciej dekady XXI wieku. Do najważniejszych z uwarunkowań zaliczono przede wszystkim: geografię, demografię, gospodarkę, siły zbrojne oraz ustrój polityczny.

Polska oraz Rosja od kilkuset lat dzielą wspólną granicę, której długość na przestrzeni wieków ulegała wielu zmianom, by ostatecznie wynieść 232 kilometry (granica z Obwodem kaliningradzkim). Pozostaje ona stosunkowo niewielka przy uwzględnieniu, że łączna długość polskich granic wynosi około 3.600 kilometrów¹⁰⁴⁰. Wartości te pozostają jeszcze bardziej niewspółmierne w stosunku do lądowej granicy Federacji Rosyjskiej, która wynosi w przybliżeniu 22.400 kilometrów¹⁰⁴¹, natomiast linia brzegowa państwa liczy około 37.600 kilometrów¹⁰⁴². Już tylko z samych długości granic można wyprowadzić wniosek, że potencjał terytorialny Rosji jest zdecydowanie większy aniżeli Polski. Pierwsze z państw posiada terytorium o wielkości około 17 milionów km²¹⁰⁴³, będąc jednocześnie największe na świecie, z kolei terytorium drugiego z nich to w przybliżeniu 312 tysięcy km² – tym samym Polska

¹⁰⁴⁰ Zgodnie z danymi Polskiej Straży Granicznej długość granicy Polski z Federacją Rosyjską (Obwodem kaliningradzkim) wynosi dokładnie 209,83 kilometra na odcinku lądowym oraz 22,21 kilometra na odcinku rozgraniczającym morza terytorialne obu państw – łącznie 232,04 kilometry. Źródło: Straż Graniczna: *Granice RP*. <https://www.strazgraniczna.pl/pl/granica/granice-rp/1910,Granice-RP.html> (dostęp: 11.12.2022).

¹⁰⁴¹ Central Intelligence Agency: *The World Factbook. Russia. Geography*. <https://www.cia.gov/the-world-factbook/countries/russia/#geography> (dostęp: 11.12.2022).

¹⁰⁴² Ministerstwo Spraw Zagranicznych: *Informator Ekonomiczny. Informacje ogólne*. <https://www.gov.pl/web/rosja/informator-ekonomiczny> (dostęp: 11.12.2022).

¹⁰⁴³ Dokładna powierzchnia Federacji Rosyjskiej wynosi 17.098.242 km², przy czym powierzchnia lądowa to 16.377.742 km², a powierzchnia morza terytorialnego 720.500 km². Źródło: World Atlas. *Maps of Russia*. <https://www.worldatlas.com/maps/russia> (dostęp: 12.12.2022). Na dzień 31 grudnia 2022 roku powierzchnia całkowita Rosji pozostaje kwestią sporną, co wiąże się z uwzględnianiem w jej granicach Półwyspu Krymskiego oraz terenów zajętych we wschodniej Ukrainie.

zajmuje 9. miejsce pod względem wielkości w Europie oraz 69. na świecie. Rosja jest również państwem o bardzo zróżnicowanej rzeźbie terenu oraz klimacie (z uwagi na wielkość zajmowanego terytorium), z kolei Polska to przede wszystkim państwo nizinne w którym występuje klimat umiarkowany.

W przypadku kolejnego z uwarunkowań jakim jest demografia (ludność państwa) nie można już mówić o tak znaczących dysproporcjach. Rosja, pomimo iż jest największym państwem na świecie, nie posiada największej liczby ludności, która oscyluje w jej przypadku na poziomie około 142 milionów¹⁰⁴⁴ obywateli (plasuje ją to na 9. miejscu na świecie)¹⁰⁴⁵. Około $\frac{3}{4}$ całkowitej liczby ludności żyje zarówno w ośrodkach miejskich jak i w zachodniej części państwa, a całkowita gęstość zaludnienia oscyluje na poziomie 8 osób na kilometr kwadratowy. Polskę z kolei zamieszkuje niecałe 38 milionów obywateli¹⁰⁴⁶, a gęstość zaludnienia wynosi 121 osób na kilometr kwadratowy¹⁰⁴⁷. Można zatem zauważyć, że Rosja posiada niecałe 4 razy więcej ludności niż Polska, jednakże biorąc pod uwagę wielkość terytorium, Polskę zamieszkuje ponad 15 razy więcej osób na kilometr kwadratowy. W Polsce, odmiennie niż w Rosji, nie występują tak znacznie mniejszości etniczne i narodowościowe, zatem w tym kontekście państwo można określić jako jednolite¹⁰⁴⁸. W odniesieniu do przyrostu naturalnego należy wskazać, że oba państwa w ujęciu rocznej zmiany odnotowują wartości ujemne na poziomie -0,4%¹⁰⁴⁹.

Pod względem gospodarczym Polska i Rosja różnią się od siebie w dość znacznym stopniu. Pomimo iż oba państwa przeszły podobny proces transformacji (tzw. terapii szokowej) z gospodarki socjalistycznej (centralnie planowanej) do gospodarki kapitalistycznej, to tylko w przypadku pierwszego z nich wystąpiły zamierzone efekty¹⁰⁵⁰. W Rosji roczne PKB wynosi około 1,8 biliona dolarów (2021) i na przestrzeni lat 2010-2022 ulegało znacznym zmianom,

¹⁰⁴⁴ Z kolei według Międzynarodowego Funduszu Walutowego Federację Rosyjską zamieszkiwało w 2021 roku około 145 milionów osób a według prognoz liczba ta ulegnie zmniejszeniu do około 144 milionów w 2027 roku. Źródło: International Monetary Fund: *World Economic Outlook Database, April 2022 Edition*. <https://www.imf.org/en/Publications/WEO/weo-database/2022/April> (dostęp: 12.12.2022).

¹⁰⁴⁵ Central Intelligence Agency: *The World Factbook. Russia. People and Society*. <https://www.cia.gov/the-world-factbook/countries/russia/#people-and-society> (dostęp: 12.12.2022).

¹⁰⁴⁶ Odnotować należy, że według ostatecznych wyników Narodowego Spisu Powszechnego Ludności i Mieszkań z 2021 roku „liczba ludności rezydującej w Polsce liczyła 37 019 327 osób i w porównaniu z wynikami spisu z 2011 r. była mniejsza o 2,7%”. Źródło: Główny Urząd Statystyczny: *Ludność rezydująca – dane NSP 2021*. <https://stat.gov.pl/obszary-tematyczne/ludnosc/ludnosc/ludnosc-rezydujaca-dane-nsp-2021,44,1.html> (dostęp: 14.12.2022).

¹⁰⁴⁷ Główny Urząd Statystyczny: *Rocznik Demograficzny 2022*. Warszawa 2022, s. 524.

¹⁰⁴⁸ Według wyników Narodowego Spisu Powszechnego z 2011 roku udział osób deklarujących narodowość wyłącznie polską lub polską i inną wyniósł ponad 97%.

¹⁰⁴⁹ World Bank: *Open Data. Russian Federation*. <https://data.worldbank.org/country/russian-federation>; <https://data.worldbank.org/country/poland> (dostęp: 16.01.2023).

¹⁰⁵⁰ M. Stolarczyk: *Rosja w polityce zagranicznej Polski w latach 1992-2015*. Katowice 2016, s. 57-58.

zarówno tendencjom wzrostowym jak i spadkowym. Tendencje spadkowe wynikały przede wszystkim z wydarzeń o charakterze międzynarodowym, takich jak aneksja Półwyspu Krymskiego, wojna we wschodniej Ukrainie, a wreszcie rozpoczęcie rosyjskiej inwazji w Ukrainie w 2022 roku. Z kolei w Polsce od 2010 roku obserwujemy co do zasady wzrost PKB, które wynosi niecałe 700 miliardów dolarów (2021). Dla porównania PKB Rosji w 2010 roku wynosiło około 1,5 biliona dolarów, z kolei PKB Polski w analogicznym czasie niecałe 0,48 biliona dolarów¹⁰⁵¹. Choć produkt krajowy brutto Federacji Rosyjskiej jest większy, to w ujęciu *per capita* gospodarkę polską należy ocenić jako zdecydowanie silniejszą. W przypadku pierwszego z państw jest to wartość około 12 tysięcy dolarów na osobę¹⁰⁵², z kolei w odniesieniu drugiego z nich prawie 18 tysięcy dolarów¹⁰⁵³.

Nie bez znaczenia pozostaje również dwustronna wymiana handlowa. Rosja na przestrzeni lat 2010-2022 eksportowała do Polski przede wszystkim surowce energetyczne takie jak węgiel, ropa naftowa oraz gaz ziemny. Są to również podstawowe towary sprzedawane przez Kreml za granicę, jak również jedno z najważniejszych źródeł dochodów budżetowych. Polska nie jest głównym rynkiem zbytu dla Rosji, jednakże rynkiem takim pozostaje Unia Europejska, której Polska jest członkiem¹⁰⁵⁴. Nie można jednak nie zauważyć, że Polska przed wstąpieniem do Unii Europejskiej również rozwijała handel zagraniczny z Rosją. Dla przykładu można wskazać, że w 1993 roku wymiana handlowa plasowała się na poziomie rocznym 2 mld dolarów podczas gdy po 15 latach, w 2008 roku już na poziomie prawie 30 mld dolarów, a w 2013 roku wyniosła ponad 36 mld dolarów¹⁰⁵⁵. Z danych rosyjskich wynika natomiast, że w 2020 roku udział Polski w handlu zagranicznym Rosji wynosił 2,8% co oznacza zajęcie 11. miejsca spośród wszystkich jej partnerów handlowych. Ponadto Rosja zajmuje 3. miejsce w imporcie Polski (przede wszystkim surowce energetyczne) po Niemczech i Chinach oraz 7. miejsce w eksporcie (głównie produkty przemysłu maszynowego i chemicznego)¹⁰⁵⁶. Co do salda importu oraz eksportu, w latach 2010-2022 zachodził wyłącznie deficyt po stronie Polski. Wynika to przede wszystkim z braku równowagi pomiędzy polskim importem surowców energetycznych z Rosji i eksportem polskich produktów do Rosji. Szacunkowo można

¹⁰⁵¹ International Monetary Fund: *World Economic Outlook Database*. 2010-2022. <https://www.imf.org/en/Publications/WEO> (dostęp: 18.12.2022).

¹⁰⁵² World Bank: *Open Data. Russian Federation*. <https://data.worldbank.org/country/russian-federation> (dostęp: 16.01.2023).

¹⁰⁵³ World Bank: *Open Data. Poland*. <https://data.worldbank.org/country/poland> (dostęp: 16.01.2023).

¹⁰⁵⁴ Polska Agencja Inwestycji i Handlu: *Rosja. Przewodnik po rynku*. Warszawa 2018, s. 18, 60.

¹⁰⁵⁵ M. Stolarczyk: *Rosja w polityce zagranicznej Polski...*, s. 247.

¹⁰⁵⁶ Oficjalna strona internetowa Ambasady Federacji Rosyjskiej w Polsce: *Rosja-Polska. Współpraca handlowo-gospodarcza*. https://poland.mid.ru/pl/rossiya_polsha/rossijsko_polskie_otnosheniya_i_voprosy_mezhdunarodnoj_bezopasnosti/torgovo_ekonomicheskoe_sotrudnichestvo/ (dostęp: 23.01.2025).

wskazać, że eksport rosyjski do Polski jest ponad dwukrotnie większy od importu z Polski do Rosji¹⁰⁵⁷. Porównując wielkość gospodarki rosyjskiej do gospodarki polskiej można jednak zauważyć, że państwo które jest o około 53 razy mniejsze pod względem powierzchni terytorium oraz posiadające niecałe 4 razy mniej obywateli, wykazuje nominalne PKB na poziomie 0,674 biliona dolarów, czyli o około 2,6 razy mniej niż Federacja Rosyjska¹⁰⁵⁸.

Następnie, przechodząc do omówienia sił zbrojnych posiadanych przez Rosję oraz Polskę, należy zaznaczyć występującą znaczną dysproporcję na korzyść Rosji, gdyż to właśnie ona jako sukcesorka ZSRR przejęła znaczną część jego arsenału militarnego, w tym nuklearnego¹⁰⁵⁹. Rosja posiada armię liczącą około 850 tysięcy żołnierzy w służbie czynnej oraz 200-250 tysięcy żołnierzy Federalnej Gwardii Narodowej. Ponadto we wrześniu 2022 roku w związku z trwającą wojną w Ukrainie powołano do czynnej służby wojskowej 300 tysięcy rezerwistów oraz zaplanowano zwiększenie ogólnej liczby personelu sił zbrojnych o 137 tysięcy¹⁰⁶⁰. Polska¹⁰⁶¹ z kolei posiada Siły Zbrojne liczące 120 tysięcy żołnierzy (aktywnego personelu wojskowego) wchodzących w skład sił lądowych, powietrznych, marynarki wojennej, wojsk specjalnych oraz wojsk obrony terytorialnej¹⁰⁶². Należy jednak zauważyć, że w najbliższych latach planowane jest istotne zwiększenie liczebności sił zbrojnych nawet do 300 tysięcy żołnierzy, co jest spowodowane wojną w Ukrainie. Ponadto wdrażane są programy modernizacyjne armii mające na celu zaopatrzenie jej w nowoczesny zachodni i krajowy sprzęt w miejsce poradzieckiego¹⁰⁶³. Polskie Siły Zbrojne posiadają około 570 czołgów, 490 jednostek artyleryjskich, ponad 2200 transporterów opancerzonych oraz 205 jednostek artylerii raketowej, ponadto 86 jednostek nawodnych różnego rodzaju oraz około 460 statków powietrznych (w tym 91 myśliwców oraz 208 śmigłowców)¹⁰⁶⁴ – łącznie nieco ponad 4.600 sztuk sprzętu. Należy jednak zauważyć, że na skutek trwającego konfliktu rosyjsko-

¹⁰⁵⁷ A. Nowak-Far: *Gospodarka*. W: *Polska i Rosja w zmieniającej się Europie*. Red. K. A. Wojtaszczyk, I. N. Novikova. Warszawa 2022, s. 117-118.

¹⁰⁵⁸ International Monetary Fund: *World Economic Outlook Database. April 2022 Edition*. <https://www.imf.org/en/Publications/WEO/weo-database/2022/April> (dostęp: 17.01.2023).

¹⁰⁵⁹ Stockholm International Peace Research Institute: *SIPRI Yearbook 2022. Armaments, Disarmament and International Security. Summary*. Solna 2022, s. 15.

¹⁰⁶⁰ Central Intelligence Agency: *The World Factbook. Russia. Military and Security*. <https://www.cia.gov/the-world-factbook/countries/russia/#military-and-security> (dostęp: 17.01.2023).

¹⁰⁶¹ W tym miejscu należy zaznaczyć, że omawiany stan Sił Zbrojnych RP, wobec wdrażanych programów zbrojeniowych i modernizacyjnych (od 2022/2023 roku), ulegnie w najbliższych latach znaczącej zmianie.

¹⁰⁶² Central Intelligence Agency: *The World Factbook. Russia. Military and Security*. <https://www.cia.gov/the-world-factbook/countries/russia/#military-and-security> (dostęp: 17.01.2023).

¹⁰⁶³ Ministerstwo Obrony Narodowej: *Wojsko Polskie silne jak nigdy*. <https://www.gov.pl/web/obrona-narodowa/wojsko-polskie-silne-jak-nigdy> (dostęp: 18.01.2023).

¹⁰⁶⁴ GlobalSecurity.org: *Poland Army Equipment*. <https://www.globalsecurity.org/military/world/europe/pl-army-equipment.htm> (dostęp: 17.01.2023); Global Firepower: *2023 Poland Military Strength*. https://www.globalfirepower.com/country-military-strength-detail.php?country_id=poland (dostęp: 17.01.2023)

ukraińskiego, przedstawione dane mogą się znacząco różnić względem stanu faktycznego. Dla porównania, Rosja posiada niecałe 65.000 sztuk różnego rodzaju sprzętu¹⁰⁶⁵. W kontekście wydatków na zbrojenia Kreml przeznaczył na ten cel równowartość 4,1% PKB w 2021 roku, co stanowi kwotę około 66 miliardów dolarów. W przypadku Polski wydatki na zbrojenia wynoszą 2,1% PKB co przekłada się na kwotę wynoszącą niecałe 14 miliardów dolarów¹⁰⁶⁶. Należy jednak zauważyć, że trwająca wojna w Ukrainie spowodowała systematyczny wzrost wydatków na zbrojenia w obu państwach. Dla przykładu, wydatki rosyjskie zwiększyły się w tym zakresie ponad dwukrotnie do kwoty 154 miliardów dolarów¹⁰⁶⁷, z kolei polskie do kwoty 97,4 miliarda złotych (równowartość około 22 miliardów dolarów¹⁰⁶⁸) w 2023 roku, co stanowi 3% PKB¹⁰⁶⁹. Reasumując, można zauważyć znaczącą dysproporcję w zakresie potencjału militarnego na korzyść Rosji i to właściwie co do każdej z przytoczonych wyżej wartości. Nie można jednak nie brać pod uwagę faktu, że Moskwa odziedziczyła swój potencjał militarny po ZSRR, słabości armii Kremla uwidocznionych podczas wojny w Ukrainie oraz faktu, że Polska od 1999 roku pozostaje aktywnym członkiem NATO prowadzącym gruntowny proces modernizacji swoich sił zbrojnych, jak i angażującym się w działania Sojuszu Północnoatlantyckiego.

Wreszcie należy omówić ustrój polityczny na tle porównawczym. Polska w przeciwieństwie do Rosji jest państwem demokratycznym, które zasady demokratycznego państwa prawnego wynikające z ustawy zasadniczej urzeczywistnia w faktycznym jego funkcjonowaniu. Rosyjska demokracja jest bowiem niezwykle słabo rozwinięta, nieustannie ewoluująca oraz o tendencjach wyraźnie autorytarnych. Ustrój polityczny występujący w Polsce to republika parlamentarna z trójpodziałem władzy. Władzę ustawodawczą sprawują Sejm i Senat, z kolei władzę wykonawczą Prezydent Rzeczypospolitej Polskiej i Rada Ministrów, a władzę sądowniczą sądy i trybunały¹⁰⁷⁰. Sejm (izba niższa) i Senat (izba wyższa) wykonują władzę ustawodawczą i zostały umiejscowione w Konstytucji przed pozostałymi organami, co może świadczyć o istotnej roli jaka została im nadana przez prawodawcę. Podobnie zresztą jak w przypadku ustawy zasadniczej obowiązującej w Federacji Rosyjskiej,

¹⁰⁶⁵ Szczegółowy wykaz posiadanego sprzętu oraz ich rodzaj został przedstawiony w poprzednim rozdziale.

¹⁰⁶⁶ Stockholm International Peace Research Institute: *Trends in World Military Expenditure 2021*. Stockholm 2022. https://www.sipri.org/sites/default/files/2022-04/fs_2204_milex_2021_0.pdf (dostęp: 20.01.2023).

¹⁰⁶⁷ TASS: *Russia's national defense budget to total \$154 bln through 2022*. <https://tass.com/defense/1080646> (dostęp: 20.01.2023).

¹⁰⁶⁸ Wartość ustalono w oparciu o kurs dolara amerykańskiego względem złotówki na dzień 31 grudnia 2022 roku.

¹⁰⁶⁹ Defence24: *Budżet MON na 2023 r. uchwalony*. <https://defence24.pl/polityka-obronna/budzet-mon-na-2023-r-uchwalony> (dostęp: 20.01.2023).

¹⁰⁷⁰ *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r.* (Dz.U. 1997 nr 78 poz. 483), art. 10.

z tą różnicą, że miejsce to zajmuje Prezydent Federacji¹⁰⁷¹. W przeciwieństwie do Rosji, zasadniczą część władzy wykonawczej pełni Rada Ministrów której przewodniczy Prezes Rady Ministrów (Premier). Prezydent z kolei jest najwyższym przedstawicielem Rzeczypospolitej Polskiej i gwarantem ciągłości władzy państwowej¹⁰⁷². Odróżnia to sposób wykonywania władzy w Rosji, gdzie można mówić o niezwykle silnej roli prezydenta (system superprezydencki). W odniesieniu do samej struktury państwa należy również zauważyć, że Polska jest państwem jednolitym¹⁰⁷³, podczas gdy Rosja federacyjnym, a więc złożonym z kilkunastu mniejszych podmiotów¹⁰⁷⁴. Co do prowadzonej polityki zagranicznej, w Rosji odpowiada za nią Prezydent Federacji, podczas gdy w Polsce jest to Rada Ministrów pod przewodnictwem Premiera.

Następnie przechodząc do uwarunkowań wewnętrznych o charakterze subiektywnym należy omówić w pierwszej kolejności miejsce Polski w koncepcjach polityki zagranicznej formułowanych przez Kreml. Jak dotąd publikowane przez Moskwę dokumenty nie zawierały bezpośrednich odniesień do Polski, inaczej niż w koncepcjach Warszawy, w których Rosja zajmuje niezwykle ważne miejsce. Polska z pewnością nie należy do priorytetowych kierunków rosyjskiej polityki zagranicznej w skali globalnej, jednakże na pewno ma to miejsce w przypadku tej realizowanej przez Kreml w stosunku do państw Europy Środkowo-Wschodniej. Odniesienia do Polski (jako państwa średniej rangi) można odnaleźć w zasadzie w kontekście jej członkostwa w organizacjach takich jak NATO czy Unia Europejska, nie jest ona natomiast wymieniana wprost, a raczej zaliczana do grupy państw. I w tym kontekście Warszawa z całą pewnością zaczęła odgrywać istotniejszą rolę w rosyjskiej polityce zagranicznej po uzyskaniu członkostwa we wskazanych wyżej organizacjach¹⁰⁷⁵. Analizując rosyjskie założenia można zauważyć pewien stały element, jakim jest postrzeganie USA w roli niezwykle istotnego partnera. Z kolei badając dokumenty wydane od lat dziewięćdziesiątych XX wieku, widać zdecydowane przejście od deklarowanej (i często faktycznej) współpracy z Zachodem do postawy konfrontacyjnej, co wiązało się ze wzrostem rosyjskiego potencjału

¹⁰⁷¹ *Konstytucja Federacji Rosyjskiej przyjęta w ogólnonarodowym referendum w dniu 12 grudnia 1993 roku.* <http://libr.sejm.gov.pl/tek01/txt/konst/rosja.html> (dostęp: 20.01.2023), art. 94 i nast.

¹⁰⁷² *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r.* (Dz.U. 1997 nr 78 poz. 483), art. 126 i nast.

¹⁰⁷³ *Ibidem*, art. 3.

¹⁰⁷⁴ *Konstytucja Federacji Rosyjskiej przyjęta w ogólnonarodowym referendum w dniu 12 grudnia 1993 roku.* <http://libr.sejm.gov.pl/tek01/txt/konst/rosja.html> (dostęp: 20.01.2023), art. 1.

¹⁰⁷⁵ M. Stolarczyk: *Rosja w polityce zagranicznej Polski...*, s. 71; *Koncepcja polityki zagranicznej Federacji Rosyjskiej zatwierdzona 30 listopada 2016 roku.* Moskwa 2016. <http://static.kremlin.ru/media/acts/files/0001201612010045.pdf> (dostęp: 20.01.2023).

i znaczenia na świecie¹⁰⁷⁶. Ostatnią z opublikowanych koncepcji jest jej wersja z 2016 roku oraz aktualizacja z 2021 roku. W szczególności jest tutaj widoczna narastająca krytyka wobec NATO w zakresie ekspansji infrastruktury militarnej Sojuszu, co z kolei przekłada się na zapowiedzi Kremla o konieczności adekwatnej reakcji na takie działania. W kontekście Unii Europejskiej należy zauważyć, że Rosja prowadzi raczej politykę polegającą na pragmatycznym partnerstwie, głównie w zakresie wymiany handlowej¹⁰⁷⁷.

Wreszcie można przejść do kolejnego z uwarunkowań, a mianowicie obrazu Polski i Polaków, jaki występuje w społeczeństwie rosyjskim. W pierwszej kolejności należy zaznaczyć, że na postrzeganie innych narodów (w tym Polaków) przez Rosjan ma wpływ geopolityczne usytuowanie państwa, jako swego rodzaju pomostu cywilizacyjnego łączącego Wschód i Zachód. Po drugie, pośród rosyjskiego społeczeństwa panuje przekonanie o jego wyjątkowości, o pewnej dziejowej misji, czego skutkiem powinno być naśladowanie ich przez inne państwa, przede wszystkim te ze wspólnego kręgu kulturowego¹⁰⁷⁸. W odniesieniu do bezpośredniego postrzegania Polski przez Rosjan trafne spostrzeżenie poczynił M. Stolarczyk który wskazał, że „mając na uwadze fakt, że w ostatnich stuleciach to Polska była przedmiotem ekspansji i agresji ze strony Rosji, a nie odwrotnie, tym samym w postrzeganiu Polaków i Polski przez Rosjan kwestie pamięci historycznej i obciążeń z tym związanych nie odgrywały większego znaczenia, w przeciwieństwie do wpływu pamięci historycznej Polaków na postrzeganie Rosjan i Rosji. Świadomość historyczna Rosjan w relacjach polsko-rosyjskich koncentruje się przede wszystkim na: przekonaniu o braku pamięci i wdzięczności Polaków za wyzwolenie Polski spod okupacji niemieckiej przez Armię Czerwoną; burzeniu pomników ku czci poległych żołnierzy armii radzieckiej; wojnie polsko-bolszewickiej w latach 1919-1920 i zmarłych w polskiej niewoli żołnierzach armii bolszewickiej; dwuletniej okupacji Moskwy przez Polaków w latach 1610-1612”¹⁰⁷⁹. Trzeba również zauważyć, że „Rosjanin nie czuje nienawiści do Polaka za stare ‘grzechy’, za to, co działo się w Moskwie w 1612 lub 1812 r., ale boleśnie dotyczą go niedawne fakty historii, żyjące w pamięci ludzi, przede wszystkim związane z II wojną światową i z wyzwoleniem Polski od faszyzmu. Rani go boleśnie burzenie pomników ku czci bohaterów wojny lub odmowa uznania dnia 9 maja za Dzień

¹⁰⁷⁶ J. Diec: *Geostrategiczny wybór...*, s. 173-185.

¹⁰⁷⁷ *Koncepcja polityki zagranicznej Federacji Rosyjskiej zatwierdzona 30 listopada 2016 roku*. Moskwa 2016. <http://static.kremlin.ru/media/acts/files/0001201612010045.pdf> (dostęp: 20.01.2023); A. M. Dyer: *Zaktualizowane kierunki polityki zagranicznej Rosji*. „Komentarz PISM” 2021, nr 88/2021 <https://pism.pl/webroot/upload/files/Komentarz%20PISM%20nr%2088-2021.pdf> (dostęp: 12.08.2022).

¹⁰⁷⁸ M. Stolarczyk: *Rosja w polityce zagranicznej Polski...*, s. 66-67.

¹⁰⁷⁹ Ibidem, s. 68-69.

Zwycięstwa”¹⁰⁸⁰. Dla zobrazowania powyższych kwestii można posłużyć się badaniem z 2020 roku, które zostało przeprowadzone celem zbadania postrzegania Polski i Polaków przez Rosjan¹⁰⁸¹. Według jego wyników 15% Rosjan wskazało, że rząd w Warszawie ma bardzo dobry i raczej dobry stosunek do Rosji. 30% uznało, że jest on raczej zły a 32%, że bardzo zły (23% badanych nie umiało udzielić odpowiedzi)¹⁰⁸². Z kolei na pytanie o postrzeganie Polski w kontekście jej przyjazności 31% badanych odpowiedziało, że Polska jest państwem przyjaznym, 35% uznało odwrotnie, a 27% udzieliło odpowiedzi neutralnej¹⁰⁸³. Natomiast na pytanie skąd badani czerpią informacje o Polsce wskazali w 62% na telewizję, w 45% na Internet oraz w 13% na rosyjskie książki i filmy o Polsce¹⁰⁸⁴. Jednocześnie 36% Rosjan uważa, że Rosja powinna rozwijać współpracę kulturalną i społeczną z Polską bez ograniczeń, gdyż jest to najlepszy sposób na przedstawienie Polakom rosyjskiej perspektywy, z kolei 35% badanych uznało, że powinna być ona rozwijana, ale w ograniczonym zakresie, gdyż współpraca może być również wykorzystana przez polskie władze ze szkodą dla interesów Rosji¹⁰⁸⁵. Należy również zaznaczyć, że zupełnie inne postrzeganie Polski będzie miał „inteligent z Moskwy czy Sankt Petersburga (...) a inaczej mieszkaniec uralskiej czy nadbajkalskiej wioski. Jeszcze inny ogląd ma mieszkaniec Obwodu Kaliningradzkiego, dla którego Rzeczpospolita nie jest żadną tytułową oddalą. Wręcz przeciwnie, jest dla niego krainą bliską w sensie nie tylko geograficznym, ale także – w coraz większym stopniu – mentalnym czy nawet światopoglądowym”¹⁰⁸⁶. M. Wołos zauważa również, że dla przeciętnego Rosjanina Polska pozostaje państwem trzeciorzędnym¹⁰⁸⁷ i to nie tylko z perspektywy politycznej¹⁰⁸⁸.

Ostatnim z uwarunkowań wymagającym omówienia jest aktywność rosyjskiej służby zagranicznej oraz dyplomacji w Polsce. Federacja Rosyjska posiada stosunkowo dobrze

¹⁰⁸⁰ S. Falkowicz: *Polska i Polacy w wyobrażeniach Rosjan: refleksje ogólne*. „Dzieje Najnowsze” 1997, nr 29/1, s. 16.

¹⁰⁸¹ Badania w zakresie wzajemnego postrzegania Polaków i Rosjan prowadzi od wielu lat Centrum Polsko-Rosyjskiego Dialogu i Porozumienia. Zobacz szerzej: Centrum Polsko-Rosyjskiego Dialogu i Porozumienia: *Projekty, badania opinii publicznej*. http://cprdip.pl/projekty,badania_opinii_publicznej.html (dostęp: 20.01.2023).

¹⁰⁸² Centrum Polsko-Rosyjskiego Dialogu i Porozumienia: *ROSJA–POLSKA DIAGNOZA SPOŁECZNA 2020. Rosjanie na temat Polski i Polaków oraz stosunków rosyjsko-polskich*. Warszawa 2020. http://cprdip.pl/assets/media/Wydawnictwa/Raporty/ROSJA_POLSKA_Diagnoza_spoleczna_2020.pdf (dostęp: 20.01.2023), s. 8.

¹⁰⁸³ Ibidem, s. 13.

¹⁰⁸⁴ Ibidem, s. 17.

¹⁰⁸⁵ Ibidem, s. 20.

¹⁰⁸⁶ M. Wołos: *Polska widziana z rosyjskiej oddali*. „Kultura Współczesna: teoria, interpretacje, krytyka” 2015, nr 1, s. 79.

¹⁰⁸⁷ Do państw pierwszego rzędu zaliczył światowe mocarstwa, do państw drugiego rzędu obszar poradziecki, z kolei do trzeciego rzędu państwa niemieszczące się ani w pierwszym ani w drugim rzędzie. Źródło: Ibidem, s. 79-80.

¹⁰⁸⁸ Ibidem, s. 79.

rozwiniętą służbę zagraniczną, co jest dla niej elementem charakterystycznym. Nie jest to również nowe zjawisko, gdyż ze znaczenia dobrze wykwalifikowanych dyplomatów zdawali sobie sprawę bolszewicy, czy też władze Związku Radzieckiego¹⁰⁸⁹. W Warszawie funkcjonuje Ambasada Federacji Rosyjskiej wraz z Wydziałem Konsularnym, a w Krakowie, Gdańsku oraz Poznaniu Konsulaty Generalne¹⁰⁹⁰. Stosunkowo duża ilość rosyjskich placówek służby zagranicznej nie jest wyłącznie pozostałością po okresie zimnowojennym, kiedy Polska należała do grupy państw satelickich ZSRR, ale jest uwarunkowane stosunkowo dużym ruchem granicznym w zakresie ilości obywateli rosyjskich wjeżdżających do Polski. Dla przykładu można wskazać na dane za 2017, 2018 i 2019 rok¹⁰⁹¹ z których wynika, że średnioroczna liczba osób wjeżdżających do Polski oraz posiadających rosyjskie obywatelstwo wynosiła około 1,5 miliona¹⁰⁹². Szacunkowo w rosyjskiej służbie dyplomatycznej w Polsce pracuje około 60 osób posiadających immunitet dyplomatyczny¹⁰⁹³. Ponadto działa Przedstawicielstwo Handlowe Rosji w Polsce prowadzące działalność z zakresu utrzymania stałych stosunków gospodarczych¹⁰⁹⁴ oraz Rosyjski Ośrodek Nauki i Kultury – Rosyjski Dom w Warszawie, będący instytucją promującą kulturę Rosji¹⁰⁹⁵. Na terytorium Polski znajduje się również wiele innych budynków dzierżawionych, najmowanych czy też należących do Federacji Rosyjskiej. Są one przede wszystkim pozostałością czasu zimnej wojny, kiedy na terytorium Polski rezydował liczny radziecki personel dyplomatyczny¹⁰⁹⁶. Jak wskazał S. Gardocki, w dwóch pierwszych dekadach XXI wieku „trwała obecność w międzynarodowej polityce zaznaczyli rosyjscy dyplomaci, m.in. tacy jak: Jewgienij Primakow (były szef rosyjskiego MSZ i premier),

¹⁰⁸⁹ S. Gardocki: *Polityka zagraniczna Rosji. Determinanty, interesy i środki*. „Studia Orientalne” 2020, nr 2 (18), s. 14.

¹⁰⁹⁰ Oficjalna strona internetowa Ambasady Federacji Rosyjskiej w Polsce. https://poland.mid.ru/web/polska_pl (dostęp: 20.01.2023).

¹⁰⁹¹ Nie uwzględniono danych o osobowym ruchu granicznym w 2020 i 2021 roku, gdyż z uwagi na wprowadzone wcześniej ograniczenia tranzytowe na przejściach granicznych w związku z pandemią wirusa SARS-CoV-2 nie są one miarodajne i porównywalne.

¹⁰⁹² Straż Graniczna. Komenda Główna Straży Granicznej: *Statystyki SG. Informacje statystyczne za lata 2017-2019*. <https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html> (dostęp: 20.01.2023).

¹⁰⁹³ Radio Free Europe: *Russia's Diplomatic Missions In Central Europe*. <https://www.rferl.org/a/russias-diplomatic-missions-in-central-europe-/31215395.html> (dostęp: 20.01.2023).

¹⁰⁹⁴ Oficjalna strona internetowa Ambasady Federacji Rosyjskiej w Polsce. https://poland.mid.ru/web/polska_pl (dostęp: 20.01.2023).

¹⁰⁹⁵ Oficjalna strona internetowa Rosyjskiego Ośrodka Nauki i Kultury - Rosyjski Dom w Warszawie <https://www.ronik.org.pl/> (dostęp: 20.01.2023).

¹⁰⁹⁶ TVP INFO: *Rosyjski ośrodek nad Zegrzem przejęty. Są zdjęcia ze środka*. <https://www.tvp.info/64310764/osrodek-nad-zegrzem-w-skubiance-rosjanie-zostawili-go-w-oplakany-m-stanie-przejmuja-lasy-panstwowe> (dostęp: 03.03.2023); NOIZZ: *Nie tylko "Szpiegowo". W Polsce są inne budynki, za które Rosja nie płaci czynszu*. <https://noizz.pl/spoleczenstwo/nie-tylko-szpiegowo-w-polsce-sa-inne-budynki-za-ktora-rosja-nie-placi-czynszu/b5w8pve> (03.03.2023); TVN WARSZAWA: *Nie tylko Szpiegowo. "Rosyjskich wysp" jest w Warszawie więcej*. <https://tvn24.pl/tvnwarszawa/najnowsze/warszawa-lista-nieruchomosci-zajmowanych-przez-rosje-zalegly-czynsz-wynosi-juz-ponad-24-miliony-zlotych-5675616> (dostęp: 03.03.2023).

Witalij Czurkin (ambasador Rosji w Belgii, w Kanadzie, a następnie stały przedstawiciel Rosji przy ONZ) czy pełniący funkcję ministra spraw zagranicznych Rosji, Sergiej Ławrow”¹⁰⁹⁷.

5.2.2. Uwarunkowania zewnętrzne polityki zagranicznej Federacji Rosyjskiej wobec Polski

Do uwarunkowań zewnętrznych polityki zagranicznej Federacji Rosyjskiej wobec Polski należy zaliczyć te o charakterze obiektywnym, jak wiążące umowy międzynarodowe oraz członkostwo Rosji i Polski w organizacjach międzynarodowych. Z kolei do uwarunkowań o charakterze subiektywnym zaliczamy: polskie koncepcje polityki zagranicznej wobec Rosji, obraz Rosji i Rosjan w polskim społeczeństwie oraz aktywność polskiej służby zagranicznej i dyplomacji w Rosji.

Pierwszym z omawianych uwarunkowań zewnętrznych o charakterze obiektywnym są wiążące Federację Rosyjską oraz Rzeczpospolitą Polską umowy międzynarodowe. Czynnikiem ten jest o tyle istotny, że rozpad Związku Radzieckiego w 1991 roku wymusił przyjęcie nowych podstaw traktatowych (formułowanych w znacznej mierze od nowa) stosunków dwustronnych. Internetowa Baza Traktatowa Ministerstwa Spraw Zagranicznych Polski zawiera informacje, że pomiędzy Rosją a Polską obowiązuje bądź obowiązywało łącznie 76 umów dwustronnych, z czego 60 zostało zawartych po rozpadzie ZSRR (co miało miejsce 26 grudnia 1991 roku)¹⁰⁹⁸. Pierwsze umowy z Federacją Rosyjską zawarto 22 maja 1992 roku, a najważniejszą z nich był Traktat między Rzeczpospolitą Polską a Federacją Rosyjską o przyjaznej i dobrosąsiedzkiej współpracy, który wszedł w życie w maju 1993 roku¹⁰⁹⁹. Traktat normował podstawowe

¹⁰⁹⁷ S. Gardocki: *Polityka zagraniczna Rosji...*, s. 14.

¹⁰⁹⁸ Ministerstwo Spraw Zagranicznych: *Internetowa Baza Traktatowa*. <https://traktaty.msz.gov.pl/umowa-1> oraz <https://traktaty.msz.gov.pl/umowa-4> (dostęp: 21.01.2023).

¹⁰⁹⁹ 22 maja 1992 roku podpisano następujące umowy dwustronne: Traktat między Rzeczpospolitą Polską a Federacją Rosyjską o przyjaznej i dobrosąsiedzkiej współpracy; Konwencja Konsularna między RP a Federacją Rosyjską; Umowa między Rządem RP a Rządem Federacji Rosyjskiej w sprawie przejść granicznych; Umowa między Rządem RP a Rządem Federacji Rosyjskiej w sprawie unikania podwójnego opodatkowania w zakresie podatków od dochodu i majątku; Porozumienie między Rządem RP a Rządem Federacji Rosyjskiej o współpracy północno-wschodnich województw RP i Obwodu kaliningradzkiego Federacji Rosyjskiej; Protokół dodatkowy między Rządem RP a Rządem Federacji Rosyjskiej w sprawie sprzedaży mienia ruchomego wojsk Federacji Rosyjskiej; Umowa między RP a Federacją Rosyjską w sprawie wycofania wojsk Federacji Rosyjskiej z terytorium Polski; Umowa między Rządem RP a Rządem Federacji Rosyjskiej o tranzycie przez terytorium RP wojsk Federacji Rosyjskiej wycofywanych z RFN; Porozumienie między Rządem RP a Rządem Federacji Rosyjskiej o uregulowaniu spraw transportowych związanych z wycofywaniem wojsk Federacji Rosyjskiej z terytorium Polski; Protokół między Rządem RP a Rządem Federacji Rosyjskiej o uregulowaniu majątkowych, finansowych i innych spraw związanych z wycofaniem wojsk Federacji Rosyjskiej z terytorium Polski. Źródło: Ibidem.

kwestie związane z relacjami dwustronnymi oraz stanowił podstawy do kreowania przyszłych stosunków polsko-rosyjskich¹¹⁰⁰. W latach dziewięćdziesiątych XX wieku podpisano również umowy dwustronne o: współpracy transgranicznej; współpracy w dziedzinie kultury, nauki i oświaty; grobach i miejscach pamięci ofiar wojen i represji; dotyczące przejść granicznych. Do początku XXI wieku podpisano łącznie 25 różnego rodzaju umów dwustronnych, natomiast ostatnią umowę dwustronną zawarto w 2015 roku¹¹⁰¹.

Drugim z uwarunkowań jest uczestnictwo Rosji i Polski w organizacjach międzynarodowych. W odniesieniu do Rosji jest to przede wszystkim członkostwo w Organizacji Narodów Zjednoczonych oraz posiadany status stałego członka w Radzie Bezpieczeństwa ONZ z prawem weta¹¹⁰², jak również członkostwo we Wspólnocie Niepodległych Państw oraz Związku Rosji i Białorusi. W kontekście Polski jest to głównie status członka w Unii Europejskiej oraz Sojuszu Północnoatlantyckim. Członkostwo Rosji w ONZ i związane z tym uprawnienia z całkowitą pewnością stawiają Kreml w niezwykle uprzywilejowanej pozycji względem innych państw na świecie i tym samym umożliwiają efektywne wpływanie na kształt ładu międzynarodowego (oczywiście z uwzględnieniem rzeczywistych możliwości jakie posiada sama organizacja)¹¹⁰³. Dużo ciekawszym zagadnieniem jest z kolei członkostwo Rosji we Wspólnocie Niepodległych Państw (WNP), czyli tworze powstałym w 1991 roku, a po rozpadzie ZSRR stanowiącym platformę współpracy Federacji Rosyjskiej ze znaczną częścią państw byłego Związku Radzieckiego¹¹⁰⁴. Nie powinno zatem stanowić zaskoczenia, że to właśnie WNP stanowi jeden z najważniejszych kierunków realizowanej przez Kreml polityki zagranicznej¹¹⁰⁵. Drugą z organizacji jest Związek Rosji i Białorusi, a właściwie Państwo Związkowe Rosji i Białorusi powstałe w 2000 roku na mocy Umowy o utworzeniu Państwa Związkowego. Celem jego istnienia jest nie tylko zacieśnienie współpracy gospodarczej, walutowej czy kulturalnej, ale również stworzenie podstaw do pogłębionej integracji rosyjsko-białoruskiej, między innymi poprzez ujednolicenie

¹¹⁰⁰ *Traktat między Rzeczpospolitą Polską a Federacją Rosyjską o przyjaznej i dobrosąsiedzkiej współpracy, sporządzony w Moskwie dnia 22 maja 1992 r.* (Dz.U. 1993 nr 61 poz. 291), art. 1.

¹¹⁰¹ Ministerstwo Spraw Zagranicznych: *Internetowa Baza Traktatowa*. <https://traktaty.msz.gov.pl/umowa-1> (dostęp: 21.01.2023).

¹¹⁰² *Karta Narodów Zjednoczonych, Statut Międzynarodowego Trybunału Sprawiedliwości i Porozumienie ustanawiające Komisję Przygotowawczą Narodów Zjednoczonych* (Dz.U. 1947 nr 23 poz. 90), art. 23 i następne.

¹¹⁰³ Sz. Kardaś: *Federacja Rosyjska w organizacjach międzynarodowych*. W: *Polityka zagraniczna Rosji*. Red. S. Bieleń, M. Raś. Warszawa 2008, s. 190-195.

¹¹⁰⁴ T. A. Olszański: *Czym (nie) jest WNP? Wspólnota Niepodległych Państw w świetle własnych dokumentów*. „EURAZJA” 1994, nr (1-2), Vol. 1, s. 28-33.

¹¹⁰⁵ J. Diec: *Geostrategiczny wybór...*, s. 173-185.

ustawodawstw państw¹¹⁰⁶. Według doniesień medialnych, w 2021 roku na Kremlu miał powstać dokument, który zakłada plan połączenia obu państw do 2030 roku¹¹⁰⁷. W odniesieniu do członkostwa Polski w organizacjach międzynarodowych należy zwrócić uwagę na dwie, które z perspektywy Kremla są niezwykle istotne, tj. NATO oraz Unię Europejską. Polska wstąpiła do wskazanych organizacji kolejno w 1999 i 2004 roku. Dla Rosji rozszerzenie Sojuszu Północnoatlantyckiego na Wschód było niewątpliwie ingerencją w jej dotychczasową strefę wpływów, co do której istniały obawy, iż będzie próbowała ją odzyskać¹¹⁰⁸. Choć początkowo rozszerzenie NATO nie spowodowało drastycznego pogorszenia stosunków pomiędzy Kremla a Zachodem (przykładem może być funkcjonowanie Rady NATO-Rosja)¹¹⁰⁹, to w kolejnych latach Sojusz był postrzegany przez Moskwę głównie jako inicjator działalności antyrosyjskiej oraz jeden z głównych konkurentów na arenie międzynarodowej¹¹¹⁰. W kontekście członkostwa Polski w Unii Europejskiej należy zaznaczyć, że Rosja postrzega Unię przede wszystkim w wymiarze pragmatycznym, jako partnera handlowego¹¹¹¹. Jednocześnie z punktu widzenia Rosji rozszerzenie organizacji na wschód doprowadziło rosyjskie elity polityczne do przekonania, że Zachód dąży do demontażu rosyjskiej państwowości oraz ingeruje w jej wyłączną strefę wpływów (przede wszystkim na obszarze poradzieckim)¹¹¹². I wreszcie należy zauważyć, że wstąpienie Polski do NATO oraz Unii Europejskiej sprawiło, że problemy w stosunkach polsko-rosyjskich stały się również problemami wymienionych organizacji, jak i odwrotnie, problemy organizacji w relacjach z Kremla stały się problemami Warszawy.

Następnie, przechodząc do uwarunkowań zewnętrznych o charakterze subiektywnym, należy omówić kierunek wschodni polskiej polityki zagranicznej, który odnosi się przede wszystkim do relacji z Moskwą. Inaczej niż w koncepcjach polityki zagranicznej Kremla,

¹¹⁰⁶ K. Kakareko: *Państwo Związkowe Białorusi i Rosji*. „Środkowoeuropejskie Studia Polityczne” 2008, nr 1, s. 293-328.

¹¹⁰⁷ The Kyiv Independent: *Leaked document reveals alleged Kremlin plan to take over Belarus by 2030*. <https://kyivindependent.com/investigations/leaked-document-reveals-alleged-kremlin-plan-to-take-over-belarus-by-2030> (dostęp: 04.03.2023); DW: *Russia plans Belarus 'absorption' by 2030 — media reports*. <https://www.dw.com/en/russia-plans-belarus-absorption-by-2030-media-reports/a-64771429> (dostęp: 04.03.2023).

¹¹⁰⁸ Zobacz szerzej: M. Stolarczyk: *Rosja w polityce zagranicznej Polski...*, s. 159-177; A. Bryc: *Cele polityki zagranicznej Federacji Rosyjskiej*. Toruń 2004.

¹¹⁰⁹ A. Bryc: *Stosunki Federacji Rosyjskiej z Sojuszem Północnoatlantyckim*. W: *Polityka zagraniczna Rosji*. Red. S. Bieleń, M. Raś. Warszawa 2008, s. 68-86.

¹¹¹⁰ Federacja Rosyjska w swoich koncepcjach, doktrynach i strategiach odnoszących się do polityki zagranicznej oraz polityki bezpieczeństwa bardzo często utożsamia działalność NATO z działalnością USA, bądź też traktuje działalność Sojuszu jako działalność inspirowaną i motywowaną przez USA.

¹¹¹¹ *Koncepcja polityki zagranicznej Federacji Rosyjskiej zatwierdzona 30 listopada 2016 roku*. Moskwa 2016. <http://static.kremlin.ru/media/acts/files/0001201612010045.pdf> (dostęp: 21.01.2023)

¹¹¹² J. Tymanowski: *Federacja Rosyjska w polityce zewnętrznej Unii Europejskiej*. W: *Polska i Rosja w zmieniającej się Europie*. Red. K. A. Wojtaszczyk, I. N. Novikova. Warszawa 2022, s. 411-437.

Federacja Rosyjska pojawia się niejednokrotnie w polskich odpowiednikach tych dokumentów. W zależności od jego wersji stosunek do Rosji bywa różny, jednakże jest przedstawiany przede wszystkim jako zagrożenie bądź jako trudny partner. Dla przykładu, w dokumencie *Priorytety Polskiej Polityki Zagranicznej 2012-2016* wskazano na otwartość oraz konieczność nawiązania dialogu z Rosją, budowania partnerstwa opartego na zasadzie wzajemności, kreowania pragmatycznych stosunków politycznych i gospodarczych¹¹¹³. Z kolei w *Strategii Polskiej Polityki Zagranicznej 2017-2021* wydźwięk względem Rosji jest już zdecydowanie chłodniejszy. Wskazano głównie na impas w relacjach Zachód-Rosja spowodowany degradacją przez Kreml budowanej od lat architektury europejskiego bezpieczeństwa, koniecznością dbania o dialog NATO-Rosja oraz ograniczaniu agresywnych działań Kremla względem państw stanowiących jego byłą bądź aktualną strefę wpływów¹¹¹⁴. Oczywiście należy zauważyć, że stosunek do Rosji jest również przejawem toczącej się w Polsce rywalizacji politycznej, a jednym z jej istotniejszych elementów jest właśnie wizja relacji z Moskwą. Wyróżnić tutaj można obóz reprezentujący centro-lewicową stronę sceny politycznej (Platforma Obywatelska, PSL, SLD¹¹¹⁵), który opowiada się za pragmatyczną polityką wschodnią oraz obóz prawicowy (Prawo i Sprawiedliwość) o *stricte* antyrosyjskim nastawieniu¹¹¹⁶. Co więcej, ponownie nie bez znaczenia pozostaje sytuacja związana z wojną rosyjsko-ukraińską, która cechuje się zdecydowanie antyrosyjskim podejściem Warszawy w ramach realizowanej wschodniej polityki zagranicznej.

Innym istotnym czynnikiem zewnętrznym pozostaje obraz Rosji i Rosjan w polskim społeczeństwie. Jak wskazał R. Zięba, „percepcja środowiska międzynarodowego przez własne społeczeństwo, media i kręgi rządzące oraz postawy społeczne wobec innych państw i narodów stanowią podstawę subiektywnych uwarunkowań wewnętrznych polityki zagranicznej państwa”¹¹¹⁷. Nie inaczej wygląda to w przypadku Polski, która w przeciwieństwie do Rosji jest znacznie bardziej obciążona wzajemnymi waśniami historycznymi, gdyż to Polska znacznie częściej doświadczała negatywnych oddziaływań oraz aktów agresji ze strony Kremla. Wciąż żywe pozostają okresy wojen, zaborów, zbrodni katyńskiej czy okresu

¹¹¹³ *Priorytety Polskiej Polityki Zagranicznej 2012-2016*. Warszawa 2012. <https://www.bbn.gov.pl/download/1/9620/prpol.pdf> (dostęp: 21.01.2023).

¹¹¹⁴ *Strategia Polskiej Polityki Zagranicznej 2017-2021*. Warszawa 2017. <https://www.gov.pl/attachment/8196524f-687b-40e6-aca8-82c53ff8e6db> (dostęp: 21.01.2023).

¹¹¹⁵ Sojusz Lewicy Demokratycznej (SLD) został rozwiązany w 2021 roku i zastąpiony przez inne ugrupowania lewicowe.

¹¹¹⁶ R. Zięba: *Uwarunkowania polityki zagranicznej Polski na początku drugiej dekady XXI wieku*. „Stosunki Międzynarodowe – International Relations” 2011, nr 1-2 (T. 43), s. 21.

¹¹¹⁷ Ibidem, s. 18.

zimnowojennego¹¹¹⁸. Analizując proces kształtowania się postrzegania Rosjan przez Polaków, można wskazać na dwie istotne płaszczyzny wpływu – polityczno-historyczną oraz kulturową. Z kolei sam stereotyp wizerunku Rosjan w polskim społeczeństwie jest nie tyle po prostu negatywny, ale niezwykle mocno w nim zakorzeniony¹¹¹⁹. M. Stolarczyk, omawiając stosunki polsko-rosyjskie, przytacza badania przeprowadzone w 1990 z których wynikało, że 60% ankietowanych dostrzegało zagrożenie ze strony Niemiec, z kolei w 2010 rok było to już tylko 14%. Inaczej ma to miejsce w przypadku Rosji, gdzie na podstawie badań z 1992 roku 45% badanych obawiało się działań Kremla, z kolei w 2015 roku było to już 85%¹¹²⁰. Obserwujemy zatem istotne zmiany w społecznym postrzeganiu dwóch największych sąsiadów Polski, choć w przypadku ostatniego z badań, należy pamiętać, że zostało ono przeprowadzone rok po rozpoczęciu wojny we wschodniej Ukrainie i aneksji Półwyspu Krymskiego. Sięgając natomiast do najnowszych badań z 2020 roku¹¹²¹ należy stwierdzić, że ich wyniki nie uległy ważniejszym zmianom względem lat ubiegłych. Na pytanie o nastawienie do Rosji tylko 21% badanych odpowiedziało, że jest ono przyjazne, z kolei 79% uznało, że jest nieprzyjazne. Z kolei badani w latach 2012 i 2014 określili swój stosunek jako nieprzyjazny odpowiednio w 80% i 82%¹¹²². Zdecydowanie lepsze nastawienie można zaobserwować przy ocenie stosunku do Rosjan, gdzie aż 64% badanych wskazało, że jest on przyjazny, a 36%, że jest nieprzyjazny. Podobne wyniki odnotowano podczas badań w roku 2012¹¹²³. Badani wskazali, że wiedzę na temat Rosji i Rosjan czerpią głównie z telewizji, Internetu oraz polskich książek i filmów o Rosji¹¹²⁴.

I wreszcie wskazać należy na aktywność polskiej służby zagranicznej oraz dyplomacji w Rosji. Polska posiada w Federacji Rosyjskiej Ambasadę w Moskwie wraz z Wydziałem Konsularnym oraz Konsulat Generalny w Sankt Petersburgu, Kaliningradzie oraz Irkucku, jak również Agencję Konsularną w Smoleńsku¹¹²⁵. Ponadto na tle współpracy kulturalnej oraz promowania polskiej kultury w Rosji funkcjonuje Instytut Polski w Moskwie oraz Instytut

¹¹¹⁸ Zobacz szerzej: *Pamięć i polityka historyczna w stosunkach polsko-rosyjskich*. Red. S. Bieliń, A. Skrzypek, Warszawa 2017.

¹¹¹⁹ M. Cybulski: *Polacy i Rosjanie. Zarys narodzin stereotypów*. „Acta Polono-Ruthenica” 2009, nr XIV 2009, s. 77.

¹¹²⁰ M. Stolarczyk: *Rosja w polityce zagranicznej Polski...*, s. 47.

¹¹²¹ Badania w analogicznym okresie zostały przeprowadzone również wobec Rosjan i ich postrzegania Polaków. Wyniki zostały przedstawione we wcześniejszej części pracy w zakresie uwarunkowań wewnętrznych o charakterze subiektywnym polityki zagranicznej Federacji Rosyjskiej.

¹¹²² Centrum Polsko-Rosyjskiego Dialogu i Porozumienia: *POLSKA–ROSJA DIAGNOZA SPOŁECZNA 2020. Polacy na temat Rosji i Rosjan oraz stosunków polsko-rosyjskich*. Warszawa 2020, s. 9.

¹¹²³ Ibidem, s. 12.

¹¹²⁴ Ibidem, s. 19.

¹¹²⁵ Ministerstwo Spraw Zagranicznych: *Polska w Rosji. Placówki*. <https://www.gov.pl/web/rosja/placowki> (dostęp: 21.01.2023).

Polski w Sankt Petersburgu, które podlegają Ministerstwu Spraw Zagranicznych. Z kolei w kontekście współpracy gospodarczej w Moskwie ma swoją siedzibę Polsko-Rosyjska Izba Handlowo-Przemysłowa, której geneza istnienia sięga dwudziestolecia międzywojennego. W odniesieniu do jakości służby zagranicznej trzeba zauważyć, że po okresie transformacji Polska wykształciła kompetentny oraz stabilny zespół dyplomatów, zdolny do należytej reprezentacji za granicą¹¹²⁶.

5.3. Zarys stosunków polsko-rosyjskich w latach 1992-2009

Stosunki bilateralne Polski oraz Federacji Rosyjskiej zostały zapoczątkowane jeszcze przed rozpadem ZSRR, a wyraźnym sygnałem w tym zakresie była wizyta ówczesnego polskiego Ministra Spraw Zagranicznych K. Skubiszewskiego w 1990 roku w Moskwie, w trakcie której podpisano Deklarację o przyjaźni i dobrosąsiedzkiej współpracy między Rzeczpospolitą Polską i Rosyjską Federacyjną Socjalistyczną Republiką Radziecką¹¹²⁷. Rozpad Związku Socjalistycznych Republik Radzieckich w 1991 roku doprowadził do szeregu implikacji determinujących politykę zagraniczną Federacji Rosyjskiej (prawnego oraz faktycznego sukcesora ZSRR), w tym kształtujących przyszłe stosunki polsko-rosyjskie. Relacje na linii Kreml-Warszawa po 1991 roku kształtowały się w nowej pozimnowojennej rzeczywistości, w ramach której Moskwa musiała ponownie ukształtować swoje stanowisko wobec państw Europy Środkowo-Wschodniej, będąc jednocześnie w przekonaniu, że region ten to nadal jej wyłączna strefa wpływów¹¹²⁸. Polska i Rosja, państwa pomiędzy którymi od wieków występowały liczne spory i konflikty, ponownie w wyniku postępujących przemian ładu międzynarodowego musiały zbudować wzajemne relacje, które nie należały do najłatwiejszych oraz nie były mniej skomplikowane niż dotychczas.

W początkowym okresie zainteresowanie Rosji Polską znacznie spadło, co było związane z koniecznością rozwiązania szeregu żywotnych dla Kremla problemów wewnętrznych¹¹²⁹. Pomimo tego podstawowymi kwestiami spornymi w pierwszej połowie lat dziewięćdziesiątych XX wieku było: wycofanie żołnierzy radzieckich/rosyjskich z terytorium Polski, odmienność wizji bezpieczeństwa narodowego i międzynarodowego w Europie

¹¹²⁶ R. Zięba: *Uwarunkowania polityki zagranicznej...*, s. 21-22.

¹¹²⁷ K. Fedorowicz: *Polska w polityce zagranicznej Rosji w latach 1991-2001*. W: *Polska w Rosji – Rosja w Polsce. Stosunki Polityczne*. Red. R. Paradowski, Sz. Ossowski. Poznań 2003, s. 17.

¹¹²⁸ M. Raś: *Polityka Rosji wobec Europy Środkowo-Wschodniej*. „Prace Instytutu Europy Środkowo-Wschodniej” 2010, Tom 16, s. 9-10.

¹¹²⁹ M. Raś: *Polityka Rosji wobec Europy...*, s. 34-35.

(w szczególności żądania ze strony radzieckiej/rosyjskiej co do ograniczenia członkostwa Polski w organizacjach, które Kreml uważał za sobie wrogie), zadłużenie oraz zaszłości historyczne (w szczególności kwestia zbrodni katyńskiej)¹¹³⁰. Rozpad Związku Radzieckiego to również następujący po nim rozpad Układu Warszawskiego oraz Rady Wzajemnej Pomocy Gospodarczej, które to podmioty stanowiły dla Kremla ważne narzędzie oddziaływania na państwa w regionie. Z takiego układu sił z całą pewnością skorzystały w kolejnych latach NATO oraz Unia Europejska, wypełniając powstałą próżnię po tych organizacjach¹¹³¹. W 1992 roku Federacja Rosyjska oraz Polska zawarły traktat o przyjaznej i dobrosąsiedzkiej współpracy na mocy którego określono podstawy wzajemnych relacji¹¹³².

Druga połowa lat dziewięćdziesiątych XX wieku to głównie spory na tle zaszłości historycznych oraz polskich planów przystąpienia do NATO. Rosja nie zgadzała się na przyjęcie nowych państw z regionu w poczet Sojuszu, pomimo jej przystąpienia do Partnerstwa dla Pokoju w 1995 roku, jak również przyjęcia w 1997 roku Aktu stanowiącego o wzajemnych stosunkach, współpracy i bezpieczeństwie między NATO a Federacją Rosyjską¹¹³³. Ostatecznie Polska w 1999 roku wraz z Czechami oraz Węgrami wstąpiła do Sojuszu Północnoatlantyckiego pomimo sprzeciwu Kremla¹¹³⁴. Wejście Polski do organizacji nie spowodowało poprawy wzajemnych relacji polsko-rosyjskich, a jednocześnie problemy na linii NATO-Rosja stały się również problemami Warszawy¹¹³⁵. Co więcej, Polska podejmowała w tym czasie działania zmierzające do wyrwania spod wpływów Kremla byłych republik radzieckich, co z kolei Federacja Rosyjska postrzegała jako wrogą ingerencję w jej wyłączną strefę wpływów¹¹³⁶. Ponadto coraz istotniejszym problemem zaczęła być kwestia bezpieczeństwa energetycznego Polski, gdyż w tamtym okresie Rosja była głównym dostawcą większości surowców takich jak ropa naftowa i gaz ziemny¹¹³⁷. Niebagatelną pozostawała również kwestia polskich aspiracji do członkostwa w Unii Europejskiej, która była podnoszona już od 1989 roku¹¹³⁸. Jeśli chodzi o ogólne zainteresowanie zwykłych Rosjan Polską należy

¹¹³⁰ M. Stolarczyk: *Rosja w polityce zagranicznej Polski...*, s. 147.

¹¹³¹ M. Raś: *Polityka Rosji wobec Europy...*, s. 12.

¹¹³² K. Fedorowicz: *Polityka Polski wobec Rosji, Ukrainy i Białorusi w latach 1989-2010*. Poznań 2011, s. 91-92.

¹¹³³ A. Bryc: *Stosunki Federacji Rosyjskiej...* W: *Polityka zagraniczna Rosji*. Red. S. Bieleń, M. Raś. Warszawa 2008, s. 68-73.

¹¹³⁴ M. Stolarczyk: *Rosja w polityce zagranicznej...*, s. 159-177.

¹¹³⁵ Ibidem, s. 179.

¹¹³⁶ R. Zięba: *Główne problemy w stosunkach polsko-rosyjskich*. „Stosunki Międzynarodowe – International Relations” 2018, nr 3 (T. 54), s. 22-23.

¹¹³⁷ Ibidem, s. 25-26.

¹¹³⁸ J. M. Fiszer: *Stanowisko Rosji wobec aneksji Polski do NATO i Unii Europejskiej*. „Myśl Ekonomiczna i Polityczna” 2018, nr 1 (60), s. 272-276.

zauważyć, że było ono zdecydowanie mniejsze, aniżeli zainteresowanie Polaków wydarzeniami w Rosji¹¹³⁹.

Początek XXI wieku to w Rosji rozpoczęcie rządów prezydenta W. Putina, który deklarował ocieplenie relacji z Zachodem. Znaczący wpływ miały na to wydarzenia z 11 września 2001 roku w wyniku których doszło do zacieśnienia współpracy na linii NATO-Rosja¹¹⁴⁰. Powyższe nie miało tak wyraźnego charakteru w stosunku do Polski. Mimo to można mówić o pewnym okresie odprężenia, w trakcie którego zarówno politycy rosyjscy jak i polscy odwiedzali się w Moskwie i Warszawie. Można zauważyć, że po dość burzliwej końcówce XX wieku nastąpiła narracja znoszenia barier oraz budowania pozytywnych relacji w stosunkach dwustronnych. Wstąpienie Polski do Unii Europejskiej w 2004 roku wraz z szeregiem innych byłych państw satelickich ZSRR spowodowało, że organizacja ta zyskała w jeszcze większym stopniu na znaczeniu w polityce zagranicznej Kremla¹¹⁴¹. Co również istotne w tym czasie najchłodniejsze relacje Rosja posiadała z państwami Europy Środkowo-Wschodniej takimi jak Litwa, Łotwa, Estonia i Polska. Zdając sobie sprawę, że państwa te próbują prowadzić politykę wobec Kremla przy użyciu instrumentów oferowanych im przez NATO oraz Unię Europejską, Moskwa dążyła (i nadal dąży) do jak największego ograniczania roli tych państw w kreowanej przez wymienione organizacje międzynarodowe polityce wschodniej. Dokonuje tego poprzez jawne dyskredytowanie uciążliwych sąsiadów na arenie międzynarodowej oraz podważając ich obraz funkcjonujący na Zachodzie¹¹⁴². Początek XXI wieku to również okres tzw. kolorowych rewolucji, gdzie w odniesieniu do stosunków polsko-rosyjskich najistotniejsza pozostaje rewolucja w Gruzji (2003) oraz w Ukrainie (2004). Polska wspierała te państwa w polityce uniezależniania się od Rosji, z kolei dla Kremla wspomniane wydarzenia były synonimem klęski prowadzonej polityki zagranicznej oraz zwiastowały utratę wpływów w regionie¹¹⁴³. Wybory parlamentarne w Polsce z 2005 roku doprowadziły do eskalacji napięcia. Zwycięska koalicja z Prawem i Sprawiedliwością na czele prowadziła wobec Moskwy politykę konfrontacyjną (wręcz antyrosyjską), w szczególności wobec zapowiedzi o budowie gazociągu Nord Stream I przez Rosję i Niemcy¹¹⁴⁴. Zmiany cen surowców energetycznych na światowych

¹¹³⁹ J. Adamowski: *Wizerunek Rosji w polskich środkach masowego przekazu (u progu nowego tysiąclecia)*. W: *Polityka zagraniczna Rosji*. Red. M. Zamarlik. Kraków 2002, s. 121-126.

¹¹⁴⁰ A. Bryc: *Stosunki Federacji Rosyjskiej...* W: *Polityka zagraniczna Rosji*. Red. S. Bieleń, M. Raś. Warszawa 2008, s. 84-86.

¹¹⁴¹ J. M. Fiszer: *Stanowisko Rosji wobec aneksji Polski...*, s. 277-279.

¹¹⁴² A. Bryc: *Stosunki Federacji Rosyjskiej...* W: *Polityka zagraniczna Rosji*. Red. S. Bieleń, M. Raś. Warszawa 2008, s. 107.

¹¹⁴³ K. Fedorowicz: *Polityka Polski wobec Rosji...*, s. 142-144; M. Stolarczyk: *Rosja w polityce zagranicznej...*, s. 190-195.

¹¹⁴⁴ R. Zięba: *Główne problemy w stosunkach polsko-rosyjskich...*, s. 32-33.

rynkach były dla Kremla niezwykle korzystne, gdyż sprowadzały się do znacznego zwiększenia wpływów do rosyjskiego budżetu. Dla przykładu, rezerwy walutowe Rosji w 2000 roku wynosiły 12,5 mld dolarów, podczas gdy w 2010 roku już ponad 514 mld dolarów¹¹⁴⁵. Doskonale zdawał sobie z tego sprawę prezydent W. Putin, który zapragnął wykreować Rosję na lidera światowej energetyki¹¹⁴⁶, tworząc jednocześnie narzędzie tzw. szantażu energetycznego. Moskwa odpowiedziała na narzuconą przez Warszawę agresywną retorykę, co wiązało się z eskalacją napięcia w stosunkach dwustronnych.

Kolejnym, szczególnie trudnym tematem poruszonym w tym okresie była budowa amerykańskiej tarczy antyrakietowej w Polsce i Czechach¹¹⁴⁷. Co ciekawe, podczas posiedzenia Rady NATO-Rosja pod koniec 2007 roku obie strony otwarcie przyznały, że jest to kwestia, która w sposób znaczący utrudnia wzajemny dialog, zwłaszcza że tarcza antyrakietowa miała być oparta przede wszystkim na systemie amerykańskim¹¹⁴⁸. Ostatecznie w 2009 roku zrezygnowano z budowy instalacji antyrakietowych¹¹⁴⁹. Wybory parlamentarne w 2007 roku oraz rządy koalicji Platformy Obywatelskiej oraz Polskiego Stronnictwa Ludowego doprowadziły do ocieplenia relacji na linii Moskwa-Warszawa. Można wręcz zaobserwować, że w latach 2008-2009 prowadzone były działania ze strony polskiej polegające na próbie poprawy relacji polsko-rosyjskich¹¹⁵⁰, co jednak było niezwykle skomplikowane wobec wybuchu wojny rosyjsko-gruzińskiej (2008)¹¹⁵¹. Wywołany w przewarżającej mierze przez rząd w Tbilisi konflikt zakończył się przegraną Gruzji oraz wojskowym i propagandowym zwycięstwem Kremla¹¹⁵². Wojna toczona pomiędzy oboma państwami negatywnie wpłynęła na relacje na linii Warszawa-Moskwa wobec silnego zaangażowania po stronie gruzińskiej przez Polskę. Ponadto, jak pisze R. Zięba, przyniosła „uszczerbek prestiżowi Polski, jako państwu zdolnemu do nieodpowiedzialnych ‘kozackich’ zachowań”¹¹⁵³. 2008 rok to również koniec prezydentury W. Putina oraz wybór na jego miejsce D. Miedwiediewa, który,

¹¹⁴⁵ M. Stolarczyk: *Rosja w polityce zagranicznej...*, s. 60.

¹¹⁴⁶ R. Lisiakiewicz: *Polityka Rosji wobec Polski za prezydentury Władimira Putina (2000-2008)*. Toruń 2011, s. 136-139.

¹¹⁴⁷ M. Sabat: *Stosunki polsko-rosyjskie. Rozbieżności interesów strategicznych*. W: *Polityka zagraniczna Federacji Rosyjskiej. Wybrane aspekty stosunków z Polską, Ukrainą i Białorusią*. Red. L. Zyblikiewicz, M. Czajkowski, P. Bajor. Kraków 2010, s. 125-127.

¹¹⁴⁸ Biuro Bezpieczeństwa Narodowego: *"Spodziewaliśmy się decyzji o przesunięciu programu w czasie, a nie całkowitej jego likwidacji."*. <https://www.bbn.gov.pl/pl/wydarzenia/1882,quotSpodziewalismy-sie-decyzji-o-przesuniecie-programu-w-czasie-a-nie-calkowitej.html> (dostęp: 22.01.2023).

¹¹⁴⁹ A. Bryć: *Stosunki Federacji Rosyjskiej...* W: *Polityka zagraniczna Rosji*. Red. S. Bieleń, M. Raś. Warszawa 2008, s. 86.

¹¹⁵⁰ K. Fedorowicz: *Polityka Polski wobec Rosji...*, s. 150-154.

¹¹⁵¹ M. Stolarczyk: *Rosja w polityce zagranicznej...*, s. 206-217.

¹¹⁵² R. Zięba: *Współczesne stosunki polsko-rosyjskie: uwarunkowania, problemy, implikacje*. „Przegląd Politologiczny” 2011, nr 3 (2011), s. 41-42.

¹¹⁵³ Ibidem, s. 59.

będąc protegowanym ustępującego na najbliższe 4 lata prezydenta, kontynuował w znacznym zakresie prowadzoną przez niego politykę zagraniczną, jak również umocnił wpływy w państwie swojego poprzednika.

Reasumując powyższe rozważania należy wskazać na kilka elementów charakteryzujących stosunki polsko-rosyjskie w latach 1992-2009. Na początku lat dziewięćdziesiątych XX wieku Rosja stanowiła niezwykle ważny kierunek w polityce zagranicznej Polski, co jednak nie występowało w przypadku polityki zagranicznej Kremla. Poruszane były kwestie związane ze wspólnym dziedzictwem historycznym (niezwykle trudnym dla strony Polskiej) oraz wycofaniem wojsk radzieckich. Stan ten uległ zmianie wobec planów rozszerzenia NATO na Wschód i włączenia w poczet członków Sojuszu byłych państw satelickich ZSRR w tym Polski. Tendencje rosyjskiej polityki zagranicznej sprowadzające się do reintegracji obszaru poradzieckiego skutkowały uznaniem Rosji przez rząd w Warszawie jako podstawowego zagrożenia dla bezpieczeństwa narodowego, co determinowało wzajemne relacje przez najbliższe lata. W związku z integracją Polski ze strukturami NATO oraz Unii Europejskiej i aktywnym wpływaniem na prowadzoną przez te organizacje międzynarodowe polityką wschodnią, Kreml podejmował działania mające na celu dyskredytowanie Polski na arenie międzynarodowej oraz podważanie jej wizerunku jako państwa stabilnego oraz dojrzałego. Działania Polski sprowadzające się do wspierania procesów demokratycznych na terenach były republik ZSRR, przede wszystkim Ukrainy, Białorusi i Gruzji, doprowadziły do zaostrzenia wzajemnych relacji, gdyż Kreml postrzegał działania Warszawy jako wrogą ingerencję w wyłączną strefę wpływów Federacji Rosyjskiej¹¹⁵⁴. Stosunki polsko-rosyjskie u progu drugiej dekady XXI wieku były niezwykle trudne, toteż zaobserwować można wiele kwestii spornych, zarówno nowych jak i starszych, lecz nadal nierozwiązanych, a najważniejsze z nich zostaną omówione w dalszej części pracy.

5.4. Cele polityki zagranicznej Federacji Rosyjskiej wobec Polski w latach 2010-2022

Omawiając cele polityki zagranicznej Federacji Rosyjskiej wobec Polski w latach 2010-2022 należy dokonać tego poprzez scharakteryzowanie oficjalnych rządowych dokumentów w tym przedmiocie. Oczywiście akty te stanowią jedynie ogólnikowe założenia, które nie korespondują w pełni z instrumentami stosowanym przez Kreml, gdyż pozostają one w części niejawne. Dokumenty te są natomiast pomocne w takim zakresie, iż określają podstawy

¹¹⁵⁴ Zobacz szerzej: K. Fedorowicz: *Polityka Polski wobec Rosji...*, s. 160-162.

prowadzonej przez Rosję polityki zagranicznej oraz pozwalają na wyprowadzenie celów jakie będzie realizować. Kluczowe pozostają tutaj Koncepcje polityki zagranicznej Federacji Rosyjskiej, a w zakresie omawianej cezury czasowej funkcjonowały łącznie 3 jej wersje z 2008, 2013 i 2016 roku oraz jedna aktualizacja z 2021 roku. Jak już wskazano wielokrotnie, Polska nie pozostaje istotnym kierunkiem rosyjskiej polityki zagranicznej, co ma swoje odbicie również we wskazanych wyżej dokumentach. Nie oznacza to jednak, że rząd w Warszawie jest traktowany marginalnie, gdyż istotnymi partnerami dla Rosji pozostają NATO oraz Unia Europejska, których to organizacji członkiem pozostaje Polska. Ponadto sam region Europy Środkowo-Wschodniej również jest w zainteresowaniu Kremla. Uznać więc należy, że stosunki z Polską, jak i cele realizowanej wobec niej polityki zagranicznej są niezwykle często prezentowane przez pryzmat powyższych podmiotów i regionu¹¹⁵⁵.

Pierwszy z dokumentów, przyjęty w 2008 roku w duchu wzrostu znaczenia Rosji na arenie międzynarodowej wobec uzyskania statusu mocarstwa energetycznego, niezmiennie dawał priorytet obszarowi poradzieckiemu oraz Wspólnocie Niepodległych Państw¹¹⁵⁶. Ponadto silnie akcentowano również potrzebę prowadzenia przyjaznych stosunków z Unią Europejską, która jest głównym partnerem handlowym i gospodarczym Rosji. Wskazano, że w interesie Rosji leży uzgodnienie z Brukselą traktatu o strategicznym partnerstwie, który ustanawiałby specjalne oraz najbardziej zaawansowane formy wzajemnej i sprawiedliwej współpracy. Kluczowe pozostaje również nawiązanie strategicznej współpracy z NATO w oparciu o równoprawne partnerstwo z wykorzystaniem Rady NATO-Rosja. Zaznaczono jednak, że Kreml sprzeciwia się rozszerzaniu Sojuszu na Wschód¹¹⁵⁷. Można zauważyć, że ostatnia z wymienionych kwestii stoi w sprzeczności z polityką zagraniczną prowadzoną przez Warszawę, której długofalowym celem jest wzmacnianie związków z Zachodem, takich państw jak Ukraina czy Gruzja. Ze strony Kremla popłynął zatem jasny sygnał, że będzie on sprzeciwiał się takim działaniom.

Druga z koncepcji, przyjęta w 2013 roku, była już wynikiem innych doświadczeń Rosji w zakresie występujących w ubiegłych latach wydarzeń na arenie międzynarodowej. Było to przede wszystkim pokłosie wojny gruzińsko-rosyjskiej z 2008 roku, jak i sygnalizowanie przygotowań to rozpoczęcia agresywnej polityki Kremla na obszarze poradzieckim. Zauważyć bowiem należy, że koncepcja została zatwierdzona przez W. Putina w lutym 2013 roku, a więc

¹¹⁵⁵ M. Stolarczyk: *Rosja w polityce zagranicznej Polski...*, s. 71-73.

¹¹⁵⁶ J. Diec: *Geostrategiczny wybór...*, s. 179-181.

¹¹⁵⁷ *Koncepcja polityki zagranicznej Federacji Rosyjskiej zatwierdzona 15 lipca 2008 roku*. Moskwa 2008. <http://kremlin.ru/acts/news/785> (dostęp: 24.10.2022).

na rok przed rozpoczęciem działań, których skutkiem była aneksja przez Rosję Półwyspu Krymskiego. Wskazano na potrzebę integracji i utrzymywania przyjaznych stosunków z Unią Europejską, jednakże nie użyto już określenia o strategicznym partnerstwie. W tym kontekście dokument mówi o potrzebie nawiązania bliskich relacji z takimi państwami jak Niemcy, Francja, Włochy czy Holandia. Nie ma tutaj żadnych wzmianek odnoszących się do Polski czy chociażby regionu Europy Środkowo-Wschodniej¹¹⁵⁸. Ponadto w kontekście NATO podkreślono sprzeciw wobec jego rozszerzania się, przez co należy rozumieć nie tylko przyjmowanie w poczet członków nowych państw, ale również ekspansję infrastruktury militarnej organizacji, między innymi na wschodniej flance Sojuszu, a więc również w Polsce¹¹⁵⁹. Można zauważyć, że wyrażanie sprzeciwu w tym zakresie jest nieodłącznym elementem każdej z wersji koncepcji, jednakże na przestrzeni lat przekaz ten stawał się coraz bardziej jednoznaczny i kategoryczny. Celem Rosji jest bowiem ograniczanie obecności militarnej NATO w państwach będących w przeszłości w strefie wpływów Związku Radzieckiego. Ponadto Rosja przedstawia Zachód jako źródło problemów zarówno w zakresie rosnącej destabilizacji systemu międzynarodowego jak i globalnego kryzysu gospodarczego¹¹⁶⁰. Kreml z kolei nie pozostanie bierny wobec tych działań, co będzie objawiać się w podjęciu odpowiednich środków zapobiegawczych¹¹⁶¹. Minister spraw zagranicznych S. Ławrow wyraził się dość precyzyjnie w tym zakresie w 2013 roku wskazując, że w koncepcji sformułowany został „jasny i spójny system poglądów, skoncentrowany na rozwiązywaniu coraz bardziej skomplikowanych problemów współczesnego świata”¹¹⁶².

W kolejnej wersji koncepcji z 2016 roku nadal nie pojawiło się jakiegokolwiek bezpośrednie nawiązanie do Warszawy. Można jednak zauważyć, że jest to wynikiem chęci marginalizowania Polski oraz jej pozycji na arenie międzynarodowej i ukazywania jako państwa, które nie jest przychylne w jakimkolwiek stopniu Kremlowi, jak również państwa z którym nawiązanie bliższego porozumienia nie jest możliwe¹¹⁶³. W koncepcji daje się zauważyć aspiracje Kremla do odgrywania roli ważnego gracza w sprawach bezpieczeństwa międzynarodowego, a istotnym przy tym ma być poszukiwanie możliwości współpracy

¹¹⁵⁸ J. Diec: *Geostrategiczny wybór...*, s. 182.

¹¹⁵⁹ *Koncepcja polityki zagranicznej Federacji Rosyjskiej zatwierdzona 12 lutego 2013 roku*. Moskwa 2013. <http://www.pircenter.org/media/content/files/9/13617765900.pdf> (dostęp: 24.10.2022).

¹¹⁶⁰ Ośrodek Studiów Wschodnich: *Koncepcja polityki zagranicznej Federacji Rosyjskiej*. <https://www.osw.waw.pl/pl/publikacje/analizy/2013-02-20/koncepcja-polityki-zagranicznej-federacji-rosyjskiej> (dostęp: 23.01.2023).

¹¹⁶¹ *Koncepcja polityki zagranicznej Federacji Rosyjskiej zatwierdzona 12 lutego 2013 roku*. Moskwa 2013. <http://www.pircenter.org/media/content/files/9/13617765900.pdf> (dostęp: 24.10.2022).

¹¹⁶² J. M. Fiszer: *Zadania i cele polityki zagranicznej Władimira Putina*. „Myśl Ekonomiczna i Polityczna” 2016, nr 1 (52), s. 182.

¹¹⁶³ S. Gardocki: *Polityka zagraniczna Rosji...*, s. 16.

z nowym prezydentem USA, D. Trumpem. Widoczne jest również stosunkowe zmarginalizowanie relacji z Unią Europejską względem poprzednich wersji koncepcji i sprowadzenie ich do pragmatycznych stosunków handlowych i gospodarczych¹¹⁶⁴. Takie nastawienie wynika z pewnością z obwinienia zarówno Unii jak i NATO o stworzenie systemowych problemów w regionie euroatlantyckim w wyniku prowadzenia polityki ekspansywnej oraz przeciwstawnej do interesów Rosji¹¹⁶⁵. W listopadzie 2021 roku Kreml dokonał aktualizacji przyjętych założeń w szczególności poprzez zapowiedzenie zaostrzenia polityki bezpieczeństwa wobec NATO. Tym samym należy spodziewać się zwiększonej aktywności militarnej Rosji w najbliższych latach. W odniesieniu do Polski, skrytykowano działania rządu w Warszawie podejmowane w związku z kryzysem uchodźczym na granicy polsko-białoruskiej. Podkreślono również konieczność obrony rosyjskich wartości, co z pewnością będzie prowadziło do eskalacji prowadzonej przez Kreml polityki historycznej wobec Polski¹¹⁶⁶.

W kontekście celów rosyjskiej polityki zagranicznej wobec Polski nie bez znaczenia pozostaje Strategia Bezpieczeństwa Narodowego Federacji Rosyjskiej z 2021 roku, w której niezwykle wiele miejsca poświęcono polityce bezpieczeństwa prowadzonej przez USA, jak również NATO¹¹⁶⁷. Choć zasadnicze założenia nie uległy większym zmianom wobec wersji strategii z 2015 roku, to w jeszcze większym stopniu podkreślono zagrożenia związane z agresywną polityką Zachodu oraz koniecznością podjęcia działań zapobiegawczych. Wymieniono w tym zakresie obowiązek zapewnienia przez Kreml bezpieczeństwa informacyjnego oraz ochrony tradycyjnych rosyjskich wartości moralno-kulturowych, jak i pamięci historycznej¹¹⁶⁸. W odniesieniu do Polski należy zauważyć, że kwestie związane z zaszłościami historycznymi oraz bezpieczeństwem Europy Środkowo-Wschodniej od lat pozostają tematem spornym w stosunkach polsko-rosyjskich, a zatem formułowane przez Kreml deklaracje należy postrzegać jako adresowane wobec Warszawy.

¹¹⁶⁴ A. M. Dyner: *Nowa Koncepcja rosyjskiej polityki zagranicznej*. „Biuletyn Polskiego Instytutu Spraw Międzynarodowych” 2017, nr 1 (1443) <https://pism.pl/upload/images/artykuly/legacy/files/22686.pdf> (dostęp: 23.01.2023).

¹¹⁶⁵ *Koncepcja polityki zagranicznej Federacji Rosyjskiej zatwierdzona 30 listopada 2016 roku*. Moskwa 2016. <http://static.kremlin.ru/media/acts/files/0001201612010045.pdf> (dostęp: 23.01.2023).

¹¹⁶⁶ A. M. Dyner: *Zaktualizowane kierunki polityki zagranicznej Rosji*. „Komentarz PISM” 2021, nr 88/2021 <https://pism.pl/webroot/upload/files/Komentarz%20PISM%20nr%2088-2021.pdf> (dostęp: 11.02.2023).

¹¹⁶⁷ *Strategia Bezpieczeństwa Narodowego Federacji Rosyjskiej zatwierdzona 2 lipca 2021 roku*. Moskwa 2021. https://poland.mid.ru/pl/press-centre/news/strategia_bezpiecze_stwa_narodowego_federacji_rosyjskiej/ (dostęp: 23.01.2023).

¹¹⁶⁸ Ośrodek Studiów Wschodni: *Wróg z Zachodu. Nowa rosyjska strategia bezpieczeństwa*. <https://www.osw.waw.pl/pl/publikacje/analizy/2021-07-08/wrog-z-zachodu-nowa-rosyjska-strategia-bezpieczenstwa> (dostęp: 23.01.2023).

Reasumując powyższe rozważania w zakresie podstawowych założeń prowadzonej przez Kreml polityki zagranicznej wobec Polski należy w pierwszej kolejności podkreślić, że Warszawa nie zajmuje w ich ramach istotnego miejsca. Odniesienia do Polski mają przede wszystkim charakter pośredni, co oznacza artykułowanie celów przez pryzmat takich organizacji jak NATO czy Unia Europejska. Brak uwzględnienia Polski w rosyjskich dokumentach nie wynika wyłącznie z małego znaczenia Warszawy w stosunkach międzynarodowych, ale przede wszystkim z chęci marginalizowania jej roli i pozycji na arenie międzynarodowej. Celem Rosji jest bowiem w jak największym stopniu umniejszanie działań Polski polegających na kreowaniu polityki wschodniej, prowadzanej przez Sojusz Północnoatlantycki oraz Brukselę. Polska jako państwo nieprzychylne Kremlowi nie jest przez niego traktowana chociażby jako ważny partner na arenie międzynarodowej, przy czym Kreml obwinia o ten stan Polskę¹¹⁶⁹.

Omawiane zagadnienia pozostają w bezpośrednim związku z kwestiami spornymi występującymi w stosunkach polsko-rosyjskich jak: polityka historyczna, dywersyfikacja źródeł energii, polityka bezpieczeństwa w Europie Środkowo-Wschodniej, polityka bezpieczeństwa NATO, katastrofa samolotu rządowego z Prezydentem Rzeczypospolitej Polskiej w Smoleńsku, aneksja Półwyspu Krymskiego i wojna w Ukrainie oraz program Partnerstwa Wschodniego¹¹⁷⁰. Dokonując analizy polityki zagranicznej Rosji wobec Polski przeprowadzonej we wcześniejszych częściach pracy, należy wskazać na następujące cele główne realizowane przez Kreml:

1. Kreowanie negatywnego wizerunku Polski oraz marginalizowanie jej pozycji na arenie międzynarodowej, a w szczególności w Europie Środkowo-Wschodniej.
2. Osłabianie polskich struktur wewnątrzpaństwowych oraz pogłębianie istniejących w państwie podziałów społecznych i politycznych.

¹¹⁶⁹ Dla przykładu na oficjalnej stronie internetowej Ambasady Federacji Rosyjskiej w Polsce zamieszczono następujące sformułowanie: „Do 2013 r. regularnie odbywały się konsultacje międzyresortowe na szczeblu wiceministrów i dyrektorów departamentów ministerstw spraw zagranicznych. Intensywność kontaktów dwustronnych gwałtownie się zmniejszyła w 2014 roku w związku z zaostreniem się kryzysu ukraińskiego i decyzją państw Zachodu o ograniczeniu stosunków z Rosją. Doprowadziło to, między innymi, do zaprzestania działalności podstawowych mechanizmów rosyjsko-polskiego współdziałania, w tym Komisji międzyrządowej ds. współpracy gospodarczej, Forum regionów (współprzewodniczący – głowy izb wyższych Rosji i Polski), Komitetu ds. strategii rosyjsko-polskiej współpracy pod przewodnictwem ministrów spraw zagranicznych, Rosyjsko-Polskiego forum społeczności, Grupy do spraw trudnych wynikających z historii stosunków rosyjsko-polskich”. Źródło: Oficjalna strona internetowa Ambasady Federacji Rosyjskiej w Polsce: *Rosja-Polska. Dialog polityczny*. https://poland.mid.ru/pl/rossiya_polsha/rossijsko_polskie_otnosheniya_i_voprosy_mezhdunarodnoj_bezopasnosti/politicheskij_dialog/ (dostęp: 23.01.2025).

¹¹⁷⁰ Zobacz szerzej: 5.5. *Stosunki polsko-rosyjskie w kontekście występujących głównych kwestii spornych w latach 2010-2022*.

3. Oddziaływanie na struktury i członków Unii Europejskiej oraz Sojuszu Północnoatlantyckiego w celu jak największego ograniczenia roli Polski w prowadzonej przez te organizacje polityce wschodniej (wobec Rosji).
4. Prowadzenie prorosyjskiej polityki historycznej w stosunkach polsko-rosyjskich w celu przedstawienia i utrwalenia rosyjskiego punktu widzenia na historię w Polsce i na świecie.
5. Ograniczanie działań Polski prowadzonych w zakresie wspierania i utrwalania procesów demokratycznych w państwach poradzieckich oraz zbliżania ich z Zachodem.
6. Prowadzenie polityki energetycznej mającej na celu uzależnienie Polski od rosyjskich źródeł energii (surowców energetycznych) oraz ograniczanie działań podejmowanych przez Polskę w celu nawiązania współpracy z alternatywnymi dostawcami surowców energetycznych.
7. Rozpowszechnianie rosyjskiego punktu widzenia na sprawy międzynarodowe oraz ideologii rosyjskiego świata (*ruskij mir*) poprzez promocję rosyjskiej kultury, wartości, poglądów, historii oraz ideologii.
8. Przeciwdziałanie polityce bezpieczeństwa i obrony NATO oraz Polski, zakładającej rozmieszczenie infrastruktury militarnej Sojuszu w Europie Środkowo-Wschodniej.

5.5. Stosunki polsko-rosyjskie w kontekście występujących głównych kwestii spornych w latach 2010-2022

Wreszcie należy omówić kwestie sporne występujące w stosunkach polsko-rosyjskich. Nie są one wskazane enumeratywnie, jednakże na podstawie wcześniejszych rozważań można wyszczególnić najważniejsze z nich takie jak: polityka historyczna, dywersyfikacja źródeł energii, polityka bezpieczeństwa w Europie Środkowo-Wschodniej, polityka bezpieczeństwa NATO, katastrofa samolotu rządowego z Prezydentem Rzeczypospolitej Polskiej w Smoleńsku, aneksja Półwyspu Krymskiego i wojna w Ukrainie oraz program Partnerstwa Wschodniego.

W odniesieniu do stosunków polsko-rosyjskich można zauważyć, że liczni badacze wypowiadają się na temat polityki zagranicznej Rosji przede wszystkim negatywnie, nie czyniąc jednocześnie podobnych rozważań w przedmiocie realizacji polskich interesów na arenie międzynarodowej. Tym samym autor w niniejszym podrozdziale podjął próbę przedstawienia kwestii spornych na linii Moskwa-Warszawa przy uwzględnieniu interesów obu państw. Należy bowiem zgodzić się ze stwierdzeniem jakie poczynił S. Bielen pisząc, że w „sprawach rosyjskich potrzeba trochę więcej empatii, czyli wczucia się w położenie Rosjan,

w ich świadomość i złożone dziedzictwo historyczne, które – podobnie jak w przypadku Polaków – determinują odczucia i zachowania”¹¹⁷¹.

5.5.1. Polityka historyczna

Polityka historyczna stanowi najważniejszą kwestię sporną występującą w stosunkach polsko-rosyjskich. W ramach wzajemnych relacji Kremla i Warszawy można wskazać na wiele spraw które dzielą, jednakże żadna z nich nie wywołuje tylu emocji oraz nie traci na aktualności jak właśnie zagadnienia dotyczące historii. Wspólne dziedzictwo Polski i Rosji nie należy do łatwych i trzeba zauważyć, że wywołuje wiele silnych emocji szczególnie w polskim społeczeństwie. Można ponownie przytoczyć tutaj pogląd jaki wyraził M. Stolarczyk pisząc, że w „ostatnich stuleciach to Polska była przedmiotem ekspansji i agresji ze strony Rosji, a nie odwrotnie, tym samym w postrzeganiu Polaków i Polski przez Rosjan kwestie pamięci historycznej i obciążeń z tym związanych nie odgrywały większego znaczenia, w przeciwieństwie do wpływu pamięci historycznej Polaków na postrzeganie Rosjan i Rosji. Świadomość historyczna Rosjan w relacjach polsko-rosyjskich koncentruje się przede wszystkim na: przekonaniu o braku pamięci i wdzięczności Polaków za wyzwolenie Polski spod okupacji niemieckiej przez Armię Czerwoną; burzeniu pomników ku czci poległych żołnierzy armii radzieckiej; wojnie polsko-bolszewickiej w latach 1919-1920 i zmarłych w polskiej niewoli żołnierzach armii bolszewickiej; dwuletniej okupacji Moskwy przez Polaków w latach 1610-1612”¹¹⁷². Podczas gdy polityka historyczna ma kluczowe znaczenie dla Polski, wydaje się, że w Rosji kwestie te już dawno przestały mieć tak doniosły wydźwięk w związku z zainteresowaniem Polską przede wszystkim w kontekście partnerstwa gospodarczego¹¹⁷³. Co więcej, kwestie historyczne w stosunkach polsko-rosyjskich są zdecydowanie częściej poruszane w polskiej przestrzeni medialnej aniżeli w Rosji, co również pokazuje stosunek stron do tej kwestii¹¹⁷⁴.

Choć, jak wskazano, wspólna historia Polski i Rosji jest pełna bolesnych i tragicznych przeżyć, to należy zauważyć, że najwięcej uwagi przywiązuje się do przyczyn wybuchu II wojny światowej oraz ofiar poniesionych przez Armię Czerwoną i pamięci z tym związanej

¹¹⁷¹ S. Bieleń: *Tożsamość międzynarodowa...*, s. 14.

¹¹⁷² M. Stolarczyk: *Rosja w polityce zagranicznej Polski...*, s. 68-69.

¹¹⁷³ A. de Lazari: *Wzajemne uprzedzenia Polaków i Rosjan*. W: *Katalog wzajemnych uprzedzeń Polaków i Rosjan*. Red. A. de Lazari. Warszawa 2006, s. 20.

¹¹⁷⁴ M. Moliński: *Refleksje nad wzajemnym postrzeganiem stosunków Polska-Rosja*. W: *Dwie dekady transformacji w Europie Środkowej i Wschodniej 1989–2009*. Red. A. Stępień-Kuczyńska, M. Potz, M. Słowikowski. Toruń 2011, s. 92.

– po stronie rosyjskiej oraz kwestii odpowiedzialności za wybuch II wojny światowej, jej skutków oraz zbrodni katyńskiej – po stronie polskiej. Podstawową kwestią sporną w prowadzonej przez Kreml i Warszawę polityce historycznej są wydarzenia związane z wybuchem i zakończeniem II wojny światowej, przy czym Polska podnosi również temat zbrodni katyńskiej. II wojna światowa była konfliktem trwającym w latach 1939-1945, a w odniesieniu do relacji polsko-rosyjskich była związana z agresją ZSRR na Polskę rozpoczętą 17 września 1939 roku. Co do tego tematu stanowisko Rosji pozostaje w zasadzie niezmiennie na przestrzeni ostatnich lat. Rosja nie potrafi zgodzić się z poglądem mówiącym o współodpowiedzialności ZSRR za wybuch wojny, powołując się na fakt, iż została zaatakowana przez Niemcy. Co więcej, w historiografii radzieckiej wybuch II wojny światowej datowano niejednokrotnie na 22 czerwca 1941 roku¹¹⁷⁵. W. Putin, pełniąc w 2009 roku urząd premiera Federacji Rosyjskiej, z okazji siedemdziesiątej rocznicy wybuchu II wojny światowej skierował do Polaków list opublikowany w Gazecie Wyborczej¹¹⁷⁶. Stwierdził w nim, że bez wątplenia można potępić pakt Ribbentrop-Mołotow z 1939 roku, jednakże nie można uznać go za wyłączną przyczynę rozpoczęcia II wojny światowej. Wskazał, iż granice Europy zaczęły być burzone na długo przed 1 września 1939 roku w wyniku anszlusu Austrii oraz zajęcia Czechosłowacji, co było możliwe dzięki ustaleniom podjętym na konferencji w Monachium w 1938 roku. Zauważył, że Rosja formalnie potępiła wskazany wyżej pakt, czego nie uczyniły inne państwa, jak również, że naród rosyjski rozumie naród polski w sprawie zbrodni katyńskiej. Zauważył, że cmentarze w Katyniu i Miednoje wraz z wzięciem do niewoli wielu czerwonoarmistów podczas wojny polsko-bolszewickiej w 1920 roku, powinny być symbolem wspólnego żalu i pojednania. Wreszcie podkreślił, że ponad 600 tysięcy żołnierzy radzieckich spoczywa na ziemiach polskich, a ponad połowa wszystkich ofiar II wojny światowej to obywatele Związku Radzieckiego¹¹⁷⁷. Jest to oczywiście oficjalny przekaz rządowy, gdyż jednocześnie w mediach rosyjskich, również tych związanych z Kreml, co roku w każdą ważną rocznicę (przeważnie rozpoczęcia i zakończenia II wojny światowej), ale również na co dzień, pojawiają się wiadomości prasowe pozostające w sprzeczności z faktami historycznymi. Można wskazać na setki bądź nawet tysiące takich przykładów, jak chociażby wiadomości o pomocy humanitarnej niesionej przez Armię Czerwoną w Polsce¹¹⁷⁸, tezie, że co piąty czołg

¹¹⁷⁵ T. A. Kisielewski: *Schylek Rosji*. Poznań 2007, s. 189.

¹¹⁷⁶ Gazeta Wyborcza: *List Putina do Polaków - pełna wersja*. <https://wyborcza.pl/7,75399,6983945,list-putina-do-polakow-pelna-wersja.html> (dostęp: 24.01.2023).

¹¹⁷⁷ K. Fedorowicz: *Polityka Polski wobec Rosji...*, s. 154-155.

¹¹⁷⁸ Sputnik News Polska: *MO Rosji: Armia Czerwona oddawała Polsce swój chleb*. <https://pl.sputniknews.com/20210509/mo-rosji-armia-czerwona-zsrr-polska-zywnosc-sputnik-14237380.html> (dostęp: 25.01.2023); Sputnik News Polska: *Rosja odtajniła dokumenty z wiosny 1945 roku. Nie wszystkim w Polsce to się podoba*.

niemiecki biorący udział w ataku na ZSRR był produkcji czeskiej¹¹⁷⁹, wyzwolenia Polski we wrześniu 1939 roku¹¹⁸⁰, jak i ogólne sformułowania o wyzwoleniu Europy Środkowo-Wschodniej spod panowania nazistów¹¹⁸¹. I choć co do zasady wiadomości takie zawierają elementy prawdziwe, zgodne z rzeczywistymi wydarzeniami, to jednak niosą ze sobą silny ładunek dezinformujący, gdyż wypaczają fakty historyczne, przytaczając wyłącznie te pozytywne dla wizerunku Armii Czerwonej, jak również deprecjonując udział ZSRR w rozpoczęciu II wojny światowej. Jako inny przykład można wskazać na działania Kremla z 2021 roku, kiedy prezydent Rosji W. Putin podpisał ustawę zakazującą zrównywania publicznego roli ZSRR i Niemiec w II wojnie światowej¹¹⁸². W rosyjskich przekazach rządowych oraz medialnych nie znajdziemy informacji o skutkach wyzwolenia Europy Środkowo-Wschodniej spod niemieckiej okupacji, czy też negatywnych ocen dla działań Armii Czerwonej. Dla Polski natomiast szczególnie istotna pozostaje sprawa zbrodni katyńskiej z 1941 roku, w wyniku której na rozkaz J. Stalina wymordowano prawie 22 tysięcy osób (znana liczba ofiar), polskich oficerów, urzędników, policjantów oraz inteligencji państwa polskiego. Choć więźnik Radziecki w 1990 przyznał się do dokonania mordu przez NKWD, a w 1992 roku ówczesny prezydent Federacji Rosyjskiej B. Jelcyń przeprosił Polaków za dokonaną zbrodnię, to kwestia ta nadal pozostaje aktualna, wobec wielu wciąż nieustalonych okoliczności i faktów¹¹⁸³.

Warszawa, dla której kwestie historyczne zawsze pozostawały istotne w prowadzonej polityce zagranicznej wobec Rosji, podejmowała próby łagodzenia wzajemnych relacji na tej płaszczyźnie. Przykładem jest zaproszenie ówczesnego premiera Federacji Rosyjskiej W. Putina na obchody siedemdziesiątej rocznicy wybuchu II wojny światowej 1 września 2009 roku. I choć na uroczystości zaproszono również innych polityków takich jak chociażby ówczesną kanclerz Niemiec A. Merkel, to jednak rosyjski premier stał się głównym punktem

<https://pl.sputniknews.com/20210513/rosja-odtajnila-dokumenty-z-wiosny-1945-roku-nie-wszystkim-w-polsce-to-sie-podoba-Sputnik-14268911.html> (dostęp: 25.01.2023); Sputnik News Polska: „*Wagony cennych leków*”: MO Rosji o pomocy wyzwolonej Polsce. <https://pl.sputniknews.com/20210507/mo-rosji-o-pomocy-wyzwolonej-polsce-sputnik-14233563.html> (dostęp: 25.01.2023).

¹¹⁷⁹ Sputnik News Polska: *Operacja Barbarossa. Co piąty czołg podczas hitlerowskiego ataku na ZSRR był produkcji czeskiej*. <https://pl.sputniknews.com/20210622/operacja-barbarossa-niemcy-czolgi-przemysl-zbrojeniowy-czechoslowacja-sputnik-14395140.html> (dostęp: 25.01.2023).

¹¹⁸⁰ Sputnik News Polska: *17 września po białorusku*. <https://pl.sputniknews.com/20210916/17-wrzesnia-po-bialorusku-16100435.html> (dostęp: 25.01.2023).

¹¹⁸¹ Russia Today: *West lying about WWII – Russia*. <https://www.rt.com/russia/547663-ussr-falsly-compated-nazi-germany/> (dostęp: 25.01.2023).

¹¹⁸² Sputnik News Polska: *Putin podpisał ustawę o zakazie zrównywania roli ZSRR i Niemiec w II wojnie światowej*. <https://pl.sputniknews.com/20210701/putin-podpisal-ustawe-o-zakazie-zrownywania-roli-zsrr-i-niemiec-w-ii-wojnie-swiatowej-15352456.html> (dostęp: 25.01.2023).

¹¹⁸³ Instytut Pamięci Narodowej: *Katyń 1940. Przyznanie się Rosji*. <https://katyn.ipn.gov.pl/kat/histori/walka-o-prawde/pryznanie-sie-rosji> (dostęp: 25.01.2023).

uroczystości, wobec szerokiej polemiki polityków i historyków na temat genezy rozpoczęcia II wojny światowej. Nie obyło się również bez prowokacji ze strony rosyjskiej. Im bliżej było do daty obchodów, tym częściej w rosyjskich mediach pojawiały się wiadomości przedstawiające genezę wybuchu II wojny światowej w niekorzystnym świetle dla Polski bądź też wypaczające powszechnie uznane fakty historyczne¹¹⁸⁴.

Dokonując rozważań w omawianym zakresie należy również zwrócić uwagę na termin *polityka historyczna*, który swoją genezę wywodzi z polityki niemieckiej prowadzonej w latach osiemdziesiątych XX wieku. S. Bieleń definiuje ją jako element marketingu politycznego, z kolei E. Ponczek jako sposób prowadzenia polityki, natomiast A. Miller uważa, że jest to zestaw narzędzi, którymi politycy starają się uwiarygodnić interpretacje wydarzeń historycznych. W jednym natomiast badacze pozostają całkowicie zgodni, wskazując, że polityka historyczna nie zajmuje się historią (czym zajmują się historycy), a wyłącznie interpretacją wydarzeń dla uwiarygodnienia określonej myśli politycznej¹¹⁸⁵. Swoją politykę historyczną prowadzi również Federacja Rosyjska. II wojna światowa znana w tym państwie pod nazwą Wielkiej wojny ojczyźnianej stanowi narzędzie ideologizacji społeczeństwa rosyjskiego jak i służące wzmocnieniu pozycji Rosji na arenie międzynarodowej. Konsolidacja społeczeństwa ma na celu wytworzenie przekonania o dziejowej roli państwa rosyjskiego, które oddając wielką ofiarę światu, wyzwoliło go spod panowania hitlerowskich Niemiec. Rosja prowadzi działania zmierzające do budowania wspólnoty narodowej, jak i wspólnoty z państwami byłego Związku Radzieckiego, które również wniosły swój istotny wkład w zwycięstwo podczas II wojny światowej. Armia Czerwona jest przedstawiana jako wyzwolicielka Europy spod okupacji nazistów, a ZSRR jako państwo całkowicie nieodpowiedzialny za wybuch II wojny światowej, w przeciwieństwie do Polski, która jest oskarżana o współpracę z III Rzeszą. Przekazy propagandowe są kolportowane przede wszystkim przez takie portale jak Sputnik News oraz Russia Today¹¹⁸⁶. Ważnym elementem rosyjskiej polityki historycznej jest obchodzony 4 listopada Dzień Jedności Narodowej, upamiętniający odbicie w 1612 roku Kremla z rąk wojsk polskich. Tym samym rosyjska

¹¹⁸⁴ K. Fedorowicz: *Polityka Polski wobec Rosji...*, s. 154.

¹¹⁸⁵ A. Barynkin: *Kwestie polityki historycznej we współczesnych stosunkach polsko-rosyjskich*. W: *Polska i Rosja w zmieniającej się Europie*. Red. K. A. Woźtaszczyk, I. N. Novikova. Warszawa 2022, s. 290-291.

¹¹⁸⁶ J. Darczewska: „Wojny pamięci”: *historia, polityka i służby specjalne Federacji Rosyjskiej*. „Przegląd Bezpieczeństwa Wewnętrznego” 2019, nr 20/19, s. 13-37; A. M. Dynier: *II wojna światowa w polityce zagranicznej Rosji*. „Biuletyn Polskiego Instytutu Spraw Międzynarodowych” 2020, nr 12 (1942). <https://www.pism.pl/upload/images/artykuly/e5d8a54c-6ead-4f12-a875-3dc94c043bc7//1580203445419.pdf> (dostęp: 25.01.2023)

polityka historyczna jest wykorzystywana w ramach prowadzonej wobec Polski wojny informacyjnej¹¹⁸⁷.

Kwestie związane z zachowaniem wspólnego dziedzictwa historycznego zostały przez Polskę oraz Rosję uregulowane prawnie w zawartym w 1992 roku traktacie o przyjaznej i dobrosąsiedzkiej współpracy¹¹⁸⁸. Artykuł 13. ust. 3. umowy wskazuje na konieczność współdziałania stron w zakresie ujawniania, zachowania i scalania, wprowadzania do obiegu kulturalnego i zapewnienia niezbędnej ochrony prawnej w odniesieniu do zabytków i obiektów związanych z historycznym i kulturowym dziedzictwem Polski i Rosji¹¹⁸⁹. Z kolei w art. 17. ust. 1. umowy ustalono, że cmentarze, miejsca pochówku, pomniki i inne miejsca pamięci będące przedmiotem czci i pamięci obywateli każdej ze stron, zarówno wojskowe jak i cywilne, będą zachowane, utrzymywane i otoczone ochroną prawną, zgodnie z normami i standardami międzynarodowymi oraz zwyczajami narodowymi i religijnymi¹¹⁹⁰.

5.5.2. Dywersyfikacja źródeł energii

Kolejną kwestią sporną w stosunkach polsko-rosyjskich jest dywersyfikacja źródeł energii. Należy przez nią rozumieć wszelkiego rodzaju kwestie związane z dostawami węgla, ropy naftowej i gazu ziemnego z Rosji do Polski, bezpieczeństwem powyższych dostaw, cen surowców energetycznych, uniezależnienia Polski od surowców energetycznych z Rosji, aktywności zagranicznych nierosyjskich firm przemysłu wydobywczego w Polsce oraz budowa gazociągów Nord Stream I i Nord Stream II.

Federacja Rosyjska pozostaje niezwykle ważnym dostawcą surowców energetycznych nie tylko do Polski, ale do większości państw Europy, w tym Unii Europejskiej. Dla przykładu, z końcem pierwszej dekady XXI wieku (2009 rok) import ropy naftowej z Rosji do państw Unii wyniósł 33,1% łącznego importu tego surowca, z kolei analogicznie w przypadku węgla było to nieco ponad 30%, a gazu ziemnego 34,2%. Ponadto surowce energetyczne były importowane przez państwa unijne również z takich państw jak Norwegia, Algieria, Libia, Kolumbia, RPA

¹¹⁸⁷ Warto odnotować, że przedmiotem rosyjskiej działalności dezinformacyjnej są również zagadnienia dotyczące Rzeczypospolitej Obojga Narodów. Zobacz szerzej: P. Lewandowski: *Rosyjska walka informacyjna z polską historią. Rzeczpospolita obojga narodów jako przedmiot rosyjskich działań dezinformacyjnych*. „Fides, Ratio et Patria. Studia Toruńskie” 2023, nr 18.

¹¹⁸⁸ A. Barynkin: *Kwestie polityki historycznej we współczesnych stosunkach polsko-rosyjskich*. W: *Polska i Rosja w zmieniającej się Europie*. Red. K. A. Wojtaszczyk, I. N. Novikova. Warszawa 2022, s. 290-291.

¹¹⁸⁹ *Traktat między Rzeczpospolitą Polską a Federacją Rosyjską o przyjaznej i dobrosąsiedzkiej współpracy, sporządzony w Moskwie dnia 22 maja 1992 r.* (Dz.U. 1993 nr 61 poz. 291), art. 13 ust. 3.

¹¹⁹⁰ Ibidem, art. 17 ust. 1.

czy USA¹¹⁹¹. Zupełnie inaczej import źródeł energii wyglądał w przypadku Polski, gdzie 92% importowanego gazu ziemnego pochodziło z Rosji (co stanowiło 55% konsumpcji tego surowca ogółem). Podobnie sytuacja wyglądała w przypadku ropy naftowej, przy czym tutaj wartość importu z Rosji wyniosła 95%, co pozwalało na zaspokojenie potrzeb konsumpcyjnych na poziomie krajowym 91%¹¹⁹². Po ponad 10 latach udział rosyjskiej ropy w imporcie do państw Unii zmalał. Było to szczególnie widoczne w przypadku Polski, która prowadząc przez ostatnie lata politykę dywersyfikacji źródeł energii rokrocznie zmniejszała udział importu z Rosji¹¹⁹³. Dla przykładu, w 2019 roku¹¹⁹⁴ w przypadku ropy naftowej było to 61,5%, a więc o około 1/3 mniej niż przed dziesięciu laty¹¹⁹⁵.

Prowadzona przez Polskę polityka dywersyfikacji źródeł energii ma swoje podłoże przede wszystkim w zakresie sporu jaki Warszawa toczy z Kremlem, w kontekście bezpieczeństwa dostaw energii, ceny surowców energetycznych oraz aktywności nierosyjskich firm wydobywczych na terenie Polski. Jest ona prowadzona już od przełomu XX i XXI wieku, a jej podstawowym elementem jest budowa nowych gazociągów i ropociągów, pozyskiwanie nowych dostawców surowców energetycznych oraz tworzenie magazynów nośników energii. Takie założenia znajdowały się w Polityce Energetycznej Polski do 2025 roku, gdzie postulowano również konieczność uniezależnienia się od dostaw surowców z Federacji Rosyjskiej¹¹⁹⁶. Analogiczne koncepcje pojawiły się w kolejnym dokumencie, tj. Polityce Energetycznej Polski do 2040 roku¹¹⁹⁷. Takie działania pozostają całkowicie uzasadnione wobec stosowania przez Kreml tzw. szantażu energetycznego. Na przestrzeni XX i XXI wieku Moskwa wielokrotnie używała surowców energetycznych jako swego rodzaju broni, czy też środka oddziaływania. Znamienne pozostają przykłady, kiedy w sytuacji wystąpienia sporów w relacjach Rosji z innymi państwami Kreml wstrzymywał dostawy zakontraktowanych

¹¹⁹¹ Eurostat: *Archive: Produkcja i import energii*. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Energy_production_and_imports/pl&oldid=83395 (dostęp: 25.01.2023).

¹¹⁹² M. Stolarczyk: *Rosja w polityce zagranicznej Polski...*, s. 248.

¹¹⁹³ Należy jednak podkreślić, że Federacja Rosyjska w latach 2007-2017 zajmowała pośród państw Unii Europejskiej pierwsze miejsce w zakresie importu surowców energetycznych takich jak ropa naftowa, gaz ziemny oraz węgiel. Źródło: Eurostat: *Energy, transport and environment statistics – 2019 edition*. <https://ec.europa.eu/eurostat/web/products-statistical-books/-/ks-dk-19-001> (dostęp: 25.01.2023).

¹¹⁹⁴ Celowo przytoczono dane w zakresie importu za 2019 rok, gdyż wobec pandemii wirusa SARS-CoV-2, która rozpoczęła się w 2020 roku, jak również wobec wojny rosyjsko-ukraińskiej rozpoczętej w 2022 roku, dane dotyczące importu ropy naftowej z Rosji we wskazanym wyżej okresie mogą być niemiernie istotne.

¹¹⁹⁵ Narodowy Bank Polski: *Bilans Płatniczy Rzeczypospolitej Polskiej za IV kwartał 2019 r.* Warszawa 2020, s. 16.

¹¹⁹⁶ *Obwieszczenie Ministra Gospodarki i Pracy z dnia 1 lipca 2005 r. w sprawie polityki energetycznej państwa do 2025 r.* (M.P. 2005 nr 42 poz. 562).

¹¹⁹⁷ *Obwieszczenie Ministra Klimatu i Środowiska z dnia 2 marca 2021 r. w sprawie polityki energetycznej państwa do 2040 r.* (Monitor Polski 2021 r. poz. 264).

surowców, wymuszając zmianę stanowiska przez dane państwo¹¹⁹⁸. Rosja, będąc dostatecznie bogata w surowce takie jak ropa naftowa, gaz ziemny czy węgiel, jak i będąc ich głównym dostawcą na przestrzeni ostatnich kilkadziesiąt lat, nie waha się wobec posiadania pozycji dominującej wykorzystywać tego jako instrumentu prowadzonej polityki zagranicznej. Nie bez znaczenia pozostaje również oferowana przez Kreml cena za dany surowiec, gdyż jest ona różna w zależności od kontrahenta bez względu na koszty związane z tranzytem przez terytoria innych państw. Dla przykładu, według danych z 2021 roku Rosja sprzedaje gaz ziemny do Chin o około 8 razy mniej niż do państw europejskich, choć biorąc pod uwagę kwestie logistyczne (odległości z miejsca wydobycia do miejsca dostawy) koszty te powinny być znacznie wyższe¹¹⁹⁹. Nie stanowi również zaskoczenia, że pośród państw członkowskich Unii Europejskiej, co do zasady, najwięcej za gaz płać państwa, które znajdowały się w byłej strefie wpływów Związku Radzieckiego, jak i państwa prowadzące politykę nieprzychylną Kremlowi¹²⁰⁰. Wobec powyższego plany dywersyfikacji pozostają w pełni uzasadnione. W przypadku Polski jest to budowa terminalu morskiego LNG w Świnoujściu, aby umożliwić sprowadzanie gazu ziemnego drogą morską¹²⁰¹ czy budowa gazociągu Baltic Pipe w celu importu tego surowca z Norwegii¹²⁰². Działania te są oczywiście utrudniane przez Kreml. Przykładowo można wskazać na doniesienia o finansowaniu przez Moskwę organizacji proekologicznych, które w ostatnich latach w państwach Zachodnich protestowały i sprzeciwiały się inwestycjom pozwalającym na dywersyfikację źródeł energii¹²⁰³. Innym przykładem mogą być działania dezinformacyjne¹²⁰⁴.

¹¹⁹⁸ DW: *Putinowskie zagrywki z gazem trafiają w punkt zapalny*. <https://www.dw.com/pl/putinowskie-zagrywki-z-gazem-trafiaj%C4%85-w-punkt-zapalny/a-60282542> (dostęp: 26.01.2023); Biznes Alert: *To nie pierwsza przerwa dostaw ropy z Rosji do Polski*. <https://biznesalert.pl/rosja-polska-ropa-przyjazn-bialorus-energetyka/> (dostęp: 26.01.2023).

¹¹⁹⁹ Rzeczpospolita: *Kto płaci najtaniej za rosyjski gaz? Niespodzianka*. <https://energia.rp.pl/gaz/art19020691-kto-placi-najtaniej-za-rosyjski-gaz-niespodzianka> (dostęp: 26.01.2023).

¹²⁰⁰ TVN24: *Kto w Europie płaci najwięcej za rosyjski gaz? Polska w czołówce*. <https://tvn24.pl/biznes/najnowsze/kto-w-europie-placi-najwiecej-za-rosyjski-gaz-polska-w-czolowce-ra380494-4437218> (dostęp: 26.01.2023); Wyborcza.biz: *Ile zapłaciliśmy za gazowy monopol Gazpromu?* <https://wyborcza.biz/biznes/51,179190,14853545.html#S.galeria-K.C-B.1-L.1.duzy> (dostęp: 26.01.2023).

¹²⁰¹ Gaz System: *Terminal LNG*. <https://www.gaz-system.pl/pl/terminal-lng/terminal-lng.html> (dostęp: 26.01.2023).

¹²⁰² Baltic Pipe Project: *O projekcie*. <https://www.baltic-pipe.eu/pl/o-projekcie/> (dostęp: 26.01.2023).

¹²⁰³ The Guardian: *This article is more than 8 years old Russia 'secretly working with environmentalists to oppose fracking'*. <https://www.theguardian.com/environment/2014/jun/19/russia-secretly-working-with-environmentalists-to-oppose-fracking> (dostęp: 26.01.2023); RMF24: *Putin opłacał ekologów? Przełaził fortunę, by blokować Zachód przed wydobyciem gazu*. <https://www.rmfm24.pl/fakty/swiat/news-putin-oplacal-ekologow-przelezal-fortune-by-blokowac-zachod-przed-wydobyciem-gazu> (dostęp: 26.01.2023).

¹²⁰⁴ Warsaw Institute: *Rosyjska dezinformacja i jej wpływ na sektor energetyczny w krajach V4*. <https://warsawinstitute.org/pl/rosyjska-dezinformacja-i-jej-wplyw-na-sektor-energetyczny-w-krajach-v4/> (dostęp: 12.03.2025).

Wreszcie, należy omówić jedną z najistotniejszych kwestii spornych jaką jest budowa gazociągów Nord Stream I i Nord Stream II przez Federację Rosyjską oraz Niemcy. W kontekście bezpieczeństwa energetycznego Polski, budowa gazociągów z jej pominięciem prowadziłaby do ograniczenia udziału w tranzycie gazu oraz stworzenia możliwości do wstrzymania jego dostaw¹²⁰⁵. Co jednak istotne, Polska nie była szczególnie zagrożona odcięciem importu z Rosji, jednakże najczęściej w Unii Europejskiej sygnalizowała zagrożenia związane z budową gazociągów¹²⁰⁶. Wiązało się to z faktem, że w przeciwieństwie do większości „krajów UE, to nie uzależnienie importowe samo w sobie uznawane jest za główny problem, co fakt zależności od kraju, który zagrażał egzystencji i suwerenności państwa polskiego. Znaczenie historycznych resentymentów w polsko-rosyjskich stosunkach wydaje się mieć kluczowe znaczenie w kształtowaniu polskiej percepcji bezpieczeństwa energetycznego”¹²⁰⁷.

Pominięcie Polski w zakresie budowy nowego gazociągu wynikało w dużej mierze z podjętych przez Warszawę działań. Sprowadzało się to do deklaracji A. Kwaśniewskiego czy J. Buzka, że Polska nie zaakceptuje rozwiązań niekorzystnych dla Ukrainy. M. Stolarczyk przytacza tutaj pogląd W. Kuczyńskiego, który w 2013 roku pisał: „jestem mianowicie przekonany, że wielki gazociąg, który ostatecznie poszedł przez Bałtyk, mógł iść przez nasz kraj. Zamiar jego zbudowania nie był w Polskę wymierzony, a do jego przebiegu przez Bałtyk przyczyniliśmy się w wielkim, może w decydującym stopniu”¹²⁰⁸. Mimo tego gazociąg Nord Stream I został otwarty w 2011 roku¹²⁰⁹. Druga nitka (Nord Stream II) pomimo iż w znacznej części ukończona, nie została otwarta wobec rosyjskiej agresji w Ukrainie¹²¹⁰. Ponadto, użytkowanie obu gazociągów pozostaje niemożliwe z powodu przeprowadzonych ataków dywersyjnych we wrześniu 2022 roku¹²¹¹. Z kolei w listopadzie tego samego roku Komisja

¹²⁰⁵ M. Sabat: *Stosunki polsko-rosyjskie. Rozbieżności interesów strategicznych*. W: *Polityka zagraniczna Federacji Rosyjskiej. Wybrane aspekty stosunków z Polską, Ukrainą i Białorusią*. Red. L. Zyblikiewicz, M. Czajkowski, P. Bajor. Kraków 2010, s. 124-125.

¹²⁰⁶ M. Stolarczyk: *Rosja w polityce zagranicznej Polski...*, s. 249.

¹²⁰⁷ K. Pronińska: *Strategie bezpieczeństwa energetycznego państwa na przykładzie wybranych krajów UE*. W: *Państwo w teorii i praktyce stosunków międzynarodowych*. Red. M. Sułek, J. Symonides. Warszawa 2009, s. 283-284.

¹²⁰⁸ M. Stolarczyk: *Rosja w polityce zagranicznej Polski...*, s. 248.

¹²⁰⁹ Ibidem, s. 249.

¹²¹⁰ Reuters: *Germany freezes Nord Stream 2 gas project as Ukraine crisis deepens*. <https://www.reuters.com/business/energy/germany-scholz-halts-nord-stream-2-certification-2022-02-22/> (dostęp: 26.01.2023).

¹²¹¹ Ośrodek Studiów Wschodnich: *Dywersja na gazociągach Nord Stream 1 i Nord Stream 2*. <https://www.osw.waw.pl/pl/publikacje/analizy/2022-09-29/dywersja-na-gazociagach-nord-stream-1-i-nord-stream-2> (dostęp: 26.01.2023).

Europejska poinformowała, że Unia całkowicie zaprzestała importu gazu ziemnego z Rosji, zastępując go surowcem od innych dostawców¹²¹².

5.5.3. Polityka bezpieczeństwa w Europie Środkowo-Wschodniej

Rozpad Związku Radzieckiego nie spowodował spadku zainteresowania Federacji Rosyjskiej regionem Europy Środkowo-Wschodniej, gdyż dla Kremla bardzo ważne pozostawały strefy wpływów w byłych państwach ZSRR, a w kolejnych latach państwach członkowskich Wspólnoty Niepodległych Państw. Relacje z nimi niezmiennie pozostają priorytetowe w każdej kolejnej Koncepcji polityki zagranicznej Federacji Rosyjskiej. Państwa środkowoeuropejskie stanowią cel oddziaływań Kreml, choć to te poradzieckie znajdujące się we wschodniej części kontynentu zajmują pozycję wiodącą¹²¹³. W stosunkach polsko-rosyjskich od momentu rozpadu ZSRR w mniejszym bądź większym stopniu pojawiał się problem podejmowania przez Warszawę działań, które zmierzały do zmniejszania strefy wpływów Kremla w tej części świata, szczególnie w takich krajach jak państwa nadbałtyckie, Białoruś oraz Ukraina. Już w 1993 roku minister spraw zagranicznych Polski K. Skubiszewski wskazywał, że do najważniejszych celów polskiej polityki wschodniej należy wspieranie transformacji demokratycznej na Wschodzie, wspieranie niezależnej państwowości oraz przyczynianie się do stabilizacji obszaru poradzieckiego. Niezwykle ważna w tym zakresie pozostawała Ukraina względem której Polska zmierzała do jak najszerzej jej integracji ze strukturami Zachodnimi (m.in. Unii Europejskiej oraz NATO), na co z kolei nie zgadzała się Federacja Rosyjska¹²¹⁴. Należy zauważyć, że „kolejne rządy III RP dążyły do zacieśnienia stosunków z Ukrainą. Wspierały tych polityków ukraińskich, którzy działali na rzecz integrowania się Ukrainy ze strukturami zachodnimi, w tym z NATO i UE, i osłabienia jej relacji z Rosją bądź tylko deklarowali wolę prowadzenia takiej polityki”¹²¹⁵.

Kreml postrzegał działania Warszawy jako daleko idące ograniczanie jego strefy wpływów w regionie. Można wręcz zauważyć, że polityka Warszawy w szczególności od momentu aneksji Krymu w 2014 roku oraz przejęcia władzy przez Prawo i Sprawiedliwość

¹²¹² Rzeczpospolita: *Historyczna chwila: Unia Europejska przestała kupować gaz ziemny z Rosji*. <https://energia.rp.pl/gaz/art37474281-historyczna-chwila-unia-europejska-przestala-kupowac-gaz-ziemny-z-rosji> (dostęp: 26.01.2023).

¹²¹³ M. Raś: *Cele oddziaływań politycznych Federacji Rosyjskiej*. W: *Rosja wobec państw Europy Środkowej i Wschodniej: zagrożenia pozamilitarne*. Red. T. Stępniewski. Lublin 2020, s. 43.

¹²¹⁴ M. Stolarczyk: *Rosja w polityce zagranicznej Polski...*, s. 158-159, 265-266.

¹²¹⁵ M. Stolarczyk: *Kontrowersje wokół koncepcji i praktyki polityki wschodniej Polski na przełomie pierwszej i drugiej dekady XXI wieku*. W: *Śląsk - Polska - Europa - świat: pamięci Profesora Jana Przewłockiego*. Red. K. Miroszewski, M. Stolarczyk. Katowice 2013, s. 309.

w 2015 roku przyjęła wymiar antyrosyjski. M. Stolarczyk wskazał, że „wiele działań w polskiej polityce wschodniej postrzeganych było przez rosyjskie grupy rządzące jako wyzywające, prowokujące bądź w ogóle lekceważące interesy Rosji”¹²¹⁶. Ponadto w perspektywie Kremla istnieje „ściśle powiązanie pomiędzy polityką zagraniczną Rosji i jej relacjami z Zachodem – szczególnie jest to widoczne w przypadku państw Europy Wschodniej. Przestrzeń pomiędzy Federacją a UE i NATO – traktowana jako ‘przedmiot rywalizacji’ – stanowi sferę ‘żywotnych interesów’ i ważną część strategii i działań Rosji wobec Zachodu”¹²¹⁷. W stosunku do Polski, Kreml dąży wobec powyższego do osłabienia jej pozycji i roli międzynarodowej pośród państw zachodnich, szczególnie Unii Europejskiej oraz NATO, jak również osłabienia więzi z byłymi państwami związkowymi ZSRR. Rosja utrudnia procesy integracyjne tych państw jak i tych ze swojej byłej strefy wpływów ze wskazanymi wyżej organizacjami międzynarodowymi. Polska z kolei wspiera te procesy co powoduje powstanie sporu na linii Kreml-Warszawa¹²¹⁸. Podsumowując można stwierdzić, że większość państw leżących na terenie Europy Środkowo-Wschodniej „jest ‘uwrażliwiona’ na oddziaływanie polityczne Federacji Rosyjskiej. Wynika to z ich doświadczeń historycznych: znajdowały się w przeszłości pod wpływem Rosji/ZSRR, a czasem stanowiły ich część składową (jak nierosyjskie republiki byłego ZSRR czy większość ziem polskich w okresie zaborów). Szczególnie podejrzliwe wobec polityki Kremla są wschodnioeuropejskie państwa poradzieckie oraz członkowie NATO i UE położeni na wschodniej flance tych organizacji”¹²¹⁹.

5.5.4. Polityka bezpieczeństwa NATO

Podstawowym celem realizowanej przez Rosję polityki zagranicznej wobec NATO jest osłabianie państw będących jego członkami, a w konsekwencji zmiana systemu bezpieczeństwa funkcjonującego w Europie. Jak pisał M. Banasik, „Moskwa będzie prawdopodobnie dążyła do ograniczenia obecności Stanów Zjednoczonych w Europie, podważenia wiarygodności NATO i dezintegracji Unii Europejskiej. Rosja postrzega Stany Zjednoczone, NATO i Unię Europejską jako relatywnie słabe podmioty i będzie dążyła do wykorzystania występujących

¹²¹⁶ Ibidem, s. 267.

¹²¹⁷ I. Topolski: *Polityka Federacji Rosyjskiej wobec państw Europy Wschodniej*. Lublin 2013, s. 139.

¹²¹⁸ M. Raś: *Cele oddziaływań politycznych Federacji Rosyjskiej*. W: *Rosja wobec państw Europy Środkowej i Wschodniej: zagrożenia pozamilitarne*. Red. T. Stępniewski. Lublin 2020, s. 43.

¹²¹⁹ T. Stępniewski: *Résumé*. W: *Rosja wobec państw Europy Środkowej i Wschodniej: zagrożenia pozamilitarne*. Red. T. Stępniewski. Lublin 2020, s. 18.

w nich podziałów”¹²²⁰. Rozszerzenie NATO na wschód, w tym byłe państwa związkowe ZSRR oraz państwa satelickie, wywarło ogromny wpływ na postrzeganie kwestii bezpieczeństwa Federacji Rosyjskiej w regionie. Skutkiem takiego rozszerzenia Sojuszu Północnoatlantyckiego było zwiększenie jego zdolności operacyjnych na kierunku wschodnim. Możliwym stało się osiągnięcie przez samoloty NATO Obwodu kaliningradzkiego w ciągu około jednej minuty, Mińska w ciągu około czterech minut, z kolei samej Moskwy w ciągu około 12-15 minut¹²²¹. W polityce zagranicznej Polski Rosja zawsze zajmowała ważne miejsce w kontekście bezpieczeństwa narodowego i międzynarodowego, przy czym odnosiło się to do przypisywania jej roli głównego zagrożenia dla istnienia państwowości, nie z kolei roli partnera. Tym samym członkostwo w Unii Europejskiej czy NATO nie zmieniło postrzegania Kremla przez Warszawę, niezależnie od przynależności partyjnej aktualnych grup rządzących¹²²².

Polska od chwili uzyskania członkostwa w Sojuszu Północnoatlantyckim prowadziła politykę, której celem było zarówno zwiększanie obecności wojskowej NATO w Polsce, jak i wspieranie dążeń i aspiracji innych państw w uzyskaniu członkostwa w organizacji. Z perspektywy Kremla takie działania stanowią zagrożenie dla interesów Federacji Rosyjskiej i jako takie podlegają nieustannej krytyce na arenie międzynarodowej. Na przełomie pierwszej oraz drugiej dekady XXI wieku Kreml promował idee wzmocnienia Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE), jak również postulat europejskiego traktatu bezpieczeństwa jako alternatywy dla działalności Sojuszu Północnoatlantyckiego. Podejmowano również próby umownego uregulowania kwestii bezpieczeństwa w Europie, lecz działania te nie przyniosły oczekiwanego rezultatu z punktu widzenia Moskwy. W kolejnych latach następowało stopniowe pogarszanie się stosunków Rosja-NATO. Nie może dziwić poczucie zagrożenia w Moskwie związane z obecnością NATO, które pod względem liczebności wojsk oraz ilości broni konwencjonalnej znacznie przewyższa potencjał Rosji¹²²³. Ze strony Zachodu podejmowano dialog z Kremlm za pośrednictwem Rady NATO-Rosja, jednakże ta platforma kontaktu nie zawsze pozostawała skuteczna.

Polska z kolei od początku swojego członkostwa w Sojuszu zabiega o rozmieszczenie jak największej ilości wojsk NATO na swoim terytorium. Choć pierwsze jednostki Sojuszu

¹²²⁰ M. Banasik: *Bezpieczeństwo Europy Środkowo-Wschodniej w aspekcie zagrożeń płynących z Federacji Rosyjskiej*. „Środkoeuropejskie Studia Polityczne” 2020, nr 2, s. 7.

¹²²¹ I. Topolski: *Polityka Federacji Rosyjskiej wobec...*, s. 106-107.

¹²²² M. Stolarczyk: *Kontrowersje wokół koncepcji i praktyki polityki wschodniej Polski na przełomie pierwszej i drugiej dekady XXI wieku*. W: *Śląsk - Polska - Europa - świat: pamięci Profesora Jana Przewłockiego*. Red. K. Miroszewski, M. Stolarczyk. Katowice 2013, s. 302.

¹²²³ A. Bodrov: *Bezpieczeństwo europejskie – wizja Rosji*. W: *Polska i Rosja w zmieniającej się Europie*. Red. K. A. Wojtaszczyk, I. N. Novikova. Warszawa 2022, s. 269-270.

zostały ulokowane w Polsce w 1999 roku¹²²⁴, to jego zauważalna obecność nastąpiła dopiero w drugiej dekadzie XXI wieku. Aneksja Półwyspu Krymskiego przez Rosję oraz jej zaangażowanie w wojnę we wschodniej Ukrainie spowodowały zwiększoną aktywność wojsk natowskich w Polsce, co było wynikiem ustaleń dokonanych podczas szczytów NATO w Newport w 2014 roku¹²²⁵ i w Warszawie w 2016 roku¹²²⁶. Pierwszy ze wskazanych szczytów był niezwykle istotny, ponieważ zdecydowano o wzmocnieniu państw Sojuszu znajdujących się na wschodzie, zobowiązano państwa członkowskie do wydatkowania 2% PKB na zbrojenia oraz utworzono brygadę sił bardzo szybkiego reagowania o liczebności około 5 tysięcy żołnierzy¹²²⁷. Z kolei po dwóch latach na szczycie w Warszawie uzgodniono, iż w Polsce, Litwie, Łotwie i Estonii zostaną rozmieszczone cztery bataliony grup bojowych, w wyniku czego od połowy 2017 roku liczebność sił NATO wynosiła 4,5 tysiąca żołnierzy a docelowo miała liczyć 7 tysięcy żołnierzy (cel ten został zrealizowany)¹²²⁸. Wydaje się, że dla Rosji decyzje podjęte w trakcie szczytów nie były zaskoczeniem, lecz spotkały się oczywiście z krytyką¹²²⁹, która trwała w kolejnych latach wraz z realizacją przyjętych przez państwa NATO postanowień¹²³⁰. Zaangażowanie Sojuszu w regionie ulegało sukcesywnie zwiększaniu¹²³¹, a w wyniku rosyjskiej inwazji w Ukrainie jego obecność wojskowa wzrosła w Polsce do łącznej szacunkowej liczby około 10 tysięcy żołnierzy¹²³². Ponadto w państwach nadbałtyckich, Słowacji, Węgrzech, Rumunii oraz Bułgarii stacjonuje około 15 tysięcy żołnierzy NATO¹²³³. Wobec trwającego konfliktu rosyjsko-ukraińskiego należy spodziewać się dalszego znacznego wzrostu zaangażowania Sojuszu w Europie Środkowo-Wschodniej (wschodniej flance).

Co istotne, rosyjscy decydenci polityczni stosunkowo często w wystąpieniach publicznych, uzasadniając swoje działania (tak było chociażby w przypadku aneksji Krymu

¹²²⁴ NATO: *History*. <https://mncne.nato.int/about-us/history> (dostęp: 27.01.2023).

¹²²⁵ S. Koziej, P. Pietrzak: *Szczyt NATO w Newport*. „Bezpieczeństwo Narodowe” 2014, nr 2014/III, s. 11-29.

¹²²⁶ P. Soloch, P. Pietrzak: *Szczyt NATO w Warszawie: uwarunkowania, rezultaty, wnioski dla Polski*. „Bezpieczeństwo Narodowe” 2016, nr 2016/I-IV, s. 13-33.

¹²²⁷ M. Banasik: *Bezpieczeństwo Europy Środkowo-Wschodniej...*, s. 9.

¹²²⁸ Ibidem, s. 9-10.

¹²²⁹ Ośrodek Studiów Wschodnich: *Rosja wobec szczytu NATO w Warszawie*. <https://www.osw.waw.pl/pl/publikacje/analizy/2016-07-13/rosja-wobec-szczytu-nato-w-warszawie> (dostęp: 27.01.2023).

¹²³⁰ TVN24: *Rzecznik Kremla: wzmocnienie wojskowe NATO w Polsce zmusza nas do podjęcia niezbędnych środków*. <https://tvn24.pl/swiat/pieskow-wojska-nato-w-polsce-zagrozeniem-dla-rosji-4615591> (dostęp: 27.01.2023).

¹²³¹ Ministerstwo Obrony Narodowej: *Siły sojusznicze w Polsce*. <https://www.gov.pl/web/obrona-narodowa/sily-sojusznicze-w-polsce> (dostęp: 27.01.2023); CNN: *US troops to deploy to Eastern Europe amid Ukraine crisis*. <https://edition.cnn.com/2022/02/02/politics/us-troops-europe-russia/index.html> (dostęp: 27.01.2023).

¹²³² Rzeczpospolita: *Ilu żołnierzy NATO przebywa obecnie w Polsce?* <https://www.rp.pl/wojsko/art35749601-ilu-zolnierzy-nato-przebywa-obecnie-w-polsce> (dostęp: 27.01.2023).

¹²³³ TVN24: *Ilu żołnierzy NATO jest w Polsce i krajach sąsiednich*. <https://tvn24.pl/swiat/ilu-zolnierzy-nato-jest-w-polsce-i-na-wschodniej-flance-infografika-5639659> (dostęp: 27.01.2023).

i wojny w Ukrainie) mitem tzw. złamanej obietnicy. Odnosi się on do sytuacji politycznej z lat dziewięćdziesiątych XX wieku, kiedy to Zachód obiecał przywódcom radzieckim, że NATO nie zostanie rozszerzone na Wschód¹²³⁴. Z kolei ze strony Sojuszu podnoszona jest kwestia, że ustalenia czy też sformułowania polityków zachodnich, na które powołuje się Kreml nie miały waloru faktycznego zobowiązania prawnomiędzynarodowego. Ponadto padły one w odniesieniu do kwestii zjednoczenia Niemiec oraz negocjacji podczas konferencji dwa plus cztery (2+4), a więc w czasie kiedy istniał jeszcze Związek Radziecki oraz Układ Warszawski. W związku z tym nikt nie mógł wtedy przypuszczać, że dojdzie w przyszłości do przyjęcia w poczet członków Sojuszu wielu państw będących stronami Układu Warszawskiego. Jednocześnie należy wziąć pod uwagę fakt, że w kolejnych latach doszło do znaczących przeobrażeń w Europie Środkowo-Wschodniej w wyniku których państwa nadbałtyckie domagały się niepodległości, mur berliński upadł, Niemcy obrały kurs na zjednoczenie się, a państwa satelickie ZSRR na Zachód¹²³⁵.

Uzupełniając należy zarysować wojnę gruzińsko-rosyjską (2008), która stanowiła w istocie reakcję Rosji na aspiracje rządu w Tbilisi do członkostwa w NATO, wspierane intensywnie przez Polskę wraz z innymi państwami Europy Środkowo-Wschodniej. Dla Kremla rozpoczęcie inwazji na terytorium gruzińskie miało wymiar prewencyjny i tak też przedstawiono podjęte działania na arenie międzynarodowej¹²³⁶. Analitycy wskazywali, że działania Rosji z tamtego okresu kończą czas ustępstw Kremla wobec Zachodu i rozpoczynają etap zdecydowanej polityki zagranicznej na obszarze swojej tradycyjnej strefy wpływów. Dla Moskwy integracja Gruzji z NATO czy Unią Europejską jest ingerencją USA oraz państw członkowskich Unii w wyłączną strefę wpływów Federacji na obszarze poradzieckim¹²³⁷. Znaczna część państw zachodnich oceniła jednak rosyjską odpowiedź na gruziński atak jako nieadekwatną oraz nieproporcjonalną, jak również przekraczającą granice dozwolonej obrony koniecznej. Należy również zauważyć, że względna akceptacja działań podjętych przez Kreml wynikała, ze świadomości oraz przekonania, która strona faktycznie rozpoczęła wojnę¹²³⁸. Na podobne wnioski wskazywał również raport przygotowany przez Unię Europejską w którym zauważono, że podjęte działania oraz użyte siły przez Tbilisi były nieuzasadnione względem

¹²³⁴ A. Bodrov: *Bezpieczeństwo europejskie – wizja Rosji*. W: *Polska i Rosja w zmieniającej się Europie*. Red. K. A. Wojtaszczyk, I. N. Novikova. Warszawa 2022, s. 268-269.

¹²³⁵ NATO Review: *Rozszerzenie NATO i Rosja: mity i rzeczywistość*. <https://www.nato.int/docu/review/pl/articles/2014/07/01/rozszerzenie-nato-i-rosja-mity-i-rzeczywistosc/index.html> (dostęp: 27.01.2023).

¹²³⁶ A. Bryc: *Ewolucja społeczności międzynarodowej w nowej dynamice stosunków międzynarodowych*. „Kultura i Edukacja” 2014, nr 2 (102), s. 54.

¹²³⁷ M. Stolarczyk: *Rosja w polityce zagranicznej Polski...*, s. 88.

¹²³⁸ M. Stolarczyk: *Rosja w polityce zagranicznej Polski w okresie pozimnowojennym (aspekty polityczne)*. „Studia Politicae Universitatis Silesiensis” 2013, Tom 11, s. 65-66.

norm prawa międzynarodowego publicznego¹²³⁹. Odmienne stanowisko prezentowała natomiast Warszawa oraz znaczna część polskiego społeczeństwa. Wręcz bezkrytycznie akceptowano wymiar polityki, jak również sposób jej prowadzenia przez Gruzję. Przejawiało się to między innymi w wizycie Prezydenta RP L. Kaczyńskiego w Tbilisi (w trakcie działań wojennych), podczas której prezentowano raczej postawę konfrontacyjną wobec Kremla¹²⁴⁰. W konsekwencji konflikt doprowadził do znacznego pogorszenia się stosunków polsko-rosyjskich. Choć od zakończenia wojny gruzińsko-rosyjskiej upłynął znaczny okres, to obserwując jej skutki w kolejnych latach można zauważyć, że Gruzja jest współcześnie o wiele dalej od członkostwa w NATO niż była w 2008 roku. Po kilkunastu latach od zakończenia wojny Kreml skutecznie realizuje swoje strategiczne interesy w Gruzji, poprzez blokowanie jej członkostwa w NATO oraz Unii Europejskiej. Ważnym elementem pozostają również kwestie związane z bezpieczeństwem energetycznym, gdyż Rosja zmierza do ograniczenia roli Gruzji jako państwa tranzytowego dla surowców energetycznych i podważania jej pozycji w tym zakresie w Europie. Można wręcz zauważyć, że oba państwa budują wzajemne relacje na warunkach narzucanych przez Federację Rosyjską¹²⁴¹.

5.5.5. Katastrofa samolotu rządowego z Prezydentem Rzeczypospolitej Polskiej w Smoleńsku

Katastrofa samolotu rządowego z Prezydentem Rzeczypospolitej Polskiej L. Kaczyńskim w Smoleńsku, która miała miejsce dnia 10 kwietnia 2010 roku, wywarła niezwykle silny wpływ na stosunki polsko-rosyjskie w drugiej dekadzie XXI wieku, nadając im zupełnie nowy wymiar, jak i zupełnie nowe brzmienie. Do katastrofy, w której zginęli wszyscy pasażerowie na pokładzie, doszło podczas państwowej delegacji udającej się na obchody siedemdziesiątej rocznicy zbrodni katyńskiej w Federacji Rosyjskiej. W wyniku tych wydarzeń społeczeństwo rosyjskie jak i najważniejsi rosyjscy politycy wykazali się niezwykle jak na dotychczasowe relacje dwustronne solidarnością oraz współczuciem. Na czele nadzwyczajnej komisji mającej za cel wyjaśnienie przyczyn katastrofy stanął sam ówczesny

¹²³⁹ Zobacz szerzej: *Raport Niezależnej Międzynarodowej Misji Wyjaśniającej w sprawie Konfliktu w Gruzji*. „Międzynarodowy Przegląd Polityczny” 2010, nr 1.

¹²⁴⁰ M. Stolarczyk: *Rosja w polityce zagranicznej Polski w okresie pozimnowojennym...*, s. 66-67.

¹²⁴¹ J. Benedyczak: *Założenia i perspektywy polityki Rosji wobec Gruzji*. „Biuletyn Polskiego Instytutu Spraw Międzynarodowych” 2018, nr 117 (1690) <https://pism.pl/upload/images/artykuly/legacy/files/24742.pdf> (dostęp: 04.03.2023); Ośrodek Studiów Wschodnich: *Gruzja: napięcia wewnętrzne i nowy kryzys w stosunkach z Rosją*. <https://www.osw.waw.pl/pl/publikacje/analizy/2019-06-26/gruzja-napięcia-wewnętrzne-i-nowy-kryzys-w-stosunkach-z-rosja> (dostęp: 04.03.2023).

premier, W. Putin (pojawił się również na miejscu katastrofy i osobiście koordynował działania), a w Rosji ogłoszono żałobę narodową. Prezydent D. Miedwiediew jak i W. Putin wygłosili odezwy do Polaków wyrażając głębokie współczucie. Pod polskimi placówkami dyplomatycznymi Rosjanie spontanicznie składali kwiaty, Duma uczciła ofiary katastrofy minutą ciszy, a w państwowej telewizji dwukrotnie wyemitowano film Katyń A. Wajdy, przez co znaczna część Rosjan mogła po raz pierwszy dowiedzieć się o dokonanej przez Związek Radziecki zbrodni¹²⁴². Wtedy też pojawiły się głosy, między innymi w części środowiska politycznego, że tak ogromna tragedia może stanowić przełom w stosunkach polsko-rosyjskich oraz być czynnikiem, który doprowadzi do wzajemnego narodowego pojednania, będąc swego rodzaju katalizatorem¹²⁴³. Katastrofa smoleńska doprowadziła do resetu we wzajemnych relacjach obu państw¹²⁴⁴. Ówczesny prezydent D. Miedwiediew podczas wizyty w Polsce w tym samym roku stwierdził w udzielonym wywiadzie, że w Rosji na najwyższych szczeblach władzy państwowej zapadła decyzja o resecie w relacjach z Polską, gdyż w niezwykle trudnej i bolesnej wspólnej historii należy wreszcie oddzielić kwestie historyczne od teraźniejszości¹²⁴⁵.

W drugiej dekadzie XXI wieku do pojednania polsko-rosyjskiego nie doszło. Stosunkowo szybko pojawił się impas we wzajemnych relacjach, który trwał w latach 2011-2013, a jego główną przyczyną były spory na tle ustalenia przyczyn katastrofy, do której doszło dnia 10 kwietnia 2010 roku. Nie mogło budzić wątpliwości, że kwestia ta jest kluczowa dla przyszłości stosunków bilateralnych. W Polsce zaczęły pojawiać się głosy o dokonaniu zamachu na prezydenta L. Kaczyńskiego, które zostały wzmocnione przez jednostronny raport rosyjskiego Międzypaństwowego Komitetu Lotniczego (MAK) ze stycznia 2011 roku w którym wskazano iż stan techniczny lotniska jak i działania rosyjskich kontrolerów ruchu lotniczego nie miały bezpośredniego wpływu na przebieg katastrofy, wskazując jednocześnie

¹²⁴² K. Fedorowicz: *Polityka Polski wobec Rosji...*, s. 157-160.

¹²⁴³ Warto zauważyć, że jak wskazał R. Zięba: „Znaczącym konstruktywnym gestem Rosji na drodze poszukiwania porozumienia z Polską była uchwała Dumy Państwowej Federacji Rosyjskiej z 26 listopada 2010r. przypominając, że „zbrodnia katyńska została dokonana z bezpośredniego rozkazu Stalina i innych radzieckich przywódców”, parlament Rosji wyraził „głębokie współczucie wszystkim ofiarom nieuzasadnionych represji, ich rodzinom i bliskim”. Oświadczenie dało wyraz przekonaniu, że proces wyjaśniania wszystkich okoliczności zbrodni katyńskiej będzie kontynuowany. Czytamy w nim: „Nasze narody zapłaciły ogromną cenę za zbrodnie totalitaryzmu. Stanowczo potępiając reżim, który gardził prawami i życiem ludzi, deputowani do Dumy Państwowej w imieniu narodu rosyjskiego wyciągają przyjazną dłoń do narodu polskiego. Wyrażają też nadzieję na początek nowego etapu w stosunkach między naszymi krajami, które będą rozwijać się na gruncie demokratycznych wartości”. To bezprecedensowe oświadczenie nie tylko wskazywało na wolę strony rosyjskiej poszukiwania pojednania z Polską, ale było także adresowane do społeczeństwa rosyjskiego”. Źródło: R. Zięba: *Główne problemy w stosunkach polsko-rosyjskich...*, s. 14-15.

¹²⁴⁴ M. Stolarczyk: *Rosja w polityce zagranicznej Polski...*, s. 219-220.

¹²⁴⁵ K. Fedorowicz: *Polityka Polski wobec Rosji...*, s. 158-160.

na znaczne zaniedbania po stronie pilotów¹²⁴⁶. Z czasem katastrofa smoleńska stała się instrumentem w realizowanej przez Prawo i Sprawiedliwość polityce wewnętrznej, a wymiar międzynarodowy przyjęła po przejęciu władzy przez tą partię w 2015 roku¹²⁴⁷. Tak ukształtowana polityka zagraniczna ze strony Polski niweczyła szanse na porozumienie z Federacją Rosyjską, a ingerencja Kremla w wewnętrzne sprawy Ukrainy w roku 2013 (Euromajdan) i 2014 (aneksja Półwyspu Krymskiego oraz wojna we wschodniej Ukrainie), doprowadziła do jej nasilenia. Rząd PiS w kolejnych latach nie osiągnął żadnych postępów w relacjach z Rosją¹²⁴⁸.

Niezwykle istotny pozostaje spór jaki ma miejsce w społeczeństwie polskim. Początkowo tragedia wywołała ogólnonarodowe poczucie wspólnoty, wspólnego przeżywania żałoby, a nawet pojawiały się głosy o pojednaniu polsko-polskim. Szybko jednak sytuacja uległa zmianie, a pierwsze spory narodowe miały miejsce jeszcze w trakcie trwania żałoby, wobec informacji o planach pochowania prezydenta L. Kaczyńskiego na Wawelu. Kolejnym aspektem istniejącego sporu jest kwestia wyjaśnienia przyczyn katastrofy, na które składają się podglądy o dokonaniu zamachu, lądowaniu w warunkach uniemożliwiających jego bezpieczne przeprowadzenie czy też prowadzeniu śledztwa w sposób niewłaściwy. Wreszcie wskazać należy na spór o krzyż umieszczony przed pałacem prezydenckim i kwestie związane z pozostawieniem go miejscu bądź też usunięciem, czy też organizowanie tzw. miesięcznic smoleńskich¹²⁴⁹. Dla Moskwy zarysowany wyżej wewnętrzny konflikt w Polsce jest niezwykle ważny. W interesie Rosji jest bowiem kreowanie wewnętrznych podziałów w państwie, co z kolei jest możliwe przy wykorzystaniu tragicznych wydarzeń z 2010 roku i ich następstw w polskim społeczeństwie. Przykładowo już tylko z tej przyczyny nie może dziwić fakt, że wrak polskiego samolotu rządowego nie został nadal zwrócony przez Kreml¹²⁵⁰. Ilość emocji

¹²⁴⁶ M. Stolarczyk: *Rosja w polityce zagranicznej Polski...*, s. 219-225.

¹²⁴⁷ W okresie rządów koalicji PO-PSL stosunki na linii Warszawa-Moskwa nie przybierały tak antagonistycznego charakteru. Dla przykładu w 2011 roku ówczesny minister spraw zagranicznych R. Sikorski stwierdził, że: „Są w Polsce ludzie, także w tej Izbie, którzy na wiecznej wrogości do Rosji budują swoje polityczne credo. My odrzuciliśmy logikę, według której wszystko, co złe dla Rosji, musi być dobre dla Polski. Lekarstwem na obawy przed Rosją jest nowoczesna Polska, silna potencjałem gospodarczym, więziami sojuszniczymi i pozycją międzynarodową oraz, na wszelki wypadek, nowoczesnym systemem obronnym. To, że nie mamy większych zatargów z Rosją, tylko wzmacnia naszą pozycję w Europie”. Źródło: Sejm RP: 6 kadencja, 87 posiedzenie, 1 dzień (16-03-2011), 2 punkt porządku dziennego: *Informacja ministra spraw zagranicznych o założeniach polskiej polityki zagranicznej w 2011 roku*. <http://orka2.sejm.gov.pl/Debata6.nsf/main/42A5B0D0> (dostęp: 28.01.2023); Ibidem, s. 221.

¹²⁴⁸ R. Zięba: *Główne problemy w stosunkach polsko-rosyjskich...*, s. 13-17.

¹²⁴⁹ T. Bojarowicz, W. Jakubowski, D. Przastek: *Spółczesność i kultura – tradycja i współczesność*. W: *Polska i Rosja w zmieniającej się Europie*. Red. K. A. Wojtaszczyk, I. N. Novikova. Warszawa 2022, s. 53.

¹²⁵⁰ PAP Polska Agencja Prasowa: *Podkomisja smoleńska zwywa MKL i rosyjską prokuraturę do zwrotu wraku Tu-154M*. <https://www.pap.pl/aktualnosci/news%2C1421216%2Cpodkomisja-smolenska-zwywa-mkl-i-rosyjska-prokuratura-do-zwrotu-wraku-tu> (dostęp: 04.03.2023); Rzeczpospolita: *Apel Strasburga do Rosji*:

jakie towarzyszą powyższej kwestii stanowi bowiem element rozgrywanej przez Rosję polityki podziału i podtrzymywania konfliktu w Polsce. Ewentualny zwrot wraku samolotu, który rozbił się pod Smoleńskiem, mógłby tylko ten konflikt częściowo zakończyć, co nie jest w interesie Federacji Rosyjskiej¹²⁵¹.

5.5.6. Aneksja Półwyspu Krymskiego i wojna w Ukrainie

Z. Brzeziński stwierdził, że „bez Ukrainy Rosja przestaje być imperium euroazjatyckim”¹²⁵². Z kolei rosyjski politolog M. Chazin ocenił utratę Ukrainy po rozpadzie Związku Radzieckiego jako utratę najważniejszej forpocztę¹²⁵³. Aneksja Półwyspu Krymskiego przez Rosję w 2014 roku oraz rozpoczęta w tym samym czasie wojna we wschodniej Ukrainie, jak również pełnowymiarowa inwazja Rosji na to państwo w 2022 roku, stanowią jedną z najważniejszych kwestii spornych występujących w stosunkach polsko-rosyjskich w drugiej i na początku trzeciej dekady XXI wieku¹²⁵⁴. Jednocześnie należy nadmienić, że omawiane zagadnienia nabierają szczególnego znaczenia nie tylko w kontekście bezpieczeństwa Polski i stosunków polsko-rosyjskich, ale również bezpieczeństwa całego kontynentu europejskiego¹²⁵⁵. Jak już zauważono, Polska od rozpadu Związku Radzieckiego wspierała Ukrainę w dążeniach niepodległościowych, a następnie jej aspiracjach do integracji z Zachodem, w tym członkostwem w Unii Europejskiej oraz NATO. To z kolei stoi w sprzeczności z interesami Kremla które zakładają, że Ukraina znajduje się w jego wyłącznej strefie wpływów.

Genezą omawianych wydarzeń jest przede wszystkim rok 2013, w którym ówczesny prezydent Ukrainy W. Janukowycz opóźnił podpisanie umowy stowarzyszeniowej z Unią Europejską. Wywołało to ogromne niezadowolenie społeczne, których skutkiem był

Oddajcie Polsce wrak Tu-154M. <https://www.rp.pl/wydarzenia/art9600151-apel-strasburga-do-rosji-oddajcie-polsce-wrak-tu-154m> (dostęp: 04.03.2023).

¹²⁵¹ TVN24: *Prezydencki minister: Wrak jest w Rosji i będzie w Rosji. Nikt z nas tego wraku nie odzyska.* <https://tvn24.pl/polska/katastrofa-smolenska-prezydencki-minister-andrzej-dera-wrak-jest-w-rosji-i-będzie-w-rosji-nikt-z-nas-tego-wraku-nie-odzyska-6118183> (dostęp: 04.03.2023); Jedyńka Polskie Radio: *Sprawa wraku Tu-154M. Guzy: Rosja chce, by wszyscy o nim zapomnieli.* <https://jedyńka.polskieradio.pl/artukul/2490525,sprawa-wraku-tu154m-guzy-rosja-chce-by-wszyscy-o-nim-zapomnieli> (dostęp: 04.03.2023).

¹²⁵² Z. Brzeziński: *Wielka szachownica: Główne cele polityki amerykańskiej*. Warszawa 1998, s. 56.

¹²⁵³ Ibidem, s. 190.

¹²⁵⁴ M. Banasik: *Bezpieczeństwo Europy Środkowo-Wschodniej...*, s. 5.

¹²⁵⁵ S. Wojciechowski: *Biała księga bezpieczeństwa narodowego RP a problemy i wyzwania w zakresie WPBiO Unii Europejskiej*. W: *Bezpieczeństwo Polski. Współczesne wyzwania*. Red. S. Wojciechowski, A. Potyrała. Warszawa 2014, s. 81.

Euromajdan¹²⁵⁶. Przede wszystkim należy zauważyć, że wydarzenia jakie miały miejsce w Kijowie od października 2013 roku do lutego 2014 roku były przedstawiane przez Moskwę jako bunt ludności cywilnej pozbawiony jakichkolwiek podstaw prawnych. Ponadto działania przeciwko legalnej władzy miały być inspirowane z zewnątrz, a więc w domyśle przez Zachód¹²⁵⁷. Rosja znalazła się w tamtym czasie w krytycznym położeniu wobec zagrożenia utraty wpływów w Ukrainie i jej integracji z Unią Europejską. Tym też zapewne można tłumaczyć zdecydowaną reakcję Moskwy, w wyniku której doszło do aneksji Półwyspu Krymskiego oraz rozpoczęcia wojny na wschodzie kraju (pomiędzy rządem a separatystami), która była wspierana przez Rosjan¹²⁵⁸. Działania podejmowane przez Kreml wobec Ukrainy w sposób znaczący zmieniły podejście państw z Europy Środkowo-Wschodniej do aktywności Federacji Rosyjskiej, zarówno w skali regionalnej jak i globalnej. Z kolei w odniesieniu do Rosji, prowadzona polityka zagraniczna okazała się w znacznym stopniu nieskuteczna wobec zakładanych celów. Nie doszło bowiem do wzrostu znaczenia Kremla na arenie międzynarodowej, a samo państwo (między innymi wobec nałożonych sankcji) osłabło¹²⁵⁹. Co zastanawiające, wobec aneksji dokonanej przez Rosję oraz wspieranych przez Kreml separatystów, działania zapobiegawcze podjęte przez NATO były niezwykle ostrożne¹²⁶⁰. Z kolei Polska przez cały czas trwania konfliktu wspierała Kijów oraz otwarcie krytykowała postępowanie Rosji. Polskie MSZ postulowało również nałożenie jak najbardziej restrykcyjnych sankcji, co doprowadziło do impasu, a wręcz zamrożenia stosunków polsko-rosyjskich¹²⁶¹. Należy zaznaczyć, że od lat dziewięćdziesiątych XX wieku Polska, jako państwo o średniej wielkości i znaczeniu na arenie międzynarodowej, deklarowała chęć odgrywania różnych ról międzynarodowych. Do najważniejszych z nich należały: rola lidera transformacji politycznej i gospodarczej, rola pewnego i silnego podmiotu wspólnoty zachodniej, rola lidera regionalnego oraz rola łącznika (transmitera) wartości, norm i interesów z Zachodu na

¹²⁵⁶ Bezpośrednią przyczyną wydarzeń, które miały miejsce od listopada 2013 roku do lutego 2014 roku było niepodpisanie przez ówczesnego prezydenta Ukrainy W. Janukowycza umowy stowarzyszeniowej z Unią Europejską, jak również umowy o pogłębieniu i wszechstronności handlu. Skutkiem tego były demonstracje i zamieszki w wielu miastach Ukrainy (głównie w zachodniej jej części), a przede wszystkim w Kijowie.

¹²⁵⁷ A. Rogozińska: *Analiza zagrożeń kreowanych w cyberprzestrzeni*. W: *Rosja wobec państw Europy Środkowej i Wschodniej: zagrożenia pozamilitarne*. Red. T. Stępniewski. Lublin 2020, s. 69.

¹²⁵⁸ R. Kłaczyński: *Rosyjsko-ukraiński konflikt 2014-2017 jako przykład wojny hybrydowej*. *Geneza, Polityka, Gospodarka*. „Rocznik Bezpieczeństwa Międzynarodowego” 2017, Vol. 11, nr 2, s. 7-8.

¹²⁵⁹ M. Raś: *Cele oddziaływań politycznych Federacji Rosyjskiej*. W: *Rosja wobec państw Europy Środkowej i Wschodniej: zagrożenia pozamilitarne*. Red. T. Stępniewski. Lublin 2020, s. 50-51.

¹²⁶⁰ M. Banasik: *Bezpieczeństwo Europy Środkowo-Wschodniej...*, s. 9.

¹²⁶¹ M. Stolarczyk: *Rosja w polityce zagranicznej Polski...*, s. 334; Polski Instytut Spraw Międzynarodowych: *Konflikt na Ukrainie ma kluczowy wpływ na relacje polsko-rosyjskie*. https://pism.pl/konferencje/Konflikt_na_Ukrainie_ma_kluczowy_wp_yw_na_relacje_polsko_rosyjskie (dostęp: 27.01.2023).

Wschód¹²⁶². W kontekście stosunków polsko-ukraińskich rosyjscy politolodzy G. Pawłowski oraz S. Markow zauważyli, że Polska bez Ukrainy to państwo ze średnim potencjałem w Europie, natomiast Polska z Ukrainą – to wielki europejski kraj¹²⁶³.

Spór wokół Ukrainy zaczął się poważnie intensyfikować w 2021 roku. Z jego końcem Federacja Rosyjska wystosowała wobec USA, ale również wobec szeroko rozumianego Zachodu, szereg postulatów dotyczących między innymi zaprzestania dalszej ekspansji NATO w kierunku wschodnim i nierozmieszczania wojsk na Ukrainie oraz w innych państwach poradzieckich. Żądania te nie spotkały się z akceptacją zachodnich decydentów politycznych, co miało istotne znaczenie dla dalszej polityki zagranicznej Rosji¹²⁶⁴. Pełnowymiarowy konflikt w Ukrainie, który rozpoczął się 24 lutego 2022 roku z całkowitą pewnością postawił przed Polską szereg wyzwań jak i szans, które dobrze wykorzystane mogą w sposób znaczący zwiększyć jej pozycję na arenie międzynarodowej, a już z całkowitą pewnością w regionie. Pozbawiona jakichkolwiek podstaw prawnych inwazja Rosji, a więc państwa będącego stałym członkiem Rady Bezpieczeństwa Organizacji Narodów Zjednoczonych, skutkuje koniecznością ponownego sformułowania przez państwa zachodnie koncepcji i celów prowadzonej wobec Moskwy polityki zagranicznej. O ile aneksja Krymu i wojna we wschodniej Ukrainie wydawała się być możliwa do względnego zaakceptowania, o tyle pełnowymiarowy konflikt w Europie, nazwany przez Kreml „operacją specjalną”, już nie. Warto zaznaczyć, że jak wskazuje A. Gruszczak „Putinowska Rosja, dokonując zbrojnej napaści na Ukrainę, postawiła siebie ponad ładem, prawem i moralnością międzynarodową, kreując swą mocarstwowość w środowisku anarchii międzynarodowej, odrzucając przyjęte przez Zachód wzorce porządku liberalnego. Rosja rzuciła wyzwanie nie tylko Zachodowi, ale i systemowi bezpieczeństwa międzynarodowego, w którym była zakotwiczona instytucjonalnie od końca II wojny światowej”¹²⁶⁵.

Działania podjęte przez Rosję tym razem skutkowały bardziej zdecydowaną reakcją ze strony Zachodu. Wiele państw nałożyło sankcje, a z perspektywy stosunków polsko-rosyjskich

¹²⁶² M. Raś: *Polska w stosunkach międzynarodowych*. W: *Polska i Rosja w zmieniającej się Europie*. Red. K. A. Wojtaszczyk, I. N. Novikova. Warszawa 2022, s. 137-143.

¹²⁶³ R. Lisiakiewicz: *Polityka Rosji wobec Polski...*, s. 138.

¹²⁶⁴ Ośrodek Studiów Wschodnich: *Rosyjski szantaż wobec Zachodu*. <https://www.osw.waw.pl/pl/publikacje/analizy/2021-12-20/rosyjski-szantaż-wobec-zachodu> (dostęp: 27.01.2023).

¹²⁶⁵ A. Gruszczak: *Kilka uwag o strategicznym wymiarze wojny w Ukrainie*. W: *THE WAR MUST GO ON: Dynamika wojny w Ukrainie i jej reperkusje dla bezpieczeństwa Polski*. Red. A. Gruszczak. Kraków 2023, s. 15-16.

należy wskazać przede wszystkim na te zastosowane przez Unię Europejską¹²⁶⁶ oraz USA¹²⁶⁷. Ponadto można zaobserwować niespotykane dotąd wsparcie militarne ze strony wielu państw, gdzie prym wiodą USA, które przeznaczyły dziesiątki miliardów dolarów na pomoc wojskową, humanitarną oraz finansową¹²⁶⁸. Jest to oczywiście uzasadnione ogromnym potencjałem ekonomicznym oraz wojskowym posiadanym przez Waszyngton, dlatego należy zasygnalizować, że gdyby ustalać kwotę udzielonej pomocy przy jej odniesieniu do procentowej wartości PKB danego kraju, to w początkowym okresie wojny pierwsze miejsce zajmowałyby kolejno takie państwa jak Estonia, Litwa i Polska¹²⁶⁹.

W tym stanie rzeczy nie można mówić o jakichkolwiek konstruktywnych stosunkach polsko-rosyjskich. Wobec wojny w Ukrainie i niezwykle aktywnego wspierania tego państwa przez Warszawę, Rosja postrzega Polskę jako państwo nieprzyjazne i wrogo nastawione. Rząd w Warszawie podejmuje bowiem działania pozostające w sprzeczności z podstawowymi interesami Kremla, jakie współcześnie realizuje w Europie Wschodniej, tj. podporządkowania sobie Ukrainy oraz państw sąsiednich. Polska dyplomacja nie zgadza się na żadne ustępstwa wobec Moskwy, postulując stosowanie jak najbardziej dotkliwych sankcji, przede wszystkim w ramach wspólnego działania Unii Europejskiej. Ponadto postuluje dostarczanie rządowi w Kijowie wsparcia w każdej formie, lecz przede wszystkim uzbrojenia. Wreszcie należy zauważyć, że Polska stała się centrum dystrybucji pomocy dla Ukrainy, która napływa z całego świata. Tym samym Rosja podejmuje wobec Polski działania, które mają na celu podważenie prowadzonej przez Warszawę polityki na arenie międzynarodowej, zdyskredytowanie wizerunku Polski oraz antagonizowanie stron w ramach stosunków polsko-ukraińskich.

5.5.7. Program Partnerstwa Wschodniego

Jednym z podstawowych celów polskiej polityki zagranicznej po 1989 roku było w ocenie ówczesnego ministra spraw zagranicznych K. Skubiszewskiego „wspieranie na Wschodzie transformacji demokratycznej, w tym tworzenie gospodarki rynkowej, wspieranie niezależnej państwowości naszych partnerów wschodnich, przyczynianie się do stabilizacji na

¹²⁶⁶ Rada Europejska, Rada Unii Europejskiej: *Reakcja UE wobec rosyjskiej inwazji na Ukrainę*. <https://www.consilium.europa.eu/pl/policies/eu-response-ukraine-invasion/> (dostęp: 28.01.2023).

¹²⁶⁷ U.S. Department of the Treasury: *Ukraine-/Russia-related Sanctions*. <https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/ukraine-russia-related-sanctions> (dostęp: 28.01.2023).

¹²⁶⁸ U.S. Department of State: *U.S. Security Cooperation with Ukraine*. <https://www.state.gov/u-s-security-cooperation-with-ukraine/> (dostęp: 28.01.2023).

¹²⁶⁹ The Kiel Institute for the World Economy: *Ukraine Support Tracker*. <https://www.ifw-kiel.de/topics/war-against-ukraine/ukraine-support-tracker/?cookieLevel=not-set> (dostęp: 28.01.2023).

całym obszarze postsowieckim z poszanowaniem prawa międzynarodowego”¹²⁷⁰, a ponadto tworzenie powiązań gospodarczych, kulturalnych, społecznych, jak również współpraca w ramach ugrupowań regionalnych¹²⁷¹. Wskazane założenia co do zasady nie uległy zmianie na przestrzeni lat, bez względu na ugrupowanie polityczne rządzące Polską. Po ponad 30 latach minister spraw zagranicznych J. Czaputowicz stwierdził, że „polityka wschodnia należy do najważniejszych wymiarów polityki zagranicznej Rzeczypospolitej. (...) W interesie Polski leży, by narody jej wschodniego sąsiedztwa cieszyły się niepodległością i bezpieczeństwem, by (...) respektowano ich prawo do suwerennego wyboru drogi rozwoju, ustroju politycznego i sojuszy. Te z nich, które zdecydują o swej opcji proeuropejskiej i prozachodniej, mogą liczyć na wytrwałą pomoc Polski na rzecz realizacji obranego przez nie celu”¹²⁷².

Jednym z elementów realizowania powyższych założeń jest program Partnerstwa Wschodniego, który został zaprezentowany w roku 2008 na forum unijnym, a zatwierdzony w 2009. Jest on polsko-szwedzką inicjatywą, której celem z punktu widzenia interesów Warszawy jest wzmocnienie polskiej obecności we wschodnim wymiarze polityki zagranicznej Unii Europejskiej¹²⁷³. Z kolei z punktu widzenia Brukseli jest to program mający na celu integrację państw nim objętych ze strukturami unijnymi z perspektywą uzyskania członkostwa w organizacji. Partnerstwo Wschodnie jest adresowane do takich państw jak: Armenia, Azerbejdżan, Gruzja, Mołdawia, Białoruś i Ukraina, a więc z wyłączeniem Rosji¹²⁷⁴. Polska jest zatem zmuszona uwzględniać stanowiska innych państw członkowskich w zakresie podejmowanych w ramach programu inicjatyw. Co również istotne, w ramach prowadzonej polityki wschodniej Unia zawsze nadaje prymat relacjom z Rosją, aniżeli państwom objętym programem Partnerstwa Wschodniego. Można więc zauważyć, że skoro Federacja Rosyjska traktuje obszar poradziecki jako swoją wyłączną strefę wpływów, do której zaliczają się również państwa będące adresatami programu Partnerstwa Wschodniego, to w przypadku kolizji interesów na linii UE-Rosja oczywistym stanie się, że Bruksela nie będzie podejmować działań, które mogą zostać odebrane przez Kreml za wrogie¹²⁷⁵. W odniesieniu do integracji

¹²⁷⁰ M. Stolarczyk: *Rosja w polityce zagranicznej Polski...*, s. 158.

¹²⁷¹ Ibidem, s. 158-159.

¹²⁷² Ministerstwo Spraw Zagranicznych: *Polityka wschodnia*. <https://www.gov.pl/web/dyplomacja/polityka-wschodnia> (dostęp: 29.01.2023).

¹²⁷³ M. Sabat: *Stosunki polsko-rosyjskie. Rozbieżności interesów strategicznych*. W: *Polityka zagraniczna Federacji Rosyjskiej. Wybrane aspekty stosunków z Polską, Ukrainą i Białorusią*. Red. L. Zyblikiewicz, M. Czajkowski, P. Bajor. Kraków 2010, s. 122-124; M. Stolarczyk: *Rosja w polityce zagranicznej Polski...*, s. 208-209.

¹²⁷⁴ Rada Europejska, Rada Unii Europejskiej: *Partnerstwo Wschodnie*. <https://www.consilium.europa.eu/pl/policies/eastern-partnership/> (dostęp: 29.01.2023).

¹²⁷⁵ P. Stawarz: *Polityka wschodnia Unii Europejskiej*. W: *Polska i Rosja w zmieniającej się Europie*. Red. K. A. Wojtaszczyk, I. N. Novikova. Warszawa 2022, s. 401-402.

międzynarodowej w regionie zarówno UE jak i Rosja mają w tym zakresie odmienne koncepcje. Jak pisze A. Legucka, „rosyjska narracja dotycząca ‘większej Europy’, od Atlantyku po Władywostok, nie znalazła zrozumienia ani w UE, ani w regionie państw postsowieckich. Jednocześnie unijna koncepcja ‘szerszej Europy’, a następnie ‘wspólnego sąsiedztwa’, czyli współodpowiedzialności za państwa PW, nie spodobała się Rosjanom”¹²⁷⁶. Odnosząc stosunki polsko-rosyjskie do programu Partnerstwa Wschodniego należy zauważyć, że celem Warszawy jest jak najszersza integracja państw objętych programem ze strukturami Unijnymi¹²⁷⁷. Polska jako jeden z inicjatorów programu aktywnie angażuje się w jego realizację, czego konsekwencją jest ingerencja w rosyjską strefę wpływów, co natomiast determinuje i antagonizuje wzajemne stosunki Moskwy z Warszawą. Co istotne, program zyskał na znaczeniu wobec rosyjskiej agresji w Ukrainie w 2022 roku, czego następstwem było między innymi szybsze uzyskanie przez nią (wraz z Mołdawią) status państwa kandydującego¹²⁷⁸. Niemniej jednak nie wydaje się, aby wobec aktualnego przebiegu konfliktu rosyjsko-ukraińskiego (stan na styczeń 2025 roku), wizja pełnoprawnego członkostwa Ukrainy w Unii Europejskiej (czy też NATO) mogła być postrzegana jako prawdopodobna na przestrzeni najbliższych lat¹²⁷⁹.

Podsumowując, Program Partnerstwa Wschodniego ma na celu nie tylko wzmocnienie stabilności na wschodnich granicach Unii Europejskiej, ale również zacieśnienie więzi między Unią a państwami w regionie, co ma przeciwdziałać potencjalnym zagrożeniom wynikającym z utrzymujących się zamrożonych konfliktów i wpływów rosyjskich. Z kolei z perspektywy Federacji Rosyjskiej, szczególnie po rozpoczęciu pełnowymiarowej inwazji na Ukrainę w 2022 roku, Program Partnerstwa Wschodniego jest postrzegany jako narzędzie rozszerzania unijnego wpływu na terytoria tradycyjnie uznawane przez Moskwę za bliską zagranicę. Rosyjscy decydenci interpretują założenia programu jako element strategii, która ma na celu wyparcie Rosji z regionu. Ponadto jak próbę narzucenia unijnych norm i wartości, co w oczach Moskwy stanowi ingerencję w jej strefę wpływów. Wreszcie jako potencjalne zagrożenie dla bezpieczeństwa narodowego, ponieważ zacieśnianie współpracy między Unią Europejską a państwami takie jak Ukraina czy Gruzja jest widziane jako działania mające na celu osłabienie

¹²⁷⁶ A. Legucka: *Rosja wobec Partnerstwa Wschodniego Unii Europejskiej*. „Rocznik Instytutu Europy Środkowo-Wschodniej” 2019, nr 17 (2019), Zeszyt 2, s. 59; Zobacz szerzej: Ibidem, s. 41-59.

¹²⁷⁷ Ministerstwo Spraw Zagranicznych: *Partnerstwo Wschodnie*. <https://www.gov.pl/web/dyplomacja/partnerstwo-wschodnie> (dostęp: 29.01.2023)

¹²⁷⁸ Rada Europejska, Rada Unii Europejskiej: *Rada Europejska, 23–24 czerwca 2022*. <https://www.consilium.europa.eu/pl/meetings/european-council/2022/06/23-24/> (dostęp: 29.01.2023).

¹²⁷⁹ E. Kaca: *Debata o Partnerstwie Wschodnim w kontekście inwazji Rosji na Ukrainę*. „Biuletyn Polskiego Instytutu Spraw Międzynarodowych” 2022, nr 181 (2600). [https://www.pism.pl/webroot/upload/files/Biuletyn/Biuletyn%20PISM%20nr%20181%20\(2600\)%2024%20listopada%202022%20r.pdf](https://www.pism.pl/webroot/upload/files/Biuletyn/Biuletyn%20PISM%20nr%20181%20(2600)%2024%20listopada%202022%20r.pdf) (dostęp: 29.01.2023).

pozycji Rosji. Program Partnerstwa Wschodniego stanowi więc dla Polski ważne narzędzie, pozwalające na umocnienie wpływów europejskich w regionie, a tym samym ograniczenie rosyjskiej dominacji. W kontekście stosunków polsko-rosyjskich program nabiera wymiaru spornego w stosunkach bilateralnych z Moskwą. Dla Rosji inicjatywa jest bowiem symbolem unijnej ingerencji i ekspansji, co intensyfikuje istniejące spory o tożsamość, bezpieczeństwo oraz strefę wpływów w regionie.

Rozdział 6. Cyberataki jako instrument wojny informacyjnej Federacji Rosyjskiej wobec Polski w latach 2010-2022

6.1. Cyberbezpieczeństwo Polski w latach 2010-2022

Wojna informacyjna w ujęciu rosyjskim jest zjawiskiem wielowymiarowym, występującym na wielu płaszczyznach oraz będącym przedmiotem aktywności jednostek, grup wysoko zorganizowanych oraz państw. Prowadzone przez Kreml działania w tym zakresie obejmują również szeroko rozumianą cyberprzestrzeń¹²⁸⁰. Wskazuje na to chociażby R. Bebbler, który pisze o występowaniu trzech podstawowych elementów w rosyjskich koncepcjach wojny informacyjnej, jak: „ukierunkowanie na ludność danego kraju przy użyciu dyplomatów, wynajętych ‘ekspertów’ i naukowców, aby wpływać na postrzeganie i opinie; wykorzystanie operacji informacyjnych, aby kontrolować przekaz; oraz ofensywne operacje cybernetyczne przeciwko komputerom i systemom komunikacyjnym”¹²⁸¹. J. Darczewska z kolei pisząc o definicjach pojęcia wojny informacyjnej w terminologii rosyjskiej zauważyła, że „nie mieszczą się one w żadnej z definicji terminów przyjętych na Zachodzie. Terminy ‘wojna cybernetyczna’, ‘wojna informacyjna’, czy ‘wojna sieciowa’ mają w Rosji zdecydowanie odmienny zakres pojęciowy. Tylko nieliczni teoretycy rozróżniają ‘cyberwar’ i ‘netwar’, przeciwstawiając technologiczny i społeczny wymiar wojen IV generacji. Dotyczy to jednak z reguły publikacji omawiających zachodnią literaturę przedmiotu; w zdecydowanej większości rosyjscy autorzy pod pojęciem ‘wojna informacyjna’ rozumieją oddziaływanie na masową świadomość w międzypaństwowej rywalizacji systemów cywilizacyjnych w przestrzeni informacyjnej, wykorzystujące szczególne sposoby kontroli nad zasobami informacyjnymi, a używane w charakterze ‘broni informacyjnej’”¹²⁸². Z powyższego wynika traktowanie przez Rosjan omawianego pojęcia w sposób niezwykle wszechstronny, sprowadzający zjawisko wojny informacyjnej również do dokonywania cyberataków w cyberprzestrzeni. Takie działania są podejmowane przez Kreml między innymi względem Polski. Wobec tego celem wprowadzenia do badań w niniejszym podrozdziale w pierwszej

¹²⁸⁰ Zobacz szerzej: *Rozdział 4. Wojna informacyjna w polityce zagranicznej Federacji Rosyjskiej*.

¹²⁸¹ R. Bebbler: *Information War and Rethinking Phase 0*. „Journal of Information Warfare” 2016, Vol. 15, Issue 2, s. 44. Tłumaczenie własne. Tekst w oryginale: „the targeting of the domestic population of a country using diplomats, hired ‘experts’ and academics to influence perceptions and opinions; the use of information operations to control the message; and offensive cyber operations against computers and communication systems”.

¹²⁸² J. Darczewska: *Anatomia rosyjskiej wojny informacyjnej Operacja Krymska – studium przypadku*. „Punkt widzenia” 2014, nr 42. https://www.osw.waw.pl/sites/default/files/anatomia_rosyjskiej_wojny_informacyjnej.pdf (dostęp: 01.02.2023), s. 12.

kolejności omówiono aspekty teoretyczne dotyczące cyberprzestrzeni. Należy przez to rozumieć stopień informatyzacji i digitalizacji w Polsce, związane z tym zagrożenia dla bezpieczeństwa teleinformatycznego oraz funkcjonujący system cyberbezpieczeństwa mający na celu przeciwdziałanie występującym zagrożeniom.

6.1.1. Stopień informatyzacji i digitalizacji w Polsce w latach 2010-2022

Zdolności danego państwa w zakresie działania w cyberprzestrzeni są uwarunkowane przede wszystkim stopniem jego informatyzacji oraz digitalizacji. Pierwsze z pojęć – *informatyzacja* – odnosi się do stosowania nowoczesnych metod przetwarzania informacji¹²⁸³, co następuje w wyniku uprzednio dokonanej *komputeryzacji*, czyli wprowadzenia nowoczesnych urządzeń jak komputery, telefony itp.¹²⁸⁴. Termin komputeryzacja może być również rozumiany jako proces używania komputera do wykonywania czynności, które wcześniej były wykonywane przez ludzi lub inne maszyny¹²⁸⁵. Drugi z terminów – *digitalizacja* – jest definiowany jako konwersja informacji z danej postaci na postać cyfrową, zdolną do bycia przetwarzaną i przechowywaną przez urządzenia elektroniczne¹²⁸⁶. Termin ten bywa również zestawiany z pojęciem *cyfryzacji*, a więc przeprowadzenia zmiany rodzaju sygnału z analogowego¹²⁸⁷ na sygnał cyfrowy (zastępowanie urządzeń działających analogowo na urządzenia cyfrowe)¹²⁸⁸. Wobec powyższego, im większa informatyzacja oraz digitalizacja danego państwa, tym lepiej jest rozwinięta jego cyberprzestrzeń.

Polskę należy zaliczyć do grupy państw o stosunkowo dobrej informatyzacji oraz digitalizacji. Nie można natomiast określić jej jako państwa wiodącego w skali globalnej w powyższych dziedzinach, jednakże nie można również nadać jej miana zacofanego, czy też nieprzystosowanego do postępującej rewolucji informacyjnej i technologicznej. Trzeba ponadto zauważyć, że różne ekipy rządzące w Polsce zdawały sobie sprawę z wagi omawianych

¹²⁸³ Słownik Języka Polskiego PWN: *informatyzacja*. <https://sjp.pwn.pl/szukaj/informatyzacja.html> (dostęp: 01.02.2023).

¹²⁸⁴ Encyklopedia PWN: *komputeryzacja*. <https://encyklopedia.pwn.pl/haslo/komputeryzacja;3924656.html> (dostęp: 01.02.2023); Słownik Języka Polskiego PWN: *komputeryzacja*. <https://encyklopedia.pwn.pl/haslo/komputeryzacja;3924656.html> (dostęp: 01.02.2023).

¹²⁸⁵ Cambridge Dictionary: *computerization*. <https://dictionary.cambridge.org/dictionary/english/computerization> (dostęp: 01.02.2023).

¹²⁸⁶ Cambridge Dictionary: *digitalize*. <https://dictionary.cambridge.org/dictionary/english/digitalize?q=digitalization> (dostęp: 01.02.2023).

¹²⁸⁷ Sygnał analogowy cechuje się tym, że może przybrać dowolną wartość. Sygnałem analogowym jest zapis na taśmie magnetycznej czy odtwarzacz płyty. Inaczej wygląda to w przypadku sygnału cyfrowego, gdzie jego przetwarzanie opiera się na systemie binarnym, czyli opartym o architekturę zero-jedynkową.

¹²⁸⁸ Encyklopedia PWN: *cyfryzacja*. <https://encyklopedia.pwn.pl/haslo/cyfryzacja;4007905.html> (01.02.2023).

zagadnień, lecz nadawanie im odpowiedniego wymiaru przebiegało z różnym skutkiem. Informacje w tym zakresie można odnaleźć w oficjalnych dokumentach rządowych, a z uwagi na przyjętą cezurę czasową są to: Plan Informatyzacji Państwa na lata 2007-2010¹²⁸⁹, projekt Planu Informatyzacji Państwa na lata 2011-2015¹²⁹⁰ oraz Program Zintegrowanej Informatyzacji Państwa na lata 2014-2022 (zaktualizowany w 2016 roku oraz w 2019 roku – przedłużony do 2022 roku)¹²⁹¹.

We wskazanych wyżej dokumentach, począwszy od pierwszego z nich, wielokrotnie zauważano, iż priorytetowym celem ich realizacji jest przekształcenie Polski w państwo nowoczesne. Jest to również neutralizacja technologiczna oraz racjonalizacja wydatków administracji publicznej, związanych z jej informatyzacją oraz rozwojem społeczeństwa informacyjnego¹²⁹². W drugim z dokumentów (projekcie) planowano przyjęcie takich celów strategicznych jak: świadczenie usług elektronicznych odpowiadających potrzebom obywateli i biznesu; zwiększenie sprawności i efektywności funkcjonowania administracji publicznej dzięki zastosowaniu nowoczesnych narzędzi teleinformatyki oraz tworzenie warunków dla rozwoju społeczeństwa informacyjnego¹²⁹³. Wreszcie ostatni z dokumentów za cel strategiczny uznał „zwiększenie zarówno podaży oczekiwanych przez społeczeństwo wysokiej jakości publicznych e-usług w Polsce, jak i poziomu ich wykorzystania mierzonego odsetkiem obywateli i przedsiębiorców, korzystających z Internetu w relacjach z administracją publiczną, zgodnie z celami strategii Sprawne Państwo oraz Europejskiej Agendy Cyfrowej, z poziomu 32% w 2012 do 64% w 2020 (w przypadku obywateli) i z poziomu 90% w 2012 do 95% w 2020 (dla przedsiębiorców) roku”¹²⁹⁴. W kolejnych latach dokonano aktualizacji przyjętych

¹²⁸⁹ Rozporządzenie Rady Ministrów z dnia 28 marca 2007 r. w sprawie Planu Informatyzacji Państwa na lata 2007-2010 (Dz.U. 2007 nr 61 poz. 415).

¹²⁹⁰ Ministerstwo Spraw Wewnętrznych i Administracji. Biuletyn Informacji Publicznej: *Projekt rozporządzenia Rady Ministrów z dnia .. 2011 r. w sprawie Planu Informatyzacji Państwa na lata 2011-2015* (skierowany do uzgodnień międzyresortowych, z 21-dniowym terminem na zgłaszanie uwag). <https://archiwumbip.mswia.gov.pl/bip/projekty-aktow-prawnyc/2011/19948,Projekt-rozporzadzenia-Rady-Ministrow-z-dnia-2011-r-w-sprawie-Planu-Informatyzac.html> (dostęp: 02.02.2023).

¹²⁹¹ Ministerstwo Cyfryzacji. Biuletyn Informacji Publicznej: *Program Zintegrowanej Informatyzacji Państwa - wrzesień 2016 r.* <https://mc.bip.gov.pl/programy-realizowane-w-mc/program-zintegrowanej-informatyzacji-panstwa-wrzesien-2016-r.html> (dostęp: 02.02.2023); gov.pl: *Program Zintegrowanej Informatyzacji Państwa*. <https://www.gov.pl/web/cyfryzacja/program-zintegrowanej-informatyzacji-panstwa> (dostęp: 02.02.2023).

¹²⁹² Rozporządzenie Rady Ministrów z dnia 28 marca 2007 r. w sprawie Planu Informatyzacji Państwa na lata 2007-2010 (Dz.U. 2007 nr 61 poz. 415), Część 1.

¹²⁹³ Ministerstwo Spraw Wewnętrznych i Administracji. Biuletyn Informacji Publicznej: *Projekt rozporządzenia Rady Ministrów z dnia .. 2011 r. w sprawie Planu Informatyzacji Państwa na lata 2011-2015* (skierowany do uzgodnień międzyresortowych, z 21-dniowym terminem na zgłaszanie uwag). <https://archiwumbip.mswia.gov.pl/bip/projekty-aktow-prawnyc/2011/19948,Projekt-rozporzadzenia-Rady-Ministrow-z-dnia-2011-r-w-sprawie-Planu-Informatyzac.html> (dostęp: 02.02.2023), s. 9.

¹²⁹⁴ Ministerstwo Cyfryzacji. Biuletyn Informacji Publicznej: *Program Zintegrowanej Informatyzacji Państwa - wrzesień 2016 r.* <https://mc.bip.gov.pl/programy-realizowane-w-mc/program-zintegrowanej-informatyzacji-panstwa-wrzesien-2016-r.html> (dostęp: 02.02.2023), s. 26.

uprzednio założeń, przede wszystkim w oparciu o wnioski z dotychczasowej ich realizacji¹²⁹⁵. Należy zauważyć, że zagadnienia związane z komputeryzacją oraz informatyzacją były dostrzegane w starszych odpowiednikach omawianych dokumentów, jak na przykład Strategii kierunkowej rozwoju informatyzacji Polski do roku 2013 oraz perspektywicznej prognozy transformacji społeczeństwa informacyjnego do roku 2020, gdzie wskazano na istotną rolę tych procesów w zakresie znaczenia pozycji Polski w Unii Europejskiej oraz konkurencyjności krajowej gospodarki w wymiarze narodowym oraz międzynarodowym¹²⁹⁶. Wartym wspomnienia jest też realizowany przy wsparciu funduszy z Unii Europejskiej program Polska Cyfrowa. Jego celem jest finansowanie projektów mających za zadanie zwiększanie dostępności Internetu, wprowadzanie nowych usług w e-administracji oraz zwiększanie kompetencji cyfrowych w społeczeństwie¹²⁹⁷.

Z zagadnieniem informatyzacji oraz digitalizacji państwa nierozzerwalnie związane pozostaje występowanie w nim społeczeństwa informacyjnego, będącego w tym zakresie jednocześnie czynnikiem o charakterze pierwotnym, jak i wtórnym. Informatyzacja oraz digitalizacja powodują bowiem powstanie i rozwój społeczeństwa informacyjnego, które ze swej istoty skutkuje pogłębianiem tych procesów. Realizowanie założeń i celów zawartych w programach krajowych nie byłoby możliwe, gdyby nie powszechna dostępność Internetu, zarówno dla gospodarstw domowych jak i podmiotów gospodarczych. W przypadku pierwszej z grup w 2010 roku dostęp do Internetu (łączy szerokopasmowych¹²⁹⁸) posiadało ogółem ponad 63% z nich, w 2014 roku było to już prawie 75%¹²⁹⁹, w 2018 roku ponad 84%, a w 2022 roku ponad 93%¹³⁰⁰. Widać zatem, że dostępność sieci internetowej dla obywateli z roku na rok wzrasta. Podobna sytuacja ma miejsce w przypadku przedsiębiorców. W 2010 roku około 70% z nich posiadało dostęp do łączy szerokopasmowych, a już w 2014 roku było to około 90%¹³⁰¹. Z kolei w 2022 roku według Głównego Urzędu Statystycznego odsetek ten wyniósł 98,5%¹³⁰².

¹²⁹⁵ gov.pl: *Program Zintegrowanej Informatyzacji Państwa*. <https://www.gov.pl/web/cyfryzacja/program-zintegrowanej-informatyzacji-panstwa> (dostęp: 02.02.2023); Ibidem.

¹²⁹⁶ M. Lakomy: *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*. Katowice 2015, s. 57.

¹²⁹⁷ Serwis Programu Polska Cyfrowa: *Dowiedz się więcej o programie*. <https://www.polskacyfrowa.gov.pl/strony/o-programie/> (03.02.2023).

¹²⁹⁸ Połączenie szerokopasmowe to „rodzaj połączeń internetowych charakteryzujących się dużą prędkością przepływu informacji”. Źródło: Główny Urząd Statystyczny: *Spółeczeństwo informacyjne w Polsce w 2020 r.* Warszawa, Szczecin 2020, s. 133.

¹²⁹⁹ Główny Urząd Statystyczny: *Spółeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2010-2014*. Warszawa 2014, s. 108.

¹³⁰⁰ Główny Urząd Statystyczny: *Spółeczeństwo informacyjne w Polsce w 2022 r.* Warszawa, Szczecin 2022, s. 108.

¹³⁰¹ Główny Urząd Statystyczny: *Spółeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2010-2014...*, s. 43.

¹³⁰² Główny Urząd Statystyczny: *Spółeczeństwo informacyjne w Polsce w 2022 r...*, s. 73.

W Polsce są również systematycznie wprowadzane nowe rozwiązania technologiczne. Przykładem mogą być nowe standardy sieci mobilnych¹³⁰³ i rok 2020 w którym rozpoczęto użytkowanie sieci 5G¹³⁰⁴.

W światowych rankingach mających za przedmiot ocenę z informatyzowania państwa i digitalizacji administracji publicznej oraz jakości życia z wykorzystaniem usług cyfrowych, Polska nie plasuje się na względnie wysokich pozycjach. Według raportu¹³⁰⁵ Organizacji Narodów Zjednoczonych United Nations E-Government Survey 2010, Polska pod względem rozwoju e-administracji zajęła 45. miejsce¹³⁰⁶, z kolei w rankingu z 2022 roku uplasowała się na 34. miejscu¹³⁰⁷. Dla porównania należy jednak zauważyć, że w 2003 roku Polska zajmowała w rankingu 32. miejsce¹³⁰⁸, natomiast raporty z 2010 i 2012 roku odnotowały najniższe pozycje w historii¹³⁰⁹. W odniesieniu do zestawienia z 2022 roku Polskę wyprzedzają takie państwa jak Łotwa (29. miejsce), Litwa (24. miejsce), Malta (15. miejsce), Estonia (8. miejsce), Finlandia (2. miejsce) czy Dania (1. miejsce). Z kolei Polska wyprzedza takie państwa jak Włochy (37. miejsce), Belgia (39. miejsce) oraz Rosja (42. miejsce)¹³¹⁰. Z państw pozaeuropejskich w czołówce znajdują się takie jak: Korea Południowa (3. miejsce), USA (10. miejsce), Japonia (14. miejsce) oraz Izrael (16. miejsce)¹³¹¹. Według innego zestawienia¹³¹² Polska pod względem jakości cyfrowego dobrobytu w 2022 roku zajęła 23 miejsce na świecie, ustępując takim państwom jak Izrael (1. miejsce), Dania (2. miejsce), Niemcy (3. miejsce), Francja (4. miejsce) oraz Szwecja (5. miejsce)¹³¹³. W 2022 roku pozycja Polski wśród państw

¹³⁰³ Zobacz szerzej: Ministerstwo Cyfryzacji, Instytut Łączności, Collegium Medicum UJ: *Przewodnik po 5G 2019*. <https://www.gov.pl/web/5g/przewodnik-po-5g> (dostęp: 03.02.2023).

¹³⁰⁴ Platforma Przemysłu Przyszłości: *Pierwszy operator uruchomił w Polsce 100 komercyjnych nadajników 5G*. <https://przemyslprzyszlosci.gov.pl/pierwszy-operator-uruchomil-w-polsce-100-komercyjnych-nadajnikow-5g/> (dostęp: 03.02.2023).

¹³⁰⁵ Raporty przygotowywane przez Organizację Narodów Zjednoczonych obejmują trzy subwskaźniki takie jak: usługi sieciowe, infrastruktura telekomunikacyjna oraz kapitał ludzki. Źródło: M. Goliński: *E-administracja w Polsce w świetle badań ONZ*. „Roczniki Kolegium Analiz Ekonomicznych” 2015, nr 38, 2015, s. 75-77.

¹³⁰⁶ United Nations. Department of Economic and Social Affairs: *E-Government Survey 2010. Leveraging e-government at a time of financial and economic crisis*. New York 2010, s. 72, 114.

¹³⁰⁷ United Nations. Department of Economic and Social Affairs: *E-Government Survey 2022. The Future of Digital Government*. New York 2022, s. 72.

¹³⁰⁸ UN E-Government Knowledgebase: *Poland*. <https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/135-Poland/dataYear/2003> (dostęp: 02.02.2023).

¹³⁰⁹ UN E-Government Knowledgebase: *Poland*. <https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/135-Poland/dataYear/2010>, <https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/135-Poland/dataYear/2012> (dostęp: 02.02.2023).

¹³¹⁰ United Nations. Department of Economic and Social Affairs: *E-Government Survey 2022...*, s. 72.

¹³¹¹ Ibidem, s. 66, 69.

¹³¹² Badanie objęło 117 państw, reprezentujących 92% populacji. Indeks bazuje na pięciu kategoriach takich jak dostępność Internetu, jakość Internetu, infrastruktura elektroniczna, cyberbezpieczeństwo oraz z informatyzowanie administracji. Źródło: DQL: *2022 Digital Quality of Life Index*. <https://surfshark.com/dql2022> (dostęp: 02.02.2023).

¹³¹³ DQL: *2022 Digital Quality of Life Index*. <https://surfshark.com/dql2022>, <https://surfshark.com/dql2022?country=PL> (dostęp: 02.02.2023).

członkowskich Unii Europejskiej pod względem dostępu do Internetu w gospodarstwach domowych (przy użyciu łącza szerokopasmowego) uplasowała się powyżej średniej unijnej z wynikiem 92%¹³¹⁴. Warto jednak przytoczyć inny wskaźnik, publikowany od 2014 roku przez Komisję Europejską, tj. Indeks gospodarki cyfrowej i społeczeństwa cyfrowego (DESI)¹³¹⁵. W tym zestawieniu według danych z 2021 roku Polska nie wypada najlepiej pod względem cyfryzacji usług publicznych dla obywateli oraz przedsiębiorstw, zajmując 24. miejsce¹³¹⁶. Zestawienie to wyglądało podobnie w 2015 roku – 22. miejsce¹³¹⁷. Należy jednak zauważyć, że w latach 2017-2022 Polska wraz z Włochami, Niemcami, Francją i Irlandią znajdowała się w grupie państw o najwyższym tempie wzrostu w zakresie rozwoju gospodarki i społeczeństwa cyfrowego¹³¹⁸. Ponadto Polska pozostaje w czołówce państw realizujących unijną inicjatywę EU Code Week, której celem jest promowanie umiejętności cyfrowych oraz programowania¹³¹⁹. Z powyższych raportów wynika również, że Polska może być traktowana jako jeden z liderów informatyzacji w regionie. Najlepiej rozwinięte pozostają cyfrowe usługi publiczne (choć nadal znajdują się one poniżej średniej unijnej)¹³²⁰, w ramach których Polska przoduje w na tle państwa Europy Środkowo-Wschodniej¹³²¹. Unia Europejska podejmuje liczne działania mające na celu cyfryzację życia publicznego państw członkowskich. Dla przykładu w ramach Instrumentu na rzecz Odbudowy i Zwiększania Odporności (Krajowy Plan Odbudowy [KPO] – nazwa w Polsce) ponad 20% środków jest przeznaczonych na transformację cyfrową¹³²². Co istotne Komisja Europejska za kluczowe osiągnięcie Polski w latach 2021-2022 uznała walkę z dezinformacją. Wskazano, że „Polska utworzyła specjalny zespół zajmujący się monitorowaniem publikacji w mediach społecznościowych i identyfikacją kampanii dezinformacyjnych. Walką z dezinformacją w sieci zajmuje się NASK (Państwowy Instytut Badawczy), który prowadzi profile #WłączWeryfikację. Profile #WłączWeryfikację

¹³¹⁴ Główny Urząd Statystyczny: *Spółeczeństwo informacyjne w Polsce...*, s. 113.

¹³¹⁵ Wskaźnik uwzględnia takie wartości jak: kapitał ludzki, łączność, integracja technologii cyfrowych oraz cyfrowe usługi publiczne. Źródło: European Commission: *The Digital Economy and Society Index (DESI)*. <https://digital-strategy.ec.europa.eu/en/policies/desi> (03.02.2023).

¹³¹⁶ European Commission: *Digital Economy and Society Index (DESI) 2022*. <https://ec.europa.eu/newsroom/dae/redirection/document/88764> (dostęp: 03.02.2023), s. 68-69.

¹³¹⁷ European Commission: *Indeks gospodarki cyfrowej i społeczeństwa cyfrowego na 2016 r. Profil krajowy Polska*. https://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=14161 (dostęp: 03.02.2023), s. 1.

¹³¹⁸ European Commission: *Digital Economy and Society Index (DESI) 2022*. <https://ec.europa.eu/newsroom/dae/redirection/document/88764> (dostęp: 03.02.2023), s. 17.

¹³¹⁹ Ibidem, s. 27

¹³²⁰ European Commission: *Indeks gospodarki cyfrowej i społeczeństwa cyfrowego (DESI) na 2022 r. Polska*. <https://ec.europa.eu/newsroom/dae/redirection/document/88756> (dostęp: 03.02.2023), s. 4.

¹³²¹ Digital Poland, Microsoft: *Stan cyfryzacji Polski na tle regionu 2022*. <https://digitalpoland.org/publikacje/pobierz?id=4ceb0166-6dd6-4c58-ab9a-cf77f56d7c20> (dostęp: 03.02.2023), s. 19.

¹³²² European Commission: *Indeks gospodarki cyfrowej i społeczeństwa cyfrowego (DESI) na 2022 r. Polska*. <https://ec.europa.eu/newsroom/dae/redirection/document/88756> (dostęp: 03.02.2023), s. 5.

prowadzą eksperci instytutu, którzy dementują nieprawdziwe informacje krążące w sieci. Niebezpieczne posty można zgłaszać administracji portalu za pomocą mediów społecznościowych albo bezpośrednio do NASK, pisząc na specjalny adres e-mail”¹³²³.

Podsumowując powyższe rozważania należy ocenić stan informatyzacji oraz digitalizacji w Polsce jako dobry. Choć państwo nie znajduje się w czołówce światowej czy europejskiej pod tym względem, to jednak w ostatnich latach procesy te cechowały się stosunkowo wysoką dynamiką – co wynika między innymi ze świadomości rządzących w Polsce i UE w zakresie znaczenia cyberprzestrzeni dla rozwoju państwa. Zarówno gospodarstwa domowe jak i przedsiębiorstwa posiadają w przeważającej liczbie podłączenie do szerokopasmowego Internetu, a dostęp do usług e-administracji należy określić jak wysoki, choć wymagający dalszego doskonalenia. Tym samym Polska posiada dobrą perspektywę do dalszego rozwoju w omawianym zakresie. Należy jednak zauważyć i szczególnie podkreślić, że im wyższy poziom zinformatyizowania państwa i digitalizacji administracji publicznej oraz wykorzystania usług cyfrowych w codziennym życiu obywateli, tym większa skala i podatność na występujące w cyberprzestrzeni zagrożenia. W kontekście problemu badawczego będącego przedmiotem niniejszej rozprawy, należy podkreślić, że wrocie działania Federacji Rosyjskiej podejmowane w cyberprzestrzeni wobec Polski, stanowią istotne zagrożenie dla bezpieczeństwa teleinformatycznego. Z uwagi na liczne kwestie sporne występujące w stosunkach bilateralnych na linii Warszawa-Moskwa, Polska pozostaje istotnym celem rosyjskich cyberataków.

6.1.2. Zagrożenia dla bezpieczeństwa teleinformatycznego Polski w latach 2010-2022

Wraz z postępującymi w państwie procesami digitalizacji i informatyzacji, należy mówić o rozwoju szeroko rozumianej cyberprzestrzeni, jak i kształtowania rozwiniętego społeczeństwa informacyjnego. Jednocześnie powyższe zjawiska implikują powstawanie szeregu zagrożeń dla bezpieczeństwa informacyjnego¹³²⁴ oraz teleinformatycznego¹³²⁵. Można więc wyróżnić ogólny katalog zagrożeń dla bezpieczeństwa informacji przyjmując, że są to

¹³²³ Ibidem, s. 19.

¹³²⁴ Bezpieczeństwo informacyjne to ogólna definicja „łącząca w sobie szereg cząstkowych ujęć, które odnieść należy do narzędzi i procedur ochrony danych, informacji i systemów informacyjnych”. Źródło: J. Kaczmarek, W. Łepkowski, B. Zdrodowski (Red.): *Słownik terminów z zakresu bezpieczeństwa narodowego*. Warszawa 2008, s. 16.

¹³²⁵ Bezpieczeństwo teleinformatyczne stanowi „ogół przedsięwzięć obejmujących ochronę zinformatyizowanych działów strategicznych, do których można dotrzeć przy pomocy połączeń sieciowych. Wszelkie aspekty bezpieczeństwa teleinformatycznego związane są z definiowaniem, osiąganiem i utrzymywaniem poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności”. Źródło: Ibidem, s. 21.

„katastrofy naturalne; błędy ludzi wykorzystujących lub obsługujących systemy informacyjne; błędy w organizacji pracy i procedurach; celowe, szkodliwe działania ludzi skierowane na systemy informacyjne; awarie sprzętu (elementów i podzespołów mechanicznych, elektronicznych, elektromechanicznych) i wady oprogramowania”¹³²⁶. Natomiast w odniesieniu do bezpieczeństwa systemów teleinformatycznych, do podstawowych zagrożeń zalicza się *hacking*, haktywizm, cyberprzestępczość, cyberterrorizm, cyberszpiegostwo oraz zbrojne wykorzystanie cyberprzestrzeni¹³²⁷.

Omawiając zagadnienie zagrożeń dla bezpieczeństwa w cyberprzestrzeni, należy szczególną uwagę zwrócić na te odnoszące się do krajowej infrastruktury krytycznej¹³²⁸. Można ją zdefiniować jako systemy, zarówno fizyczne jak i wirtualne, których zakłócenie funkcjonowania może mieć istotny wpływ na bezpieczeństwo narodowe i publiczne, kwestie gospodarcze czy zdrowotne¹³²⁹. Według Rządowego Centrum Bezpieczeństwa w Polsce składają się na nią systemy „zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, sieci teleinformatycznych, finansowe, zaopatrzenia w żywność, zaopatrzenia w wodę, ochrony zdrowia, transportowe, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych”¹³³⁰. Powyższe systemy pełnią kluczową rolę dla funkcjonowania państwa oraz życia obywateli, a postępująca informatyzacja oraz digitalizacja – również w tych przestrzeniach – sprawia, że są one podatne na szereg zagrożeń o charakterze naturalnym, technicznym czy terrorystycznym¹³³¹. Należy jednocześnie zauważyć, iż w przeszłości elementy omawianej infrastruktury działały co do zasady niezależnie od siebie, z kolei wobec zachodzących procesów globalizacyjnych, stają się współzależne i to nie tylko w skali danego państwa, ale również regionu czy świata¹³³².

¹³²⁶ K. Liderman: *Bezpieczeństwo informacyjne*. Warszawa 2012, s. 33.

¹³²⁷ M. Lakomy: *Zagrożenia dla bezpieczeństwa teleinformatycznego państw - przyczynek do typologii*. „Kwartalnik Naukowy OAP UW e-Politikon” 2013, Nr 6, s. 102-110.

¹³²⁸ Pojęcie infrastruktury krytycznej pojawiło się w Polsce na gruncie prawnym po raz pierwszy w ustawie z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym, gdzie przyjęto definicję legalną tego terminu, wskazując, że są to „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców”. Źródło: *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* (Dz.U. 2007 nr 89 poz. 590), s. 1.

¹³²⁹ C. Alcaraz, S. Zeadally: *Critical Infrastructure Protection: Requirements and Challenges for the 21st Century*. „International Journal of Critical Infrastructure Protection” 2015, Vol. 8, s. 1-5.

¹³³⁰ Rządowe Centrum Bezpieczeństwa: *Systemy infrastruktury krytycznej*. <https://www.gov.pl/web/rcb/systemy-infrastruktury-krytycznej> (dostęp: 04.02.2023).

¹³³¹ J. Milewski: *Identyfikacja infrastruktury krytycznej i jej zagrożeń*. „Zeszyty naukowe AON” 2016, nr 4 (105) 2016, s. 99-101, 107-108.

¹³³² T. Szewczyk, M. Pyznar: *Ochrona infrastruktury krytycznej a zagrożenia asymetryczne*. „Przegląd Bezpieczeństwa Wewnętrznego” 2010, nr 2/10, s. 54-55.

Niezbędne jest zatem zapewnienie im dostatecznej ochrony, co na gruncie polskiego porządku prawnego zdefiniowano w ustawie jako „wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie”¹³³³. Co jednak szczególnie ważne, zagrożenia związane z funkcjonowaniem infrastruktury krytycznej to nie tylko oddziaływanie fizyczne na obiekty, ale przede wszystkim działalność prowadzona w cyberprzestrzeni. Ataki stają się coraz bardziej rozproszone, mając zarówno charakter prosty jak i zorganizowany¹³³⁴. W kontekście prezentowanego w pracy problemu badawczego do ważniejszych zagrożeń zaliczono incydenty cybernetyczne (ataki DoS, *malware*, *phishing*), incydenty kryminalne, ataki terrorystyczne oraz ataki na łańcuchy dostaw (spowodowanie awarii systemu lub sieci), ale również operacje wywierania wpływu z zagranicy (rozpowszechnianie dezinformacji oraz podważanie wartości demokratycznych)¹³³⁵. Zagrożenia dla infrastruktury krytycznej są spowodowane głównie przez luki istniejące w jej zasobach, które mogą być wykorzystane do wprowadzenia zmian uniemożliwiających jej prawidłowe funkcjonowanie¹³³⁶.

Przechodząc do zagrożeń dla bezpieczeństwa cybernetycznego Polski w latach 2010-2022 należy wskazać na podstawowe wnioski płynące z corocznych raportów publikowanych przez Zespół CERT Polska oraz Zespół CSIRT GOV (wcześniej CERT GOV, CERT.GOV.PL)¹³³⁷. Według raportu CERT z 2010 roku Polska korzystnie wypadła „na tle innych państw, jeśli chodzi o liczbę zagrożeń mających źródło w danym państwie. We wszystkich statystykach Polska jest poza pierwszą dziesiątką, pośród państw o porównywalnej wielkości i o podobnym stopniu z informatyzowania”¹³³⁸. W tym samym roku ujawniono robaka Stuxnet¹³³⁹, który pojawił się również w polskiej cyberprzestrzeni, atakując instalacje

¹³³³ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2007 nr 89 poz. 590), s. 2.

¹³³⁴ Cybersecurity and Infrastructure Security Agency: *A Guide to Critical Infrastructure Security and Resilience*. November 2019. <https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf> (dostęp: 04.02.2023), s. 6.

¹³³⁵ Ibidem, s. 7.

¹³³⁶ C. Alcaraz, S. Zeadally: *Critical Infrastructure Protection...*, s. 5-7.

¹³³⁷ W odniesieniu do raportów rocznych opublikowanych przez Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV należy zaznaczyć, że autor w pracy posługuje się nazwą podmiotu obowiązującą na dzień 31 grudnia 2022 roku (koniec cezury czasowej badań). Uwzględnić jednak należy, że do wejścia w życie w 2018 roku ustawy o krajowym systemie cyberbezpieczeństwa, instytucja działała pod nazwą: Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL. Dlatego też w raportach rocznych za lata 2010-2017 występuje nazwa CERT GOV (CERT.GOV.PL), z kolei za lata 2018-2022 nazwa CSIRT GOV.

¹³³⁸ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2010. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2010.pdf (dostęp: 05.02.2023), s. 3.

¹³³⁹ M. Lakomy: *Cyberprzestrzeń jako nowy...*, s. 125 i nast.

przemysłowe¹³⁴⁰. Ciekawy w ujęciu globalnym pozostaje udział Rosji, gdyż spekuluje się, iż robak dostał się do sieci teleinformatycznej elektrowni w Iranie za pośrednictwem komputerów należących do rosyjskiej firmy wykonującej prace kontraktowe¹³⁴¹. Zauważono również zmianę charakteru cyberzagrożeń z cyberataków o podłożu czysto kryminalnym na cyberataki o znamionach cyberszpiegostwa (cyberwojny). Tym samym nastąpił wzrost znaczenia problematyki bezpieczeństwa teleinformatycznego w sferze państwowej, a spadł w kontekście obszaru ochrony bezpieczeństwa i porządku publicznego¹³⁴². W 2011 roku zaobserwowano na duży atak przeprowadzony poprzez rozsyłanie fałszywej faktury, po której otwarciu następowała instalacja złośliwego oprogramowania przejmującego kontrolę nad komputerem. Ponad zaznaczono, że połowa obsługiwanych przez Zespół CERT Polska incydentów dotyczyła *phishingu*, do którego wykorzystywano głównie polskie domeny w sieci¹³⁴³. Wskazano na ewolucję metod przeprowadzania cyberataków, jak również niespotykaną dotąd liczbę podejmowanych prób przełamania zabezpieczeń sieci podmiotów należących do administracji państwowej¹³⁴⁴. W 2012 roku zaobserwowano wzrost incydentów związanych z *phishingiem*. Polska ponownie dobrze wypadła pod względem liczby zagrożeń na tle innych państw. Ponadto wzrosła liczba incydentów obsługiwanych przez Zespół ręcznie, jak również tych pochodzących z zagranicy od podmiotów komercyjnych w stosunku do osób prywatnych z Polski¹³⁴⁵. W 2012 roku doszło do licznych protestów społecznych związanych z ratyfikacją umowy ACTA¹³⁴⁶. Ich konsekwencją był znaczny wzrost dokonanych ataków na Polskę w cyberprzestrzeni, przede wszystkim typu DDoS. Ich ofiarami padła grupa instytucji państwowych, w tym między innymi: Kancelaria Sejmu RP, Kancelaria Prezydenta RP, Kancelaria Premiera Rady Ministrów, Ministerstwo Spraw Zagranicznych, Ministerstwo Sprawiedliwości, Ministerstwo Edukacji Narodowej, Kancelaria Senatu RP, Ministerstwo Kultury i Dziedzictwa Narodowego, Ministerstwo Obrony Narodowej, Komenda Główna

¹³⁴⁰ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2010...*, s. 4.

¹³⁴¹ Ibidem, s. 37.

¹³⁴² Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2010 roku*. <https://csirt.gov.pl/download/3/121/Analizaroczna2010.pdf> (dostęp: 21.02.2023), s. 6.

¹³⁴³ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2011. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2011.pdf (dostęp: 05.02.2023), s. 5-7.

¹³⁴⁴ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2011 roku*. <https://csirt.gov.pl/download/3/137/Raportroczny2011.pdf> (dostęp: 21.02.2023), s. 5.

¹³⁴⁵ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2012. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2012.pdf (dostęp: 05.02.2023), s. 6.

¹³⁴⁶ Rzeczpospolita: *Atak za ACTA: Rządowe strony zablokowane*. <https://www.rp.pl/kraj/art6300061-atak-za-acta-rzadowe-strony-zablokowane> (dostęp: 24.04.2023).

Policji oraz Centralne Biuro Antykorupcyjne¹³⁴⁷. W roku 2013 stwierdzono coraz bardziej nowatorskie narzędzia wyłudzenia danych oraz kradzieży środków z kont bankowych. Spadła liczba spamu rozsyłanego z polskich sieci oraz wykorzystanie polskich domen w złośliwych celach¹³⁴⁸. W raporcie Zespołu CSIRT GOV zaobserwowano wzrost liczby występujących zagrożeń, co było jednak spowodowane rozpoczęciem funkcjonowania platformy N6, której celem jest gromadzenie, przetwarzanie oraz przekazywanie informacji o incydentach teleinformatycznych¹³⁴⁹. Z raportu CERT Polska za rok 2014 wynika, iż według szacunków Zespołu codziennie w ciągu 24 godzin w Polsce jest zainfekowanych około 280 tysięcy komputerów. W stosunku do ataków na sektor finansowy zauważono trend wzrostowy, co miało miejsce również wobec klientów korporacyjnych oraz administracji samorządowej¹³⁵⁰. Z kolei CSIRT GOV (ówcześnie CERT.GOV.PL) raportował o wzroście liczby obsługiwanych incydentów, jak również o nowym trendzie w kontekście cyberzagrożeń, jakim stała się wojna informacyjna¹³⁵¹. W 2015 roku zaobserwowano, że wzmożenie ataków ukierunkowanych na duże instytucje oraz przedsiębiorstwa, jak również przeciwko całym branżom oraz grupom firm i organizacji¹³⁵². Znamienne jest również stwierdzenie, że „Internet stał się, otwarcie i jawnie, piątym polem walki (cyber-walki), co stało się jasne dzięki ujawnieniu zakresu internetowej działalności szpiegowskiej i sabotażowej”¹³⁵³. Wskazano również na kolejne istotne zagrożenie jakim pozostaje inżynieria społeczna. Uplasowała się ona na trzecim miejscu pod względem zarejestrowanych incydentów przez Zespół CSIRT GOV¹³⁵⁴. W 2016 roku *phishing* ponownie był najczęściej obsługiwanym przez Zespół typem incydentów stanowiącym ponad połowę wszystkich zgłoszonych, a za duże zagrożenie uznano ataki typu *ransomware*. Podniesiono, że nadal nierozwiązaną pozostaje kwestia dokonania ataków o wielkiej skali, jak kradzież

¹³⁴⁷ Zespół Reagowania na Incydynty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2012 roku*. <https://csirt.gov.pl/download/3/158/RaportostaniebezpieczenstwacyberprzestrzeniRPw2012roku.pdf> (dostęp: 21.02.2023), s. 23.

¹³⁴⁸ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2013. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2013.pdf (dostęp: 05.02.2023), s. 6.

¹³⁴⁹ Zespół Reagowania na Incydynty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 roku*. <https://www.csirt.gov.pl/download/3/165/RaportostaniebezpieczenstwacyberprzestrzeniRPw2013roku.pdf> (dostęp: 21.02.2023), s. 5-6.

¹³⁵⁰ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2014. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2014.pdf (dostęp: 05.02.2023), s. 6.

¹³⁵¹ Zespół Reagowania na Incydynty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 roku*. <https://csirt.gov.pl/download/3/172/RaportostaniebezpieczenstwacyberprzestrzeniRPw2014roku.pdf> (dostęp: 21.02.2023), s. 48-49.

¹³⁵² Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2015. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2015.pdf (dostęp: 05.02.2023), s. 5.

¹³⁵³ Ibidem, s. 5.

¹³⁵⁴ Zespół Reagowania na Incydynty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku*. <https://csirt.gov.pl/download/3/183/RaportostaniebezpieczenstwacyberprzesytrzeniRPw2015roku.pdf> (dostęp: 23.02.2023), s. 12-13, 41-43.

pieniędzy z systemu SWIFT czy też ingerencja w wybory prezydenckie w USA¹³⁵⁵. Ponadto 2016 rok był pierwszym w którym w sposób pełny funkcjonował nowy system ARAKIS 2.0. Przełożyło się to na wygenerowanie prawie 340 milionów przepływów i w konsekwencji prawie 450 tysięcy alarmów, podczas gdy w 2015 roku odnotowano ich około 37 tysięcy¹³⁵⁶. W 2017 roku przeprowadzono poważny atak na Komisję Nadzoru Finansowego, co było pierwszym dużym incydentem nakierowanym na cały sektor gospodarki (finansowy) oraz inspirowanym (dokonanym) przez obce państwo. Ponadto pojawiła się po raz pierwszy wzmianka o organizowanych kampaniach dezinformacyjnych w ramach których dążono do zdyskredytowania innych państw bądź organizacji, czy też do polaryzacji poglądów¹³⁵⁷. W tym samym roku nastąpiło również nasilenie zjawiska fałszywych ofert sprzedaży, nie tylko na tworzonych w tym celu stronach internetowych, ale również na popularnych serwisach aukcyjnych i ogłoszeniowych¹³⁵⁸. Wspomnieć należy o pojawiających się w Ministerstwie Obrony Narodowej koncepcjach utworzenia wojsk przeznaczonych do działań w cyberprzestrzeni¹³⁵⁹. W 2018 roku wskazano na ponowny wzrost zgłaszanych incydentów (na co miało również wpływ zwiększenie świadomości co do istnienia i funkcjonowania Zespołu), a najczęstsze z nich dotyczyły *phishingu* (44%), dystrybucji złośliwego oprogramowania oraz spamu¹³⁶⁰. Ważnym wydarzeniem było wejście w życie ustawy o krajowym systemie cyberbezpieczeństwa, która zreorganizowała funkcjonujący w Polsce system jego zapewniania¹³⁶¹. W 2019 roku ponownie stwierdzono, że fałszywe informacje są coraz częściej wykorzystywane w kampaniach oddziaływania informacyjnego, prowadzonych przez rządy, ale również przez organizacje przestępcze. Co również istotne odnotowano wzrost infekcji typu *ransomware* w sektorze przemysłowym, medycznym i administracji rządowej oraz samorządowej¹³⁶². Natomiast według raportu rocznego CSIRT GOV w 2019 roku można

¹³⁵⁵ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2016. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2016.pdf (dostęp: 05.02.2023), s. 7.

¹³⁵⁶ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2016 roku*. <https://csirt.gov.pl/download/3/185/RaportostaniebezpieczenstwacyberprzesytrzeniRPw2016roku.pdf> (dostęp: 22.02.2023), s. 7.

¹³⁵⁷ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2017. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2017.pdf (dostęp: 05.02.2023), s. 8.

¹³⁵⁸ Ibidem, s. 37-39.

¹³⁵⁹ Niebezpiecznik: *MON stworzy "wojsko cybernetyczne" z komponentem informacyjno-psychologicznym (INFOOPS)*. <https://niebezpiecznik.pl/post/mon-stworzy-wojsko-cybernetyczne-z-komponentem-informacyjno-psychologicznym-infoops/> (dostęp: 24.04.2023).

¹³⁶⁰ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2018. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2018.pdf (dostęp: 05.02.2023), s. 6.

¹³⁶¹ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 roku*. <https://csirt.gov.pl/download/3/191/RaportostaniebezpieczenstwacyberprzesytrzeniRPw2018roku.pdf> (dostęp: 22.02.2023), s. 3.

¹³⁶² Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2019. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2019.pdf (dostęp: 05.02.2023), s. 9.

było zaobserwować wzrost liczby zgłoszonych i obsługiwanych incydentów, który względem lat ubiegłych okazał się rekordowy. W odniesieniu do systemu ARAKIS GOV pod względem generowanych przepływów, po raz pierwszy najaktywniejszym z państw była Federacja Rosyjska¹³⁶³. Natomiast autorzy raportu CERT Polska z 2020 roku odnieśli się ponownie do zagrożeń związanych z działaniami dezinformacyjnymi zauważając, że dokonano licznych włamań na portale informacyjne oraz konta polskich polityków. Celem tych działań było obniżenie zaufania społecznego do osób sprawujących oficjalne funkcje w państwie oraz kreowanie negatywnych emocji wobec obecności wojsk USA w Polsce. Stwierdzono serię cyberataków – włamań do infrastruktury teleinformatycznej polskich uczelni oraz instytucji badawczych. Zespół obsługiwał również liczne incydenty związane z funkcjonowaniem usług kluczowych, których przerwanie miałyby poważny skutek dla realizacji ich zadań¹³⁶⁴. W tym samym roku według raportu CSIRT GOV miała miejsce wzmożona aktywność grup APT¹³⁶⁵. Rok 2021 to natomiast wzrost obsługiwanych incydentów o 182% względem roku ubiegłego, przy czym najczęściej zgłaszanym ponownie był *phishing*. Stwierdzono zwiększenie liczby incydentów typu *ransomware*, szczególnie w podmiotach infrastruktury cyfrowej, osób fizycznych oraz administracji publicznej¹³⁶⁶. Zaobserwowano również liczne ataki socjotechniczne, zauważając, że na przestrzeni ostatnich kilku lat pozostają one niezmiennie jednym z częstszych sposobów cyberataków¹³⁶⁷. Z kolei według najnowszych badań przeprowadzonych przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) do najważniejszych zagrożeń w cyberprzestrzeni zaliczono: ataki *ransomware*, *malware*, zagrożenia związane z socjotechniką, zagrożenia dla danych, zagrożenia dla dostępności, dezinformację/informacje wprowadzające w błąd oraz zagrożenia dla łańcucha dostaw. Z kolei do głównych sektorów dotkniętych cyberatakami należały: administracja publiczna (24%), dostawcy usług cyfrowych (13%), ogół społeczeństwa (12,4%), usługi (11,8%),

¹³⁶³ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 roku*. <https://csirt.gov.pl/download/3/199/raportostaniebezpieczenstwacyberprzestrzeniRPw2019.pdf> (dostęp: 16.02.2023), s. 45-47.

¹³⁶⁴ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2020. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2020.pdf (dostęp: 05.02.2023), s. 13.

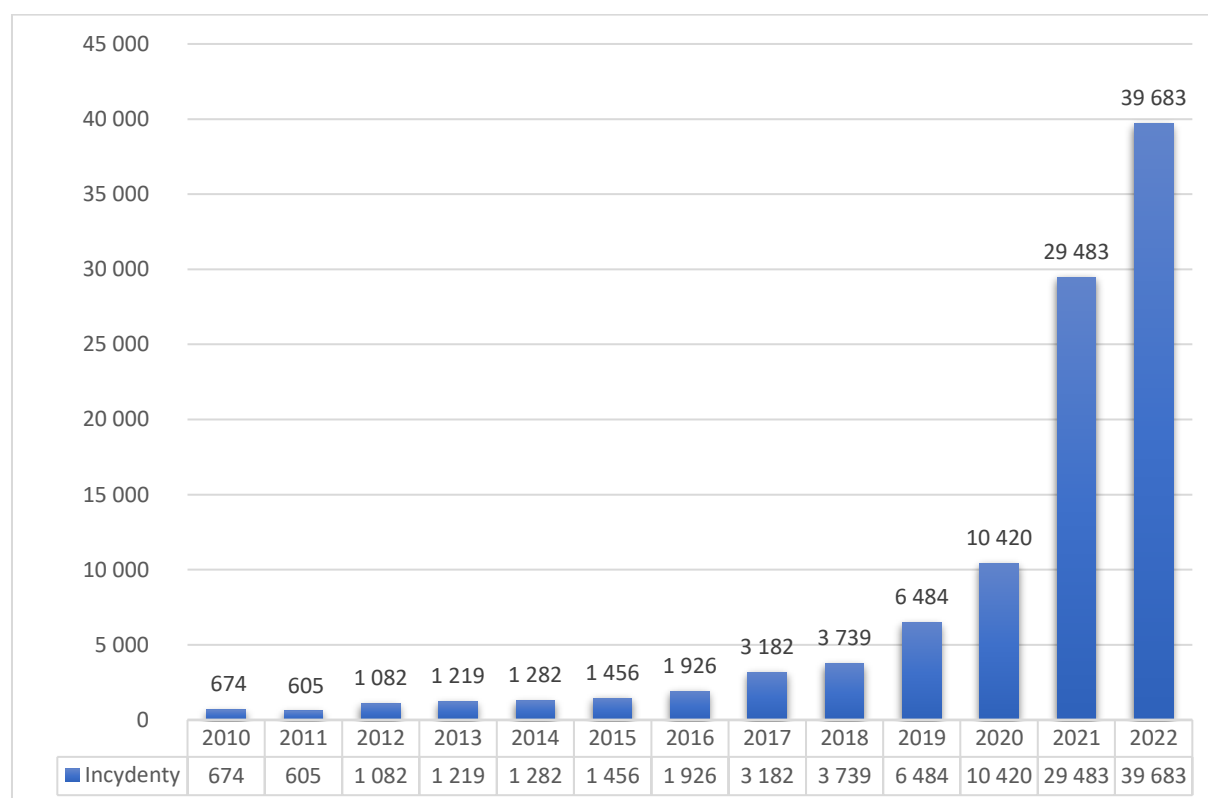
¹³⁶⁵ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2020 roku*. <https://csirt.gov.pl/download/3/201/RaportostaniebezpieczenstwacyberprzestrzeniRPw2020.pdf> (dostęp: 22.02.2023), s. 68-70.

¹³⁶⁶ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2021. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2021.pdf (dostęp: 05.02.2023), s. 12-13.

¹³⁶⁷ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku*. <https://csirt.gov.pl/download/3/204/RaportostaniebezpieczenstwacyberprzestrzeniRPw2021compressed.pdf> (dostęp: 16.02.2023), s. 64-65.

finanse/bankowość (9%) oraz zdrowie (7%)¹³⁶⁸. Podobne dane przedstawiono w raporcie z 2021 roku¹³⁶⁹. Według raportu CERT Polska rok 2022 charakteryzował się nasileniem dotychczasowych zagrożeń, jednakże na skutek wojny rosyjsko-ukraińskiej wzrosła świadomość użytkowników w tym zakresie. Do licznych należy zaliczyć cyberataki, które wykorzystywały sytuację jaka zaistniała w 2022 roku za wschodnią granicą Polski. Wskazano na wybrane przykłady najważniejszych incydentów, jak atak na Lotnicze Pogotowie Ratunkowe, zhakowanie portalu Money.pl przez podmioty pochodzące z Rosji, działalność białoruskiej grupy UNC1151 (Ghostwriter), zhakowanie rządowego serwisu eFaktura.gov.pl czy też cyberatak na szereg podmiotów z sektorów edukacji oraz zdrowia¹³⁷⁰.

Wykres 1. Liczba incydentów obsługiwanych ręcznie¹³⁷¹ (tzw. unikalnych incydentów cyberbezpieczeństwa) przez Zespół CERT Polska w latach 2010-2022.



Źródło: Opracowanie własne na podstawie raportów rocznych Zespołu CERT Polska za lata 2010-2022.

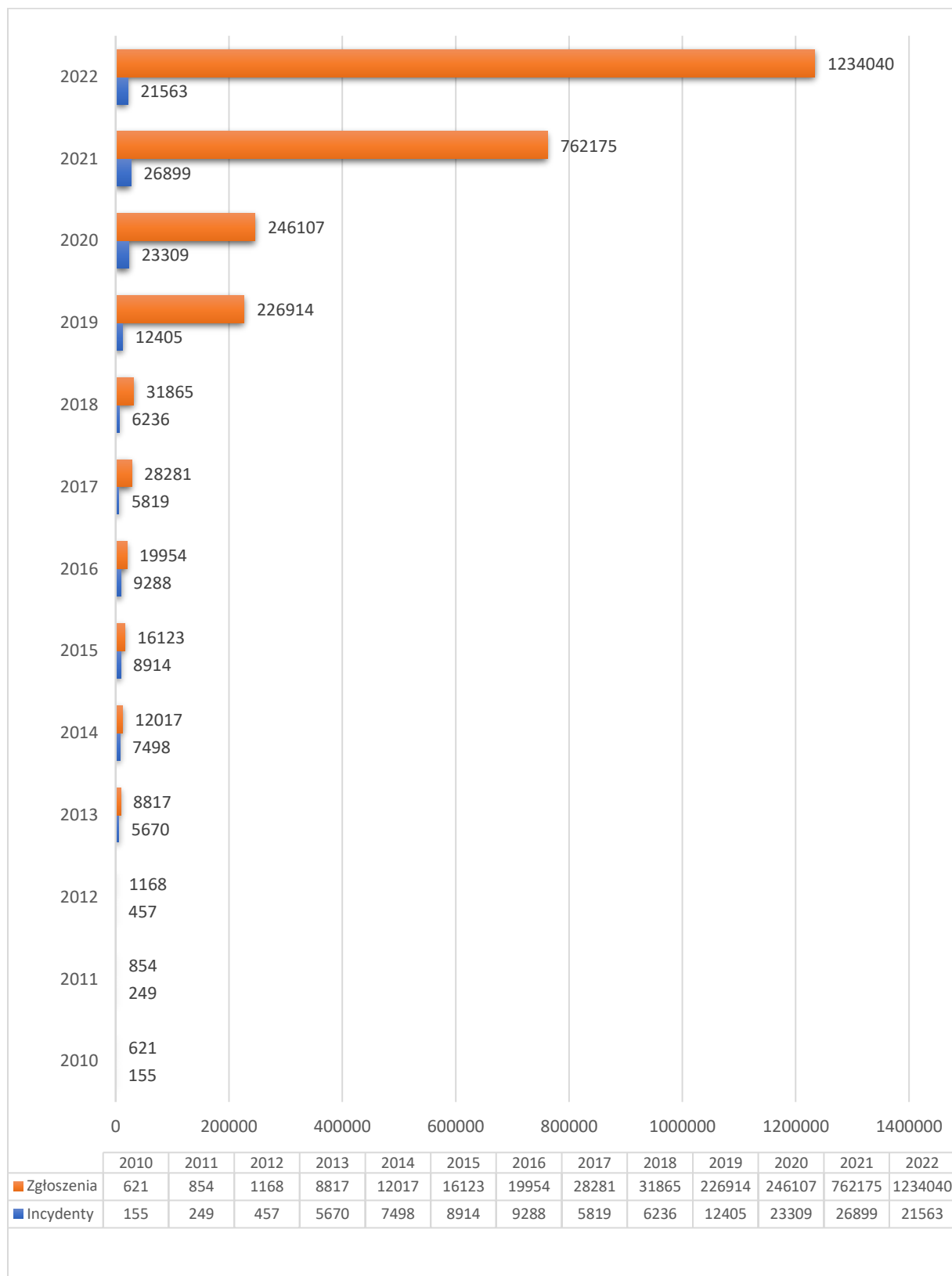
¹³⁶⁸ Parlament Europejski: *Cyberbezpieczeństwo: główne i nowe zagrożenia*. https://www.europarl.europa.eu/pdfs/news/expert/2022/1/story/20220120STO21428/20220120STO21428_pl.pdf (dostęp: 13.02.2023), s. 2-4.

¹³⁶⁹ gov.pl: *Krajobraz (cyber)zagrożeń 2021. Raport Europejskiej Agencji ds. Cyberbezpieczeństwa*. <https://www.gov.pl/web/baza-wiedzy/krajobraz-cyberzagrozen-2021---raport-europejskiej-agencji-ds-cyberbezpieczenstwa-enisa> (dostęp: 05.02.2023).

¹³⁷⁰ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2022. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2022.pdf (dostęp: 24.05.2023), s. 9-16.

¹³⁷¹ Incydenty obsługiwane ręcznie to incydenty, które zostały zarejestrowane oraz wymagają bezpośredniego działania przez członka Zespołu.

Wykres 2. Liczba zgłoszonych oraz faktycznych incydentów odnotowanych przez Zespół CSIRT GOV w latach 2010-2022.



Źródło: Opracowanie własne na podstawie raportów rocznych Zespołu CSIRT GOV za lata 2010-2022.

Z wykresu numer 1 wynika, że w badanym okresie od 2010 do 2022 roku można zaobserwować lawinowy wzrost rejestrowanych przez CERT Polska tzw. unikalnych incydentów cyberbezpieczeństwa. Podsumowując powyższe rozważania trzeba wskazać, że ma to związek nie tylko ze wzrostem świadomości użytkowników co do działalności samego Zespołu, ale również rozpoczęciem funkcjonowania Krajowego systemu cyberbezpieczeństwa i jednoczesnym zwiększeniem skali zagrożeń wobec Polski w cyberprzestrzeni.

Na wykresie numer 2 zauważalny pozostaje roczny wzrost zgłaszanych incydentów, który jednak nie koreluje w stosunku do faktycznych incydentów. Można wręcz stwierdzić, że ich liczba do 2021 roku wzrastała, a w 2022 roku pomimo rekordowej liczby zgłoszeń, liczba faktycznych spadła. Na powyższe dane ma oczywiście wpływ wdrożenie Krajowego systemu cyberbezpieczeństwa, funkcjonującego od 2018 roku. Należy odnotować wzrost zgłoszonych incydentów w 2022 roku względem 2021 roku, co ma oczywiście swoje implikacje w konflikcie rosyjsko-ukraińskim. Niebagatelny jest również fakt, że w tych latach większość zgłoszonych incydentów dotyczących zagrożeń wobec Polski w cyberprzestrzeni miała miejsce w III i IV kwartale 2021 roku¹³⁷² oraz w I i II kwartale 2022 roku – a więc w okresie poprzedzającym rozpoczęcie konfliktu rosyjsko-ukraińskiego oraz w początkowej jego fazie¹³⁷³.

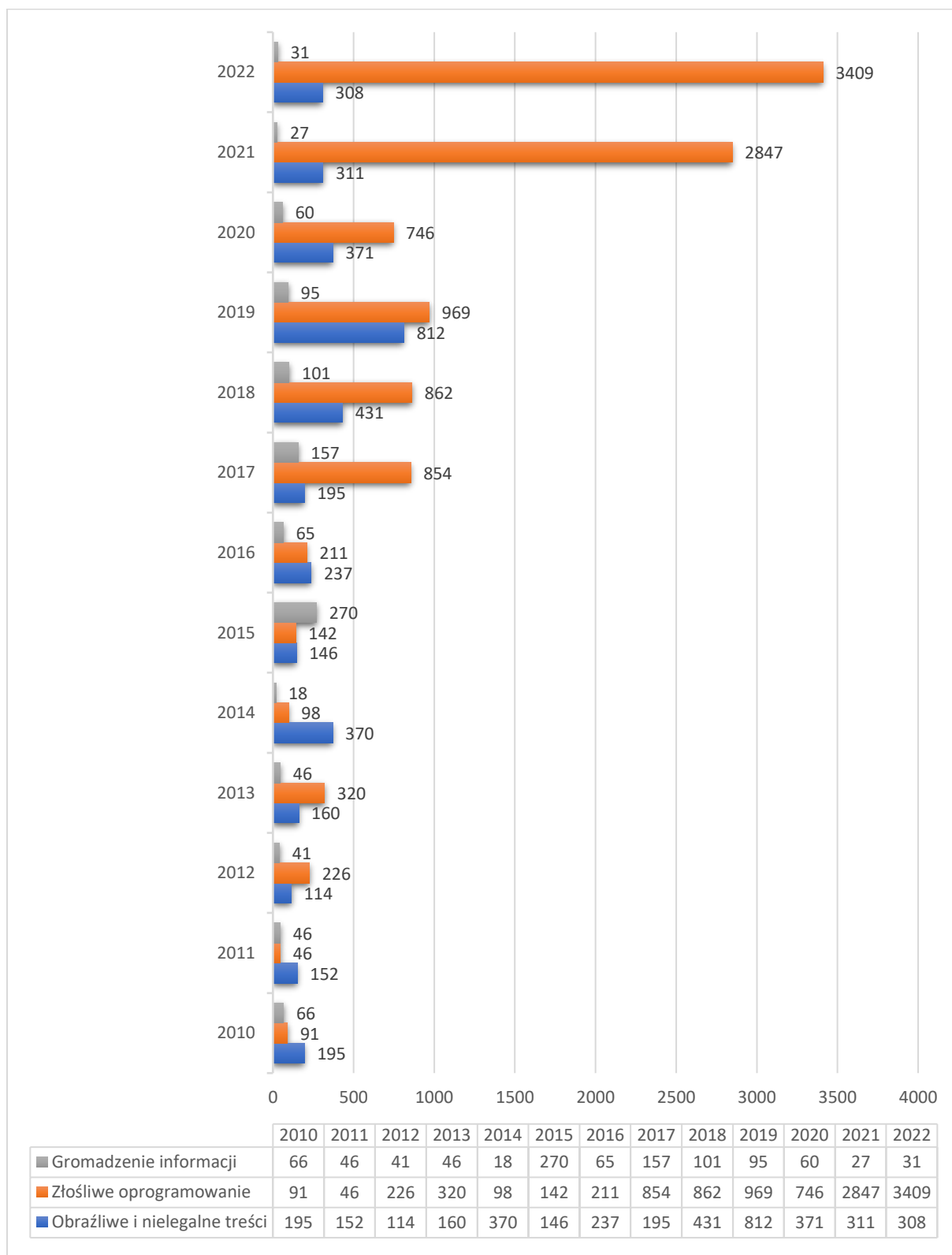
Wskazane spostrzeżenie należy powiązać z kwestią sporną w stosunkach polsko-rosyjskich jaką jest aneksja Półwyspu Krymskiego i wojna na Ukrainie. Polska, będąc państwem które aktywnie wspierało Kijów właściwie na każdej płaszczyźnie, była narażona na negatywne konsekwencje tych działań ze strony Federacji Rosyjskiej – właśnie w postaci dokonywanych cyberataków.

Poniżej przedstawiono wykresy obejmujące wybrane typy incydentów (wraz z liczbą) obsługane przez Zespół CERT Polska w latach 2010-2022, wybrane typy incydentów (wraz z liczbą) obsługane przez Zespół CERT Polska w latach 2010-2022, wybrane typy incydentów (wraz z liczbą) obsługane przez Zespół CERT Polska w latach 2010-2022 oraz zestawienie procentowe wszystkich typów incydentów obsługanych przez Zespół CERT Polska w latach 2010-2022.

¹³⁷² Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni w 2021 roku...*, s. 11.

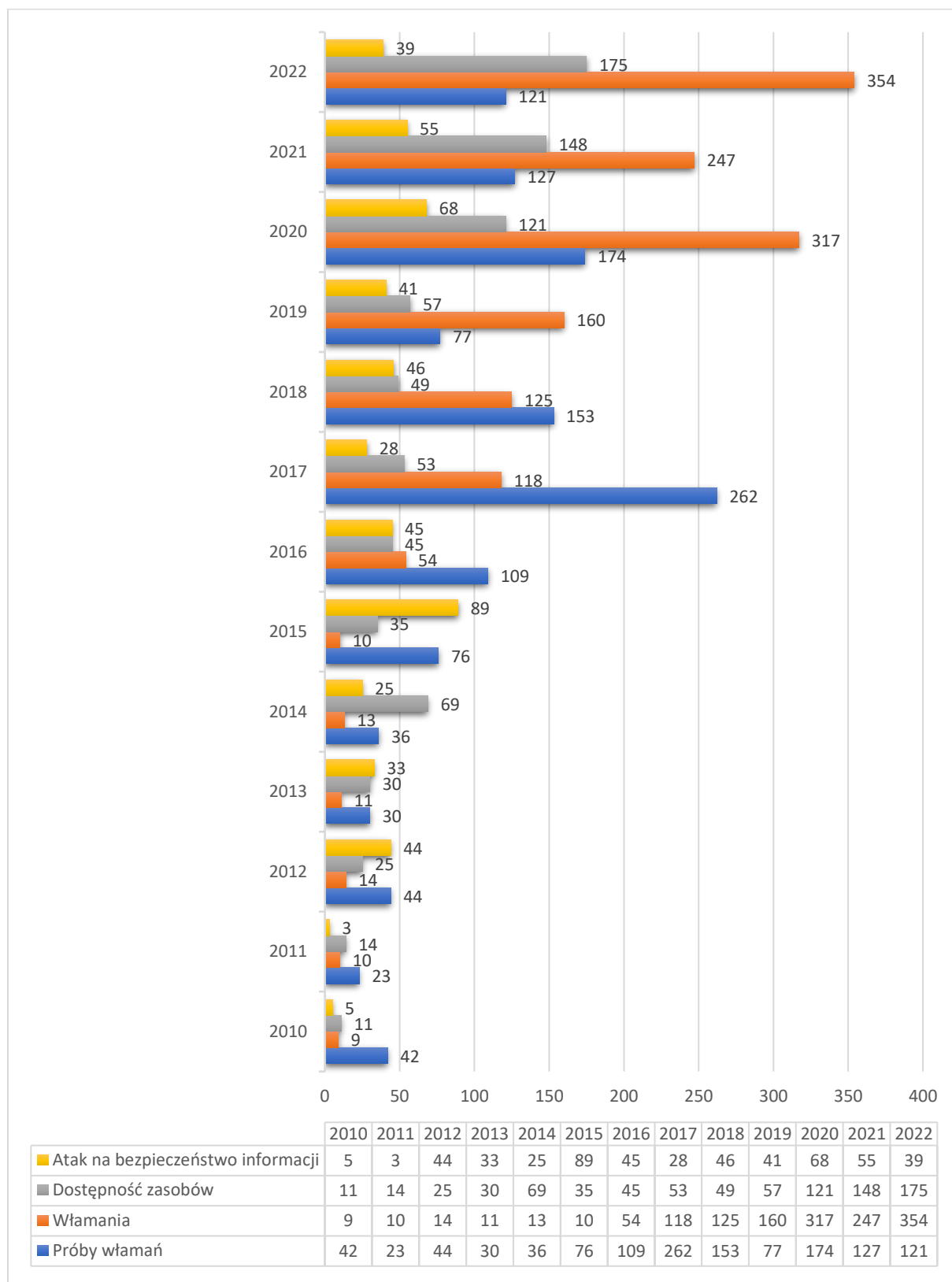
¹³⁷³ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku*. <https://csirt.gov.pl/download/3/213/RaportostaniebezpieczenstwacyberprzestrzeniRPw2022.pdf> (dostęp: 24.05.2023), s. 10-12.

Wykres 3. Wybrane typy incydentów (wraz z liczbą) obsługane przez Zespół CERT Polska w latach 2010-2022.



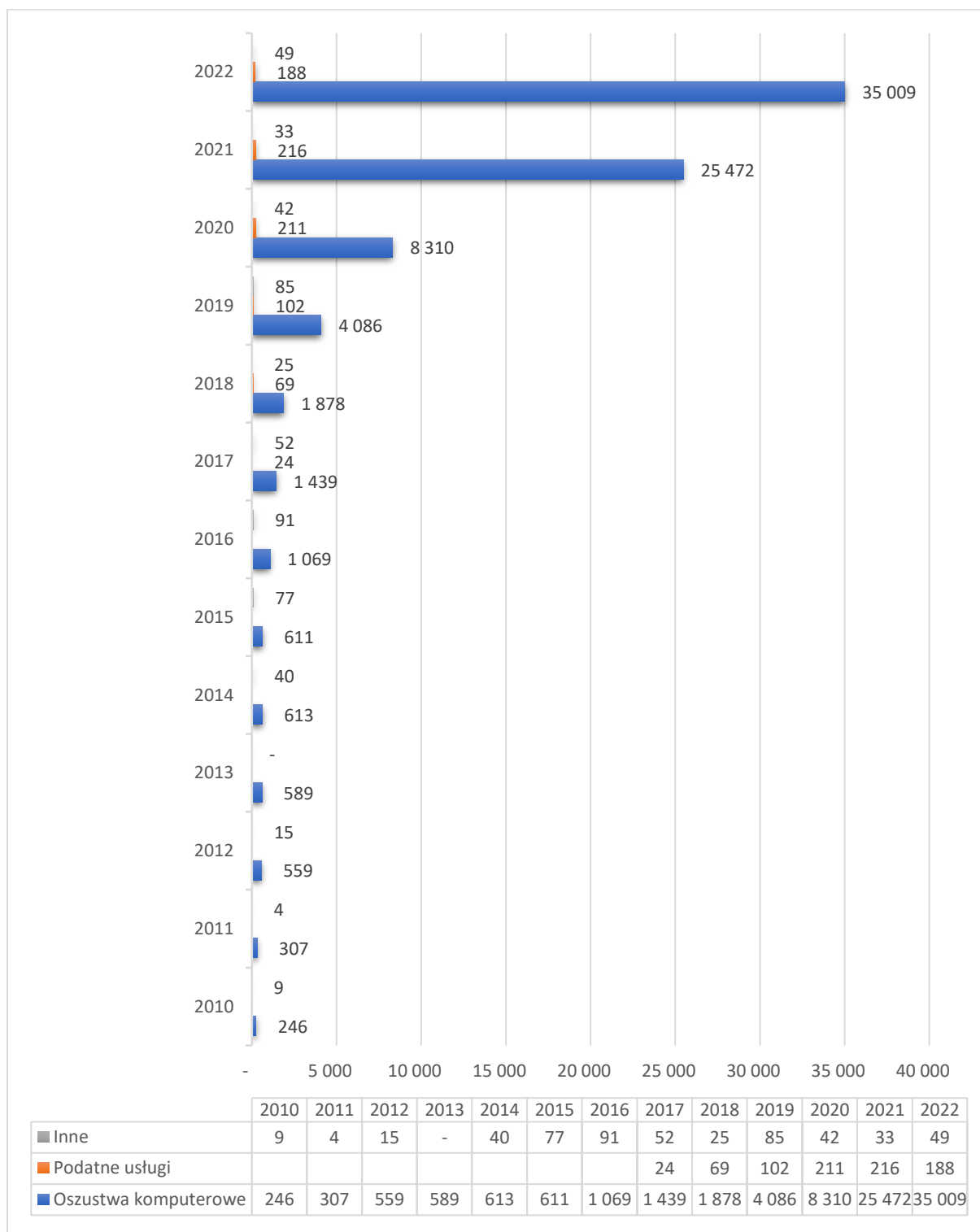
Źródło: Opracowanie własne na podstawie raportów rocznych Zespołu CERT Polska za lata 2010-2022.

Wykres 4. Wybrane typy incyidentów (wraz z liczbą) obsługane przez Zespół CERT Polska w latach 2010-2022.



Źródło: Opracowanie własne na podstawie raportów rocznych Zespołu CERT Polska za lata 2010-2022.

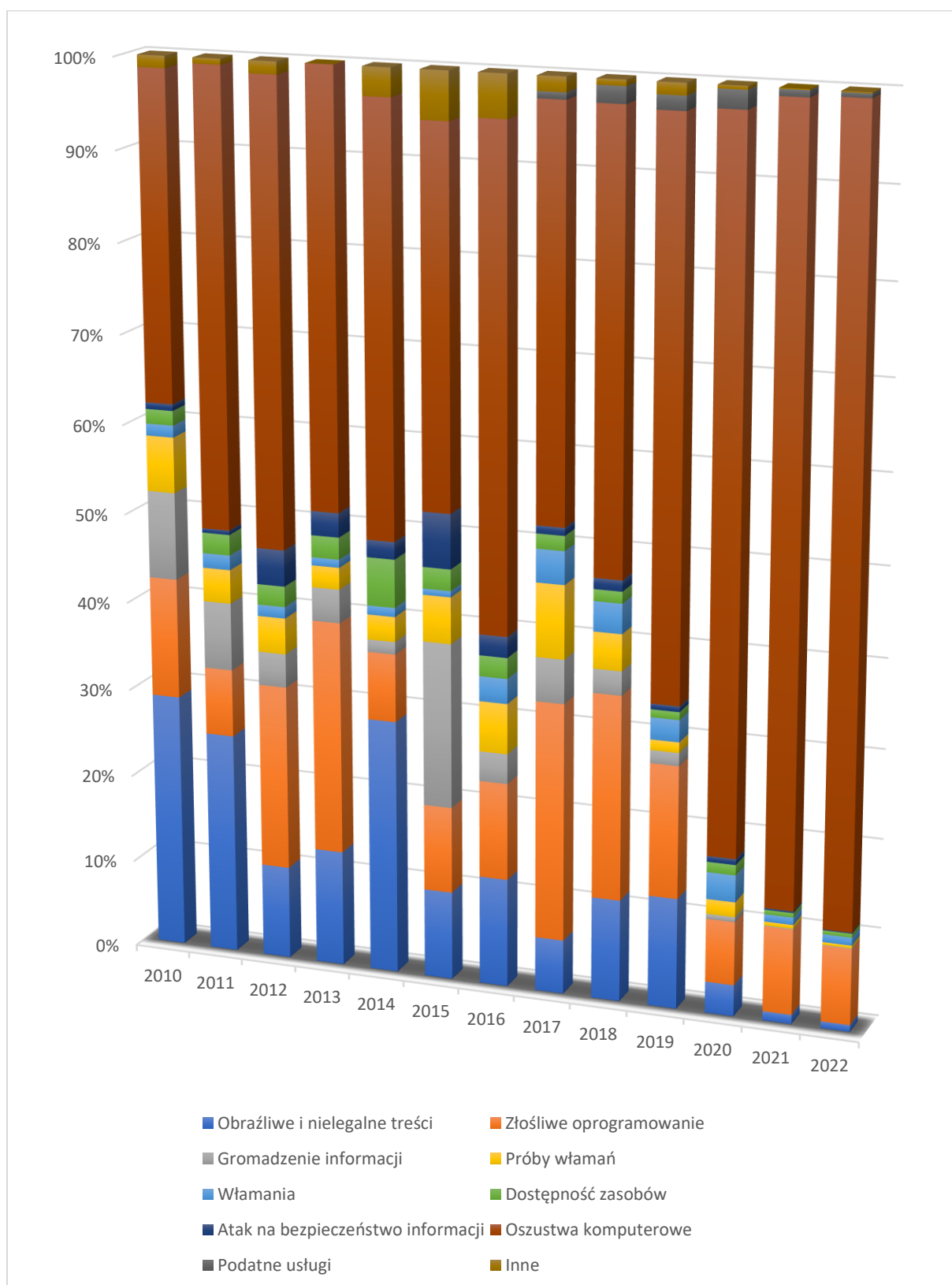
Wykres 5. Wybrane typy incydentów (wraz z liczbą) obsługane przez Zespół CERT Polska w latach 2010-2022¹³⁷⁴.



Źródło: Opracowanie własne na podstawie raportów rocznych Zespołu CERT Polska za lata 2010-2022.

¹³⁷⁴ Typ incydentów o nazwie *Podatne usługi* wprowadzono po raz pierwszy do raportu rocznego Zespołu CERT Polska za 2017 rok, stąd też brak jest danych za lata 2010-2016.

Wykres 6. Zestawienie procentowe wszystkich typów incydentów obsługiwanych przez Zespół CERT Polska w latach 2010-2022.



Źródło: Opracowanie własne na podstawie raportów rocznych Zespołu CERT Polska za lata 2010-2022.

W odniesieniu do omawianego problemu badawczego, w drugiej dekadzie XXI wieku odnotowywano coraz liczniejsze cyberataki wymierzone w infrastrukturę krytyczną, które zostały przeprowadzone przez Federację Rosyjską. Ich celem była nie tylko infrastruktura cybernetyczna Polski, ale również pozostałych państw członkowskich Unii Europejskiej oraz NATO. W kontekście wojny rosyjsko-ukraińskiej takie działanie ma podsycać poczucie strachu oraz obaw przed dalszą eskalacją konfliktu. Według Agencji Unii Europejskiej ds. Cyberbezpieczeństwa, od rozpoczęcia rosyjskiej agresji można zaobserwować wzmożoną aktywność służb Kremla w cyberprzestrzeni, czego skutkiem jest wzrost zagrożenia dla rządów, podmiotów gospodarczych oraz infrastruktury informacyjnej państw¹³⁷⁵. Z kolei według raportu przygotowanego przez Microsoft, działania Rosji w cyberprzestrzeni stanowią uzupełnienie ataków dokonywanych w świecie rzeczywistym na Ukrainie¹³⁷⁶. Ponadto zaznaczono, że szczególnie istotne w działaniach Kremla było przeprowadzanie operacji wpływu (oddziaływania informacyjnego), które składały się z trzech etapów. Pierwszego w którym rozpowszechniane są fałszywe informacje, a dodatkowo następuje atak za pomocą złośliwego oprogramowania na wybrany podmiot. Następnie w drugim etapie dochodzi do zmasowanej kampanii oddziaływania informacyjnego w ramach której fałszywe treści są rozpowszechniane na masową skalę. Z kolei w ostatnim etapie Kreml przy użyciu przychylnych sobie podmiotów (np. farm *trolli*, ale również *botów*) wzmacnia wykreowany przekaz i utrwała go w krajowej i globalnej przestrzeni informacyjnej (medialnej)¹³⁷⁷.

Reasumując powyższe rozważania należy w pierwszej kolejności wskazać na fakt, że w Polsce w latach 2010-2022 zauważalny był dynamiczny oraz wyraźny trend wzrostowy w zakresie powstawania nowych oraz intensyfikacji dotychczasowych cyberzagrożeń. Ich liczba oraz skala zwiększała się rokrocznie, co miało swój związek z postępującą w kraju informatyzacją oraz digitalizacją, a w konsekwencji skutkowało opisanymi wyżej wydarzeniami. Największym z nich jest *phishing*, który dotyczy przede wszystkim osób fizycznych oraz przedsiębiorstw. Niezmiennie pozostaje również wysokie zainteresowanie atakujących polską infrastrukturą krytyczną, względem której notowanych jest coraz więcej incydentów teleinformatycznych. W kolejnych latach można było zaobserwować zwiększenie liczby cyberataków, których celem jest szeroko rozumiana administracja publiczna.

¹³⁷⁵ A. M. Dyer: *Działania hybrydowe Rosji przeciw państwom NATO i UE*. „Biuletyn Polskiego Instytutu Spraw Międzynarodowych” 2022, nr 183 (2602). [https://www.pism.pl/webroot/upload/files/Biuletyn/Biuletyn%20PISM%20nr%20183%20\(2602\)%2025%20listopada%202022%20r.pdf](https://www.pism.pl/webroot/upload/files/Biuletyn/Biuletyn%20PISM%20nr%20183%20(2602)%2025%20listopada%202022%20r.pdf) (dostęp: 04.02.2023).

¹³⁷⁶ Microsoft: *Microsoft Digital Defense Report 2022. Illuminating the threat landscape and empowering a digital defense*. <https://go.microsoft.com/fwlink/?linkid=2213817&clcid=0x409&culture=en-us&country=us> (dostęp: 04.02.2023), s. 41.

¹³⁷⁷ Ibidem, s. 74.

W kontekście omawianego problemu badawczego ważna w omawianym zakresie pozostaje aktywność Rosji, z terenów której pochodzi znaczna liczba cyberataków. Nowymi oraz niezwykle istotnymi zagrożeniami są coraz częstsze i powszechniejsze działania dezinformacyjne, nakierowane przede wszystkim przeciwko państwowym, grupom społecznym, partiom politycznym oraz podmiotom gospodarczym¹³⁷⁸.

6.1.3. Ewolucja systemu cyberbezpieczeństwa Polski w latach 2010-2022

Jak już wskazano, infrastruktura teleinformatyczna, czy też po prostu szeroko rozumiana cyberprzestrzeń, jest podatna na szereg zagrożeń, których intensywność oraz skala wzrastają wraz z jej rozwojem. Cyberprzestrzeń stała się ponadto sferą walki nie tylko takiej o charakterze wojskowym, ale również wywiadowczym, sabotażowym, propagandowym czy politycznym. Tym samym można zaobserwować, że różnego rodzaju infrastruktura, a przede wszystkim krytyczna, funkcjonująca w danym państwie oraz tworzona w oparciu o technologie informacyjne, staje się niezwykle podana na zagrożenia¹³⁷⁹. Zapewnienie odpowiedniego poziomu cyberbezpieczeństwa jest zatem obowiązkiem każdego państwa, które chce w sposób efektywny rozwijać usługi cyfrowe. W zależności od danego państwa system zapewniania cyberbezpieczeństwa może być różny, jednakże pewne elementy w każdym przypadku pozostają stałe. Chodzi bowiem o stworzenie ogólnokrajowej infrastruktury zapewniającej skuteczną ochronę, poprzez stałe monitorowanie procesów zachodzących w cyberprzestrzeni, natomiast w razie wystąpienia jakiegokolwiek zagrożenia, zapewnienie zdolności do skutecznej oraz szybkiej reakcji przez odpowiedzialne za to podmioty¹³⁸⁰.

Omówienie w zarysie polskiego systemu cyberbezpieczeństwa trzeba rozpocząć od scharakteryzowania podstawowych dokumentów rządowych określających jego ramy. Należą do nich Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011 – założenia¹³⁸¹, Rządowy program w zakresie ochrony cyberprzestrzeni RP na lata 2011-2016¹³⁸², Doktryna

¹³⁷⁸ Szczegółowe opracowanie rosyjskiej aktywności w tym zakresie zostało przedstawione w kolejnym rozdziale rozprawy.

¹³⁷⁹ M. Lakomy: *Cyberprzestrzeń jako nowy...*, s. 103.

¹³⁸⁰ R. Lelito: *Idea systemu cyberobronności państwa*. W: *Wsparcie teleinformatyczne i bezpieczeństwo cyberprzestrzeni w SZ RP*. Red. B. Biernacik, L. Kalman, G. Pilariski. Warszawa 2018, s. 99-103.

¹³⁸¹ *Rządowy program ochrony cyberprzestrzeni RP na lata 2009 – 2011 – założenia*. <https://csirt.gov.pl/download/3/40/ZalozeniaRzadowyProgramOchronyCyberprzestrzeniRP2009-2011.pdf> (dostęp: 07.02.2023).

¹³⁸² *Rządowy program w zakresie ochrony cyberprzestrzeni RP na lata 2011 – 2016*. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf (dostęp: 07.02.2023).

cyberbezpieczeństwa Rzeczypospolitej Polskiej 2015¹³⁸³, Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022¹³⁸⁴ oraz Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024¹³⁸⁵.

Pierwszy z dokumentów w założeniach miał być swego rodzaju kamieniem milowym w realizacji polskiej polityki cyberbezpieczeństwa oraz wyznaczać ramy długofalowych celów dla kolejnych rządów. Program powstawał w okresie następującym po wydarzeniach w Estonii z 2007 roku, kiedy doszło do jednego z największych ataków cybernetycznych inspirowanych przez Federację Rosyjską¹³⁸⁶. Jako najważniejsze spodziewane efekty realizacji programu wskazano podniesienie bezpieczeństwa krytycznej infrastruktury teleinformatycznej, zespojenie organów administracji publicznej w zakresie wspólnej polityki bezpieczeństwa cyberprzestrzeni, zwiększenie kompetencji podmiotów odpowiedzialnych za obronę infrastruktury krytycznej, zwiększanie świadomości obywateli co do metod użytkowania systemów teleinformatycznych oraz zaufania do właściwego zabezpieczenia tych usług przez państwo, jak również upowszechnienie wiedzy co do oferowanych w tym zakresie możliwości¹³⁸⁷. W odniesieniu do programu można więc zauważyć dwie podstawowe sfery, po pierwsze ochronę infrastruktury krytycznej w cyberprzestrzeni oraz po drugie zwiększanie świadomości obywateli w zakresie bezpiecznego korzystania z infrastruktury teleinformatycznej (Internetu). Ponadto, implikacje rosyjskich cyberataków w Estonii (2007) jak i dotychczasowe doświadczenia, skutkowały rozpowszechnieniem w Polsce koncepcji stworzenia osobnego rodzaju wojsk – informacyjnych/cybernetycznych¹³⁸⁸. W związku z tym u schyłku pierwszej dekady XXI wieku w Polsce powołano Zespół CERT funkcjonujący w ramach Departamentu Bezpieczeństwa Teleinformatycznego ABW. Do jego zadań należało między innymi koordynowanie działań podejmowanych względem występujących incydentów w cyberprzestrzeni, publikacja alertów i ostrzeżeń w tym zakresie, czy też obsługa i analiza

¹³⁸³ Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej 2015. <https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf> (dostęp: 07.02.2023).

¹³⁸⁴ gov.pl: Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022. <https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022> (dostęp: 07.02.2023).

¹³⁸⁵ gov.pl: Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024. <https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024> (dostęp: 07.02.2023).

¹³⁸⁶ M. Lakomy: *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku*. „Stosunki Międzynarodowe” 2010, nr 3/4, Tom 42, s. 66-67.

¹³⁸⁷ Rządowy program ochrony cyberprzestrzeni RP na lata 2009 – 2011 – założenia. <https://csirt.gov.pl/download/3/40/ZalozeniaRzadowyProgramOchronyCyberprzestrzeniRP2009-2011.pdf> (dostęp: 07.02.2023), s. 27-28.

¹³⁸⁸ M. Lakomy: *Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek do typologii*. „Kwartalnik Naukowy OAP UW e-Politikon” 2013, nr 6, s. 134.

incydentów. Co ważne, Zespół zajmował się tylko infrastrukturą krytyczną państwa oraz domeną rządową gov.pl. Istotnym aspektem było również stworzenie systemu ARAKIS-GOV¹³⁸⁹. Mimo to, w ramach omawianego tematu można wyróżnić szereg zaniedbań w zakresie funkcjonowania polskiego systemu cyberbezpieczeństwa, które legły u podstaw wyzwań w tym przedmiocie na najbliższe lata. Tylko do najważniejszych zaliczono: brak uczestnictwa w międzynarodowych inicjatywach na rzecz rozwijania zdolności w zakresie przeciwdziałania zagrożeniom w cyberprzestrzeni (np. NATO Cooperative Cyber Defence Centre of Excellence); niedostateczną świadomość w zakresie omawianych zagadnień, a w konsekwencji nieliczne nakłady finansowe na tą dziedzinę; brak istnienia wyspecjalizowanej jednostki wojskowej zajmującej się działaniami ofensywnymi i defensywnymi w cyberprzestrzeni; istnienie rozproszonego systemu zapewnienia cyberbezpieczeństwa, przez co należy rozumieć brak zorganizowania i zinstytucjonalizowania odpowiednich podmiotów i instytucji¹³⁹⁰.

Drugi z dokumentów w zasadzie powielał przyjęte przez swojego poprzednika założenia, jednakże w znacznym stopniu dokonywał ich uszczegółowienia oraz rozszerzał zakres działania państwa w tej materii. Podkreślono konieczność wzajemnego współdziałania organów administracji publicznej w zapewnianiu bezpieczeństwa ich infrastrukturze w cyberprzestrzeni. Ponownie największy nacisk w tym zakresie położono na bezpieczeństwo infrastruktury krytycznej. Do innych celów zaliczono wdrożenie w administracji publicznej mechanizmów służących wczesnemu wykrywaniu oraz zapobieganiu zagrożeniom w cyberprzestrzeni, jak również powszechną edukację społeczną w tym zakresie¹³⁹¹. W ramach realizacji programu w pierwszej kolejności dokonano procesów legislacyjnych w celu wypracowania podstaw jego wykonania, następnie przeprowadzono działania proceduralno-organizacyjne, aby zapewnić optymalizację wykorzystania istniejącej infrastruktury teleinformatycznej. Trzecim krokiem były działania edukacyjne dla użytkowników infrastruktury, aby możliwe stało się zrealizowanie działań technicznych, czyli zmniejszenie ryzyka występowania zagrożeń w cyberprzestrzeni¹³⁹². Trzeba podkreślić, że duży nacisk położono na współpracę z sektorem cywilnym na forum krajowym jak i międzynarodowym, za co miał być odpowiedzialny Rządowy Zespół Reagowania na Incydenty Komputerowe –

¹³⁸⁹ System został omówiony szerzej w dalszej części rozdziału.

¹³⁹⁰ M. Lakomy: *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku*. „Stosunki Międzynarodowe” 2010, nr 3/4, Tom 42, s. 67-70.

¹³⁹¹ *Rządowy program w zakresie ochrony cyberprzestrzeni RP na lata 2011 – 2016*. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf (dostęp: 07.02.2023), s. 7.

¹³⁹² Ibidem, s. 14-15.

CERT.GOV.PL (CSIRT GOV)¹³⁹³. Co więcej, wskazano na konieczność podjęcia współpracy z Unią Europejską (Agencją Unii Europejskiej ds. Cyberbezpieczeństwa) oraz Sojuszem Północnoatlantyckim w tym zakresie¹³⁹⁴. W kontekście funkcjonującego w tamtym okresie systemu cyberbezpieczeństwa istotną rolę odgrywały służby specjalne, do których należy zaliczyć wojskowe służby wywiadowcze i kontrwywiadowcze. Służba Kontrwywiadu Wojskowego zajmowała się udzielaniem akredytacji bezpieczeństwa teleinformatycznego oraz certyfikacją środków ochrony elektromagnetycznej. Służba Wywiadu Wojskowego z kolei realizowała zadania z zakresu wywiadu elektronicznego. W ramach Ministerstwa Obrony Narodowej funkcjonowały Resortowe Centrum Zarządzania Sieciami i Usługami Teleinformatycznymi oraz Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych. Wskazane – wybrane – podmioty kooperowały z ich cywilnymi odpowiednikami. Była to przede wszystkim Agencja Bezpieczeństwa Wewnętrznego w ramach której funkcjonował wspomniany już Zespół CERT (CERT.GOV.PL). Utworzony w 2008 roku był w tamtym czasie odpowiedzialny za wszelkie cyberataki na rządową infrastrukturę teleinformatyczną (w tym krytyczną). Drugim ważnym podmiotem był działający przy Naukowej i Akademickiej Sieci Komputerowej (NASK) Zespół CERT Polska. Do podstawowych mankamentów systemu nadal zaliczano: niskie finansowanie, niedostateczny poziom świadomości w zakresie istotności i wagi cyberprzestrzeni, niewystarczające tempo prac legislacyjnych i prawotwórczych oraz rozproszenie kompetencji pomiędzy poszczególnymi podmiotami i brak jednoznacznego ich rozdzielenia¹³⁹⁵.

Trzeci z dokumentów został określony jako wykonawczy względem Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2014¹³⁹⁶ oraz stanowił podstawę koncepcyjną do przygotowania i realizacji w skali ogólnokrajowej działań na rzecz zapewniania cyberbezpieczeństwa, zarówno w sektorze publicznym, jak i prywatnym. Zawierał również szereg rekomendacji, jak również zaznaczał, że jego treść powinna być „rozwinęta przede wszystkim w Polityczno-Strategicznej Dyrektywie Obronnej oraz w kolejnej edycji Strategii (Programu) Rozwoju Systemu Bezpieczeństwa Narodowego, a także w planach

¹³⁹³ Do dnia wejścia w życie ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1506) pod taką nazwą funkcjonował Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. Źródło: Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: FAQ. <https://csirt.gov.pl/cer/faq/22,FAQ-NAJCZESCIEJ-ZADAWANE-PYTANIA.html> (dostęp: 18.02.2023).

¹³⁹⁴ Rządowy program w zakresie ochrony cyberprzestrzeni RP na lata 2011 – 2016. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf (dostęp: 07.02.2023), s. 28.

¹³⁹⁵ M. Lakomy: *Polityka bezpieczeństwa teleinformatycznego Polski*. W: *Dylematy polityki zagranicznej Polski na początku XXI wieku*. Red. K. Czornik, M. Lakomy, M. Stolarczyk. Katowice 2014, s. 378-402.

¹³⁹⁶ *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2014*. <https://www.bbn.gov.pl/ftp/SBN%20RP.pdf> (dostęp: 07.02.2023).

zarządzania kryzysowego oraz operacyjnych planach funkcjonowania struktur państwa w czasie zagrożenia i wojny, jak również w programach rozwoju sił zbrojnych i programach pozamilitarnych przygotowań obronnych”¹³⁹⁷. Dokument zawiera ogólne założenia, które co do zasady nie obiegały od dotychczas przyjętych.

Rok 2015 rozpoczyna okres ewolucji polskich polityk publicznych dotyczących zagadnienia cyberbezpieczeństwa. Lata 2015-2018 stanowią swego rodzaju okno czasowe w trakcie którego postępowała transformacja dotychczasowych działań i założeń, a jej konsekwencją było stworzenie Krajowego systemu cyberbezpieczeństwa. Co znamienne, podstawowym motywatorem do podejmowanych przez decydentów politycznych działań nie były czynniki dotyczące zagrożeń w cyberprzestrzeni, lecz te odnoszące się do zagadnień *stricte* prawnych i politycznych. W omawianym zakresie warto podkreślić, że rozpoczęcie rozmów o kształcie przyszłej ustawy o krajowym systemie cyberbezpieczeństwa otworzyło możliwość debaty – prowadzonej już od dłuższego czasu – pomiędzy Ministerstwem Obrony Narodowej oraz Ministerstwem Cyfryzacji. Zarzewiem swego rodzaju konfliktu był spór kompetencyjny na linii wskazanych resortów. Sprowadzał się on do innego definiowania zadań oraz postrzegania roli poszczególnych instytucji administracji publicznej w cyberprzestrzeni. Wskazać należy w tym kontekście na koncepcję bezpieczeństwa cyberprzestrzeni forsowaną przez MON oraz koncepcję bezpieczeństwa sieci i systemów informatycznych promowaną przez Ministerstwo Cyfryzacji¹³⁹⁸.

W przedostatnim z aktów zaznaczono, że jest on kontynuacją przyjętych uprzednio programów, jednakże dokonano widocznej modyfikacji celów szczegółowych. Przede wszystkim zrezygnowano z nacisku na zapewnienie cyberbezpieczeństwa infrastrukturze krytycznej na rzecz osiągnięcia „zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa”¹³⁹⁹. Można zatem wyprowadzić wniosek, że intencją autorów dokumentu było rozszerzenie aktywności państwa w omawianym zakresie, nie tylko do infrastruktury określanej mianem krytycznej, ale w ogóle do systemów teleinformatycznych istotnych dla funkcjonowania państwa (co jest terminem zdecydowanie szerszym). Ponadto wskazano na

¹³⁹⁷ *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*. <https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf> (dostęp: 07.02.2023), s. 23.

¹³⁹⁸ R. Siudak: *Cyberbezpieczeństwo w Polsce. Od dyskursów do polityk publicznych*. Kraków 2022, s. 368-372.

¹³⁹⁹ gov.pl: *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022*. <https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022> (dostęp: 07.02.2023), s. 8.

konieczność wzmacniania zdolności do przeciwdziałania cyberzagrożeniom, zwiększania zasobów oraz potencjału w tym zakresie. W ostatnim z celów szczegółowych po raz pierwszy pojawia się bezpośrednie odniesienie do powinności „zbudowania silnej pozycji międzynarodowej RP i obszarze cyberbezpieczeństwa”¹⁴⁰⁰. W tym kontekście można zauważyć, że „Polskie podejście do problematyki cyberbezpieczeństwa wynika w znaczącej mierze z członkostwa w organizacjach międzynarodowych i podejmowanych w ich ramach prac”¹⁴⁰¹. Wydaje się, że szczególną rolę należy tutaj przypisać Unii Europejskiej i obowiązku implementacji przyjętych przez nią dyrektyw, bądź bezpośredniego stosowania wydanych rozporządzeń. Istotne pozostają również decyzje podejmowane przez rządzących w ramach współpracy międzynarodowej w ramach NATO. Powyższe przejawia się chociażby w zawartym w dokumencie odniesieniu, do nałożonego na Polskę obowiązku implementacji dyrektywy NIS¹⁴⁰², która zawiera „dyspozycje do określenia wymagań bezpieczeństwa w odniesieniu do podmiotów prywatnych i państwowych z sektorów energetycznego, transportowego, bankowości i infrastruktury rynków finansowych, służby zdrowia, zaopatrzenia w wodę oraz infrastruktury cyfrowej, świadczących usługi kluczowe”¹⁴⁰³. Co ciekawe, w dokumencie zrezygnowano z określenia oceny skuteczności realizacji programu, ze wskazaniem przewidywanych efektów jego wykonania.

W ostatnim z wymienionych dokumentów przyjęto pięć celów szczegółowych w ramach, których uwzględniono większość dotychczasowych założeń. Sam dokument jest również konsekwencją nie tylko zmieniającego się środowiska międzynarodowego, ale jednocześnie przyjęciem ustawy o krajowym systemie cyberbezpieczeństwa¹⁴⁰⁴. Za najważniejsze zadania dla organów państwowych ponownie uznano rozwój krajowego systemu cyberbezpieczeństwa, podniesienie odporności sektora administracji publicznej oraz prywatnego na cyberzagrożenia. Ponadto istotnym nadal pozostawało budowanie potencjału kraju w omawianym zakresie, zwiększanie polskiego zaangażowania na arenie międzynarodowej w obszarze cyberbezpieczeństwa, jak również zwiększanie świadomości społecznej (edukacja). Niezwykle ważnym założeniem jest przyjęcie, iż dokument będzie podlegał okresowej kontroli w zakresie jego wykonania, a w razie takiej konieczności

¹⁴⁰⁰ Ibidem, s. 8; Zobacz szerzej: Ibidem, s. 24-25.

¹⁴⁰¹ M. Porzeżyński: *Cyberbezpieczeństwo dostawców usług cyfrowych*. Warszawa 2021, s. 85.

¹⁴⁰² Zobacz szerzej: NASK Cyber POLICY: *Dyrektywa NIS, czyli pierwsze europejskie prawo w zakresie cyberbezpieczeństwa*. <https://cyberpolicy.nask.pl/dyrektywa-nis-czyli-pierwsze-europejskie-prawo-w-zakresie-cyberbezpieczenstwa/> (dostęp: 09.02.2023).

¹⁴⁰³ gov.pl: *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022*. <https://www.gov.pl/web/cyfrizacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022> (dostęp: 07.02.2023), s. 9.

¹⁴⁰⁴ *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (Dz.U. 2018 poz. 1560).

stosownej modyfikacji, bądź też nastąpi przyjęcie jego nowej wersji na kolejne 5 lat¹⁴⁰⁵. Pokazuje to, że jego autorzy zdają sobie sprawę z dynamiki rozwoju cyberprzestrzeni, jak i środowiska międzynarodowego w tej materii.

W 2018 roku doszło do gruntownego przemodelowania polskiego aparatu bezpieczeństwa, co było związane z wejściem w życie wspomnianej już ustawy o krajowym systemie cyberbezpieczeństwa¹⁴⁰⁶. Nastąpiło to również w konsekwencji przyjęcia przez Unię Europejską dyrektywy NIS¹⁴⁰⁷, mającej na celu zapewnienie wszystkim krajom członkowskim jednolitego systemu w przedmiotowym zakresie¹⁴⁰⁸. Z oficjalnych informacji zamieszczonych na stronach rządowych wynika, że Krajowy system cyberbezpieczeństwa to system, który „obejmuje operatorów usług kluczowych (m.in.: z sektora energetycznego, transportowego, zdrowotnego i bankowości), dostawców usług cyfrowych, zespoły CSIRT (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego) poziomu krajowego, sektorowe zespoły cyberbezpieczeństwa, podmioty świadczące usługi z zakresu cyberbezpieczeństwa, organy właściwe do spraw cyberbezpieczeństwa oraz pojedynczy punkt kontaktowy do komunikacji w ramach współpracy w Unii Europejskiej w dziedzinie spraw cyberbezpieczeństwa”¹⁴⁰⁹. Z założenia Krajowy system cyberbezpieczeństwa ma więc tworzyć zintegrowany ogólnopaństwowy system nakładający na poszczególne podmioty określone obowiązki, a celem jest zapewnienie niezakłóconego świadczenia usług kluczowych oraz cyfrowych¹⁴¹⁰. Do podstawowych z nich zaliczamy prowadzenie czynności umożliwiających wykrywanie, rejestrowanie, analizowanie i klasyfikowanie incydentów. Ponadto jest to zgłaszanie incydentów, przekazywanie danych umożliwiających obsługę incydentów czy też oceny lub szacowania ryzyka wystąpienia zagrożeń¹⁴¹¹. Trzeba zauważyć, że katalog podmiotów, których ustawa dotyczy jest stosunkowo szeroki, gdyż odnosi się nie tylko do podmiotów państwowych, ale również prywatnych¹⁴¹². Zarówno w odniesieniu do dyrektywy NIS, jak

¹⁴⁰⁵ gov.pl: *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*. <https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024> (dostęp: 07.02.2023), s. 11, 30.

¹⁴⁰⁶ *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (Dz.U. 2018 poz. 1560).

¹⁴⁰⁷ *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii* (Dziennik Urzędowy Unii Europejskiej L 194/1).

¹⁴⁰⁸ M. Porzeżyński: *Cyberbezpieczeństwo dostawców...*, s. 116-117.

¹⁴⁰⁹ gov.pl: *Krajowy system cyberbezpieczeństwa*. <https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa-> (dostęp: 09.02.2023).

¹⁴¹⁰ Ibidem.

¹⁴¹¹ *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (Dz.U. 2018 poz. 1560), s. 8 i następne (Rozdział 3), s. 17 i następne (Rozdział 4), s. 20 i następne (Rozdział 5).

¹⁴¹² gov.pl: *Krajowy system cyberbezpieczeństwa*. <https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa-> (dostęp: 09.02.2023).

i ustawy o krajowym systemie cyberbezpieczeństwa, należy spodziewać się w przyszłości ich nowelizacji, co nie powinno być nadspodziewane wobec szczególnego charakteru materii jaka jest we wskazanych aktach regulowana¹⁴¹³.

Krajowy system cyberbezpieczeństwa opiera się na działalności szeregu podmiotów, przy czym do najważniejszych z nich zaliczyć należy: Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV, Ministerstwo Obrony Narodowej (w zakresie realizacji programu CYBER.MIL.PL), Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT MON, Wojska Obrony Cyberprzestrzeni, wojskowe służby specjalne (SKW i SWW), Zespół CERT Polska (realizujący obowiązki Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT NASK – zgodnie z ustawą z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa), Pełnomocnika Rządu ds. Cyberbezpieczeństwa, Policję oraz cywilne służby specjalne (ABW, AW, CBA). Wymieniony katalog nie jest oczywiście enumeratywny, jednakże w ocenie autora wymienione podmioty odpowiadają w największym stopniu za realizację zadań z zakresu funkcjonowania polskiego systemu cyberbezpieczeństwa, dlatego niezbędne jest ich zarysowanie.

Wyjątkową uwagę należy poświęcić Zespołowi CSIRT GOV, gdyż jego status w polskim prawie jest szczególny. To na nim ciąży obowiązek współpracy z innymi podmiotami w zakresie tworzenia spójnego krajowego systemu cyberbezpieczeństwa¹⁴¹⁴. Zespół jest zarządzany przez Szefa Agencji Bezpieczeństwa Wewnętrznego oraz odpowiada za „koordynację procesu reagowania na incydenty komputerowe występujące w obszarze wskazanym w art. 26. ust. 7. ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa”¹⁴¹⁵. Do podstawowych zadań Zespołu zalicza się również „rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7. pkt. 1. ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym”¹⁴¹⁶. Ponadto, odpowiada za koordynację i obsługę incydentów zgłaszanych przez organy władzy publicznej, ZUS, NFZ, NBP oraz sądy

¹⁴¹³ M. Porzeżyński: *Cyberbezpieczeństwo dostawców...*, s. 122-128.

¹⁴¹⁴ Ibidem, s. 146-147.

¹⁴¹⁵ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *O nas*. <https://csirt.gov.pl/> (dostęp: 17.02.2023).

¹⁴¹⁶ Ibidem.

i trybunały¹⁴¹⁷. Niezwykle istotnym zadaniem jest kooperacja z innymi zespołami CSIRT oraz współpraca z „organami właściwymi do spraw cyberbezpieczeństwa, ministrem właściwym do spraw informatyzacji oraz Pełnomocnikiem, zapewniając spójny i kompletny system zarządzania ryzykiem na poziomie krajowym, realizując zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewniając koordynację obsługi zgłoszonych incydentów”¹⁴¹⁸. Ponadto Zespół publikuje każdego roku Raport o stanie bezpieczeństwa cyberprzestrzeni RP, który zawiera statystyki koordynowanych incydentów, zidentyfikowane zagrożenia (w tym dotyczące złośliwego oprogramowania), sprawozdanie z działania systemu ARAKIS, ocenę bezpieczeństwa systemów IT, jak również wymienia zagrożenia dla funkcjonowania infrastruktury krytycznej państwa¹⁴¹⁹.

Kolejnym podmiotem stanowiącym niezwykle ważny element polskiego systemu cyberbezpieczeństwa jest Ministerstwo Obrony Narodowej. Jego działalność w tym zakresie jest niezwykle szeroka i została omówiona również w dalszej części pracy, niemniej jednak w tym miejscu przedstawiono zarys realizowanego przez resort programu CYBER.MIL.PL. Obejmuje on cztery obszary sprowadzające się do: konsolidacji i budowy struktur systemu cyberbezpieczeństwa; edukacji, szkoleń i treningów; współpracy międzynarodowej oraz podnoszenia poziomu bezpieczeństwa resortowych i wojskowych sieci oraz systemów¹⁴²⁰. Za jego realizację odpowiada kooperacja szeregu podmiotów, do których należy zaliczyć: Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni, Służbę Kontrwywiadu Wojskowego, Wojska Obrony Terytorialnej, Wojskowy Instytut Łączności¹⁴²¹, Akademię Marynarki Wojennej, Wojskową Akademię Techniczną oraz Eksperckie Centrum Szkolenia Cyberbezpieczeństwa¹⁴²². W latach 2019-2021 w ramach realizacji programu podjęto szereg działań, a do najważniejszych z nich należy zaliczyć: zwiększanie ochrony kryptograficznej podmiotów wchodzących w skład MON, podpisanie licznych porozumień z państwami unijnymi w zakresie współpracy wojskowych zespołów reagowania na incydenty bezpieczeństwa komputerowego, przejęcie funkcji koordynatora unijnego Zespołu Szybkiego

¹⁴¹⁷ Zobacz szerzej: *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (Dz. U. 2018 poz. 1560), art. 26 ust 3.

¹⁴¹⁸ Ibidem, art. 26.

¹⁴¹⁹ Zobacz szerzej: Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raporty o stanie bezpieczeństwa cyberprzestrzeni RP*. <https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi> (dostęp: 17.02.2023).

¹⁴²⁰ Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni: *Podsumowanie programu CYBER.MIL.PL 2019-2021*. https://www.cyber.mil.pl/c/articles/atts/2022/2/CYBER.MIL.PL_2019-2021.pdf (DOSTĘP: 09.05.2023), s. 4.

¹⁴²¹ Wojskowy Instytut Łączności im. prof. Janusza Groszkowskiego - Państwowy Instytut Badawczy.

¹⁴²² CYBER.MIL.PL: *O nas*. <https://www.cyber.mil.pl/o-nas/> (dostęp: 09.05.2023).

Reagowania, organizacja ćwiczeń, rozpoczęcie funkcjonowania Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni oraz uczestnictwo w formowaniu Wojsk Obrony Cyberprzestrzeni. Warto również wspomnieć o działaniach edukacyjnych do których należało przeprowadzenie licznych szkoleń, rozpoczęcie funkcjonowania Wojskowego Ogólnokształcącego Liceum Informatycznego czy też utworzenie studiów Master of Business Administration (MBA) z zakresu zarządzania cyberbezpieczeństwem¹⁴²³.

Kolejnym podmiotem są Wojska Obrony Cyberprzestrzeni (WOC), których powstanie było bezpośrednio związane z ustaleniami ze szczytu NATO, który odbył się w Warszawie w 2016 roku. Wynikiem obrad było potwierdzenie, że cyberprzestrzeń stanowi kolejną sferę konfliktów międzynarodowych w związku z czym niezbędne jest zapewnienie kolektywnej obrony Sojuszu Północnoatlantyckiego również w tym zakresie¹⁴²⁴. Działalność tego podmiotu sprowadza się przede wszystkim do aktywności o charakterze militarnym, czyli działań rozpoznawczych, defensywnych oraz ofensywnych¹⁴²⁵. Ponadto WOC odpowiadają w Ministerstwie Obrony Narodowej za „kluczowe obszary związane z kryptologią, cyberbezpieczeństwem oraz budową i eksploatacją systemów IT”¹⁴²⁶. W ramach tego składnika Sił Zbrojnych RP funkcjonuje również – w ramach Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT MON, którego celem jest „zapewnienie bezpieczeństwa teleinformatycznego całego resortu, prowadzenie badań projektowanie, budowa, wdrażanie, użytkowanie oraz ochrona narodowych technologii kryptologicznych czy wytwarzanie nowych produktów dla państwa”¹⁴²⁷. Jest on w zasadzie komórką organizacyjną resortu, zajmującą się incydentami zgłaszanymi przez podmioty podległe Ministrowi Obrony Narodowej oraz przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym wobec których minister jest organem organizującym oraz nadzorującym wykonywanie zadań na rzecz obronności państwa polskiego¹⁴²⁸.

Wreszcie należy dokonać zarysowania działalności wojskowych służb specjalnych, tj. Służby Wywiadu Wojskowego (SWW) oraz Służby Kontrwywiadu Wojskowego (SKW), przy czym z punktu widzenia systemu cyberbezpieczeństwa kluczową rolę pełni drugi z nich. Służba Wywiadu Wojskowego w celu zapewnienia cyberbezpieczeństwa państwa realizuje

¹⁴²³ Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni: *Podsumowanie programu CYBER.MIL.PL...*, s. 6-33.

¹⁴²⁴ CYBER.MIL.PL: *Wojska Obrony Cyberprzestrzeni*. <https://www.cyber.mil.pl/wojska-obrony-cyberprzestrzeni/> (dostęp: 11.02.2023).

¹⁴²⁵ gov.pl: *Wojska Obrony Cyberprzestrzeni*. <https://www.gov.pl/web/obrona-narodowa/wojska-obrony-cyberprzestrzeni> (11.02.2023).

¹⁴²⁶ Wojsko Polskie: *Zadania – DKWOC*. <https://www.wojsko-polskie.pl/woc/zadania/> (dostęp: 11.02.2023).

¹⁴²⁷ Ibidem.

¹⁴²⁸ gov.pl: *Krajowy system cyberbezpieczeństwa*. <https://www.gov.pl/web/cyfrizacja/krajowy-system-cyberbezpieczenstwa-> (dostęp: 10.02.2023).

przede wszystkim działania o charakterze wywiadowczym¹⁴²⁹, podczas gdy Służba Kontrwywiadu Wojskowego certyfikuje urządzenia kryptograficzne¹⁴³⁰ oraz prowadzi szkolenia dla administratorów systemów teleinformatycznych¹⁴³¹. SKW w tym zakresie „udziela akredytacji w celu dopuszczenia systemu teleinformatycznego do przetwarzania informacji niejawnych oraz prowadzi audyty bezpieczeństwa akredytowanych systemów”¹⁴³². Ponadto realizuje czynności sprowadzające się do „badania wpływu incydentów komputerowych na bezpieczeństwo systemów teleinformatycznych resortu obrony narodowej”¹⁴³³ oraz „współuczestniczenia w monitorowaniu stanu bezpieczeństwa resortowych systemów teleinformatycznych”¹⁴³⁴. Należy zasygnalizować, że na przestrzeni lat struktura zadań realizowanych przez SKW była poddana wielu modyfikacjom, jednakże niniejsze opracowanie nie pozwala na szczegółowe omówienie tego zagadnienia. W dużym stopniu ogólności zadania służby (między innymi w ramach obrony polskiej cyberprzestrzeni) można sprowadzić do: zwalczania przestępstw, ochrony informacji niejawnych, analizy i zwalczania zagrożeń, działań z zakresu kontrwywiadu radioelektronicznego oraz kryptografii i analizy, czy też ochrony badań naukowych¹⁴³⁵.

Następnym z podmiotów jest Zespół CERT Polska, który działa w strukturach NASK – Państwowego Instytut Badawczego. Zespół wykonuje obowiązki o których mowa w ustawie o krajowym systemie cyberbezpieczeństwa, między innymi w zakresie przyjmowania zgłoszeń incydentów, analizy zagrożeń, ryzyk z tym związanych oraz ostrzegania przed nimi¹⁴³⁶. CERT Polska jest członkiem międzynarodowej organizacji FIRST (Forum of Incidents and Security Teams), zrzeszającej podmioty zajmujące się reagowaniem na incydenty w cyberprzestrzeni¹⁴³⁷. Zespół podobnie jak CSIRT GOV publikuje każdego roku raporty, które prezentują incydenty teleinformatyczne dotyczące Polski w cyberprzestrzeni. Od

¹⁴²⁹ M. Lakomy: *Polityka bezpieczeństwa teleinformatycznego Polski*. W: *Dylematy polityki...*, s. 379.

¹⁴³⁰ Zobacz szerzej: Biuletyn Informacji Publicznej. Służba Kontrwywiadu Wojskowego: *Certyfikacja wyrobów przeznaczonych do ochrony informacji niejawnych*. <https://bip.skw.gov.pl/skw/bezpieczenstwo-teleinfo/certyfikacja-wyrobow-pr/5110,Certyfikacja-wyrobow-przeznaczonych-do-ochrony-informacji-niejawnych.html> (dostęp: 12.05.2023).

¹⁴³¹ M. Lakomy: *Wymiar informacyjny i telekomunikacyjny bezpieczeństwa Polski*. W: *Polska w systemie bezpieczeństwa międzynarodowego*. Red. M. Pietraś, K. A. Wojtaszczyk. Warszawa 2016, s. 152.

¹⁴³² CYBER.MIL.PL: *Służba Kontrwywiadu Wojskowego*. <https://www.cyber.mil.pl/articles/o-nas-f/2018-11-20m-suzba-kontrwywiadu-wojskowego/> (dostęp: 12.05.2023).

¹⁴³³ Ibidem.

¹⁴³⁴ Ibidem.

¹⁴³⁵ Służba Kontrwywiadu Wojskowego: *Zadania*. <https://www.skw.gov.pl/zadania.html> (dostęp: 12.05.2023); Zobacz szerzej: *Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (Dz.U. 2006 nr 104 poz. 709).

¹⁴³⁶ CERT.PL NASK: *O nas*. <https://cert.pl/o-nas/> (dostęp 10.02.2023).

¹⁴³⁷ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2021. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2021.pdf (dostęp: 05.02.2023), s. 10.

początku jego istnienia „rdzeniem działalności jest obsługa incydentów bezpieczeństwa i współpraca z podobnymi jednostkami na całym świecie, zarówno w działalności operacyjnej, jak i badawczo-wdrożeniowej”¹⁴³⁸. Co należy szczególnie podkreślić to to, że od 2018 roku „wobec wejścia w życie ustawy o krajowym systemie cyberbezpieczeństwa, Zespół CERT Polska realizuje część zadań CSIRT NASK”¹⁴³⁹. Do najważniejszych zadań Zespołu w tym zakresie należy: „monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym; przekazywanie informacji dotyczących incydentów i ryzyk podmiotom krajowego systemu cyberbezpieczeństwa; wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa; reagowanie na zgłoszone incydenty; klasyfikowanie incydentów, w tym incydentów poważnych oraz incydentów istotnych, jako incydenty krytyczne oraz koordynowanie obsługi incydentów krytycznych”¹⁴⁴⁰. W corocznych raportach publikowanych przez Zespół (Krajobraz bezpieczeństwa polskiego Internetu) znajdują się informacje na temat najważniejszych obserwacji w danym roku, kalendarium wydarzeń, działań podjętych przez CERT Polska w zakresie ochrony cyberprzestrzeni (ćwiczenia, konkursy, projekty itp.), zarejestrowanych incydentów oraz statystyki występowania i oddziaływania wykrytych zagrożeń na bezpieczeństwo w cyberprzestrzeni¹⁴⁴¹.

Ważną rolę w polskim systemie cyberbezpieczeństwa pełni również Pełnomocnik Rządu ds. Cyberbezpieczeństwa. Nie jest on podmiotem bezpośrednio odpowiedzialnym za jego funkcjonowanie, jednakże pełni istotną rolę w koordynowaniu działań i realizowaniu polityki rządu w omawianym zakresie¹⁴⁴². Do jego najważniejszych zadań należy analiza oraz ocena funkcjonowania krajowego systemu cyberbezpieczeństwa, nadzór nad procesem zarządzania ryzykiem tego systemu oraz opiniowanie dokumentów mających wpływ na realizację zadań związanych z cyberbezpieczeństwem¹⁴⁴³. Ponadto „Pełnomocnik opracowuje i przedkłada Radzie Ministrów w terminie do dnia 31 marca każdego roku sprawozdanie za poprzedni rok kalendarzowy zawierające informacje o prowadzonej działalności w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym”¹⁴⁴⁴.

Kolejnym wymagającym omówienia podmiotem jest Policja, która stanowi trzon wśród instytucji zajmujących się zwalczaniem przestępczości w Internecie. Wskazać bowiem należy, że omawiane dotychczas działania (cyberataki) dokonywane wobec Polski w cyberprzestrzeni

¹⁴³⁸ CERT Polska: *O nas*. <https://cert.pl/o-nas/> (dostęp 17.02.2023).

¹⁴³⁹ Ibidem.

¹⁴⁴⁰ Ibidem.

¹⁴⁴¹ Zobacz szerzej: CERT Polska: *Publikacje CERT Polska*. <https://cert.pl/publikacje/> (dostęp: 17.02.2023).

¹⁴⁴² *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (Dz.U. 2018 poz. 1560), art. 60.

¹⁴⁴³ Ibidem, art. 62.

¹⁴⁴⁴ Ibidem, art. 63.

są penalizowane przez prawo, w szczególności przez kodeks karny. Do przykładowych czynów zabronionych w tej materii należą: bezprawne wyzyskanie informacji (art. 267. KK), utrudnianie zapoznania się z informacją (art. 268. KK), niszczenie danych informatycznych (art. 268a. KK), uszkodzenie danych informatycznych (art. 269. KK) oraz oszustwo komputerowe (art. 287. KK)¹⁴⁴⁵. Powracając jednak do omawianej formacji, kluczową rolę w jej strukturach pełni Centralne Biuro Zwalczania Cyberprzestępczości. Jego główne zadania sprowadzają się do „rozpoznawania i zwalczania przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej oraz zapobiegania tym przestępstwom, a także wykrywania i ścigania sprawców tych przestępstw”¹⁴⁴⁶ oraz „wspierania w niezbędnym zakresie jednostek organizacyjnych Policji w rozpoznawaniu, zapobieganiu i zwalczaniu tych przestępstw”¹⁴⁴⁷. Biuro jest względnie nowym podmiotem, gdyż powstało w wyniku przyjęcia ustawy z dnia 17 grudnia 2021 roku o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości¹⁴⁴⁸. Wcześniej zwalczanie przestępczości komputerowej było realizowane za pośrednictwem odpowiednich wydziałów funkcjonujących w Komendzie Głównej Policji oraz komendach wojewódzkich¹⁴⁴⁹.

Wreszcie wskazać należy na cywilne służby specjalne. Podstawowym celem działalności służb w każdym państwie jest zapewnienie jego bezpieczeństwa, zarówno w wymiarze wewnętrznym jak i zewnętrznym oraz na płaszczyźnie cywilnej (jak i wojskowej)¹⁴⁵⁰. W Polsce do cywilnych służb specjalnych realizujących te zadania zaliczamy Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu oraz Centralne Biuro Antykorupcyjne¹⁴⁵¹. Ważnym aspektem ich funkcjonowania pozostaje obrona Polski w cyberprzestrzeni¹⁴⁵². Wskazuje na to między innymi Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022¹⁴⁵³. Dokument przyjęty w 2013

¹⁴⁴⁵ Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny (Dz.U. 1997 nr 88 poz. 553).

¹⁴⁴⁶ Centralne Biuro Zwalczania Cyberprzestępczości: *Zadania Centralnego Biura Zwalczania Cyberprzestępczości*. <https://cbzc.policja.gov.pl/bzc/o-cbzc/podstawowe-zadania/5,Zadania-Centralnego-Biura-Zwalczania-Cyberprzestepczosci.html> (dostęp: 12.05.2023).

¹⁴⁴⁷ Ibidem.

¹⁴⁴⁸ Ustawa z dnia 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości (Dz.U. 2021 poz. 2447).

¹⁴⁴⁹ M. Lakomy: *Wymiar informacyjny i telekomunikacyjny bezpieczeństwa Polski*. W: *Polska w systemie bezpieczeństwa...*, s. 152.

¹⁴⁵⁰ Z. Grzegorowski: *Służby specjalne a bezpieczeństwo państwa Polskiego*. Toruń 2013, s. 38-41.

¹⁴⁵¹ gov.pl: *O służbach specjalnych*. <https://www.gov.pl/web/sluzby-specjalne/o-sluzbach-specjalnych3> (dostęp: 14.02.2023).

¹⁴⁵² P. Dobrzycki: *Cywilne służby specjalne*. Warszawa 2020, s. 236-237.

¹⁴⁵³ *Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022*. https://www.bbn.gov.pl/ftp/dok/01/strategia_rozwoju_systemu_bezpieczenstwa_narodowego_rp_2022.pdf (dostęp: 14.02.2023).

roku¹⁴⁵⁴ formułuje wobec określonych służb obszary zadaniowe, a największą rolę w tym zakresie przyznaje Agencji Bezpieczeństwa Wewnętrznego, której zadaniem jest „doskonalenie zasad i mechanizmów współpracy z właściwymi podmiotami na rzecz zapewnienia bezpieczeństwa cybernetycznego; rozwijanie Systemu Reagowania na Incydynty Komputerowe”¹⁴⁵⁵. Należy również zasygnalizować, że w dokumencie – jak zresztą w wielu innych regulujących podobną materię – pojawiają się sformułowania dotyczące konieczności zacieśnienia współpracy w tym zakresie z organizacjami międzynarodowymi, takimi jak Unia Europejska oraz NATO¹⁴⁵⁶. Agencja Bezpieczeństwa Wewnętrznego pozostaje najistotniejszym ogniwem polskich cywilnych służb specjalnych w przedmiocie zapewnienia bezpieczeństwa Polski w cyberprzestrzeni. To właśnie w ramach tej organizacji funkcjonuje omówiony we wcześniejszych częściach pracy Zespół Reagowania na Incydynty Bezpieczeństwa Komputerowego CSIRT GOV, podległy Szefowi ABW¹⁴⁵⁷.

W przedmiotowym kontekście istotnym narzędziem jest system ARAKIS-GOV¹⁴⁵⁸ (AgRegacja, Analiza i Klasyfikacja Incydentów Sieciowych). Z uwagi na niejawny charakter wielu informacji, nie jest możliwe szczegółowe przedstawienie sposobu jego działania, a jedynie zarysowanie charakterystyki. Powstały w pierwszej dekadzie XXI wieku system ma za zadanie wykrywanie oraz opisywanie zagrożeń, które występują w sieci (Internecie), a w 2005 roku stał się źródłem raportowania incydentów Zespołu CERT Polska¹⁴⁵⁹. Z końcem 2015 roku został zastąpiony przez nową generację systemu ARAKIS 2.0¹⁴⁶⁰, a następnie ARAKIS 3.0¹⁴⁶¹. ARAKIS to „dedykowany, rozproszony system wczesnego ostrzegania o zagrożeniach teleinformatycznych występujących na styku sieci wewnętrznej z siecią Internet. Głównym zadaniem systemu jest wykrywanie i zautomatyzowane opisywanie zagrożeń występujących w sieciach teleinformatycznych na podstawie agregacji, analizy

¹⁴⁵⁴ Uchwała Nr 67 Rady Ministrów z dnia 9 kwietnia 2013 r. w sprawie przyjęcia „Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022” (M.P. 2013 poz. 377).

¹⁴⁵⁵ *Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022*. https://www.bbn.gov.pl/ftp/dok/01/strategia_rozwoju_systemu_bezpieczenstwa_narodowego_rp_2022.pdf (dostęp: 14.02.2023), s. 92.

¹⁴⁵⁶ Ibidem, s. 42-43.

¹⁴⁵⁷ Zespół Reagowania na Incydynty Bezpieczeństwa Komputerowego CSIRT GOV: *O nas*. <https://csirt.gov.pl/> (dostęp: 14.02.2023).

¹⁴⁵⁸ Dla ujednolicenia autor posługuje się w pracy sformułowaniem ARAKIS, bez względu na wersję systemu.

¹⁴⁵⁹ Zespół CERT Polska: *Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2005*. https://cert.pl/uploads/docs/Raport_CP_2005.pdf (dostęp: 15.02.2023), s. 3, 9.

¹⁴⁶⁰ Zespół Reagowania na Incydynty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku...*, s. 33.

¹⁴⁶¹ Zespół Reagowania na Incydynty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 roku...*, s. 19.

i korelacji danych z różnych źródeł”¹⁴⁶². Jest programem realizowanym przez Agencję Bezpieczeństwa Wewnętrznego oraz wynikiem kooperacji Departamentu Bezpieczeństwa Teleinformatycznego ABW oraz działającego w strukturach NASK zespołu CERT Polska¹⁴⁶³. Istota działania systemu sprowadza się więc przede wszystkim do funkcji informacyjnej, a więc zawiadamiania administratorów o występujących w sieci zagrożeniach. Dla przykładu można zauważyć, że w 2019 roku system zanotował łącznie ponad 1 miliard przepływów, co przełożyło się na wygenerowanie ponad 800 tysięcy alarmów¹⁴⁶⁴. W 2020 roku odnotowano ponad 1,8 miliarda przepływów i ponad 1,7 miliona alarmów¹⁴⁶⁵. Natomiast w 2021 roku było to około 1,7 miliarda przepływów, co przełożyło się aż na ponad 3,3 miliona alarmów¹⁴⁶⁶. Można więc wyprowadzić wniosek, że liczba zarejestrowanych incydentów, jak i wygenerowanych alarmów wzrosła tylko na przestrzeni trzech lat¹⁴⁶⁷. Działalność systemu ARAKIS nie obejmuje oczywiście całej polskiej cyberprzestrzeni, jednakże monitoruje najważniejsze jej elementy, kluczowe dla funkcjonowania państwa (w tym infrastrukturę krytyczną). Warto również wspomnieć o drugiej generacji systemu – ARAKIS 2 Enterprise, którego celem jest zapewnienie cyberbezpieczeństwa, również w przedsiębiorstwach o znaczeniu strategicznym dla państwa¹⁴⁶⁸.

Jak już wspomniano, cyberprzestrzeń Polski podlega nieustannemu monitorowaniu. Jednym ze skutków takiego działania może być ogłaszanie stopni alarmowych na wypadek wystąpienia zagrożenia, bądź też w charakterze prewencyjnym. Stopnie zostały wprowadzone do polskiego porządku prawnego ustawą z dnia 10 czerwca 2016 roku o działaniach antyterrorystycznych¹⁴⁶⁹. We wskazanym akcie dokonano wyszczególnienia czterech ich typów, które można wprowadzić w przypadku „zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym dotyczącego systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład

¹⁴⁶² Zespół Reagowania na Incydynty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku...*, s. 38.

¹⁴⁶³ Zespół Reagowania na Incydynty Bezpieczeństwa Komputerowego CSIRT GOV: *System ARAKIS-GOV*. <https://csirt.gov.pl/cer/system-arakis-gov/310,system-arakis-gov.html> (dostęp: 16.02.2023).

¹⁴⁶⁴ Zespół Reagowania na Incydynty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 roku...*, s. 23.

¹⁴⁶⁵ Zespół Reagowania na Incydynty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2020 roku...*, s. 38.

¹⁴⁶⁶ Zespół Reagowania na Incydynty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku...*, s. 38.

¹⁴⁶⁷ Szczegółowe zestawienie w tym zakresie zostało przedstawione w kolejnym podrozdziale.

¹⁴⁶⁸ NASK: *System wczesnego ostrzegania o cyberzagrożeniach (ARAKIS)*. <https://www.nask.pl/pl/dzialalnosc/nauka-i-biznes/projekty-badawcze/2075,system-wczesnego-ostrzegania-o-cyberzagrozeniach-ARAKIS.html> (dostęp: 16.02.2023); ARAKIS Enterprise NASK: *Arakis - Innowacyjny system wczesnego ostrzegania o cyberzagrożeniach IT i SCADA*. <https://www.arakis.pl/> (dostęp: 16.02.2023).

¹⁴⁶⁹ Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz.U. 2016 poz. 904).

infrastruktury krytycznej albo w przypadku wystąpienia takiego zdarzenia”¹⁴⁷⁰. Do rodzajów stopni zaliczamy: pierwszy stopień alarmowy CRP (stopień ALFA-CRP), drugi stopień alarmowy CRP (stopień BRAVO-CRP), trzeci stopień alarmowy CRP (stopień CHARLIE-CRP) oraz czwarty stopień alarmowy CRP (stopień DELTA-CRP)¹⁴⁷¹. W zależności od występujących okoliczności czy też przewidywanego bądź zaistniałego zagrożenia, wprowadza się stopnie alarmowe poczynając od pierwszego, a kończąc na czwartym. Do przykładów takich działań można zaliczyć 21 lutego 2022 roku i wprowadzenie trzeciego stopnia alarmowego, co miało bezpośredni związek z przewidywaniami co do rozpoczęcia rosyjskiej inwazji w Ukrainie i konsekwencji z tym związanych dla bezpieczeństwa Polski w cyberprzestrzeni¹⁴⁷². W związku z faktycznym wystąpieniem konfliktu obowiązywanie stopnia alarmowego zostało przedłużone¹⁴⁷³. Stopnie wprowadzano podczas ważnych wydarzeń jak chociażby w trakcie organizowanego Szczytu Cyfrowego ONZ w Katowicach¹⁴⁷⁴ czy też Konferencji dotyczącej bezpieczeństwa na Bliskim Wschodzie¹⁴⁷⁵.

Reasumując należy wskazać na następujące wnioski. W Polsce funkcjonuje złożony oraz zdecentralizowany system cyberbezpieczeństwa¹⁴⁷⁶. Fakt ten legł u podstaw problemów związanych z jego funkcjonowaniem, które sprowadzały się przede wszystkim do rozproszenia kompetencji w ramach wielu podmiotów i braku jednoznacznego ich rozdzielenia. W konsekwencji na powyższym tle dochodziło do licznych konfliktów kompetencyjnych pomiędzy instytucjami, w wyniku czego zmniejszono skuteczność oraz obniżono zdolność do zwalczania cyberzagrożeń. Problem ten został względnie rozwiązany wraz z przyjęciem ustawy o krajowym systemie cyberbezpieczeństwa. Mimo to polscy decydenci polityczni, bez względu na przynależność partyjną, co do zasady zdawali sobie sprawę ze znaczenia omawianych w niniejszym podrozdziale zagadnień. Wyrazem tego były publikowane dokumenty w których zawierano podstawowe założenia w przedmiotowym zakresie, i choć z ich realizacją bywało również to należy zauważyć, że na koniec 2022 roku w Polsce funkcjonuje rozbudowany

¹⁴⁷⁰ Ibidem, art. 15 ust. 2.

¹⁴⁷¹ Ibidem, art. 15 ust. 2 pkt 1-4.

¹⁴⁷² gov.pl: *UWAGA – wprowadzono 3 stopień alarmowy CHARLIE-CRP*. <https://www.gov.pl/web/baza-wiedzy/uwaga--wprowadzono-3-stopien-alarmowy-charlie-crp> (dostęp: 16.02.2023).

¹⁴⁷³ gov.pl: *Przedłużenie obowiązywania stopni alarmowych BRAVO oraz CHARLIE-CRP – do 30 listopada 2022r.* <https://www.gov.pl/web/rcb/przedluzenie-obowiazywania-stopni-alarmowych-bravo-oraz-charlie-crp--do-30-listopada-2022r> (dostęp: 16.02.2023); gov.pl: *Przedłużenie obowiązywania stopni alarmowych do 28 lutego 2023r.* <https://www.gov.pl/web/rcb/przedluzenie-obowiazywania-stopni-alarmowych-do-28-lutego-2023r> (dostęp: 16.02.2023).

¹⁴⁷⁴ gov.pl: *Stopień alarmowy ALFA-CRP na terenie całego kraju*. <https://www.gov.pl/web/rcb/stopien-alarmowy-alfa-crp-na-terenie-calego-kraju> (dostęp: 16.02.2023).

¹⁴⁷⁵ gov.pl: *Stopień alarmowy BRAVO-CRP*. <https://www.gov.pl/web/mswia/stopien-alarmowy-bravo-crp> (dostęp: 16.02.2023).

¹⁴⁷⁶ K. Chałubińska-Jentkiewicz: *Cyberodpowiedzialność*. Toruń 2019, s. 361 i nast.

system zapewniania cyberbezpieczeństwa, z perspektywą jego dalszego rozwoju. Liczba niepożądanych aktywności wobec Polski w cyberprzestrzeni z roku na rok wyraźnie wzrasta, czego konsekwencją jest zwiększenie zakresu działalności podmiotów odpowiedzialnych za ich zwalczanie. Odzwierciedleniem tego stało się przyjęcie wspomnianej ustawy o krajowym systemie cyberbezpieczeństwa, będącej implementacją dyrektywy NIS. Nie jest wykluczone, a powinno być wręcz pewne, że w kolejnych latach można spodziewać się dalszego rozwoju Krajowego systemu cyberbezpieczeństwa, zwiększania kompetencji podmiotów w nim uczestniczących oraz wzrostu ilości zasobów przeznaczanych na jego funkcjonowanie. Choć na przestrzeni lat system zapewnienia bezpieczeństwa Polski w cyberprzestrzeni ulegał licznym reorganizacjom to nadal należy zauważyć, że cechuje się on wysokim stopniem rozproszenia pomiędzy licznymi podmiotami, które w nim uczestniczą.

6.2. Charakterystyka, przebieg i implikacje rosyjskich ataków teleinformatycznych wobec Polski w cyberprzestrzeni w latach 2010-2022

Aby zrozumieć *modus operandi* Federacji Rosyjskiej w zakresie wykorzystania wojny informacyjnej jako instrumentu polityki zagranicznej wobec Polski, należy w pierwszej kolejności poddać analizie znane przypadki przeprowadzonych bądź inspirowanych przez Kreml cyberataków wobec Polski w cyberprzestrzeni. Z uwagi na fakt, że wojna informacyjna na gruncie przedmiotowej rozprawy jest traktowana nie tylko jako oddziaływanie informacyjne na odbiorców w Internecie, ale również jako dokonywanie cyberataków w cyberprzestrzeni, niezbędne jest omówienie działań podejmowanych przez Kreml w tym zakresie. Nie można bowiem dokonać rozdzielenia wskazanych wyżej zagadnień w sytuacji, w której pozostają one względem siebie całkowicie komplementarne. Rosyjska aktywność wobec Polski w cyberprzestrzeni jest oczywiście niezwykle złożonym zjawiskiem, jednakże przede wszystkim na podstawie rocznych raportów publikowanych przez Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV oraz Zespół CERT Polska jest możliwe wskazanie jej charakteru, uwarunkowań oraz najważniejszych implikacji, zarówno tych o wewnątrzpolskich, jak i tych na gruncie stosunków polsko-rosyjskich. Raporty wskazanych podmiotów zostały wybrane z uwagi na fakt, że instytucje te zajmują się badaniem incydentów teleinformatycznych kierowanych wobec Polski w cyberprzestrzeni oraz mają kluczowy udział w tworzeniu i funkcjonowaniu polskiego systemu cyberbezpieczeństwa – na co wskazano

między innymi w ustawie¹⁴⁷⁷. W celu uzupełnienia badań zostały w nich wykorzystane między innymi raporty publikowane przez takie podmioty jak na przykład Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), Kaspersky Lab, Symantec, FireEye, F-Secure oraz Microsoft.

Dane dotyczące rosyjskich incydentów teleinformatycznych w cyberprzestrzeni są rozproszone wśród różnych dokumentów i raportów, przygotowanych przez szereg instytucji oraz podmiotów gospodarczych. Celem rozprawy realizowanym w przedmiotowym podrozdziale jest ich zebranie, wyszczególnienie rosyjskich ataków teleinformatycznych dokonanych wobec Polski w cyberprzestrzeni w omawianym okresie. Następnie zestawienie ich z kwestiami spornymi występującymi w stosunkach polsko-rosyjskich oraz ukazanie najważniejszych implikacji z tym związanych. Należy jednak zaznaczyć, że znaczna część informacji dotyczących źródeł oraz skutków cyberataków przeprowadzonych wobec Polski w cyberprzestrzeni nie jest jawna. Podstawową przyczyną są względy bezpieczeństwa państwa i tego też powodu odpowiednie służby nie publikują szeregu kluczowych informacji. Tym samym raporty Zespołu CERT Polska czy CSIRT GOV stanowią swego rodzaju zarys raportowanej za dany rok sytuacji. W związku z tym niezbędne jest odwołanie się do szeregu innych źródeł, zarówno rządowych jak i pozarządowych, których skutkiem będzie kompilacja i analiza znajdujących się tam danych.

Dokonano podziału niniejszej części rozprawy na trzy podrozdziały. Pierwszy, obejmujący lata 2010-2013, a więc od katastrofy samolotu z Prezydentem RP pod Smoleńskiem do Euromajdanu na Ukrainie, który rozpoczął się pod koniec 2013 roku. Drugi podrozdział obejmuje przedział czasowy od 2014 roku do 2019 roku, tj. od aneksji Półwyspu Krymskiego przez Federację Rosyjską oraz rozpoczęcia wojny we wschodniej Ukrainie. Następne lata do 2019 roku to okres napięć w stosunkach polsko-rosyjskich, związanych z polską polityką dywersyfikacji dostaw źródeł energii, zwiększaniem obecności Sojuszu Północnoatlantyckiego na tzw. wschodniej flance NATO, oraz wzmożone zaangażowanie rządu w Warszawie we wspieranie procesów integracyjnych na linii Kijów – Unia Europejska oraz NATO. Trzeci z podrozdziałów obejmuje lata 2020-2022, a więc od rozpoczęcia pandemii wirusa SARS-CoV-2 i zwiększonej aktywności Rosjan w polskiej przestrzeni informacyjnej w kontekście realizowanych działań dezinformacyjnych i propagandowych. Z kolei rok 2022 roku to rozpoczęcie przez Kreml pełnowymiarowej inwazji na Ukrainę i niespotykany dotąd impas w relacjach bilateralnych.

¹⁴⁷⁷ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560).

6.2.1. Charakterystyka, przebieg i implikacje rosyjskich ataków teleinformatycznych wobec Polski w cyberprzestrzeni w latach 2010-2013

[2010] W raporcie CERT Polska z 2010 roku wskazano, że „Polska korzystnie wypada na tle innych państw, jeśli chodzi o liczbę zagrożeń mających źródło w danym kraju. We wszystkich statystykach Polska jest poza pierwszą dziesiątką, za krajami porównywalnej wielkości i w podobnym stopniu zinformatyizowanymi”¹⁴⁷⁸. W tym samym roku na stronach rosyjskich odnotowano znaczną liczbę plików ze złośliwym oprogramowaniem (czwarte miejsce na świecie pod względem ich źródeł), co może mieć jednak związek ze złą opinią dostawców usług hostingowych w Rosji, którzy nie są skory do współpracy w zakresie usuwania szkodliwych zasobów, i być może z tej przyczyny pozostają w zainteresowaniu podmiotów wykorzystujących taki typ oprogramowania¹⁴⁷⁹. Z kolei według raportu Zespołu CSIRT GOV (wcześniej CERT GOV, CERT.GOV.PL¹⁴⁸⁰) w 2010 roku rozkład cyberataków dokonanych na sieci monitorowane przez system ARAKIS wyniósł 6,83% w przypadku Rosji (3 miejsce wśród ustalonych źródeł ataków¹⁴⁸¹)¹⁴⁸².

Rok 2010 pod względem stosunków polsko-rosyjskich był szczególny. Dotychczas trudne relacje sąsiadów zostały skonfrontowane z wydarzeniami jakie miały miejsce 10 kwietnia tego roku w Smoleńsku. Katastrofa samolotu rządowego z Prezydentem Rzeczypospolitej Polskiej nie doprowadziła jednak do długotrwałej normalizacji wzajemnych relacji. Polska w omawianym okresie w zasadzie przez cały czas była celem rosyjskich cyberataków, podobnie jak przed rokiem 2010. Dla przykładu, w marcu tego roku NATO i Unia Europejska informowały o znacznym wzroście dokonanych ataków teleinformatycznych w ciągu ostatnich dwunastu miesięcy, a jako ich źródła wskazano Federację Rosyjską¹⁴⁸³. Z kolei w okolicach kwietnia 2010 roku doszło do cyberataków na polski sektor finansowy oraz

¹⁴⁷⁸ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2010...*, s. 3.

¹⁴⁷⁹ Ibidem, s. 11-12.

¹⁴⁸⁰ Nazwa Zespołu była poddana w badanym okresie zmianie, dlatego też w tekście dla uproszczenia autor posługuje się jedynie zastosowanym skrótem, który jest używany na dzień 31 grudnia 2022 roku – CSIRT GOV. Poprzednia nazwa Zespołu – CERT.GOV.PL.

¹⁴⁸¹ Prawie 39% cyberataków pochodziło z terytorium Chin, a 25% z terytorium USA. Źródło: Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2010 roku...*, s. 11.

¹⁴⁸² Ibidem, s. 11.

¹⁴⁸³ K. Liedel, P. Piasecka: *Wojna cybernetyczna – wyzwanie XXI wieku*. „Bezpieczeństwo narodowe” 2011, nr I-2011/17, s. 20.

administrację rządową¹⁴⁸⁴. Odwilż w stosunkach bilateralnych jaka miała miejsce pomiędzy Polską a Rosją, co ciekawe nie przełożyła się więc na zmniejszenie liczby przeprowadzonych przez Moskwę cyberataków.

W listopadzie 2010 roku doszło do cyberataku, którego celem było Ministerstwo Spraw Zagranicznych. Polegał on na rozesłaniu wiadomości e-mail, które zawierały plik w formacie PDF ze złośliwym oprogramowaniem. Wiadomość sugerowała, że jej nadawcą jest członek organu Unii Europejskiej, podczas gdy prawdziwym jej źródłem była maszyna zlokalizowana na terytorium Federacji Rosyjskiej. Miesiąc później doszło do kolejnego dużego ataku, tym razem na szereg instytucji, między innymi MSZ oraz ABW. Wiadomości były rozsyłane w analogiczny sposób jak wskazano wyżej, przy czym tym razem atakujący podszył się pod organy NATO. Dochodzenie wykazało, że ich masowe kolportowanie przeprowadzono z terytorium Rosji¹⁴⁸⁵. Z kolei wydarzenia z 10 kwietnia 2010 roku zostały wykorzystane do przeprowadzenia ataków na podmioty polskiej administracji publicznej, co polegało ponownie na rozsyłaniu zainfekowanych złośliwym oprogramowaniem wiadomości e-mail z kont pocztowych z domeną rosyjską – .ru¹⁴⁸⁶. Opisane wyżej ataki nawiązywały więc do kwestii spornych w stosunkach polsko-rosyjskich dotyczących polityki bezpieczeństwa NATO oraz katastrofy smoleńskiej.

[2011] W 2011 roku w przypadku systemu ARAKIS odnotowano, przy uwzględnieniu jak i bez uwzględnienia unikalnych adresów IP, liczne cyberataki ze strony Rosji, która zajęła w tym aspekcie kolejno drugie i trzecie miejsce¹⁴⁸⁷. Co ciekawe, względem roku ubiegłego doszło do spadku liczby ataków dokonywanych z Rosji na sieci monitorowane przez system ARAKIS, co przełożyło się na 3,72% ich ogółu, choć należy zauważyć, że wzrosła aktywność ze strony Turcji, z terytorium której dokonano 4,55% cyberataków¹⁴⁸⁸. Pod względem liczby serwerów C&C¹⁴⁸⁹ Rosja zajęła 3. miejsce w rankingu światowym z wynikiem 5,9%. Została w tym zakresie zdeklasowana przez Niemcy (13,4%) oraz USA (29,4%), co jednak nie oznacza, że jej udział jest niewielki. Dla przykładu Polska w tym zestawieniu zajmuje dopiero 23.

¹⁴⁸⁴ J. Małycha: *Cyberwojna. „Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej”* 2016, nr 4(20), s. 217-218.

¹⁴⁸⁵ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2010 roku...*, s. 24.

¹⁴⁸⁶ Ibidem, s. 26.

¹⁴⁸⁷ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2011...*, s. 62.

¹⁴⁸⁸ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2011 roku...*, s. 12.

¹⁴⁸⁹ Serwery C&C (ang. *Command & Control*) można zdefiniować jako centra każdej operacji wykorzystującej złośliwe oprogramowanie. To za ich pomocą atakujący kontroluje oprogramowanie, które zainfekowało dany system. Chodzi więc o wydawanie komend np. blokujących zainfekowane urządzenie, wprowadzających zmiany do takiego urządzenia, czy też wykradających z niego dane.

miejsce¹⁴⁹⁰. Federacja Rosyjska zajęła również wysoką pozycję w zestawieniu państw w których były hostowane pliki ze złośliwym oprogramowaniem – 4. miejsce i wynik 5,48%¹⁴⁹¹. Wyższe pozycje zajęły już tradycyjnie Chiny oraz USA.

Twórcy raportu zauważyli jednak, że: „z drugiej strony dość częste są spekulacje, że internetowi przestępcy działają w Chinach, Rosji czy na Ukrainie za cichym przyzwoleniem wpływowych środowisk”¹⁴⁹². Federacja Rosyjska była również w tym czasie klasyfikowana jako kraj będący jednym z największych producentów złośliwego oprogramowania, ustępując jedynie Chinom oraz państwom w Ameryce Łacińskiej. Ponadto w raporcie podkreślono, że pomimo iż centralna oraz wschodnia część Europy jest klasyfikowana jako rynek wschodzący, to posiada pewne charakterystyczne cechy dla rynków rozwiniętych, jak wysoki poziom kształcenia specjalistów, co przekłada się z kolei na bardzo dobrą kadrę programistów, jak i wykwalifikowanych hakerów¹⁴⁹³.

[2012] W 2012 roku w kontekście funkcjonowania systemu ARAKIS zauważono, że znacząco wzrosła aktywność z Rosji, jako źródła cyberataków dokonywanych na sieci objęte programem i wyniosła 7,74% (5. miejsce). Co ciekawe, cyberataki przeprowadzone przy użyciu adresów IP przypisanych do terytorium Polski stanowiły 9,97% (4. miejsce). Należy zasygnalizować, że w omawianym zestawieniu, jak i w zestawieniach z 2010 i 2011 roku pojawia się kategoria *nieznany*, która oznacza określenie adresów IP, których nie można przypisać jakiegokolwiek podmiotowi (dokonano więc podmiany prawdziwego źródłowego adresu IP), a zatem część ataków Kremla mogła być przeprowadzona w ten sposób¹⁴⁹⁴. W raporcie stwierdzono również, że w 2012 roku zaobserwowano zjawisko coraz częstszego stosowania nazw domenowych z końcówką .pl do zarządzania złośliwym oprogramowaniem oraz *botnetami*. Według autorów, większość *botów* znajdujących się za granicą działała z terytorium Chin, Rosji oraz Łotwy¹⁴⁹⁵.

W odniesieniu do ogólnej liczby incydentów teleinformatycznych w Polsce, dane na ten temat przedstawiono w raporcie Norton Cybercrime Report 2012, przygotowanym przez Symantec. Według jego autorów, w 2012 roku ofiarami cyberprzestępców miało paść ponad

¹⁴⁹⁰ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2011...*, s. 23.

¹⁴⁹¹ Ibidem, s. 13.

¹⁴⁹² Ibidem, s. 13.

¹⁴⁹³ IDC Analyze the Future: *The Dangerous World of Counterfeit and Pirated Software How Pirated Software Can Compromise the Cybersecurity of Consumers, Enterprises, and Nations ... and the Resultant Costs in Time and Money Sponsored by: Microsoft*. <https://news.microsoft.com/download/presskits/antipiracy/docs/IDC030513.pdf> (dostęp: 24.02.2023).

¹⁴⁹⁴ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2012 roku...*, s. 9.

¹⁴⁹⁵ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2012...*, s. 50.

siedem milionów Polaków, przy czym celem ataku były przede wszystkim smartfony oraz sieci społecznościowe¹⁴⁹⁶. Zwrócono również uwagę, że największy odsetek osób dorosłych które doświadczyły przestępstw w sieci był w Rosji (92%), a następnie w Chinach (84%), z kolei dla porównania w Polsce było to 68%¹⁴⁹⁷. Co ciekawe, powyższe zestawienie nie koreluje z wartością poniesionych strat finansowych wskutek dokonanych cyberataków, gdyż w przypadku Rosji są to 2 miliardy dolarów, w USA 21 miliardów dolarów, w Europie 16 miliardów dolarów, natomiast w przypadku Chin aż 46 miliardów dolarów, co plasuje ten kraj na pierwszym miejscu na świecie¹⁴⁹⁸.

[2013] W 2013 roku rosyjska aktywność (liczba ataków) w sieciach monitorowanych przez system ARAKIS znajdowała się na podobnym poziomie względem roku ubiegłego. Wyniosła 7,27%, przy czym ponownie ustąpiła USA (18,10%) oraz Chinom (16,01%)¹⁴⁹⁹. Można również zauważyć stosunkowo dużą penetrację Polski w cyberprzestrzeni przez Rosję. W tym kontekście 7,3% wszystkich skanowań polskich sieci pochodziło z Federacji Rosyjskiej, choć tutaj ponownie widać większą aktywność po stronie USA (około 8%) oraz Chin (prawie 27%)¹⁵⁰⁰. W przypadku serwerów C&C Federacja Rosyjska ponownie zajęła wysokie miejsce pośród krajów w których są one hostowane, plasując się na 3. miejscu na świecie z wynikiem 7,75%, co oznacza wzrost względem lat ubiegłych. Mimo to została wyprzedzona przez Niemcy (7,89%) oraz USA (31,98%), natomiast Polska zajęła 25. miejsce¹⁵⁰¹.

W kontekście incydentów teleinformatycznych w 2013 roku doszło do wykrycia przez Kaspersky Lab wirusa, który infekował od około 5 lat urządzenia na całym świecie. Według raportu, wirus rozprzestrzeniał się poprzez wysłanie do użytkowników wiadomości e-mail z załączonym zainfekowanym dokumentem w formacie PDF, programu Word albo Excel. Nazwa dokumentu miała oczywiście zachęcać do jego otwarcia, dlatego też jeden z tytułów którego użyto brzmiał *Katyn_-_opinia_Rosjan.xls*, co wskazuje, że celem wirusa miały być również polskie instytucje. Analizując nazwę pliku ze złośliwym oprogramowaniem warto zauważyć nawiązanie do kwestii spornej w stosunkach polsko-rosyjskich, jaką jest polityka historyczna, a w tym przypadku zbrodnia katyńska. Faktem jest, że złośliwe oprogramowanie zostało napisane w języku rosyjskim co z dużą dozą pewności wskazuje, iż autorzy cyberataku

¹⁴⁹⁶ Rzeczpospolita: *Norton Cybercrime Report 2012: Polacy na celowniku hakerów*. <https://www.rp.pl/media/art5923571-norton-cybercrime-report-2012-polacy-na-celowniku-hakerow> (dostęp: 25.02.2023).

¹⁴⁹⁷ Symantec: *Norton Cybercrime Report 2012*. https://biz-file.com/f/1311/2012_Norton_Cybercrime_Report_.pdf (dostęp: 25.02.2023), s. 22.

¹⁴⁹⁸ Ibidem, s. 7.

¹⁴⁹⁹ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 roku...*, s. 12.

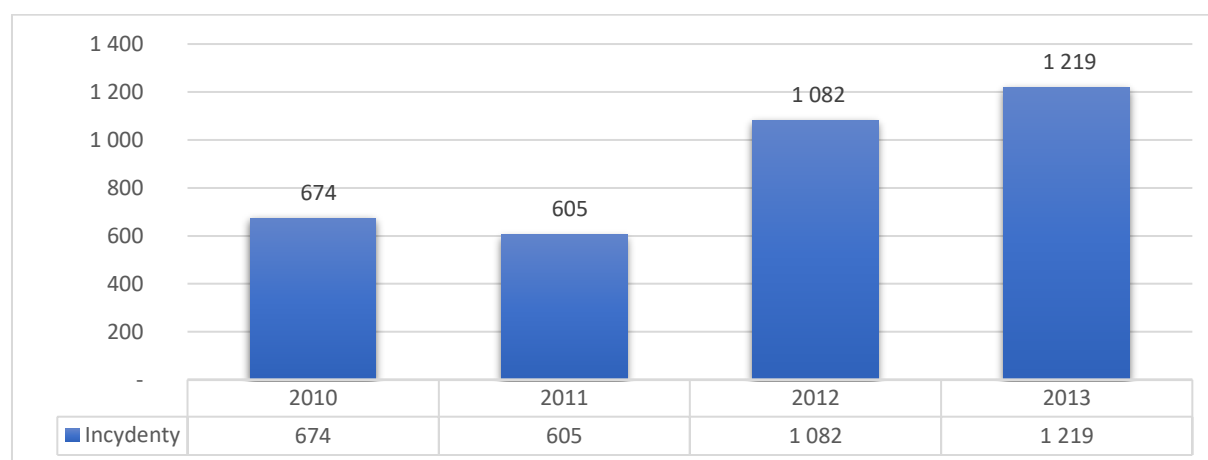
¹⁵⁰⁰ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2013...*, s. 46.

¹⁵⁰¹ Ibidem, s. 41.

pochodzą z Federacji Rosyjskiej¹⁵⁰². W ujęciu globalnym, znaczna część ataków o podłożu finansowym również pochodziła z terytorium Rosji¹⁵⁰³. W raporcie Zespołu CERT Polska za 2013 roku wskazano, że zaobserwowano stosunkowo „niewielką aktywność związaną z tzw. atakami APT przeciwko polskim podmiotom lub w polskiej przestrzeni adresowej. Nawet jeśli dotyczą one „polskich IP”, to niekoniecznie polskich podmiotów”¹⁵⁰⁴.

W odniesieniu do powyższych rozważań należy szczególnie podkreślić, że realizowanie wrogiej aktywności wobec Polski w cyberprzestrzeni nie jest wyłączną domeną działalności służb specjalnych oraz sił zbrojnych danego kraju. Istotną rolę ogrywają bowiem podmioty pozapaństwowe, przede wszystkim cyberprzestępcy i hakywiści. Niejednokrotnie są oni autorami przeprowadzanych cyberataków, będąc powiązani pośrednio lub bezpośrednio z organami danego państwa. Wreszcie, prowadzą również działania na zlecenie oraz z inspiracji samego Kremla – w zgodzie z interesami rosyjskiej polityki zagranicznej. Moskwa nie wyciąga wobec nich żadnych negatywnych konsekwencji, o ile pozostała prowadzona przez nie działalność jest skierowana wyłącznie wobec państw, czy też podmiotów zachodnich¹⁵⁰⁵.

Wykres 7. Liczba incydentów obsługiwanych ręcznie¹⁵⁰⁶ przez Zespół CERT Polska w latach 2010-2013.



Źródło: Opracowanie własne na podstawie raportów rocznych Zespołu CERT Polska za lata 2010-2013.

¹⁵⁰² Niebezpiecznik: *Rosyjskojęzyczny wirus infekował Polaków plikiem o Katyniu*. <https://zaufanatrzeciastrona.pl/post/rosyjskojeczny-wirus-infekowal-polakow-plikiem-o-katyniu/> (dostęp: 25.02.2023).

¹⁵⁰³ Verizon RISK Team: *2013 Data Breach Investigations Report*. <https://www.netsurion.com/eventtracker/media/eventtracker/files/collateral/verizon-data-breach-2013.pdf> (dostęp: 25.02.2023).

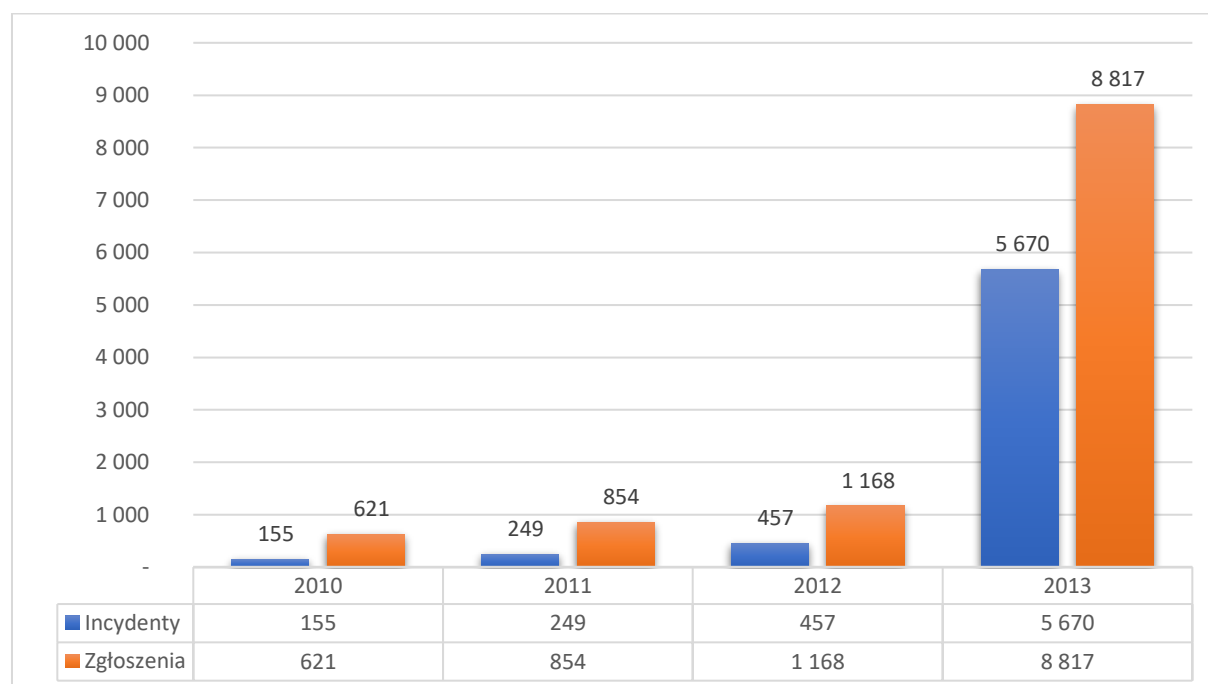
¹⁵⁰⁴ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2013...*, s. 6.

¹⁵⁰⁵ A. Kozłowski: *Działalność Rosji w cyberprzestrzeni zagrożeniem dla bezpieczeństwa państw regionu euroatlantyckiego*. W: *Informacja czynnikiem warunkującym bezpieczeństwo. Kontekst rosyjski*. Red. M. Banasik. Warszawa 2021, s. 99; The Register: *Leaked IT contractor files detail Kremlin's stockpile of cyber-weapons*. https://www.theregister.com/2023/03/31/vulkan_files_russia/ (dostęp: 25.05.2023).

¹⁵⁰⁶ Incydenty obsługiwane ręcznie to incydenty, które zostały zarejestrowane oraz wymagają bezpośredniego działania przez członka Zespołu.

W odniesieniu do wykresu należy jednak zauważyć, że liczba incydentów w latach poprzedzających 2010 rok sukcesywnie malała od 2005 roku¹⁵⁰⁷ i tak w tym roku wynosiła 2516, w 2006 roku 2427, w 2007 roku 2108, w 2008 roku 1796, a w 2009 roku 1292¹⁵⁰⁸. Spadek incydentów na przestrzeni lat 2005-2009, ale również w latach 2010-2011, koresponduje z ówczesnymi stosunkami bilateralnymi na linii Warszawa-Moskwa. Lata 2005-2007 to bowiem okres eskalacji napięć w okresie rządów sprawowanych między innymi przez Prawo i Sprawiedliwość, z kolei od 2007/2008 roku, po przejęciu władzy przez koalicję PO-PSL, nastąpiła pragmatyzacja relacji dwustronnych. Następnie w latach 2011-2013 w stosunkach polsko-rosyjskich zauważalny był impas, który eskalował po aneksji Półwyspu Krymskiego w 2014 roku. Choć powyższe zestawienie odnosi się do łącznej liczby incydentów obsługiwanych przez CERT Polska w poszczególnych latach, to zauważalna jest korelacja podanych wartości ze stanem stosunków polsko-rosyjskich w danym okresie.

Wykres 8. Liczba zgłoszonych oraz faktycznych incydentów odnotowanych przez Zespół CSIRT GOV w latach 2010-2013.

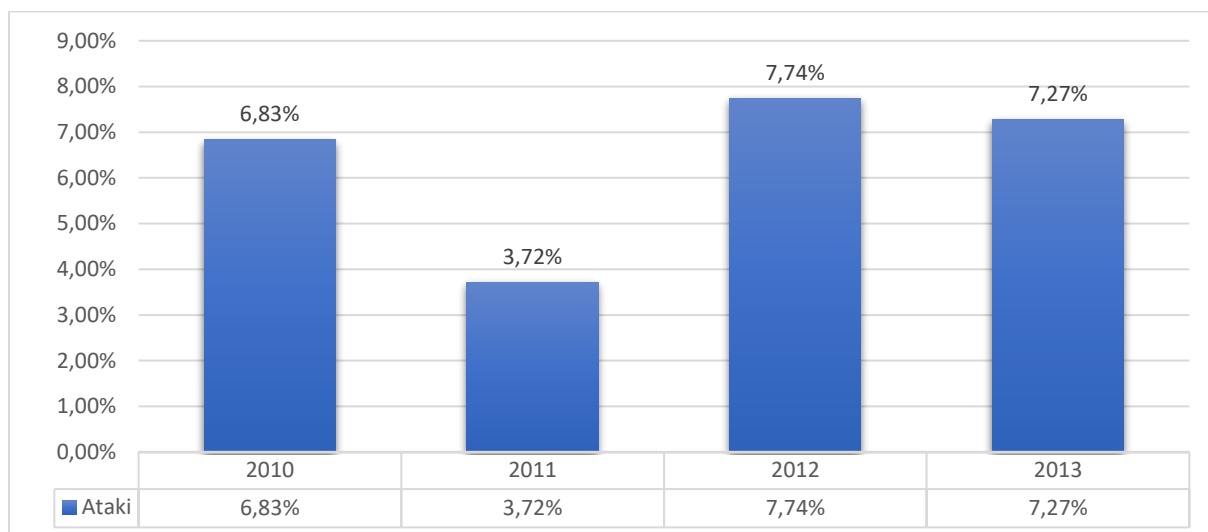


Źródło: Opracowanie własne na podstawie raportów rocznych Zespołu CSIRT GOV za lata 2010-2013.

¹⁵⁰⁷ W roku 2001 liczba incydentów obsługiwanych przez CERT Polska wyniosła 741, w 2002 roku 1013 incydentów, w 2003 roku 1196 incydentów, a w 2004 roku 1222 incydenty. Źródło: Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2010...*, s. 27.

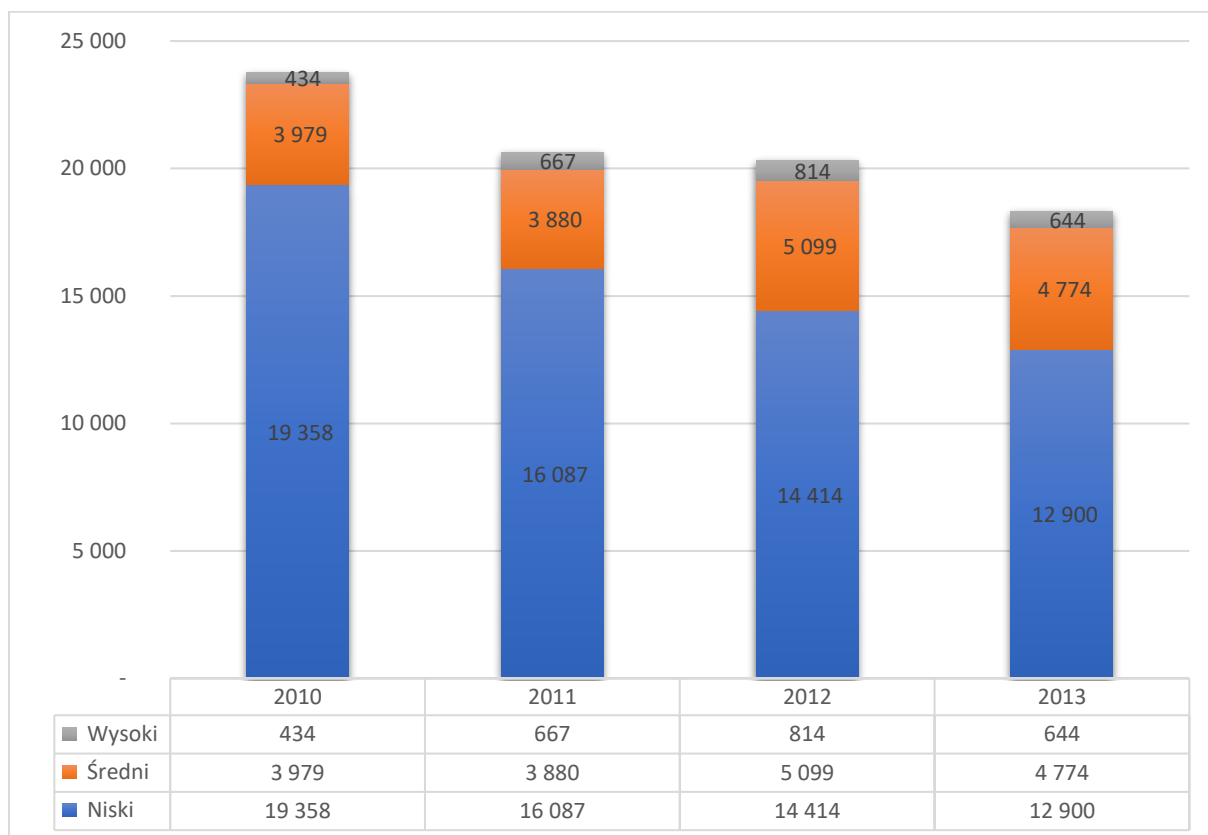
¹⁵⁰⁸ Ibidem, s. 27.

Wykres 9. Rozkład procentowy ataków z Federacji Rosyjskiej na monitorowane przez system ARAKIS sieci w latach 2010-2013.



Źródło: Opracowanie własne na podstawie raportów rocznych Zespołu CSIRT GOV za lata 2010-2013.

Wykres 10. Liczba zarejestrowanych alarmów (z podziałem na priorytety¹⁵⁰⁹) przez system ARAKIS w latach 2010-2013.



Źródło: Opracowanie własne na podstawie raportów rocznych Zespołu CSIRT GOV za lata 2010-2013.

¹⁵⁰⁹ Raporty roczne Zespołu CSIRT GOV w zakresie analizy alarmów wygenerowanych przez system ARAKIS obejmują podział ich priorytetów na: niski, średni oraz wysoki.

Podsumowując podrozdział można wskazać na następujące wnioski. W zakresie rosyjskiej ingerencji w sieci monitorowane przez system ARAKIS odnotowano stosunkowo dużą aktywność, która w badanym okresie mieści się w przedziale od 3,72% do 7,74% łącznej liczby dokonanych cyberataków. Co ciekawe, w zasadzie w każdym roku, Rosja była wyprzedzana w przytaczanej statystyce przez Chiny oraz USA.

Polska w cyberprzestrzeni nie pozostawała w relatywnie dużym zainteresowaniu Rosji, jednakże z roku na rok zainteresowanie wzrastało. W omawianych raportach wielokrotnie wskazywano, że jednym z głównych zagrożeń był *phishing* i w tym kontekście można przytoczyć dokument zgodnie z którym w latach 2011-2013 ataki tego typu były najczęściej dokonywane z takich krajów jak USA, Wielka Brytania, Niemcy, Indie oraz Federacja Rosyjska, co jednak ważną część z tych podmiotów była nie tylko ich źródłem, ale również celem¹⁵¹⁰. Choć najczęstszym źródłem cyberataków były Chiny oraz USA, to Rosja nadal była aktywnym podmiotem realizującym wrogie działania wobec Polski w cyberprzestrzeni. Podejmowane przez nią działania korespondowały z kwestiami spornymi występującymi w stosunkach dwustronnych.

Ważną rolę w realizowanych przez Kreml operacjach odgrywały grupy APT, a jedną z najaktywniejszych była APT-28. Stała ona za atakami na szereg państw i instytucji, między innymi w Polsce. Ponadto zauważalne było, że działania grup APT były również ukierunkowane na oddziaływanie na opinię publiczną¹⁵¹¹.

W kontekście relacji bilateralnych warto zaznaczyć, że rozkład procentowy ataków z Federacji Rosyjskiej na sieci monitorowane przez system ARAKIS odpowiada ówczesnym celom polityki zagranicznej Rosji wobec Polski. W latach 2010-2011 (6,83% i 3,72%), a więc w okresie odwilży w stosunkach dwustronnych widoczny był spadek aktywności Kremla w omawianym zakresie. Z kolei w latach 2012-2013, a więc w czasie impasu na linii Warszawa-Moskwa, liczba ataków wzrosła względem lat ubiegłych (7,74% i 7,27%).

¹⁵¹⁰ Kaspersky Lab: *The evolution of phishing attacks: 2011-2013*. https://media.kaspersky.com/pdf/kaspersky_lab_ksn_report_the_evolution_of_phishing_attacks_2011-2013.pdf (dostęp: 23.02.2023), s. 4, 9.

¹⁵¹¹ FireEye: *APT28: A window into Russia's cyber espionage operations?* <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf> (dostęp: 25.05.2023); Rzeczpospolita: *Hakerzy Putina atakują rząd*. <https://www.rp.pl/polityka/art4814691-hakerzy-putina-atakuja-rzad> (dostęp 25.05.2023).

6.2.2. Charakterystyka, przebieg i implikacje rosyjskich ataków teleinformatycznych wobec Polski w cyberprzestrzeni w latach 2014-2019

[2014] Według raportu Zespołu CSIRT GOV w 2014 roku znacząco spadła liczba cyberataków dokonywanych przez Federację Rosyjską na sieci monitorowane przez system ARAKIS, plasując się na poziomie 2,68% (9 miejsce i spadek z 7,27% w 2013 roku). Co niezwykle ciekawe została ona wyprzedzona przez takie kraje jak Holandia Portugalia, Japonia, Korea Południowa oraz Francja (nie wliczając USA oraz Chin)¹⁵¹². Powyższy trend jest o tyle interesujący, iż występuje w 2014 roku, a więc w czasie ukraińskiego Euromajdanu, aneksji przez Federację Rosyjską Półwyspu Krymskiego oraz rozpoczęcia wojny we wschodniej Ukrainie. W trakcie tych wydarzeń rząd w Warszawie jawnie sprzeciwiał się działaniom podejmowanym przez Kreml, a w konsekwencji narażał się na wrogą działalność z jego strony. Trzeba jednak odnotować, że właściwości techniczne cyberprzestrzeni umożliwiają dokonywanie cyberataków za pośrednictwem innego państwa. W dużym stopniu ogólności należy przez to rozumieć, iż autor ataku znajdujący się w Rosji, może przeprowadzić go przy użyciu sieci innego państwa, np. Francji. W konsekwencji dany incydent zostanie zaklasyfikowany jako przeprowadzony potencjalnie przez podmiot francuski, a nie rosyjski. Identyfikacja następuje bowiem wyłączenie na podstawie określenia państwa, z którego nastąpiło połączenie.

Rosja ponownie znalazła się w pierwszej dziesiątce krajów hostujących serwery C&C¹⁵¹³ oraz pośród państw w których hostowano najwięcej złośliwych adresów URL z domeny .pl¹⁵¹⁴. W skali globalnej Rosję ponownie wskazano jako państwo będące w gronie państw, w których hostowano najwięcej złośliwych adresów URL z dowolną domeną¹⁵¹⁵. Z kolei w odniesieniu do skanowań polskiej infrastruktury teleinformatycznej, Rosja zajęła trzecie miejsce z wynikiem 4,7%, ustępując USA (7,4%) oraz Chinom (35,5%)¹⁵¹⁶. Analogiczny wynik Federacja osiągnęła w zakresie ilości zgłoszonych nazw domenowych, które pełniły funkcję serwerów zarządzających *botnetami*¹⁵¹⁷.

Zauważalny jest jednak inny trend w kontekście działalności Rosji w wobec Polski w cyberprzestrzeni. Raport wskazuje bowiem na nowe zagrożenie jakim stała się wojna

¹⁵¹² Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 roku...*, s. 11.

¹⁵¹³ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2014...*, s. 47.

¹⁵¹⁴ Ibidem, s. 52.

¹⁵¹⁵ Ibidem, s. 54.

¹⁵¹⁶ Ibidem, s. 64.

¹⁵¹⁷ Ibidem, s. 49.

informacyjna, która sprowadza się do działalności propagandowej w Internecie¹⁵¹⁸. Jego autorzy zauważyli, że „informacje i komentarze pisane są według podobnego szablonu, zwykle mają obszerną treść i są wysoko oceniane przez innych ‘użytkowników’. Opinie stojące w opozycji do treści zleconych są źle oceniane przez kolejnych ‘dyskutantów’. Wpisy w znacznym stopniu są kopią poprzednich, zamieszczanych na innych portalach, często w niewielkim, sekundowym odstępie czasu. Z czasem tego typu publikacje zaczęły być formułowane poprawną polszczyzną”¹⁵¹⁹. Co więcej zauważono, iż „wiele osób bezwiednie staje się uczestnikiem potyczki, która zwykle rozgrywana jest w ramach komentowania artykułów znajdujących się na ogólnodostępnych i popularnych portalach internetowych. Analiza dyskusji internetowych (również w sieciach społecznościowych) na przestrzeni ostatniego roku wskazała na gwałtowny i nienaturalny w stosunku do innych tematów wzrost aktywności Internautów w tym zakresie, a także zjawiska tzw. *trollingu* w komentowaniu działań Federacji Rosyjskiej związanych z aneksją Krymu i konfliktem na Ukrainie. Tego typu wpisy dosłownie ‘zalewały’ polskie portale informacyjne w początkowej fazie konfliktu”¹⁵²⁰. W tym kontekście wskazano na śledztwa dziennikarskie, które demaskowały działalność rosyjską, jak również zarekomendowano polskim użytkownikom Internetu zachowanie ostrożności oraz wyczulenie na próby wciągnięcia w tego typ dyskusje¹⁵²¹. Powyższe działania ponownie wpisywały się więc kwestie sporne w stosunkach polsko-rosyjskich, a w tym przypadki w aneksję Półwyspu Krymskiego.

W raporcie Zespołu CERT Polska opublikowano informacje na temat grup SandWorm oraz APT-28¹⁵²² pochodzących z Rosji. Celami ataków pierwszej z nich (również w Polsce) były placówki rządowe oraz NATO, jak również ośrodki akademickie, sektor telekomunikacyjny oraz energetyczny. W przypadku drugiego z wymienionych podmiotów autorzy zauważyli, że jego działania były wspierane przez Kreml oraz polegały na złożonych cyberatakach, których celami było również NATO oraz placówki rządowe, między innymi

¹⁵¹⁸ Należy tutaj szczególnie podkreślić, że zjawisko wojny informacyjnej jest prezentowane w raporcie Zespołu CSIRT GOV zajmującego się incydentami teleinformatycznymi, co potwierdza, że wojna informacyjna to nie tylko oddziaływanie na odbiorców w Internecie, ale również dokonywanie cyberataków. W raporcie wskazano, że „Internet i media społecznościowe z jednej strony dają możliwość szybkiego rozpowszechnienia informacji i interakcji: publikujących z Internautami. Z drugiej jednak strony, ze względu na dostępność i łatwość korzystania z powyższych udogodnień stają się także narzędziem stosowanym, do wspomagania militarnych i wywiadowczych działań prowadzonych przez państwa, poprzez uskutecznianie szeroko rozumianej akcji propagandowo-dezinformacyjnej”. Źródło: Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 roku...*, s. 48.

¹⁵¹⁹ Ibidem, s. 48.

¹⁵²⁰ Ibidem, s. 48.

¹⁵²¹ Ibidem, s. 48-49.

¹⁵²² Według informacji, w tym od rządu USA, grupa APT-28 jest komórką wywiadu wojskowego Federacji Rosyjskiej – GRU. Nazwa grupy (jak i jej podobnych) pochodzi z języka ang. *Advanced Persistent Threat*.

w Polsce¹⁵²³. Zauważono, że: „Polskie podmioty były atakowane w ramach kampanii APT, takich jak Pawn Storm, Black Energy, Energetic Bear, ale Polska nie była głównym celem ataków”¹⁵²⁴. Z kolei FireEye w swoim raporcie stwierdził, że choć nie udało się w sposób jednoznaczny powiązać działań grupy APT-28 z Kreml, to jednak zauważono, że dane wywiadowcze, które pozyskano w ramach operacji były zgodne z rosyjskimi interesami. Na ten kierunek wskazuje również fakt, że większość złośliwego oprogramowania jakie przeanalizowano zostało utworzone w godzinach 8:00-18:00 czasu moskiewskiego. Zaznaczono również, że grupa z całą pewnością korzysta ze wsparcia rządu państwa, co umożliwia zapewnienie bieżących zasobów finansowych i organizacyjnych na jej funkcjonowanie¹⁵²⁵. Grupa APT-28 była również odpowiedzialna za kampanię, w ramach której starano się wykorzystać zestrzelenie samolotu Malaysia Airlines (2014). W tym celu zastosowano polską domenę rządową gov.pl z której rozesłano do szeregu instytucji państwowych wiadomości e-mail zawierające złośliwe oprogramowanie¹⁵²⁶. Natomiast według opublikowanych przez Prevenity danych atak nie był skuteczny. Ofiarami rosyjskich hakerów padł również sektor energetyczny, co należy odnieść do kwestii spornej w stosunkach bilateralnych jaką jest dywersyfikacja źródeł energii. Według raportu Symantec za ataki była odpowiedzialna prorosyjska grupa Dragonfly, natomiast raport iSight stwierdzał, że prokremlowska grupa SandWorm, która wykorzystując lukę w systemie Windows, szpiegowała polską firmę energetyczną. Powyższe działania realizowane przez Kreml należy wiązać z aneksją Półwyspu Krymskiego (2014) oraz wybuchem wojny we wschodniej Ukrainie, jak również zaangażowaniem polskiego rządu w konflikt. Podczas gdy dotychczas raporty poszczególnych instytucji wzmiankowały o incydentach w Polsce stosunkowo rzadko, tak w związku z powyższymi wydarzeniami Polska w cyberprzestrzeni stała się szczególnym przedmiotem zainteresowania Kremla¹⁵²⁷. Podkreślić należy, że choć celów ataków tych grupy było wiele, to najwięcej z nich znajdowało się w Polsce i na Ukrainie¹⁵²⁸. Do innych działań grupy APT-28 w Polsce można zaliczyć „incydenty powiązane z kampanią APT, nazwaną przez firmę Trend Micro „Pawn Storm”. Operatorzy tej kampanii – grupa APT28 – prowadzili

¹⁵²³ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2014...*, s. 18.

¹⁵²⁴ Ibidem, s. 6.

¹⁵²⁵ The Guardian: 'State sponsored' Russian hacker group linked to cyber attacks on neighbours. <https://www.theguardian.com/technology/2014/oct/29/russian-hacker-group-cyber-attacks-apt28> (dostęp: 23.05.2023).

¹⁵²⁶ FireEye: *APT28: A window into Russia's cyber espionage operations?* <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf> (dostęp: 24.02.2023), s. 12-13, 18, 28.

¹⁵²⁷ Rzeczpospolita: *Hakerzy Putina atakują rząd*. <https://www.rp.pl/polityka/art4814691-hakerzy-putina-atakujaz-rzad> (dostęp 25.05.2023); INFOSEC: *APT28: Cybercrime or State-sponsored Hacking?* <https://resources.infosecinstitute.com/topic/apt28-cybercrime-or-state-sponsored-hacking/> (dostęp: 25.05.2023).

¹⁵²⁸ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2014...*, s. 18.

w sierpniu 2014 r. celowane ataki *phishingowe* na polską administrację publiczną, a w lipcu udało im się zamieścić na stronach bip.gov.pl i ośrodka badawczego OBRUM *exploit kity* instalujące robaka Sednit. We wrześniu ofiarą podobnego ataku była strona irgit.pl – Izby Rozliczeniowej Giełd Towarowych. Polskie przedsiębiorstwa zostały zaatakowane w wyniku kampanii Black Energy i Energetic Bear¹⁵²⁹. Wskazano jednak, że pomimo tych incydentów Polska nie znalazła się w „obszarze zainteresowań znaczących operatorów kampanii APT”¹⁵³⁰.

W 2014 roku przeprowadzono również liczne cyberataki, za które wysoce prawdopodobną odpowiedzialność ponosi Federacja Rosyjska. Jednym z ważniejszych przykładów są ataki na sektor finansowy, a najgłośniejszym z nich był ten na Giełdę Papierów Wartościowych w Warszawie dokonany przez wspomnianą wyżej grupę APT-28, znaną również pod nazwami STRONTIUM, Sofacy oraz Fancy Bear¹⁵³¹. Ta sama grupa dokonała również ataków na polskie ministerstwa, w tym MON¹⁵³². Ataki przeprowadzono przede wszystkim w oparciu o utworzone fałszywe domeny, przypominające do złudzenia adresy należące do Ministerstwa Obrony Narodowej¹⁵³³, na przykład poczta.mon.q0v.pl, podczas gdy rzeczywisty adres to poczta.mon.gov.pl¹⁵³⁴. Sprawców ataków ustalono między innymi po przeprowadzeniu analizy z której wynikało, że „6% próbek ich oprogramowania zostało skompilowane między poniedziałkiem a piątkiem a 89% między 8 rano a 6 wieczorem czasu UTC+4, obowiązującego w Moskwie i Sankt Petersburgu”¹⁵³⁵. Raport FireEye wskazuje, że celem działalności grupy APT-28 była w tym okresie nie tylko Warszawa, ale również rząd Węgier, ministerstwa spraw zagranicznych w krajach Europy Wschodniej oraz NATO¹⁵³⁶. W tym samym roku inna grupa powiązana z Rosją dokonała również cyberataków na polski sektor energetyczny¹⁵³⁷. W październiku 2014 roku opublikowano dane o prowadzeniu przez

¹⁵²⁹ Ibidem, s. 10.

¹⁵³⁰ Ibidem, s. 10.

¹⁵³¹ Zaufana Trzecia Strona: *Podobno to Rosjanie stali za zeszłorocznym atakiem na Giełdę Papierów Wartościowych*. <https://zaufanatrzeciastrona.pl/post/podobno-to-rosjanie-stali-za-zeszlorocznym-atakiem-na-gielde-papierow-wartosciowych/> (dostęp: 24.02.2023).

¹⁵³² TREND: *Operation Pawn Storm: The Red in SEDNIT*. https://www.trendmicro.com/en_us/research/14/j/operation-pawn-storm-the-red-in-sednit.html (dostęp: 24.02.2023).

¹⁵³³ Rzeczpospolita: *Hakerzy Putina atakują rząd*. <https://www.rp.pl/polityka/art4814691-hakerzy-putina-atakuja-rzad> (dostęp: 25.05.2023).

¹⁵³⁴ FireEye: *APT28: A window into Russia's cyber espionage operations?* <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf> (dostęp: 24.02.2023), s. 13.

¹⁵³⁵ Zaufana Trzecia Strona: *Ataki rosyjskich cyberszpiegów na polskie instytucje rządowe*. <https://zaufanatrzeciastrona.pl/post/ataki-rosyjskich-cyberszpiegow-na-polskie-instytucje-rzadowe/> (dostęp: 24.02.2023).

¹⁵³⁶ FireEye: *APT28: A window into Russia's cyber espionage operations?* <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf> (dostęp: 24.02.2023).

¹⁵³⁷ Rzeczpospolita: *Cyberatak na polskie firmy energetyczne*. <https://energia.rp.pl/energetyka/art4985261-cyberatak-na-polskie-firmy-energetyczne> (dostęp: 24.02.2023).

grupę APT-28 długoterminowej kampanii szpiegowskiej, której celami były między innymi organizacje w Gruzji, Europie Wschodniej (w tym w Polsce), NATO, OBWE¹⁵³⁸.

[2015] Dane za 2015 rok kształtują inny obraz rosyjskiej działalności wobec Polski w cyberprzestrzeni. Doszło bowiem do wzrostu aktywności wobec sieci monitorowanych przez system ARAKIS, która wyniosła 4,15%, jednakże co bardzo istotne wartość ta dotyczy wyłącznie ataków dokonanych z wykorzystaniem unikalnych adresów IP. W przypadku rozkładu źródeł ataków pod kątem liczby generowanych połączeń, co ciekawe, w 2015 roku Federacja Rosyjska nie została uwzględniona w raporcie (nie znalazła się w pierwszej dziesiątce państw objętych zestawieniem). Należy jednak uwzględnić stosunkowo wysoki odsetek źródeł ataków określonych jako nieznany (2. miejsce – 21,5%), czyli z wykorzystaniem adresów IP, które nie są przypisane do żadnego podmiotu. Oznacza to, iż dokonano podmiany prawdziwego źródłowego adresu IP. Pod takim adresem IP mogły zostać przeprowadzone cyberataki przez Federację Rosyjską, co jest wysoce prawdopodobne biorąc pod uwagę fakt, że Rosja rokrocznie znajdowała się w omawianym zestawieniu dziesięciu państw z których dokonywanych jest najwięcej cyberataków na monitorowane przez system ARAKIS sieci¹⁵³⁹. Uzasadniając dalej to stwierdzenie trzeba zauważyć, że w roku 2014 odsetek źródeł ataków określonych jako *nieznany* wynosił zaledwie 9,95%, a więc ponad dwa razy mniej niż w roku 2015¹⁵⁴⁰. Z kolei w roku 2016 odsetek ten wyniósł w przybliżeniu 13%, a więc o około 1/3 mniej niż w roku 2015¹⁵⁴¹.

Powracając jednak do pierwotnego zestawienia trzeba zauważyć, że wyższe wyniki odnotowano w stosunku do Tajwanu, Turcji, USA oraz Chin. Z kolei w zakresie dokonanych ataków przy uwzględnieniu liczby generowanych przepływów – gdzie jak wskazano nie znalazła się Rosja – najwyższa ich liczba została przeprowadzona z terytorium Chin (45,61%), z nieznanych źródeł (kategoria: nieznany) – 21,5% oraz USA – 15,27%¹⁵⁴². Rosja ponownie znalazła się w gronie państw z największą liczbą serwerów C&C na świecie¹⁵⁴³ oraz w grupie pierwszych dziesięciu krajów, w których hostowano najwięcej złośliwych adresów w domenie .pl¹⁵⁴⁴. Zmniejszyła się natomiast liczba skanowań polskiej infrastruktury teleinformatycznej

¹⁵³⁸ T. Hoffmann: *Wybrane aspekty cyberbezpieczeństwa w Polsce*. Poznań 2018, s. 72.

¹⁵³⁹ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku...*, s. 25.

¹⁵⁴⁰ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 roku...*, s. 11.

¹⁵⁴¹ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2016 roku...*, s. 21.

¹⁵⁴² Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku...*, s. 25.

¹⁵⁴³ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2015...*, s. 38.

¹⁵⁴⁴ Ibidem, s. 49.

pochodząca z Rosji (4,15% – 5. miejsce). Wyżej uplasowały się Tajwan (4,35%), Turcja (6,11%) oraz już tradycyjnie USA (6,38%) i Chiny (37,61%)¹⁵⁴⁵. W raporcie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa wskazano, iż w Federacji Rosyjskiej jest hostowane około 50% złośliwego oprogramowania online, w USA jest to około 12%, w Holandii około 8%, a w Niemczech około 5%¹⁵⁴⁶. Rosja znajduje się również w pierwszej dziesiątce państw z których pochodzą ataki z wykorzystaniem serwerów C&C i choć statystyki te nie są w pełni reprezentatywne to dają obraz o zagęszczeniu sieci *botnetów*¹⁵⁴⁷.

W 2015 roku ujawniono ponownie liczne ataki APT¹⁵⁴⁸ pochodzące najczęściej z Rosji, których celami była Polska. Wartym odnotowania są działania prowadzone przez prorosyjską APT Turla. Według raportu Kaspersky Lab grupa działająca w tamtym okresie od ponad 8 lat dokonała cyberataków na co najmniej 45 krajów, w tym na Polskę¹⁵⁴⁹. W 2015 roku pojawiły się również informacje o rzekomym cyberataku ze strony Federacji Rosyjskiej na Sztab Generalny Wojska Polskiego. Miał on być nakierowany głównie na prywatną pocztę elektroniczną osób pracujących w Ministerstwie Obrony Narodowej oraz w Sztabie Generalnym, a jego skutkiem wyciek około tysiąca wiadomości mailowych¹⁵⁵⁰. Warto w tym kontekście odnotować, iż według byłego szefa ABW K. Bondaryka „od kilku lat z serwerów Ministerstwa Obrony Narodowej, hakerzy związani najprawdopodobniej z Federacją Rosyjską, pozyskiwali adresy e-mailowe pracowników. Sprawa dotyczy kadry i wyższych pracowników cywilnych takich instytucji jak Inspektorat Uzbrojenia czy ścisła obsługa sekretariatu ministra. Atak miał miejsce na jawną część cyberstruktury ministerstwa INTER-MON jak i niejawną MIL-WAN”¹⁵⁵¹. Do interesującego zdarzenia doszło w październiku 2015 roku, w którym na telefony korporacyjne MON zarejestrowane w sieci Plus GSM, wykonano od kilkuset do kilku tysięcy połączeń z numerów telefonów z prefiksem „+7”, a więc przypisanych do Federacji

¹⁵⁴⁵ Ibidem, s. 51.

¹⁵⁴⁶ European Union Agency for Cybersecurity: *ENISA Threat Landscape 2015*. <https://www.enisa.europa.eu/publications/etl2015/@@@download/fullReport> (dostęp: 24.02.2023), s. 20.

¹⁵⁴⁷ Ibidem, s. 27.

¹⁵⁴⁸ APT czyli „Advanced Persistent Threat, to nazwa nadawana zaawansowanym technicznie atakom teleinformatycznym na cele polityczne, ekonomiczne, techniczne i wojskowe. Głównym zadaniem takich ataków jest wykradanie informacji”. Źródło: Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2015...*, s. 24.

¹⁵⁴⁹ Ibidem, s. 24-26.

¹⁵⁵⁰ Wprost: *Rosjanie szpiegowali Sztab Generalny Wojska Polskiego*. <https://www.wprost.pl/496099/rosjanie-szpiegowali-sztab-generalny-wojska-polskiego.html> (dostęp: 25.02.2023); Niebezpiecznik: *Co wiemy o rosyjskich szpiegach w poczcie polskich wojskowych*. <https://zaufanatrzeciastrona.pl/post/co-wiemy-a-czego-nie-o-rosyjskich-szpiegach-w-poczcie-polskich-wojskowych/> (dostęp: 25.02.2023).

¹⁵⁵¹ Defence24: *Wtorek z Defence24.pl: Jak służby monitorują kanały komunikacyjne; Były szef ABW ujawnił cyberatak na MON; Rosyjskie wojny o wpływy; Szczyt NATO w Warszawie coraz bliżej; Rosyjski bombowiec na granicy izraelskiej*. <https://defence24.pl/wtorek-z-defence24pl-jak-sluzby-monitoruja-kanały-komunikacyjne-byly-szef-abw-ujawnil-cyberatak-na-mon-rosyjskie-wojny-o-wplywy-szczyt-nato-w-warszawie-coraz-bliżej-rosyjski-bombowiec-na-granicy-izraelskiej> (dostęp: 25.05.2023).

Rosyjskiej. Ofiarami powyższego działania miało paść nawet 10 tysięcy żołnierzy. Według oświadczenia Ministerstwa Obrony Narodowej nie doszło jednak do jakiegokolwiek wycieku baz danych z numerami telefonów, a wszystkie połączenia zostały wykonane na numery z określonego przedziału liczbowego, jak również do innych osób niezwiązanych z resortem obrony narodowej¹⁵⁵².

[2016] W 2016 roku Rosja ponownie pojawiła się w zestawieniu państw dokonujących największej liczby cyberataków na sieci monitorowane przez system ARAKIS, zajmując 5. miejsce – 4%, będąc jednak wyprzedzona przez Wietnam (4%), Niemcy (9%), USA (15%) oraz Chiny (40%)¹⁵⁵³. Oczywiście należy zauważyć – na co wskazują również sami twórcy raportu – że przytoczone dane, jak i te prezentowane w poprzednich raportach, należy traktować w kategoriach poglądowych. Wynika to z faktu, że infrastruktura teleinformatyczna podmiotów dokonujących ataków może być rozproszona i znajdować się w dowolnym miejscu na świecie. W roku 2016 wzrosła liczba serwerów C&C zlokalizowanych w Rosji, co stanowiło w skali globalnej 8,2%. Wyżej uplasowały się Niemcy (8,3%) oraz USA (30,4%)¹⁵⁵⁴. W odniesieniu do cyberataków dokonywanych z terytorium Federacji Rosyjskiej ciekawe zestawienie zostało przygotowane przez F-Secure. Według autorów raportu pierwsze miejsce w cyberatakach, przeprowadzonych w Polsce w wybranych miesiącach lat 2016-2017 zajmowała Rosja – było to około 65 tysięcy ataków dziennie. Drugie miejsce zajęły Niemcy z wynikiem około 13 tysięcy ataków, a trzecie sama Polska, z terytorium której dokonano niecałych 12 tysięcy ataków¹⁵⁵⁵.

2016 rok to również wybory prezydenckie w Stanach Zjednoczonych oraz przeprowadzona w tym czasie rosyjska ingerencja w amerykański proces wyborczy, czemu poświęcone zostały liczne opracowania¹⁵⁵⁶. Jednocześnie wydarzenia te potwierdziły zdolności jakie posiada Rosja nie tylko do przeprowadzania cyberataków, ale ich kompilacji

¹⁵⁵² Niebezpiecznik: *Masowe telefony z Rosji na numery polskich żołnierzy*. <https://niebezpiecznik.pl/post/kto-masowo-dzwonil-do-polskich-zolnierzy-z-rosyjskiego-numeru/> (dostęp: 25.05.2023).

¹⁵⁵³ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2016 roku...*, s. 21.

¹⁵⁵⁴ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2016...*, s. 64.

¹⁵⁵⁵ M. Frączek: *(Nie)bezpieczna cyberprzestrzeń 2017*. W: *Wsparcie teleinformatyczne i bezpieczeństwo cyberprzestrzeni w SZ RP*. Red. B. Biernacik, L. Kalman, G. Pilarski. Warszawa 2018, s. 225.

¹⁵⁵⁶ Zobacz szerzej: Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1: *Russian Efforts Against Election Infrastructure with Additional Views*. <https://www.hsdl.org/?abstract&did=830205> (dostęp: 24.02.2023); The United States Department of Justice: *Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election*. <https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election> (dostęp: 24.02.2023).

z prowadzonymi równolegle kampaniami z zakresu oddziaływania informacyjnego na odbiorców w Internecie¹⁵⁵⁷.

Z końcem 2016 roku doszło również do próby cyberataku na polskie Ministerstwo Spraw Zagranicznych przy użyciu serwerów należących do resortu dyplomacji jednego z państw znajdujących się w Ameryce Łacińskiej, natomiast prawdopodobnym sprawcą była ponownie rosyjska grupa APT-28¹⁵⁵⁸. W 2016 roku miał również miejsce szczyt NATO w Warszawie, podczas którego cyberprzestrzeń uznano za kolejną domenę operacji, podobnie jak powietrze, ląd czy morze¹⁵⁵⁹. W konsekwencji, jakkolwiek cyberatak dokonany na któregośkolwiek z członków NATO może być uznany za wypełniający przesłanki zastosowania art. 5. (klauzula o wzajemnej pomocy).

[2017] W 2017 roku ARAKIS wykrył cyberataki ze strony Rosji, które stanowiły 7% wszystkich wykrytych oraz dokonanych na sieci monitorowane przez system. Wyżej uplasowały się te dokonane z terytorium Polski (15%) oraz typowo z USA (17%) i Chin (35%)¹⁵⁶⁰. Raport Zespołu CERT Polska umieścił Rosję na czwartej pozycji pod względem liczby serwerów C&C, co stanowiło w skali globalnej 5,9%. Wyżej znalazły się, co ciekawe, Algieria (5,98%) oraz Niemcy (6,18%) i USA (30,92%)¹⁵⁶¹. W szerszym ujęciu przytoczonego raportu należy zauważyć, że odniesienia do Federacji Rosyjskiej pojawiają się niezwykle często w porównaniu do raportów CERT Polska z lat ubiegłych. Odniesienia te dotyczą nie tylko polskiej infrastruktury teleinformatycznej, ale ogólnej aktywności Rosji na świecie¹⁵⁶². Natomiast według raportu F-Secure w drugim i trzecim kwartale 2017 roku około 67% wszystkich cyberataków pochodziło z Rosji, 6% z Niemiec, po 5% z Chin i USA oraz po 4% z Francji i Holandii¹⁵⁶³. Rosyjska działalność, według autorów raportu, sprowadzała się głównie do podejmowania prób uzyskania nieautoryzowanego dostępu do urządzeń oraz

¹⁵⁵⁷ Zobacz szerzej: Niebezpiecznik: *Przełomowy raport CIA, FBI i NSA: to Rosja wpływała na przebieg wyborów prezydenckich w USA*. <https://niebezpiecznik.pl/post/jak-rosjanie-wplywali-na-przebieg-wyborow-prezydenckich-w-usa/> (dostęp: 24.02.2023).

¹⁵⁵⁸ Rzeczpospolita: *Hakerzy Putina z GRU bez sukcesów w Polsce*. <https://www.rp.pl/polityka/art1570411-hakerzy-putina-z-gru-bez-sukcesow-w-polsce> (dostęp: 25.05.2023).

¹⁵⁵⁹ NASK Cyber POLICY: *Sojusz Północnoatlantycki – ewolucja w podejściu do cyberobrony*. <https://cyberpolicy.nask.pl/nato-cyberobrona-zagrozenia-hybrydowe/> (dostęp: 25.05.2023).

¹⁵⁶⁰ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2017 roku*. <https://csirt.gov.pl/download/3/186/RaportostaniebezpieczenstwacyberprzesytrzeniRPw2017roku.pdf> (dostęp: 22.02.2023), s. 21.

¹⁵⁶¹ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2017...*, s. 93.

¹⁵⁶² Zobacz szerzej: Ibidem.

¹⁵⁶³ T. Hoffmann: *Wybrane aspekty cyberbezpieczeństwa...*, s. 77-78; Dziennik.pl: *Hakerzy z Rosji, Niemiec i Chin najczęściej atakują Polskę. Oto miejsca, które są na celowniku cyberwłamywaczy*. <https://technologia.dziennik.pl/internet/artykuly/563147,ktore-kraje-najczesciej-przeprowadzaja-cyberataki-na-polske.html> (dostęp: 23.05.2023).

rozsyłania spamu¹⁵⁶⁴. Mogło mieć to związek z ówczesnymi stosunkami polsko-rosyjskimi, w ramach których dominujące było zwiększanie amerykańskiej obecności wojskowej w Polsce¹⁵⁶⁵.

W szczególności w roli uzupełniającej można zwrócić uwagę na szereg cyberataków dokonanych na Światową Agencję Antydopingową, co miało zapewne związek z równoległymi zarzutami zgłoszonymi przez tą instytucję co do stosowania niedozwolonych środków przez rosyjskich sportowców¹⁵⁶⁶. Natomiast w związku z planami budowy gazociągu Baltic Pipe doszło do ataku na podmioty w Norwegii, Czechach oraz w Polsce, co należy powiązać z kwestią sporną w stosunkach polsko-rosyjskich jaką jest dywersyfikacja źródeł energii. Gazociąg Baltic Pipe odgrywał bowiem w polskiej polityce energetycznej strategiczną rolę jako alternatywa dla dostaw surowców energetycznych z Rosji. Celem polityki zagranicznej Federacji Rosyjskiej w tym zakresie jest niweczenie polskich działań polegających na ograniczaniu popytu na rosyjskie surowce energetyczne w Europie. W 2017 roku projekt wchodził w decydującą fazę w kontekście rozpoczęcia faktycznych prac nad jego wykonaniem, co z kolei stanowiło zagrożenie dla gazowej dominacji Gazpromu w tej części Europy. Autorami ataków byli hakerzy z grup APT-28 i APT-29 powiązani z rosyjskimi służbami specjalnymi¹⁵⁶⁷. Trzeba podkreślić, że autorami cyberataków nie zawsze są instytucje państwowe (służby specjalne i wojsko), ale niezwykle często również organizacje i grupy pośrednio lub bezpośrednio z nimi związane¹⁵⁶⁸.

W 2017 roku przeprowadzono poważny atak na Komisję Nadzoru Finansowego, co było pierwszym dużym incydem nakierowanym na cały sektor gospodarki (finansowy) oraz inspirowanym (dokonanym) przez obce państwo¹⁵⁶⁹. Ciekawym incydem z 2017 roku jest włamanie na stronę internetową Żagania oraz ponad stu innych gmin. Podczas powitania wojsk amerykańskich we wskazanej gminie doszło do cyberataku, w wyniku którego na stronie internetowej zamieszczono informacje sprzeciwiające się obecności wojsk NATO w Polsce,

¹⁵⁶⁴ NOIZZ: *F-Secure, firma specjalizująca się w cyberbezpieczeństwie, opublikowała mapę ataków wymierzonych w polski internet. Najwięcej włamań przeprowadzają Rosjanie*. <https://noizz.pl/nauka-i-technologia/rosjanie-przeprowadzaja-14-tys-cyberatakow-na-polske-dziennie/w847mxq> (dostęp: 23.05.2023).

¹⁵⁶⁵ M. Banasik: *Bezpieczeństwo Europy Środkowo-Wschodniej w aspekcie zagrożeń płynących z Federacji Rosyjskiej*. „Środkoeuropejskie Studia Polityczne” 2020, nr (2), s. 9-10.

¹⁵⁶⁶ Ibidem, s. 40-42.

¹⁵⁶⁷ Energetyka24: *Cyberwojna o Baltic Pipe? Ataki rosyjskich służb na Czechy, Polskę i Norwegię [ANALIZA]*. <https://energetyka24.com/cyberwojna-o-baltic-pipe-ataki-rosyjskich-sluzb-na-czechy-polske-i-norwegie-analiza> (dostęp: 24.02.2023).

¹⁵⁶⁸ Przykładem takich działań może być wojna gruzińsko-rosyjska z 2008 roku podczas której organizacje przestępcze oraz hakywiści, inspirowani bądź współpracujący z rosyjskimi służbami specjalnymi, dokonywali ataków w gruzińskiej cyberprzestrzeni. Analogicznym przykładem jest seria cyberataków przeprowadzonych przez Kreml w Estonii w 2007 roku.

¹⁵⁶⁹ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2017...*, s. 8.

nazywając ich okupantami¹⁵⁷⁰. Z kolei we wrześniu tego samego roku nastąpił atak rosyjskich *botów*, którego celem była przestrzeń informacyjna Polski oraz państw bałtyckich¹⁵⁷¹. Wskazane ataki stanowią kolejny przykład wrogich działań realizowanych przez Kreml w cyberprzestrzeni wobec Polski, które mają związek z kwestiami spornymi występującymi w relacjach bilateralnych, jak również celami polityki zagranicznej Federacji Rosyjskiej. Omówione ataki odnoszą się bowiem do polityki bezpieczeństwa w Europie Środkowo-Wschodniej oraz polityki bezpieczeństwa NATO i mają na celu skompromitowanie Sojuszu jak i Polski oraz podważenie słuszności podejmowanych działań. Nie ulega żadnej wątpliwości, że z punktu widzenia interesów Kremla, zwiększanie obecności NATO na wschodniej flance Sojuszu, stanowi zagrożenie dla rosyjskiej strefy wpływów w regionie oraz bezpieczeństwa państwa.

Nie pozostaje również tajemnicą, że działania realizowane przez rosyjskie służby specjalne w cyberprzestrzeni są wspierane przez podmioty gospodarcze. Przykładem może być Kaspersky Lab i informacje o możliwym wykradaniu danych użytkowników z dysków twardych na których zainstalowano oprogramowanie producenta. Prawdopodobnie komputery z zainstalowanymi produktami przedsiębiorstwa mogły tworzyć sieć *botnet* liczącą nawet 400 milionów komputerów. Skutkiem tego było chociażby zaprzestanie użytkowania przez instytucje amerykańskie programów oferowanych przez Kaspersky Lab¹⁵⁷². W 2017 roku doszło również do poważnego ataku przy użyciu złośliwego oprogramowania nazwanego NotPetya. Jego ofiarami padły przede wszystkim przedsiębiorstwa z branży logistycznej na całym świecie, między innymi w Polsce¹⁵⁷³. Rok później za przeprowadzenie ataku rządu Wielkiej Brytanii oraz USA oficjalnie oskarżyły Federację Rosyjską¹⁵⁷⁴.

[2018] System ARAKIS w 2018 roku wykrył cyberataki dokonane przez Rosję na monitorowane przez niego sieci, które stanowiły rekordowe 13% względem analizowanych uprzednio lat. Ponownie w zestawieniu pojawiła się znaczna liczba przepływów z Polski – 12%. Pierwsze miejsce zajęły Chiny, lecz z nieco skromniejszym wynikiem 22% oraz USA –

¹⁵⁷⁰ M. Frączek: *(Nie)bezpieczna cyberprzestrzeń 2017*. W: *Wsparcie teleinformatyczne i bezpieczeństwo cyberprzestrzeni w SZ RP*. Red. B. Biernacik, L. Kalman, G. Pilarski. Warszawa 2018, s. 221.

¹⁵⁷¹ Ibidem, s. 227.

¹⁵⁷² Niebezpiecznik: *Skandal w Kaspersky. Ten antywirus pomagał rosyjskim służbom wykradać dane z komputerów na całym świecie*. <https://niebezpiecznik.pl/post/skandal-w-kaspersky-ten-antywirus-pomagal-rosyjskim-sluzbom-wykradac-dane-z-komputerow-na-calym-swiecie/> (dostęp: 24.02.2023).

¹⁵⁷³ Niebezpiecznik: *[AKTUALIZACJA #10] Kolejny groźny globalny atak: ransomware Petya (NotPetya). Ofiary także w Polsce. Dotyczy również zaktualizowanych Windowsów!* <https://niebezpiecznik.pl/post/kolejny-grozny-globalny-atak-tym-razem-ransomware-petya-ofiary-sa-takze-w-polsce/> (dostęp: 24.02.2023).

¹⁵⁷⁴ The Guardian: *US joins UK in blaming Russia for NotPetya cyber-attack*. <https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine> (dostęp: 23.02.2023).

19%¹⁵⁷⁵. W tym samym roku przyjęto ustawę o krajowym systemie cyberbezpieczeństwa, wobec czego temu zagadnieniu poświęcono stosunkowo obszerną część dokumentu¹⁵⁷⁶.

Z kolei w raporcie CERT Polska dostrzeżono obecność rosyjskiej dezinformacji w skali globalnej, co miało swoją genezę przede wszystkim w doniesieniach o ingerencji służb specjalnych w procesy wyborcze w USA¹⁵⁷⁷. Liczba serwerów C&C zlokalizowanych na terytorium Federacji Rosyjskiej uplasowała się na poziomie 7,09% zajmując 3. miejsce na świecie, zaraz po Niemczech (7,12%) oraz USA (37,61%)¹⁵⁷⁸. W światowej czołówce grup hakerskich kolejny rok z rzędu znalazły się te pochodzące z Rosji jak APT-28, APT-29, Turla oraz GreyEnergy¹⁵⁷⁹.

Według raportu ESET, grupa APT-28 dokonała cyberataków przy użyciu zaawansowanego technicznie konia trojańskiego o nazwie LoJax, niezwykle trudnego do wykrycia oraz usunięcia. Jego ofiarami padło kilka instytucji rządowych na Bałkanach oraz w krajach Europy Środkowo-Wschodniej, w tym w Polsce. Mechanizm działania trojana polegał na jego ukryciu w UEFI, czyli oprogramowaniu będącym interfejsem pomiędzy oprogramowaniem wbudowanym w podzespoły komputerowe, a samym systemem operacyjnym. Oznacza to, że ponowna instalacja systemu operacyjnego czy wymiana dysku twardego nie usunie oprogramowania, gdyż zainstaluje się ono ponownie przy każdym pierwszym uruchomieniu urządzenia. Usunięcie może zatem nastąpić poprzez reinstalację UEFI, co jest z reguły dość rzadkie, czy też wymianę płyty głównej¹⁵⁸⁰. Na sprawstwo grup APT-28 wskazuje, że „po pierwsze część serwerów C&C była wcześniej używana w atakach tej grupy. Po drugie na komputerach zainfekowanych LoJaxem regularnie znajdowano oprogramowanie takie jak SedUploader, XAgent i Xtunnel, którego wyłącznymi użytkownikami są przedstawiciele APT28”¹⁵⁸¹. Niezwykle poważne ataki zostały przeprowadzone w Niemczech, gdzie ofiarą hakerów stał się Bundestag oraz sieć rządowa¹⁵⁸².

¹⁵⁷⁵ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 roku...*, s. 21-22.

¹⁵⁷⁶ Ibidem, s. 31-36.

¹⁵⁷⁷ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2018...*, s. 89-90.

¹⁵⁷⁸ Ibidem, s. 109.

¹⁵⁷⁹ Ibidem, s. 6.

¹⁵⁸⁰ WeLiveSecurity by ESET: *LoJax: First UEFI rootkit found in the wild, courtesy of the Sednit group*. <https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/> (dostęp: 24.02.2023)

¹⁵⁸¹ Zaufana Trzecia Strona: *Wyrafinowany backdoor UEFI obecny także w polskich sieciach*. <https://zaufanatrzeciastrona.pl/post/wyrafinowany-backdoor-uefi-obecny-takze-w-polskich-sieciach/> (dostęp: 24.02.2023).

¹⁵⁸² The Guardian: *German government intranet under 'ongoing attack'*. <https://www.theguardian.com/world/2018/mar/01/german-government-intranet-under-ongoing-attack> (dostęp: 24.02.2023).

Ponadto warto odnotować, że w raporcie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa stwierdzono, że do 2022 roku USA staną się znaczącym „eksporterem netto ropy naftowej i gazu ziemnego i jeśli ta prognoza się spełni, Stany Zjednoczone będą bezpośrednio konkurować z Rosją na rynku europejskim. Rosyjskie podmioty państwowe mogą sponsorować zakłócające lub szpiegowskie operacje cybernetyczne lub wspierać hakytywistów w imię ochrony środowiska, aby powstrzymać tę nową konkurencję na jednym z największych rynków energetycznych”¹⁵⁸³. Przytoczona kwestia ma szczególne znaczenie wobec prowadzonej przez Polskę polityki zmierzającej do dywersyfikacji źródeł energii oraz zmniejszania importu surowców energetycznych z Federacji Rosyjskiej. Ponadto w raporcie określono Federację Rosyjską mianem jednego z najsukuteczniejszych i najaktywniejszych podmiotów cybernetycznych powiązanych z działaniami szpiegowskimi na świecie¹⁵⁸⁴.

W tym samym roku doszło również do próby włamania o charakterze cyberszpiegowskim do polskiego Ministerstwa Spraw Zagranicznych oraz Ministerstwa Obrony Narodowej. Cyberatak polegał na wysłaniu do wybranych pracowników resortów wiadomości e-mail z załącznikami o następujących nazwach: *Brexit 15.11.2018.docx*, *Note 77 Pakistan.docx* oraz *Rocket Attacks on Israel.docx*. Po ich otwarciu pojawiał się komunikat zachęcający użytkownika do kliknięcia w określonym miejscu, w wyniku czego na urządzeniu było instalowane złośliwe oprogramowanie. Biorąc pod uwagę metody działania, za atak najprawdopodobniej odpowiadała grupa APT-28 lub Fancy Bear¹⁵⁸⁵. Wskazane wyżej nazwy załączników nie nawiązują do kwestii spornych w stosunkach polsko-rosyjskich, lecz do wydarzeń, które miały ówczesnie miejsce na arenie międzynarodowej. Na tej podstawie można wyprowadzić wniosek, że Federacja Rosyjska wykorzystuje tego rodzaju wydarzenia w realizowanych przez siebie działaniach, przy wykorzystaniu narzędzi właściwych dla wojny informacyjnej.

[2019] Rok 2019 pod względem źródeł ataków wykrytych przez system ARAKIS był przełomowy. Wskazać bowiem należy, że liczba ataków na monitorowane sieci pod kątem generowanych przepływów w przypadku Federacji Rosyjskiej wyniosła aż 28% i uplasowała

¹⁵⁸³ European Union Agency for Cybersecurity: *ENISA Threat Landscape Report 2018*. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/@@download/fullReport> (dostęp: 24.02.2023), s. 108.

¹⁵⁸⁴ Ibidem, s. 109.

¹⁵⁸⁵ Rzeczpospolita: *Hakerzy Putina z GRU bez sukcesów w Polsce*. <https://www.rp.pl/polityka/art1570411-hakerzy-putina-z-gru-bez-sukcesow-w-polsce> (dostęp: 25.05.2023); Onet Wiadomości: *Rosyjscy hakerzy odbili się od ściany w polskich ministerstwach*. <https://wiadomosci.onet.pl/kraj/hakerski-atak-gru-apt28-na-polskie-msz-i-mon/yhx4xjn> (dostęp: 24.05.2023).

ją tym samym na pierwszym miejscu w zestawieniu. Wyprzedziła takie kraje jak USA (13%), Niderlandy (12%), Polskę (10%) oraz Chiny (8%)¹⁵⁸⁶. Zauważono, że Rosja na pierwszym miejscu w zestawieniu znalazła się po raz pierwszy w historii, jak również, że „intensyfikacja złośliwego ruchu z cyberprzestrzeni Federacji Rosyjskiej szczególnie znacząco wzrastała w okresach poprzedzających ważne wydarzenia polityczne odbywające się na terytorium Rzeczypospolitej Polskiej”¹⁵⁸⁷.

Zespół CERT Polska oszacował natomiast liczbę serwerów C&C zlokalizowanych w Federacji Rosyjskiej, która wyniosła 4,51% (4 miejsce na świecie). Wyżej znalazły się co ciekawe Brazylia (7,45%) oraz Kanada (13,54%) i wreszcie USA z wynikiem 20,72%, co oznacza spadek względem roku ubiegłego o prawie połowę¹⁵⁸⁸. Ponownie podkreślono znaczącą rolę rosyjskich grup APT, tj. APT-28 oraz APT-29. Wskazano, że celami ich działalności były między innymi państwa członkowskie NATO oraz *think tanki* krytykujące politykę prowadzoną przez Kreml¹⁵⁸⁹. W kontekście Sojuszu Północnoatlantyckiego wartym odnotowania jest fakt, iż od 2016 roku (szczyt w Warszawie) artykuł 5 traktatu może być zastosowany w przypadku przeprowadzenia ataku w cyberprzestrzeni na któregośkolwiek członka Sojuszu¹⁵⁹⁰.

W 2019 roku odbyły się wybory do Parlamentu Europejskiego, co skutkowało wzmożoną aktywnością hakerów w wielu krajach członkowskich. Microsoft poinformował, że „europejskie instytucje demokratyczne, w tym ośrodki analityczne, organizacje pozarządowe i grupy non-profit, zostały zaatakowane przez hakerów”. Według analityków autorami cyberataków miała być wspomniana już wielokrotnie grupa APT-28 powiązana z rosyjskimi służbami specjalnymi¹⁵⁹¹. Atak miał charakter cyberszpiegowski a celem hakerów było ponad 100 kont należących do pracowników różnych podmiotów publicznych zlokalizowanych w Belgii, Francji, Niemczech, Rumunii, Serbii i Polsce. Cyberataki typu *spear phishing*

¹⁵⁸⁶ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 roku...*, s. 24.

¹⁵⁸⁷ Ibidem, s. 46.

¹⁵⁸⁸ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2019...*, s. 116.

¹⁵⁸⁹ Ibidem, s. 99-100.

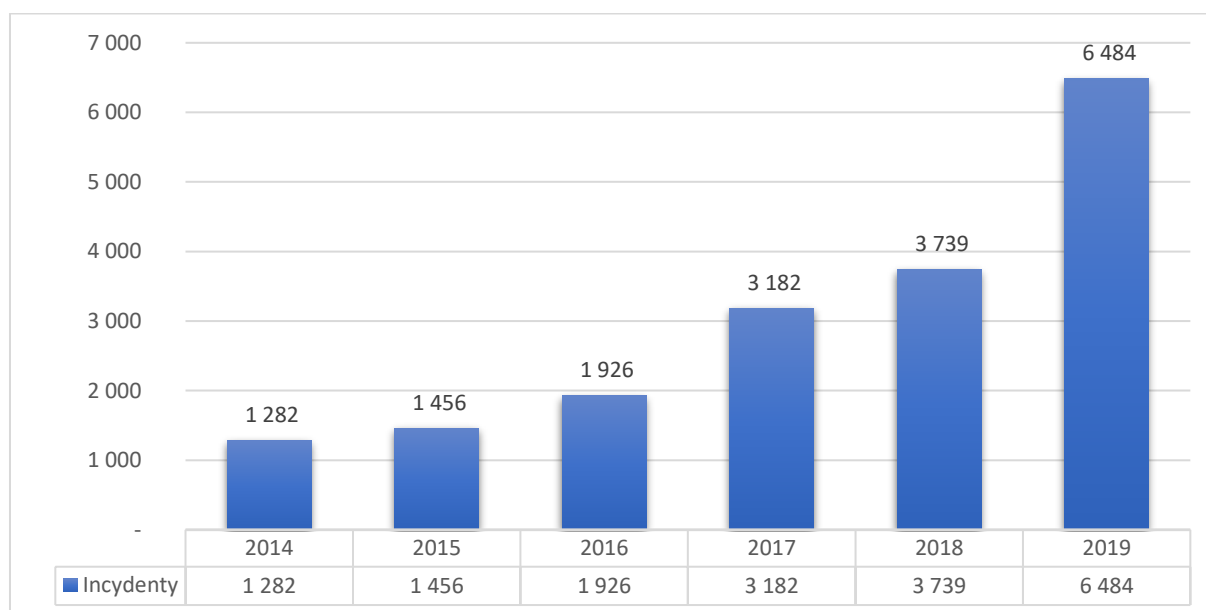
¹⁵⁹⁰ CyberDefence24: *NATO: Artykuł 5 działa również w wypadku cyberataków*. <https://cyberdefence24.pl/polityka-i-prawo/nato-artykul-5-dziala-rowniez-w-wypadku-cyberatakow> (dostęp: 24.02.2023).

¹⁵⁹¹ Microsoft: *New steps to protect Europe from continued cyber threats*. <https://blogs.microsoft.com/eupolicy/2019/02/20/accountguard-expands-to-europe/> (dostęp: 24.02.2023); TVN24: *Microsoft says discovers hacking targeting democratic institutions in Europe*. <https://tvn24.pl/tvn24-news-in-english/democratic-institutions-in-europe-attacked-by-hackers-says-microsoft-ra911507-2297074> (dostęp: 23.02.2023).

zmierzały do pozyskania danych do logowania bądź zainfekowania ofiar złośliwym oprogramowaniem¹⁵⁹².

W tym samym roku w Polsce włamano się również do wielu serwisów internetowych w których zamieszczono informacje o rzekomej ewakuacji Polaków przez żandarmerię i wojska USA. Choć sprawca nie został zidentyfikowany, to okoliczności w jakich doszło do ataku – ćwiczenia Dragon 19 – organizowane wraz z wojskami NATO, zdają się wskazywać na Federację Rosyjską (tym bardziej, że ataki z tego kraju oraz o podobnym mechanizmie działania były już przeprowadzane w przeszłości). Omawiany atak stanowi przykład łączenia przez Federację Rosyjską wrogich działań przeciwko Polsce w cyberprzestrzeni, polegających na dokonywaniu cyberataków (w tym przypadku włamań do serwisów internetowych) z oddziaływaniem informacyjnym na odbiorców w Internecie. We wspomnianym przypadku sprowadzało się ono do dezinformowania oraz kompromitowania Polski w kontekście współpracy wojskowej z USA oraz integracji ze strukturami NATO¹⁵⁹³.

Wykres 11. Liczba incydentów obsługiwanych ręcznie¹⁵⁹⁴ przez Zespół CERT Polska w latach 2014-2019.



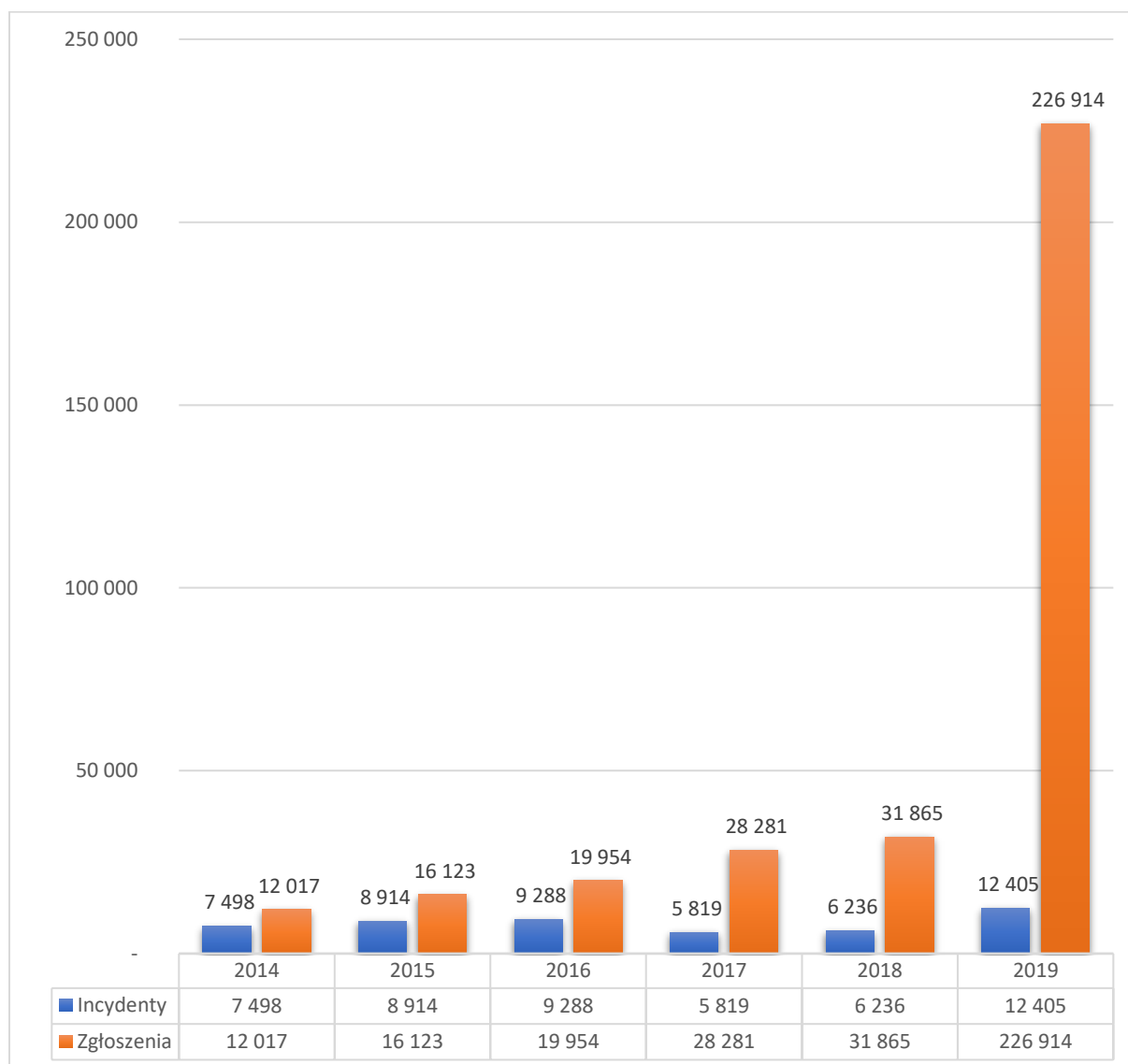
Źródło: Opracowanie własne na podstawie raportów rocznych Zespołu CERT Polska za lata 2014-2019.

¹⁵⁹² ZDNET: *Microsoft reveals new APT28 cyber-attacks against European political entities*. <https://www.zdnet.com/article/microsoft-reveals-new-apt28-cyber-attacks-against-european-political-entities/> (dostęp: 25.05.2023).

¹⁵⁹³ Niebezpiecznik: *Niezależna.pl i wiele innych serwisów w Polsce zhackowanych. Rozsiewały plotki o ewakuacji Polaków przez żandarmerię i wojska USA*. <https://niebezpiecznik.pl/post/niezalezna-pl-i-inne-serwisy-w-polsce-zhackowane-rozsiewaly-plotki-o-ewakuacji-polakow-przez-zandarmerie-i-wojska-usa/> (dostęp: 24.02.2023).

¹⁵⁹⁴ Incydenty obsługiwane ręcznie to incydenty, które zostały zarejestrowane oraz wymagają bezpośredniego działania przez członka Zespołu.

Wykres 12. Liczba zgłoszonych oraz faktycznych incydentów odnotowanych przez Zespół CSIRT GOV w latach 2014-2019.

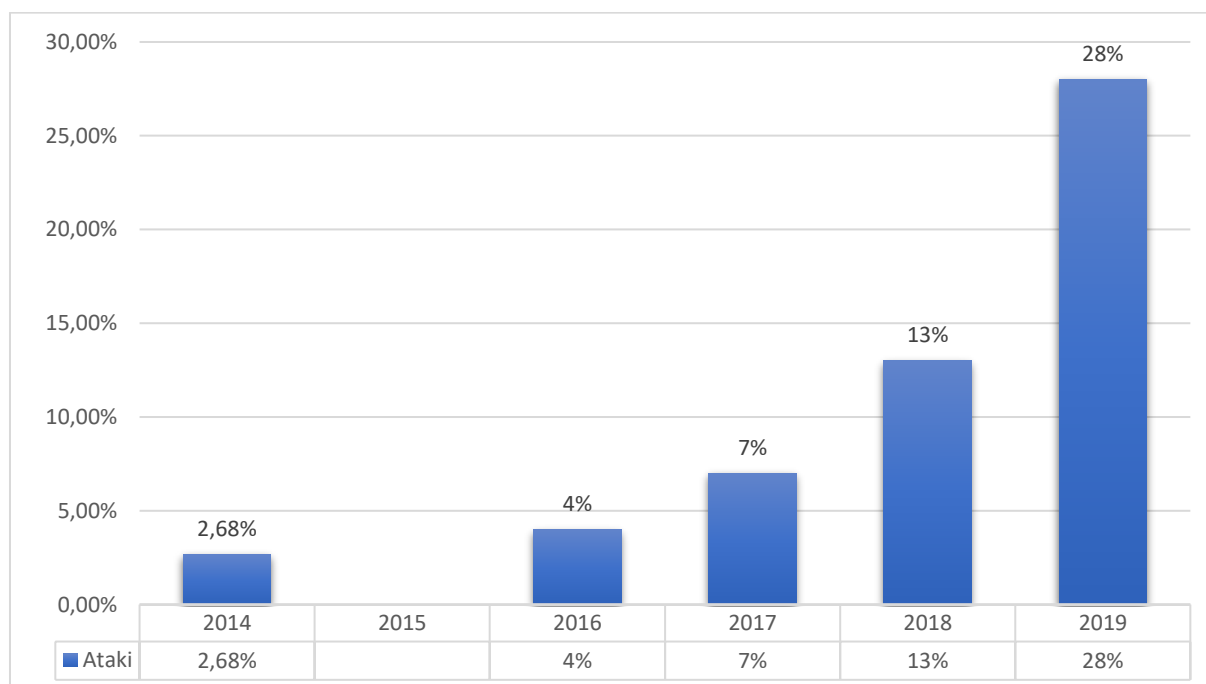


Źródło: Opracowanie własne na podstawie raportów rocznych Zespołu CSIRT GOV za lata 2014-2019.

W przypadku zaprezentowanego wyżej wykresu w 2019 roku, można zauważyć ponad siedmiokrotny wzrost zgłaszanych incydentów względem roku ubiegłego, z kolei liczba rzeczywistych incydentów wzrosła dwukrotnie. Taki stan rzeczy najprawdopodobniej wynika z wejścia w życie w połowie 2018 roku ustawy o krajowym systemie cyberbezpieczeństwa, która nakłada na określone podmioty obowiązek zgłaszania incydentów do zespołu CSIRT GOV¹⁵⁹⁵.

¹⁵⁹⁵ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560), Rozdział 3, 4, 5, 6.

Wykres 13. Rozkład procentowy ataków z Federacji Rosyjskiej na monitorowane przez system ARAKIS sieci w latach 2014-2019 pod kątem liczby generowanych przepływów.



Źródło: Opracowanie własne na podstawie raportów rocznych Zespołu CSIRT GOV za lata 2014-2019¹⁵⁹⁶.

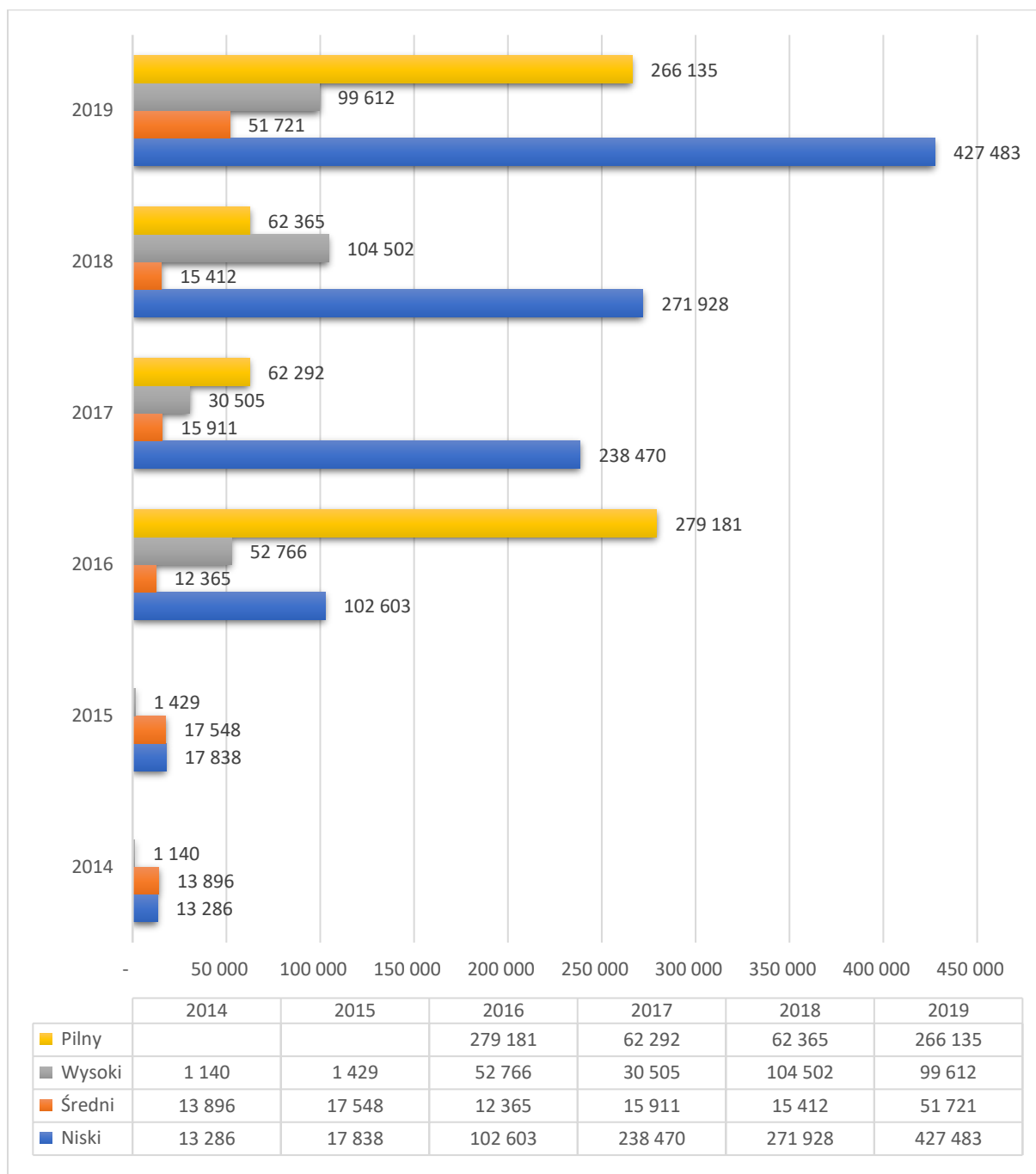
Na powyższym wykresie można zauważyć, że w 2015 roku nie odnotowano w pierwszej dziesiątce państw, cyberataków przeprowadzonych z terytorium Federacji Rosyjskiej pod względem liczby generowanych przepływów. Biorąc jednak pod uwagę nienaturalny, ponad dwukrotny, wzrost cyberataków dokonanych z adresów IP, których nie można było przypisać do żadnego państwa, wysoce prawdopodobnym jest, iż ataki zostały dokonane przez Rosję właśnie w ten sposób. Tym bardziej wobec faktu, że analizując procentowy rozkład źródeł ataków na sieci monitorowane przez system ARAKIS pod kątem unikalnych adresów IP Federacja Rosyjska uplasowała się na 5 miejscu, z wynikiem 4,15%¹⁵⁹⁷. Zasygnalizować należy, że szczegółowe rozważania w tym zakresie przeprowadzono we wcześniejszej części niniejszego podrozdziału. Jednocześnie wartym odnotowania jest fakt, iż

¹⁵⁹⁶ W 2015 roku Federacja Rosyjska nie została uwzględniona w raporcie CSIRT GOV (nie znalazła się w pierwszej dziesiątce państw objętych zestawieniem). Należy jednak uwzględnić stosunkowo wysoki odsetek źródeł ataków określonych jako nieznan (2 miejsce – 21,5%), czyli z wykorzystaniem adresów IP, które nie są przypisane do żadnego podmiotu. Oznacza to, iż dokonano podmiany prawdziwego źródłowego adresu IP. Pod takim adresem IP mogły zostać przeprowadzone cyberataki przez Federację Rosyjską, co jest wysoce prawdopodobne biorąc pod uwagę fakt, że Rosja rokrocznie znajdowała się w omawianym zestawieniu dziesięciu państw z których dokonywanych jest najczęściej cyberataków na monitorowane przez system ARAKIS sieci.

¹⁵⁹⁷ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku...*, s. 25.

Rosjanie, aby zachować anonimowość w sieci, atakują połączenia satelitarne. Skutkiem tego jest uniemożliwienie zlokalizowania atakującego. Na takie działania wskazywano chociażby w 2015 roku¹⁵⁹⁸.

Wykres 14. Liczba zarejestrowanych alarmów (z podziałem na priorytety) przez system ARAKIS w latach 2014-2019.

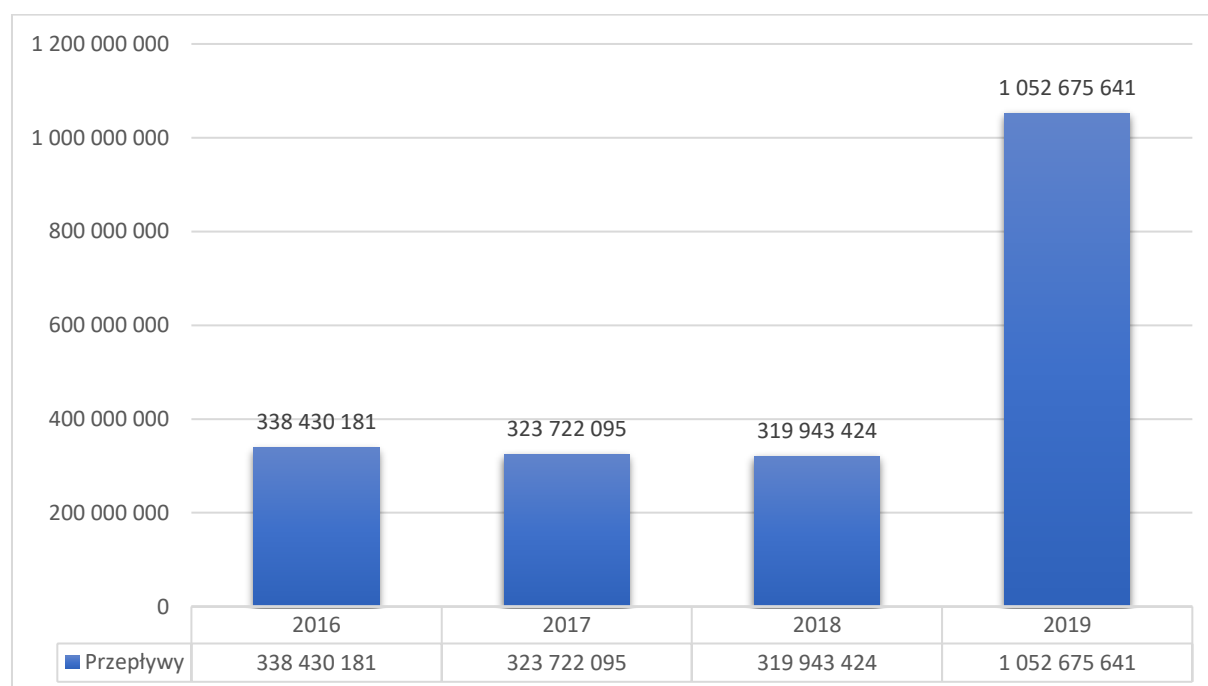


Źródło: Opracowanie własne na podstawie raportów rocznych Zespołu CSIRT GOV za lata 2014-2019.

¹⁵⁹⁸ Niebezpiecznik: *Rosjanie atakują połączenia satelitarne, aby zachować anonimowość w sieci*. <https://niebezpiecznik.pl/post/rosjanie-atakują-satelity-aby-zachowac-anonimowosc-w-sieci/> (dostęp: 24.02.2023).

Na powyższym wykresie w odniesieniu do 2014 oraz 2015 roku nie uwzględniono danych dotyczących liczby wygenerowanych alarmów o priorytecie *pilny*. Wynika to z faktu, iż dopiero od 2016 roku – w związku z wprowadzonymi zmianami w funkcjonowaniu systemu ARAKIS (ARAKIS 2.0¹⁵⁹⁹) – podział priorytetów alarmów oznaczany jest jako: niski, średni, wysoki oraz pilny. Z kolei w 2016 roku zauważalny jest niewspółmierny względem pozostałych lat wysoki odsetek alarmów o priorytecie pilny, jednakże raport roczny Zespołu CSIRT GOV nie zawiera informacji o przyczynach takiej kategoryzacji, co może uzasadniać przypuszczenie autora, iż powodem są kwestie metodologiczne¹⁶⁰⁰.

Wykres 15. Rozkład przepływów w sieciach teleinformatycznych uczestniczących w projekcie ARAKIS w latach 2016-2019.



Źródło: Opracowanie własne na podstawie raportów rocznych Zespołu CSIRT GOV za lata 2016-2019.

Na powyższym wykresie zaprezentowano rozkład przepływów w sieciach teleinformatycznych uczestniczących w projekcie ARAKIS w latach 2016-2019. Przyjęcie takiej cezurę czasowej wynika z faktu, iż z końcem 2015 wprowadzono nową wersję systemu – ARAKIS 2.0, co wiązało się nie tylko ze wzrostem liczby podmiotów nim objętych

¹⁵⁹⁹ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2016 roku...*, s. 19.

¹⁶⁰⁰ Ibidem, s. 19-20.

(a w konsekwencji większą liczbą rejestrowanych incydentów), ale również rozpoczęciem raportowania łącznej liczby przepływów, które przekładają się na generowanie poszczególnych rodzajów alarmów¹⁶⁰¹.

Reasumując omawiany okres należy w pierwszej kolejności zwrócić uwagę na niezwykle dużą dynamikę zmian w zakresie podmiotów przeprowadzających cyberataki na sieci monitorowane przez system ARAKIS, a więc sieci mające kluczowe znaczenie dla prawidłowego funkcjonowania państwa. Należy również pamiętać, że infrastruktura teleinformatyczna podmiotów przeprowadzających cyberataki może być rozproszona po całym świecie i w ten sposób zaburzać rozkład źródeł ataków. Mimo to bezsprzecznym wnioskiem jest, że udział Federacji Rosyjskiej w zakresie ataków na sieci monitorowane przez system ARAKIS pod kątem liczby generowanych przepływów znacząco wzrósł. Istotnym pozostaje również przyjęcie ustawy o krajowym systemie cyberbezpieczeństwa¹⁶⁰², co spowodowało wzrost rejestrowanych incydentów przez Zespoły CERT Polska i CSIRT GOV wynikający z większej liczby zgłoszeń. Rosja nadal pozostawała istotnym podmiotem realizującym działania wobec Polski w cyberprzestrzeni, a jej aktywność systematycznie wzrastała, w szczególności w obszarze infrastruktury krytycznej.

W działaniach Kremla aktywne pozostawały grupy hakerskie powiązane ze służbami specjalnymi, a najważniejszą z nich była APT-28. Zauważalna pozostaje korelacja dokonywanych cyberataków z kwestiami spornymi występującymi w stosunkach dwustronnych, jak również korelacja z oddziaływaniem informacyjnym na odbiorców w Internecie (propaganda/dezinformacja). Szczególnie widoczne było to w 2014 i 2015 roku, a więc w okresie po dokonanej przez Federację Rosyjską aneksji Półwyspu Krymskiego oraz rozpoczęciu wojny we wschodniej Ukrainie¹⁶⁰³. Wsparcie jakiego udzieliła Warszawa rządowi w Kijowie spowodowało wzrost rosyjskiej aktywności wobec Polski w cyberprzestrzeni. Chodzi tutaj przede wszystkim o zaangażowanie grup APT, głównie APT-28, a więc podmiotów powiązanych z Kremlm. Ich działalność uległa zauważalnemu zwiększeniu względem lat ubiegłych – szczególnie okresu 2010-2013. Celami ataków były przede wszystkim obiekty, które można określić mianem infrastruktury krytycznej. Atakowano całe sektory gospodarki (głównie finanse oraz energetykę), jak również administrację rządową (między innymi Ministerstwo Obrony Narodowej). Szczyt NATO w Warszawie z 2016

¹⁶⁰¹ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku...*, s. 33.

¹⁶⁰² Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560).

¹⁶⁰³ M. Banasik: *Bezpieczeństwo Europy Środkowo-Wschodniej...*, s. 5.

roku¹⁶⁰⁴, podczas którego uznano cyberprzestrzeń za obszar operacji militarnych, jak również dalsze ustalenia dotyczące zwiększania obecności wojskowej NATO w Polsce, kolorowały ze wzrostem zainteresowania oraz wrogim oddziaływaniem Kremla na Polskę w cyberprzestrzeni. Zauważalne były w szczególności cyberataki o charakterze cyberszpiegowskim ale również takie, które korelowały z równoczesnym prowadzeniem kampanii z zakresu oddziaływania informacyjnego na odbiorców w Internecie. Takie działania wpisują się w przyjętą w rozprawie hipotezę badawczą, która zakłada między innymi komplementarność dokonywanych przez Rosję ataków na Polskę w cyberprzestrzeni z działalnością o charakterze propagandowym.

6.2.3. Charakterystyka, przebieg i implikacje rosyjskich ataków teleinformatycznych wobec Polski w cyberprzestrzeni w latach 2020-2022

[2020] Według raportu CSIRT GOV za 2020 rok krajem najbardziej aktywnym pod względem generowanych przepływów zarejestrowanych w sieciach monitorowanych przez system ARAKIS była ponownie Rosja, która odpowiadała za 22% z nich. Świadczy to o utrzymaniu ogromnego zainteresowania polską infrastrukturą teleinformatyczną przez ten kraj. Na drugim miejscu znalazły się USA (16%), Polska (12%) oraz Chiny (4%). Drugą niezwykle ciekawą kwestią na którą należy zwrócić uwagę jest po raz kolejny (na przestrzeni ostatnich kilku lat) obecność Polski w zaprezentowanym zestawieniu¹⁶⁰⁵. CERT Polska raportuje natomiast o względnym utrzymaniu przez Rosję liczby serwerów C&C, których liczba stanowi około 5,11% w skali globalnej. Więcej serwerów omawianego typu jest zlokalizowanych w Holandii (5,57%), Niemczech (6,36%) oraz USA z wynikiem 47,45%, co oznacza ponad dwukrotny wzrost względem roku ubiegłego i względny powrót do stanu sprzed dwóch lat¹⁶⁰⁶. Według Agencji Unii Europejskiej ds. Cyberbezpieczeństwa ze strony Rosji zaobserwowano znaczący ruch *botnetów*, podobnie jak miało to miejsce w 2019 roku. Natomiast ogólny ruch *botnetów* wzrósł od 2018 roku o ponad 70%¹⁶⁰⁷.

Rok 2020 najprawdopodobniej będzie już zawsze kojarzył się pandemią COVID-19 wykorzystywanej przez Rosjan do szerzenia dezinformacji, której towarzyszyły liczne

¹⁶⁰⁴ Ibidem, s. 9-10.

¹⁶⁰⁵ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2020 roku...*, s. 41-42.

¹⁶⁰⁶ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2020...*, s. 152.

¹⁶⁰⁷ European Union Agency for Cybersecurity: *From January 2019 to April 2020. Malware ENISA Threat Landscape*. <https://www.enisa.europa.eu/publications/malware/@@download/fullReport> (dostęp: 25.02.2023).

cyberataki¹⁶⁰⁸. W przypadku Polski, w kwietniu 2020 roku na stronie internetowej Akademii Sztuki Wojennej ukazał się fałszywy list Rektora (Komendanta) uczelni, w którym w sposób skrajny odniesiono się negatywnie do polsko-amerykańskiego sojuszu wojskowego. Według przypuszczeń, sprawcami tego ataku były podmioty powiązane z rosyjskimi służbami, na co wskazywać może również nawiązanie do polityki bezpieczeństwa NATO i USA w Europie Środkowo-Wschodniej¹⁶⁰⁹. Wraz z rozprzestrzenianiem się wirusa SARS-CoV-2 oraz rozpoczęciem prac nad szczepionką przeciwko niemu nastąpiły działania ze strony Rosji mające na celu pozyskanie informacji na temat ich przebiegu oraz rezultatów. Na takie przypadki wskazywała chociażby Wielka Brytania, obwiniając o dokonywanie cyberataków powiązaną z rosyjskimi służbami specjalnymi grupę APT-29¹⁶¹⁰. Podobne doniesienia napływały z USA i Kanady, przy czym wskazywano, że celem hakerów było nie tylko zdobycie informacji o pracach nad szczepionką, ale również o przebiegu pandemii w poszczególnych krajach. Mając na względzie długą oraz bogatą historię rosyjskich grup hakerskich można z dużą dozą prawdopodobieństwa, graniczącą wręcz z pewnością domniemywać, że cyberataki miały miejsce również w Polsce¹⁶¹¹. W 2020 roku miało miejsce włamanie do Europejskiej Agencji Leków, w wyniku którego starano się pozyskać informacje na temat szczepionki przeciwko SARS-CoV-2, o co oskarżono między innymi hakerów z Rosji¹⁶¹². Można więc wyprowadzić wniosek, że w omawianym kontekście pandemia została wykorzystana przez Federację Rosyjską jako czynnik destabilizujący wewnętrznie państwa członkowskie NATO, poprzez podsycanie napięć wewnętrznych o charakterze społeczno-politycznym.

Do innych przykładów można zaliczyć cyberataki dokonane przez APT Gamaredon na polskie placówki dyplomatyczne oraz inne instytucje działające na terytorium Ukrainy, co

¹⁶⁰⁸ Zobacz szerzej: Rand: *Reining in COVID-19 Disinformation from China, Russia, and Elsewhere*. <https://www.rand.org/blog/2021/11/reining-in-covid-19-disinformation-from-china-russia.html> (dostęp: 16.03.2023); Reuters: *COVID-19 disinformation backfires as Russian deaths climb, EU says*. <https://www.reuters.com/world/europe/covid-19-disinformation-backfires-russian-deaths-climb-eu-says-2021-10-21/> (dostęp: 17.03.2023); gov.pl: *Polska na celowniku dezinformacji*. <https://www.gov.pl/web/sluzby-specjalne/polska-na-celowniku-dezinformacji> (dostęp: 17.03.2023); A. Legucka, M. Przychodniak: *Dezinformacja Chin i Rosji w trakcie pandemii COVID-19*. „Biuletyn Polskiego Instytutu Spraw Międzynarodowych” 2020, nr 86 (2018) <https://pism.pl/upload/images/artykuly/acecc09f-a097-43cf-b933-9a0e562345a3/1587464655532.pdf> (dostęp: 18.03.2023); gov.pl: *Disinformation against Poland in 2020 – special services’ view*. <https://www.gov.pl/web/sluzby-specjalne/disinformation-against-poland-in-2020--special-services-view> (dostęp: 20.03.2023).

¹⁶⁰⁹ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2020...*, s. 119-120.

¹⁶¹⁰ National Cyber Security Centre: *Advisory: APT29 targets COVID-19 vaccine development*. <https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf> (dostęp: 24.02.2023), s. 3-5.

¹⁶¹¹ Niebezpiecznik: *Informacje o szczepionce na COVID-19 celem hakerów z Rosji – uważają służby USA, UK*. <https://niebezpiecznik.pl/post/informacje-o-szczepionce-na-covid-19-celem-hackerow-z-rosji-uwazaja-sluzby-usa-uk/> (dostęp: 25.02.2023).

¹⁶¹² CyberDefence24: *Włamanie do Europejskiej Agencji Leków mniej poważne niż zakładano*. <https://cyberdefence24.pl/polityka-i-prawo/wlamanie-do-europejskiej-agencji-lekow-mniej-powazne-niz-zakladano> (dostęp: 25.02.2023).

wpisuje się w kwestie sporne w stosunkach polsko-rosyjskich. Ataki przeprowadzono poprzez rozesłanie do wybranych hostów wyspecjalizowanego złośliwego oprogramowania¹⁶¹³. Grupa jest podejrzewana o bliskie powiązania z rosyjskimi służbami specjalnymi¹⁶¹⁴. Inny podmiot również powiązany z Rosją – APT Turla – dokonał zaawansowanego ataku na polskie instytucje rządowe przy wykorzystaniu autorskiego oprogramowania oraz *exploitów*. Jak wskazano, celem tych działań było zdobycie informacji powszechnie niedostępnych¹⁶¹⁵. Warto zaznaczyć, że przeprowadzone przez Rosję bądź podmioty z nią powiązane (na przykład grupy APT) cyberataki, korelowały z działaniami z zakresu oddziaływania informacyjnego na odbiorców w Internecie. Nastąpiło zintensyfikowanie działań propagandowych i dezinformacyjnych, do których głównych celów należy zaliczyć „oczernianie Warszawy na arenie międzynarodowej; osłabianie relacji Polski z krajami sąsiednimi i partnerami; destabilizacja współpracy wojskowej Polski w ramach NATO; wzniecanie działań wojennych między Polską a USA; atak na polską politykę energetyczną; ośmieszanie i poniżanie Sił Zbrojnych RP; piętnowanie Polski jako przesiąkniętej nastrojami antyrosyjskimi; obwinianie Polski za pogorszenie stosunków między Rosją a Zachodem”¹⁶¹⁶. Trzeba zauważyć, że wskazane cele wiążą się z kwestiami spornymi występującymi w stosunkach bilateralnych na linii Warszawa-Moskwa, a w szczególności z tymi dotyczącymi polityki bezpieczeństwa w Europie Środkowo-Wschodniej oraz polityki bezpieczeństwa NATO.

Wartym odnotowania jest również fakt, że w 2020 roku Unia Europejska po raz pierwszy w historii nałożyła sankcje na osoby oraz podmioty odpowiedzialne za dokonanie cyberataków lub w nie zaangażowane. Są one wynikiem niedoszłego do skutku cyberataku na Organizację ds. Zakazu Broni Chemicznej oraz ataków znanymi pod nazwami WannaCry, Operation Cloud Hopper oraz wspomnianego już NotPetya¹⁶¹⁷. Podstawą sankcji były również działania podjęte w Polsce – ataki dokonane na Komisję Nadzoru Finansowego. Nałożone sankcje objęły obywateli Korei Północnej, Chin oraz Rosji, przy czym dotyczyły cyberataków dokonanych przed kilkoma laty, wobec czego należy poddać pod rozwałę opóźnienie z jakim

¹⁶¹³ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2020 roku...*, s. 17.

¹⁶¹⁴ Security Week: *Russian APT Gamaredon Changes Tactics in Attacks Targeting Ukraine*. <https://www.securityweek.com/russian-apt-gamaredon-changes-tactics-attacks-targeting-ukraine/> (dostęp: 25.02.2023).

¹⁶¹⁵ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2020 roku...*, s. 18.

¹⁶¹⁶ gov.pl: *Disinformation against Poland in 2020 – special services’ view*. <https://www.gov.pl/web/sluzby-specjalne/disinformation-against-poland-in-2020--special-services-view> (dostęp: 25.05.2023).

¹⁶¹⁷ Rada Europejska, Rada Unii Europejskiej: *Cyberataki: UE nakłada pierwsze w historii sankcje*. <https://www.consilium.europa.eu/pl/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/> (dostęp: 25.02.2023).

zostały wdrożone¹⁶¹⁸. Po kilku miesiącach Unia Europejska nałożyła kolejne sankcje, tym razem za rosyjskie cyberataki na niemiecki parlament do których doszło w 2015 roku¹⁶¹⁹. Innym ciekawym wydarzeniem z 2020 roku jest przedstawienie oficerom GRU aktów oskarżenia przez amerykańską prokuraturę. Objęły one szereg ataków dokonanych przez rosyjską służbę specjalną w wielu państwach na świecie, między innymi takich których skutki były odczuwalne w Polsce¹⁶²⁰.

[2021] W 2021 roku w ramach funkcjonowania systemu ARAKIS odnotowano wzrost ataków dokonanych ze strony Federacji Rosyjskiej – 25% (1. miejsce). Na drugim miejscu znalazły się USA (15%), Chiny (7%) oraz Wielka Brytania (7%). W zestawieniu nie ma natomiast Polski, która występowała w nim w latach ubiegłych¹⁶²¹. Odnotowano również (podobnie jak rok wcześniej) szereg ataków socjotechnicznych, jednakże raport nie wiąże ich bezpośrednio z działalnością Federacji Rosyjskiej¹⁶²². Jednym ze szczególnie aktywnych podmiotów w cyberprzestrzeni była natomiast grupa APT-29, powiązana ze służbami specjalnymi Kremla¹⁶²³. W zakresie serwerów C&C Rosja ponownie znalazła się w światowej czołówce. Prawie 5% serwerów znajdowało się właśnie w tym kraju, a więcej tylko w Niemczech (6,01%), Holandii (7,38%) oraz USA (32,83%)¹⁶²⁴. Ponadto, jak szacuje KPMG w Polsce wzrosła skala cyberataków na przedsiębiorstwa. W 2021 roku 69% podmiotów zanotowało co najmniej jeden cyberincydent¹⁶²⁵. Podobne wnioski co do aktywności Federacji Rosyjskiej w globalnej cyberprzestrzeni (w tym również odniesienia do Polski) zostały zawarte w raporcie Microsoft Digital Defense Report October 2021¹⁶²⁶.

Znamiennym jest również raport Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) z 2021 roku, który niezwykle wiele uwagi poświęca właśnie działalności prowadzonej z terenów bądź przez Federację Rosyjską. Podczas gdy raporty z ubiegłych lat wzmiankowały

¹⁶¹⁸ Niebezpiecznik: *UE odpowiedziała sankcjami na WannaCry oraz... atak na polską KNF*. <https://niebezpiecznik.pl/post/ue-odpowiedziala-sankcjami-na-wannacry-oraz-atak-na-polska-knf/> (dostęp: 25.02.2023).

¹⁶¹⁹ Niebezpiecznik: *UE nakłada sankcje za cyberataki m.in. na rosyjskiego admirała*. <https://niebezpiecznik.pl/post/ue-naklada-sankcje-za-cyberataki-m-in-na-rosyjskiego-admiraala/> (dostęp: 25.02.2023); Zobacz szerzej: Congressional Research Service: *Cybersecurity: Selected Cyberattacks, 2012-2021*. <https://crsreports.congress.gov/product/pdf/R/R46974> (dostęp: 24.02.2023), s. 6-20.

¹⁶²⁰ CyberDefence24: *Oficerowie GRU z aktem oskarżenia. Świat poznał sprawców „największych cyberataków w historii”*. <https://cyberdefence24.pl/polityka-i-prawo/oficerowie-gru-z-aktem-oskarzenia-swiat-poznal-sprawcow-najwiekszych-cyberatakow-w-historii> (dostęp: 25.02.2023).

¹⁶²¹ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku...*, s. 40-41.

¹⁶²² Ibidem, s. 22 i nast.

¹⁶²³ Ibidem, s. 29.

¹⁶²⁴ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2021...*, s. 89.

¹⁶²⁵ KPMG: *Barometr cyberbezpieczeństwa*. <https://kpmg.com/pl/pl/home/insights/2022/05/barometr-cyberbezpieczenstwa-ochrona-cyfrowej-tozsamosci.html> (dostęp: 26.02.2023).

¹⁶²⁶ Zobacz szerzej: Microsoft: *Microsoft Digital Defense Report OCTOBER 2021*. <https://info.microsoft.com/ww-landing-Microsoft-Digital-Defense-Report-Gate.html> (dostęp: 25.02.2023).

kilkanaście razy o działalności Kremla, tak już raporcie z 2021 roku można mówić o dziesiątkach razy. Autorzy wskazują na przeprowadzoną kampanię Ghostwriter, która była nakierowana na Litwę, Łotwę i Polskę oraz sprowadzała się do krytycznych narracji wobec obecności NATO w Europie Wschodniej. Szczególnie ważne pozostaje to, że wrogie działania miały być podejmowane już od 2017 roku, a w ich ramach hakerzy włamywali się na strony internetowe oraz konta e-mail, a następnie wykorzystywali je do publikowania sfabrykowanych dokumentów. Ponadto podszywali się pod krajowych urzędników, aby rozpowszechniać sfabrykowane treści. Jak zaznaczają autorzy raportu, analitycy ENISA powiązali te działania z rosyjskimi interesami bezpieczeństwa¹⁶²⁷. Co również ważne w odniesieniu do ataków typu DDoS, Polska w 2021 roku weszła do pierwszej dziesiątki zestawienia państw będących najczęstszymi celami¹⁶²⁸.

W pierwszej połowie 2021 roku nasiliły się ataki hakerskie wobec Polski w cyberprzestrzeni. Według szacunków Check Point Software Polska, podstawową metodą dystrybucji wirusów były wiadomości e-mail, ale również strony internetowe. Szczególnie wrażliwy był natomiast sektor instytucji naukowych, jak uczelnie i placówki badawcze, ale również sektor finansowy oraz administracja publiczna¹⁶²⁹. W 2021 roku doszło do włamania na stronę internetową Państwowej Agencji Atomistyki w wyniku czego atakujący zamieścili na niej informację o rzekomym wystąpieniu zagrożenia radiologicznego. Informacje zostały zdementowane, natomiast biorąc pod uwagę fakt, że w tym samym roku pojawiły się plany budowy tzw. reaktorów modułowych w Polsce, celem zastąpienia dotychczas wykorzystywanych elektrowni węglowych, korzystających z surowca z Rosji, można domniemywać kto stał za tym atakiem¹⁶³⁰. Podobną próbę włamania podjęto zresztą w 2020 roku, co miało związek z pojawieniem się fałszywych informacji o radioaktywnej chmurze zmierzającej do Polski z Czarnobyla na Ukrainie¹⁶³¹.

W 2021 roku doszło do kilku głośnych ataków na Polskę, przeprowadzonych z terytorium Federacji Rosyjskiej. Ich celem, w kontekście napięć w relacjach bilateralnych oraz polityki zagranicznej Kremla, była destabilizacja wewnętrzna państwa oraz podsycanie

¹⁶²⁷ European Union Agency for Cybersecurity: *ENISA Threat Landscape 2021*. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021/@/download/fullReport> (dostęp: 23.02.2023), s. 109.

¹⁶²⁸ Ibidem, s. 71.

¹⁶²⁹ Rzeczpospolita: *Nasilają się ataki hakerskie na Polskę*. <https://www.rp.pl/biznes/art18454601-nasilaja-sie-ataki-hakerskie-na-polske> (dostęp: 25.02.2023).

¹⁶³⁰ CyberDefence24: *Dezinformacja w polski atom*. <https://cyberdefence24.pl/polityka-i-prawo/dezinformacja-w-polski-atom> (dostęp: 25.02.2023).

¹⁶³¹ Konkret24: *Fałszywe wiadomości o "radioaktywnej chmurze nad Czarnobyla". PAA: "Nie ma żadnego zagrożenia"*. <https://konkret24.tvn24.pl/polska/falszywe-wiadomosci-o-radioaktywnej-chmurze-znad-czarnobyla-paa-nie-ma-zadnego-zagrozenia-ra1013183> (dostęp: 25.02.2023).

sporów społeczno-politycznych. Jednym z najgłośniejszych – również ze względów politycznych – był cyberatak, którego celem stała się grupa polskich polityków, między innymi członków rządu. Początkowo Agencja Bezpieczeństwa Wewnętrznego oraz Służba Kontrwywiadu Wojskowego ustaliły, że za omawianymi działaniami stali hakerzy z Rosji. W wyniku ataku doszło do włamania na skrzynkę e-mail szefa Kancelarii Prezesa Rady Ministrów (KPRM) M. Dworczyka oraz członka jego rodziny, a ich zawartość miała być skopiowana. Następnie celem atakujących było co najmniej 4350 adresów e-mail, przy czym co do nie mniej niż 500 z nich atak był skuteczny¹⁶³². W kolejnym okresie pojawiły się informacje o tym, że autorami ataku byli w rzeczywistości Białorusini z grupy UNC1151, choć nie wykluczono pomocy ze strony Federacji Rosyjskiej. Z kolei według raportu Recorded Future sprawcami przeprowadzonych cyberataków były podmioty związane lub działające na zlecenie Kremla. Mając na względzie powyższe rozważania wydaje się, że Moskwa dąży nie tylko do tworzenia własnych zdolności w zakresie działania w cyberprzestrzeni, ale tworzy również swego rodzaju sieć zleceńobiorców z wielu państw, co z kolei będzie utrudniało w przyszłości powiązanie poszczególnych incydentów z Rosją¹⁶³³. Należy również zastanowić się na ile służby białoruskie są w tym zakresie samodzielne, a na ile stanowią jedynie narzędzie służb specjalnych Kremla¹⁶³⁴. W następnych miesiącach ujawniono, że celami niezwykle szerokiego ataku byli najważniejsi urzędnicy, ministrowie oraz posłowie z różnych opcji politycznych¹⁶³⁵. Co jednak w przypadku tego incydentu szczególnie istotne to to, że wykradzione dane były od czasu do czasu publikowane fragmentami i wydaje się, że miały za zadanie skompromitowanie rządu¹⁶³⁶. Może to sugerować, że cyberatak posłużył Rosjanom do pozyskania materiałów w celu zrealizowania zaplanowanej kampanii oddziaływania informacyjnego. W przeciągu kilku miesięcy opublikowano dane pozyskane z konta szefa KPRM, jak chociażby zdjęcie jego dowodu osobistego i prawa jazdy¹⁶³⁷ oraz korespondencję

¹⁶³² Niebezpiecznik: *ABW i SKW potwierdza: to Rosjanie zhackowali Dworczyka i resztę polskich polityków*. <https://niebezpiecznik.pl/post/abw-i-skw-rosjanie-unc1151-dworczyk-ghostwriter/> (dostęp: 25.02.2023).

¹⁶³³ OKO.press: *Jednak Rosja! To ona według analityków USA stała za operacją, której częścią było #DworczykLeaks*. <https://oko.press/jednak-rosja-tstala-za-dworczykileaks> (dostęp: 25.05.2023).

¹⁶³⁴ Niebezpiecznik: *To nie Rosjanie a Białorusini zhackowali polskich polityków*. <https://niebezpiecznik.pl/post/bialorus-stoi-za-atakami-na-polskich-politykow-unc1151/> (dostęp: 25.02.2023).

¹⁶³⁵ Wprost: *Kaczyński wydał oświadczenie po cyberatakach. „Przeprowadzone z terenu Federacji Rosyjskiej”*. <https://www.wprost.pl/polityka/10458686/cyberataki-na-polskich-politykow-oswiadczenie-jaroslaw-kaczynskiego.html> (dostęp: 25.02.2023).

¹⁶³⁶ Polskie Radio 24: *Cyberataki na Polskę. Departament Stanu USA: Rosja używa narzędzia do siania dezinformacji i podziałów*. <https://polskieradio24.pl/5/1223/artukul/2761363,cyberataki-na-polske-departament-stanu-usa-rosja-uzywa-narzedzia-do-siania-dezinformacji-i-podzialow> (dostęp: 25.02.2023).

¹⁶³⁷ Niebezpiecznik: *Zdjęcie dowodu i prawa jazdy ministra Dworczyka wykradzione i opublikowane. Razem z “memem”*. <https://niebezpiecznik.pl/post/skany-dowodu-osobistego-i-prawa-jazdy-dworczyka-wykradzone/> (dostęp: 25.05.2023).

prywatną i służbową (dotyczącą między innymi Trybunału Konstytucyjnego, przekazów prezentowanych w mediach publicznych – TVP, spraw koalicji z partią Z. Ziobry)¹⁶³⁸. Ponadto, opublikowane zostały dane stanowiące tajemnicę państwową, w tym oznaczone klauzulą „ściśle tajne”, jak również takie dotyczące polskiej obronności (na przykład notatki o systemie obrony powietrznej „Narew”), czy wreszcie informacje chronione klauzulami niejawności NATO¹⁶³⁹. Wskazać należy, że treści publikowane za pośrednictwem serwisu Telegram, a pochodzące według publikujących z danych wykradzonych M. Dworczykowi, ukazywały nadużycia polskiego rządu. Istotnym jest również fakt, że szef KPRM miał korzystać z prywatnego adresu e-mail do załatwiania spraw służbowych – państwowych, co już samo w sobie stanowi naruszenie prawa. Polski rząd konsekwentnie odmawiał wypowiedzania się w kwestii prawdziwości publikowanych wiadomości e-mail, jednakże autentyczność wybranej części korespondencji potwierdzili ich niektórzy uczestnicy co wskazuje, że do włamania faktycznie musiało dojść¹⁶⁴⁰. Ostatecznie M. Dworczyk po ponad roku złożył rezygnację z pełnionej funkcji, jednakże konsekwentnie nie wskazał by powodem był przeprowadzony wstosunku do jego osoby cyberatak¹⁶⁴¹. Opisane wyżej działania wpisują się w cele rosyjskiej polityki zagranicznej realizowanej względem Polski. Należy do nich zaliczyć przede wszystkim ośmieszanie Polski na arenie międzynarodowej, prezentowanie Polski jako partnera niestabilnego i niewiarygodnego oraz podważanie istniejących sojuszy.

[2022] W 2022 roku doszło do pełnowymiarowej agresji Federacji Rosyjskiej na Ukrainę (choć faktywnie wojna rozpoczęła się już w 2014 roku). Wydarzenia z tym związane

¹⁶³⁸ Niebezpiecznik: *Włamywacze opublikowali treść e-maila ze skrzynki ministra Dworczyka*. <https://niebezpiecznik.pl/post/wyciek-e-mail-do-ministra-dworczyka/> (dostęp: 25.05.2023); Rzeczpospolita: *Afera mailowa: Odebranie Ziobrze kontroli nad prokuraturą i sprawdzenie finansów Solidarnej Polski*. <https://www.rp.pl/polityka/art37341181-afere-mailowa-odebranie-ziobrze-kontroli-nad-prokuratura-i-sprawdzenie-finansow-solidarnej-polski> (dostęp: 25.05.2023); OKO.press: *Afera mailowa. Jak Przylębska z Dworczykiem oszczędzali na obywatelach, odraczając rozstrzygnięcia w TK*. <https://oko.press/afere-mailowa-przylebska-dworczyk> (dostęp: 25.05.2023); Gazeta.pl: *Afera mailowa. Dworczyk miał pisać do Klarenbacha ws. caracali. "Przekaz jest taki..."*. <https://wiadomosci.gazeta.pl/wiadomosci/7,114884,29592952,afere-mailowa-dworczyk-mial-pisac-do-klarenbacha-ws-caracali.html> (dostęp: 25.05.2023); Onet Wiadomości: *Afera e-mailowa. Doradca premiera prosi Kurskiego i szefa "Wiadomości" o "ładny atak w TVP" na sędziego*. https://wiadomosci.onet.pl/kraj/afere-e-mailowa-doradca-premier-prosil-kurskiego-o-ladny-atak-w-tvp/z12hy7e?utm_source=pl.wikipedia.org_viasg_wiadomosci&utm_medium=referral&utm_campaign=leo_automatic&srcc=undefined&utm_v=2 (dostęp: 25.05.2023).

¹⁶³⁹ Rzeczpospolita: *Afera mailowa. Tajne informacje w wiadomościach ze skrzynki Dworczyka? Jest śledztwo*. <https://www.rp.pl/polityka/art38044011-afere-mailowa-tajne-informacje-w-wiadomosciach-ze-skrzynki-dworczyka-jest-sledztwo> (dostęp: 25.05.2023).

¹⁶⁴⁰ Rzeczpospolita: *Gowin: Wśród maili ze skrzynki Dworczyka znalazł się mój. Był prawdziwy*. <https://www.rp.pl/polityka/art36905441-gowin-wsrod-maili-ze-skrzynki-dworczyka-znalazl-sie-moj-byl-prawdziwy> (dostęp: 25.05.2023); Wirtualne Media: *Jacek Sasin potwierdza ujawnione maile ze skrzynki Dworczyka. Ambasador Niemiec wezwany z powodu tekstu w „Fakcie”*. <https://www.wirtualnemedia.pl/artukul/jacek-sasin-maile-dworczyka-mateusz-morawiecki> (dostęp: 25.05.2023).

¹⁶⁴¹ TVN24: *Dworczyk: złożyłem rezygnację*. <https://tvn24.pl/polska/michal-dworczyk-podal-sie-dymisji-odchodzi-z-funkcji-szefa-kancelarii-prezesa-rady-ministrow-6140126> (dostęp: 25.05.2023).

są najistotniejszą kwestią sporną w stosunkach polsko-rosyjskich z jaką przyszło mierzyć się Warszawie oraz Moskwie w drugiej dekadzie XXI wieku. Polska udzieliła ogromnego wsparcia Ukrainie, zarówno w wymiarze politycznym, ekonomicznym, wojskowym czy społecznym. W tym czasie to również przez Polskę do Kijowa dociera największa część pomocy jaka jest przekazywana przez inne państwa. To wszystko sprawia, że polska cyberprzestrzeń stała się jak nigdy dotąd narażona na wrogie działania ze strony Federacji Rosyjskiej.

Według raportów zespołów CERT Polska oraz CSIRT GOV, stan bezpieczeństwa Polski w cyberprzestrzeni przedstawiał się w sposób następujący. W odniesieniu do lokalizacji serwerów C&C na świecie Federacja Rosyjska zajęła piąte miejsce z udziałem 2,75%. Została wyprzedzona przez Niemcy (3,19%), Holandię (4,18%), Rumunię (6,42%) oraz USA (39,51%)¹⁶⁴². Z kolei w odniesieniu do rozkładu źródeł ataków na sieci monitorowane przez system ARAKIS GOV pod kątem liczby generowanych przepływów, udział Rosji wyniósł 18% (drugie miejsce) – spadł on względem roku 2021 (25%). Co szczególnie ciekawe Federacja została wyprzedzona tylko przez USA z wynikiem 28%. Kolejne miejsca zajęły kolejno Chiny (14%), Niderlandy (7%), Niemcy (7%) oraz Wielka Brytania (7%)¹⁶⁴³. Należy jednak ponownie zasygnalizować, że źródło przepływów niekoniecznie musi wskazywać na sprawcę danego działania. Jest bowiem możliwe dokonywanie cyberataków przez określone państwa lub podmioty z nim powiązane, z wykorzystaniem infrastruktury teleinformatycznej innego kraju w dowolnym miejscu na świecie.

Raport roczny Zespołu CERT Polska z 2022 roku stosunkowo dużą część opracowania poświęcił agresji Federacji Rosyjskiej na Ukrainę, która rozpoczęła się w 24 lutego 2022 roku (należy również podkreślić, że raporty zespołów są niezwykle obszerne względem tych publikowanych w latach ubiegłych). Wskazano, że „już w miesiącach poprzedzających wojnę Rosja prowadziła nasilone działania w cyberprzestrzeni, przygotowujące grunt pod to, co miało się wydarzyć. W styczniu rosyjscy hakerzy doprowadzili do paraliżu ukraińskie strony rządowe, a tuż przed rozpoczęciem inwazji przeprowadzono także cyberatak na sieć satelitarną KA-SAT. Celem działań było uniemożliwienie komunikacji między tysiącami użytkowników w Ukrainie, a także zerwanie łączności z szerokopasmowym Internetem dla dziesiątek tysięcy odbiorców w niektórych państwach członkowskich Unii Europejskiej. Po upływie roku od rozpoczęcia wojny można było zaobserwować, jak Rosja próbuje wykorzystywać ataki cybernetyczne, aby destabilizować sytuację wewnętrzną w państwach wspierających Ukrainę.

¹⁶⁴² Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2022...*, s. 118.

¹⁶⁴³ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku...*, s. 82-83.

Ataki na instytucje publiczne i infrastrukturę krytyczną wzmogły się, co wpisuje się w realizację rosyjskiej strategii wojskowej”¹⁶⁴⁴.

Autorzy raportu zauważyli, że po atakach przeprowadzonych na Ukrainie celem rosyjskich grup cyberprzestępczych i hakywistów stały się kraje takie jak Polska, Litwa, Łotwa, Estonia oraz państwa skandynawskie, ale również CyberPol oraz Centrum Doskonalenia Cyberobrony NATO. Szczególną aktywnością wykazywała się nowa grupa APT o nazwie Killnet (powstała prawdopodobnie w 2022 roku), będąca podmiotem mniej sformalizowanym niż na przykład SandWorm czy Fancy Bear. Killnet jest raczej organizacją składającą się z mniejszych grup sympatyzujących z Rosją oraz zajmującą się szerzeniem propagandy i dezinformacji. Do grup powiązanych z Killnetem zalicza się między innymi Legion oraz Xaknet¹⁶⁴⁵.

Pod koniec marca 2022 roku grupa Killnet przeprowadziła atak typu DDoS na stronę internetową Sądu Najwyższego oraz Narodowego Banku Polskiego, Policji, ośmiu polskich lotnisk, ale również na szereg innych podmiotów rządowych oraz prywatnych przedsiębiorstw (na przykład Castorama, mBank, Orange)¹⁶⁴⁶. Efektem działalności grupy w 2022 roku był między innymi cyberatak na szereg państw Europy, które wspierały Ukrainę w wojnie rosyjsko-ukraińskiej. W przypadku Polski skutkiem było wyłączenie kilku rządowych stron internetowych, jak również podszycie się pod szereg witryn w celu wyłudzenia danych do logowania. Podczas wejścia na taką stronę wyświetlał się komunikat „wystąpił błąd podczas logowania do aplikacji. Przejdź do strony głównej i spróbuj ponownie. Jeśli błąd będzie się powtarzał, skontaktuj się z pomocą techniczną”. W konsekwencji, użytkownik logował się ponownie, udostępniając jednocześnie swoje dane dostępne¹⁶⁴⁷. Przeprowadzone przez grupę ataki wobec Polski należy osadzić w szerszym kontekście, jako jeden z przejawów wrogiej kampanii wymierzonej w państwa członkowskie NATO w związku z ich zaangażowaniem w konflikt rosyjsko-ukraiński.

Ponadto Zespół CSIRT GOV w 2022 roku zidentyfikował proceder polegający na rejestracji domen przypominających nazwy oficjalnych witryn rządowych. Wskazano między innymi na możliwość ich potencjalnego wykorzystania do działań dezinformacyjnych¹⁶⁴⁸.

¹⁶⁴⁴ Zespół CERT Polska: *Raport roczny z działalności CERT Polska 2022...*, s. 91.

¹⁶⁴⁵ Ibidem, s. 93.

¹⁶⁴⁶ Ibidem, s. 94-95.

¹⁶⁴⁷ EXPRESS: *Russia launches attack on Poland as hackers declare war on 10 countries, including UK*. <https://www.express.co.uk/news/science/1638740/russia-launches-cyberattack-poland-government-sites-shut-down-killnet-ukraine-war> (dostęp: 25.05.2023).

¹⁶⁴⁸ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku...*, s. 31.

Z kolei w październiku miała miejsce kampania *phishingowa* w ramach której podszyto się pod portal gov.pl. Strona zarejestrowana w domenie gov.pl zawierała treści o fikcyjnej pomocy dla obcokrajowców mających zamiar zamieszkać w Polsce. Na portalu posługiwano się językiem rosyjskim¹⁶⁴⁹.

Kolejnym z incydentów była atak na stronę internetową Urzędu Transportu Kolejowego pasazer.gov.pl w wyniku którego dokonano podmiany jej zawartości, poprzez umieszczenie treści o charakterze antyukraińskim. Ponadto nawiązano do rzezi wołyńskiej oraz zachęcano do antyrządowych protestów, co wpisywało się w działalność Kremla o charakterze dezinformacyjnym. Do cyberataku przyznała się nowa (powstała w 2022 roku) rosyjska grupa hakywistyczna o nazwie NoName057(16)¹⁶⁵⁰. Oczywisty jest kontekst dokonanych ataków, który sprowadzał się do potępienia realizowanych przez Polskę transportów z zaopatrzeniem na Ukrainę oraz wsparcia jakie zostało udzielone przez Warszawę rządowi w Kijowie. Warto tutaj ponownie wspomnieć – o czym było już w niniejszej pracy – że działalność z zakresu ataków przeprowadzanych wobec Polski w cyberprzestrzeni, nie zawsze jest dokonywana przez rosyjskie służby specjalne, ale również przez podmioty z nimi powiązane lub działające za ich przyzwoleniem. Nie można zatem takich działań identyfikować wyłącznie z Kremlem oraz organami państwa rosyjskiego.

W odniesieniu do wojny informacyjnej, w szczególności do działań z zakresu dezinformacji, raport Zespołu CSIRT GOV wskazał, że „od lutego 2022 r., tj. od czasu wprowadzenia stopnia alarmowego CHARLIE CRP na terenie kraju, CSIRT GOV zarejestrował znaczny wzrost liczby ataków DDoS, a także szereg socjotechnicznych kampanii *phishingowych*, czy podmian stron internetowych. Jednocześnie, miały miejsce incydenty”¹⁶⁵¹. Ponadto podniesiono, iż „rok 2022 to także czas intensyfikacji działań grup APT – wielu z nich działających w kontekście konfliktu zbrojnego w Ukrainie. Szczególnym, relatywnie nowym rodzajem zagrożenia, który został zidentyfikowany m.in. w Ukrainie było wykorzystanie szkodliwego oprogramowania typu *wiper*, mającego na celu uszkodzenie przetwarzanych na zaatakowanym systemie danych, a tym samym doprowadzenie do jego całkowitej nieużyteczności”¹⁶⁵².

Dalej w raporcie wskazano, że „zespół CSIRT GOV zarejestrował aktywność innych grup APT, które od lat wpisują się w polski krajobraz cyberzagrożeń, w szczególności APT28,

¹⁶⁴⁹ Ibidem, s. 39.

¹⁶⁵⁰ Ibidem, s. 29.

¹⁶⁵¹ Ibidem, s. 122.

¹⁶⁵² Ibidem, s. 122.

APT29, Turla, czy Mustang Panda. Natomiast, rozpoznany wektor ataku opierał się przede wszystkim o tradycyjne techniki, tj. ataki socjotechniczne, mające na celu propagację szkodliwego oprogramowania, którego zadaniem była¹⁶⁵³. Podstawową techniką wykorzystywaną przez grupy APT był *phishing*, mający kontekst dotyczący wojny rosyjsko-ukraińskiej¹⁶⁵⁴. Od lutego 2022 roku, po wprowadzeniu stopnia alarmowego CHARLIE CRP w ramach polskiej infrastruktury teleinformatycznej zaobserwowano liczne ataki typu DDoS realizowane przez grupy hakywistyczne, w tym między innymi NoName057(16), Killnet, CyberArmia Ludowa. Ich głównym celem było „ograniczenie dostępności witryn internetowych atakowanych podmiotów oraz świadczonych przy ich wykorzystaniu usług. Akty tego rodzaju działania nosiły znamiona kampanii propagandowych (informacje na ich temat były intensywnie rozpowszechniane za pośrednictwem popularnych mediów społecznościowych), podkreślających domniemaną skuteczność grup przy jednoczesnej próbie uwypuklenia słabości atakowanych celów”¹⁶⁵⁵.

Polska cyberprzestrzeń w 2022 roku, niezwykle często względem lat ubiegłych, była obiektem ataków teleinformatycznych ze strony Federacji Rosyjskiej. Znamiennym pozostaje, że w okresie poprzedzającym bezpośrednio rosyjską inwazję w styczniu 2022 roku wprowadzono na terenie całej Polski stopień alarmowy ALFA-CRP (najniższy ze stopni)¹⁶⁵⁶, a już w lutym podniesiono go do stopnia CHARLIE-CRP (trzeci stopień)¹⁶⁵⁷, przy czym obowiązywał on przez cały 2022 rok¹⁶⁵⁸. Należy zestawić ogłoszone przez rząd alarmy dotyczące bezpieczeństwa polskiej infrastruktury teleinformatycznej ze wzrostem rosyjskiej aktywności w tym obszarze, jaka miała miejsce w ciągu ostatnich kilku lat, jak i obawami o konsekwencje wsparcia i pomocy udzielanej przez Polskę Ukrainie¹⁶⁵⁹. Przypomnieć należy, że stopień CHARLIE-CRP jest wprowadzany na wypadek: wystąpienia zdarzenia potwierdzającego prawdopodobny cel ataku o charakterze terrorystycznym¹⁶⁶⁰, uzyskania

¹⁶⁵³ Ibidem, s. 122.

¹⁶⁵⁴ Ibidem, s. 56-66.

¹⁶⁵⁵ Ibidem, s. 25.

¹⁶⁵⁶ gov.pl: *Stopień alarmowy ALFA-CRP na terenie całej Polski*. <https://www.gov.pl/web/cyfryzacja/stopien-alarmowy-alfa-crp-na-terenie-calej-polski> (dostęp: 26.02.2023).

¹⁶⁵⁷ gov.pl: *Trzeci stopień alarmowy CRP na terenie całego kraju*. <https://www.gov.pl/web/rcb/trzeci-stopien-alarmowy-crp-na-terenie-calego-kraju> (dostęp: 26.02.2023).

¹⁶⁵⁸ gov.pl: *Przedłużenie stopni alarmowych BRAVO oraz CHARLIE-CRP - do 28 lutego 2023*. <https://www.gov.pl/web/cea/przedluzenie-stopni-alarmowych-bravo-oraz-charlie-crp3> (dostęp: 26.02.2023).

¹⁶⁵⁹ Zobacz na przykład rozkład procentowy ataków z Federacji Rosyjskiej na monitorowane przez system ARAKIS sieci pod kątem liczby generowanych przepływów.

¹⁶⁶⁰ Przy czym „godzącego w: a) bezpieczeństwo lub porządek publiczny albo b) bezpieczeństwo Rzeczypospolitej Polskiej, albo c) bezpieczeństwo innego państwa lub organizacji międzynarodowej oraz stwarzającego potencjalne zagrożenie dla Rzeczypospolitej Polskiej”. Źródło: *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* (Dz.U. 2016 poz. 904), art. 15 ust. 5 pkt. 1 litera a-c.

wiarygodnych i potwierdzonych informacji o planowanym zdarzeniu o charakterze terrorystycznym na terytorium Polski, jak również zdarzenia, którego skutki mogą dotyczyć obywateli polskich przebywających za granicą lub instytucji albo infrastruktury mieszczących się poza granicami Polski¹⁶⁶¹. Z kolei w dniu wybuchu konfliktu (24 luty 2022 roku) CERT Polska wydało rekomendujące dla obywateli oraz przedsiębiorstw w związku z ogłoszeniem trzeciego stopnia alarmowego oraz rosyjską inwazją¹⁶⁶².

Według raportu Agencji Unii Europejskiej ds. Cyberbezpieczeństwa, konflikt pomiędzy Rosją i Ukrainą na nowo ukształtował krajobraz zagrożeń w cyberprzestrzeni. Do najważniejszych z nich zaliczono: wzrost aktywności hakytywistów, prowadzenie operacji przez podmioty o charakterze niewojskowym i wojskowym, wzrost cyberprzestępczości oraz działania ze strony określonych grup w cyberprzestrzeni, motywowanych przez państwa uczestniczące w konflikcie. Co równie ważne wskazano, że dezinformacja jest narzędziem w cyberwojnie oraz że została użyta w charakterze przygotowawczym, a więc przed rozpoczęciem fizycznych działań zbrojnych na Ukrainie¹⁶⁶³. Podczas gdy w raportach za ubiegłe lata o Rosji wzmiankowano kilkanaście razy, w 2021 roku kilkadziesiąt, tak w raporcie z 2022 roku odniesień można odnaleźć ponad kilkaset. W dokumencie zauważono również, że celem rosyjskich cyberataków był szereg państw wspierających Ukrainę, przy czym priorytetowo Kreml traktował USA, Unię Europejską, Polskę, kraje graniczące z Rosją oraz Sojusz Północnoatlantycki¹⁶⁶⁴.

W raporcie przygotowanym przez Microsoft wskazano natomiast, że w przeddzień rosyjskiej inwazji (podobnie zresztą jak miało to miejsce w przypadku Gruzji w 2008 roku i aneksji Krymu w 2014 roku) przeprowadzono zmasowany cyberatak, którego celem była Ukraina¹⁶⁶⁵. Już w połowie lutego Kijów informował o atakach typu DDoS na sektor bankowy oraz Ministerstwo Obrony Narodowej, jednakże wtedy nie stwierdzono kto może być ich autorem¹⁶⁶⁶. Raport Microsoft wskazuje, że od lutego do czerwca 2022 roku wykryto poza Ukrainą rosyjskie próby włamania do 128 organizacji w 42 krajach. USA pozostawały celem numer jeden, jednakże Polska, przez którą dostarczano znaczną część międzynarodowej pomocy wojskowej i humanitarnej dla Ukrainy, również znajdowała się w zainteresowaniu

¹⁶⁶¹ Ibidem, art. 15 ust. 5 pkt. 1-3.

¹⁶⁶² CERT Polska: *Rekomendacje w związku ze zwiększonym zagrożeniem w cyberprzestrzeni wywołanym sytuacją na Ukrainie*. <https://cert.pl/posts/2022/02/rekomendacje-cyberprzestrzen-ukraina/> (dostęp: 26.02.2023).

¹⁶⁶³ European Union Agency for Cybersecurity: *ENISA Threat Landscape 2022*. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@/download/fullReport> (dostęp: 26.02.2023), s. 4.

¹⁶⁶⁴ Ibidem, s. 27.

¹⁶⁶⁵ Microsoft: *Microsoft Digital Defense Report 2022...*, s. 2.

¹⁶⁶⁶ Niebezpiecznik: *Ukraina informuje o atakach DDoS na MON i banki*. <https://niebezpiecznik.pl/post/ukraina-informuje-o-atakach-ddos-na-mon-i-banki/> (dostęp: 26.02.2023).

Kremla¹⁶⁶⁷. Raport podkreśla, że cyberprzestrzeń stała się obszarem przeprowadzania przez Rosję operacji wpływu mających na celu wpojenie odbiorcy oraz narzucenie mu rosyjskiego punktu widzenia na sprawy międzynarodowe¹⁶⁶⁸.

Polska stała się jednym z najważniejszych celów dla Federacji Rosyjskiej pod względem przeprowadzanych cyberataków w 2022 roku. Nie ulega wątpliwości, że bezprecedensowe wsparcie jakiego udzieliła Warszawa rządowi w Kijowie, wpłynęło na rosyjską aktywność wobec Polski w cyberprzestrzeni. Polska w zasadzie od pierwszych dni wojny stała się azylem dla setek tysięcy, a następnie milionów ukraińskich uchodźców uciekających przed wojną¹⁶⁶⁹. Ponadto rząd w Warszawie udzielił ogromnego wsparcia politycznego na arenie międzynarodowej dla zaatakowanej Ukrainy. Wymiernym efektem tych działań stało się przeobrażenie Polski w swego rodzaju *hub* logistyczny dla wsparcia materialnego (w tym militarnego), które jest przekazywane Ukraińcom przez wiele państw na świecie. To właśnie w polskich portach morskich oraz na lotniskach czy dworcach kolejowych jest przeładowywana broń, która trafia następnie na Ukrainę¹⁶⁷⁰.

Do skutków działania rządu w Warszawie można zaliczyć szereg incydentów do których doszło wobec Polski w cyberprzestrzeni. W lipcu dokonano ataków typu DDoS na strony internetowe polskiej Policji w wyniku których przestały działać niektóre witryny komend wojewódzkich¹⁶⁷¹. W sierpniu informowano o zmasowanych cyberatakach ze strony

¹⁶⁶⁷ Microsoft: *Microsoft Digital Defense Report 2022*..., s. 41.

¹⁶⁶⁸ Ibidem, s. 73-78.

¹⁶⁶⁹ gov.pl: *Сайт для громадян України*. <https://www.gov.pl/web/ua> (dostęp: 24.05.2023); Kancelaria Prezesa Rady Ministrów: *#PomagamUkrainie Szukasz ratunku przed wojną? Chcesz wesprzeć uchodźców? Tu znajdziesz pomoc lub jej udzielisz*. <https://pomagamukrainie.gov.pl/> (dostęp: 24.05.2023); Ministerstwo Spraw Wewnętrznych i Administracji: *Informacja dla uchodźców z Ukrainy*. <https://www.gov.pl/web/mswia/informacja-dla-uchodzcow-z-ukrainy> (dostęp: 24.05.2023).

¹⁶⁷⁰ Kancelaria Prezesa Rady Ministrów: *Polska hubem humanitarnym dla Ukrainy*. <https://www.gov.pl/web/premier/polska-hubem-humanitarnym-dla-ukrainy> (dostęp: 25.05.2023); Polska Agencja Prasowa: *Polska przekazała czołgi PT-91 Twardy. Sąd już w Ukrainie*. <https://www.pap.pl/aktualnosci/news%2C1381879%2Cpolska-przekazala-czolgi-pt-91-twardy-sa-juz-w-ukrainie.html> (dostęp: 25.05.2023); Dziennik Gazeta Prawna: *W ciągu roku od napaści Rosji Polska przekazała Ukrainie uzbrojenie o wartości ponad 2,2 mld euro*. <https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/8667242,polska-dostawy-broni-dla-ukrainy-o-wartosci-ponad-22-mld-euro.html> (dostęp: 25.05.2023); Polska Agencja Prasowa: *Jak Polska pomaga Ukrainie? Sprzęt wojskowy, który przekazujemy*. <https://www.pap.pl/aktualnosci/news%2C1557048%2Cjak-polska-pomaga-ukrainie-sprzet-wojskowy-ktory-przekazujemy.html> (dostęp: 25.05.2023); Ministerstwo Obrony Narodowej: *W Polsce będą serwisowane czołgi Leopard z Ukrainy*. <https://www.gov.pl/web/obrona-narodowa/w-polsce-beda-serwisowane-czolgi-leopard-z-ukrainy> (dostęp: 25.05.2023); Rzeczpospolita: *Polska otworzyła hub energetycznej pomocy dla Ukrainy*. <https://energia.rp.pl/elektroenergetyka/art37853981-polska-otworzyla-hub-energetycznej-pomocy-dla-ukrainy> (dostęp: 25.05.2023); Rzeczpospolita: *Polska remontowym hubem dla ukraińskiego uzbrojenia. Firmy pracują dyskretnie*. <https://www.rp.pl/biznes/art37872631-polska-remontowym-hubem-dla-ukraińskiego-uzbrojenia-firmy-pracuja-dyskretnie> (dostęp: 25.05.2023); Logistyka: *Polska stała się portem zastępczym i hubem logistycznym dla Ukrainy*. <https://www.logistyka.net.pl/aktualnosci/item/93456-polska-stala-sie-portem-zastepczym-i-hubem-logistycznym-dla-ukrainy> (dostęp: 25.05.2023).

¹⁶⁷¹ CyberDefence24: *Cyberatak na Polską Policję. Znamy szczegóły*. <https://cyberdefence24.pl/armia-i-sluzby/cyberatak-na-polska-policje-znamy-szczegoly> (dostęp: 26.02.2023).

Rosji, Białorusi oraz Chin na polskie siły zbrojne, co było zmianą względem ubiegłego roku w którym celem był przede wszystkim sektor edukacji, badań i nauki¹⁶⁷². We wrześniu ukraiński wywiad wskazywał na planowane cyberataki ze strony Rosji, których celem miałyby być między innymi Polska¹⁶⁷³. W drugiej połowie roku przeprowadzono natomiast cyberatak na serwery Senatu RP i choć nie potwierdzono kto był jego autorem to fakt, że dzień wcześniej przyjęto uchwałę uznającą Federację Rosyjską za reżim terrorystyczny może wskazywać prawdopodobnego sprawcę¹⁶⁷⁴. Według raportu KPMG co piąte przedsiębiorstwo w Polsce zaobserwowało zwiększoną aktywność w zakresie działań podejmowanych przeciwko niemu w cyberprzestrzeni w związku z inwazją Rosji w Ukrainie¹⁶⁷⁵.

Po rozpoczęciu inwazji na Ukrainę przez Kreml zarówno cyberprzestrzeń Rosji jak i państw zachodnich została poddana licznym cyberatakom, których celem nie było wyłącznie jej sparaliżowanie, ale również promowanie określonych ocen politycznych oraz poglądów na sprawy międzynarodowe. Dla przykładu, na początku marca 2022 roku polski portal internetowy Money.pl w wyniku cyberataku przekierowywał odwiedzających na stronę z komunikatem, informującym że Ukraina musi przegrać wojnę¹⁶⁷⁶.

Z kolei w stosunku do Rosji niezwykle aktywna była grupa Anonymous, która przeprowadziła od początku inwazji szereg cyberataków, których celem stał się nie tylko Kreml, ale również podmioty go wspierające, media oraz przemysł¹⁶⁷⁷. Przykładowo, świętowany w Rosji 9 maja Dzień Zwycięstwa został wykorzystany do przeprowadzenia cyberataków na systemy telewizyjne i w ich wyniku pokazywanie informacji o skutkach wojny na Ukrainie¹⁶⁷⁸.

¹⁶⁷² Rzeczpospolita: *Zmasowane cyberataki Rosji, Białorusi i Chin na polską armię*. <https://www.rp.pl/gospodarka/art36801221-zmasowane-cyberataki-rosji-bialorusi-i-chin-na-polska-armie> (dostęp: 26.02.2023).

¹⁶⁷³ PAP Polska Agencja Prasowa: *Rosja szykuje masowe cyberataki. Na celowniku też Polska*. <https://www.pap.pl/aktualnosci/news%2C1435328%2Crosja-szykuje-masowe-cyberataki-na-celowniku-tez-polska.html> (dostęp: 26.02.2023).

¹⁶⁷⁴ CyberDefence24: *Cyberatak na Senat. Między innymi z terenu Rosji [AKTUALIZACJA]*. <https://cyberdefence24.pl/cyberbezpieczenstwo/cyberatak-na-senat-marszalek-potwierdza> (dostęp: 26.02.2023).

¹⁶⁷⁵ Polskie Radio 24: *Atak Rosji na Ukrainę. KPMG: co piąta firma odnotowała wzrost cyberataków od czasu wojny*. <https://polskieradio24.pl/42/259/artykul/3120078,atak-rosji-na-ukraine-kpmg-co-piata-firma-odnotowala-wzrost-cyberatakow-od-czasu-wojny> (dostęp: 26.02.2023).

¹⁶⁷⁶ Niebezpiecznik: *Portal Money.pl zhackowany. Włamywacz życzył porażki Ukrainie*. <https://niebezpiecznik.pl/post/portal-money-pl-zhackowany-przez-sily-prorosyjskie/> (dostęp: 26.02.2023).

¹⁶⁷⁷ BBC: *Anonymous: How hackers are trying to undermine Putin*. <https://www.bbc.com/news/technology-60784526> (dostęp: 26.02.2023); The Guardian: *Anonymous: the hacker collective that has declared cyberwar on Russia*. <https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia> (dostęp: 26.02.2023); CNBC: *Hacktivist group Anonymous is using six top techniques to 'embarrass' Russia*. <https://www.cnbc.com/2022/07/28/how-is-anonymous-attacking-russia-the-top-six-ways-ranked-.html> (dostęp: 26.02.2023).

¹⁶⁷⁸ RMF24: *"Dzień wstydu". Hakerzy z grupy Anonymous atakują Rosję*. https://www.rmfm24.pl/raporty/raport-wojna-z-rosja-nie-dzien-wstydu-hakerzy-z-grupy-anonymous-atakuja-rosje,nId,6012474#crp_state=1 (dostęp: 26.02.2023).

Kolejnym incydemem był cyberatak dokonany na polskie oraz ukraińskie sieci logistyczne za pomocą złośliwego oprogramowania Prestige. Atak został przeprowadzony przez powiązaną z rosyjskimi służbami specjalnymi (GRU) grupę SandWorm¹⁶⁷⁹. Innym przykładem było zhakowanie strony internetowej Sejmu przez grupę NoName057(16). Cyberatak nastąpił w związku z przyjęciem przez polski parlament uchwały uznającej Rosję za państwowego sponsora działań terrorystycznych¹⁶⁸⁰. Cyberatak został również przypisany grupie Killnet, a jego skutkiem była częściowa niedostępność portalu. Następnie można przytoczyć atak na system Internetu satelitarnego Viasat, w wyniku którego za pomocą złośliwego oprogramowania rosyjscy hakerzy próbowali odciąć określone podmioty (w tym wojsko) od Internetu. W przypadku Polski działanie to nie było tak dotkliwe jak dla Ukrainy. Ponadto przez cały luty oraz marzec 2022 roku (początek rosyjskiej inwazji) polskie adresy e-mail były wręcz zalewane rosyjskimi wiadomościami stanowiącymi próby *phishingu*¹⁶⁸¹.

Działalność Federacji Rosyjskiej wynika z zaangażowania rządu w Warszawie w „pomoc Ukrainie, ale także z faktu, że Polska zdecydowanie opowiada się na arenie międzynarodowej za udzieleniem Kijowowi pomocy. Poprzez wrogie działania w cyberprzestrzeni Rosja chce wyrzucić presję na Polskę jako kraj frontowy i kluczowego sojusznika Ukrainy na wschodniej flance NATO”¹⁶⁸². W 2022 roku ponownie zaobserwowano prowadzenie przez Rosję wojny informacyjnej poprzez dokonywanie cyberataków na konta e-mail oraz konta w mediach społecznościowych w celu pozyskania informacji na potrzeby kampanii oddziaływania informacyjnego (dezinformacji i propagandy). Takie ataki wpisują się rosyjskie postrzeganie wojny informacyjnej¹⁶⁸³.

Według raportu Thales Cyber Threat Intelligence, w III kwartale 2022 roku nastąpił punkt zwrotny w zakresie rosyjskich ataków przeprowadzanych w cyberprzestrzeni. W tym okresie główne wysiłki Kremla zostały bowiem skoncentrowane nie tylko na Ukrainie, ale również na Polsce, krajach nadbałtyckich oraz państwach skandynawskich. W przypadku tych ostatnich było to zapewne spowodowane planami przystąpienia Finlandii i Szwecji do NATO. Według twórców raportu największy nacisk Rosjanie położyli na infrastrukturę kolejową, lotnictwo, energetykę, opiekę zdrowotną, bankowość oraz usługi publiczne. Są to więc sektory

¹⁶⁷⁹ Council on Foreign Relations: *Polish Cyber Defenses and the Russia-Ukraine War*. <https://www.cfr.org/blog/polish-cyber-defenses-and-russia-ukraine-war> (dostęp: 25.05.2023).

¹⁶⁸⁰ gov.pl: *Russian cyberattacks*. <https://www.gov.pl/web/special-services/russian-cyberattacks> (dostęp: 25.05.2023).

¹⁶⁸¹ Council on Foreign Relations: *Polish Cyber Defenses and the Russia-Ukraine War*. <https://www.cfr.org/blog/polish-cyber-defenses-and-russia-ukraine-war> (dostęp: 25.05.2023).

¹⁶⁸² Ibidem.

¹⁶⁸³ Ibidem.

niezwykle istotne z punktu widzenia wspierania Ukrainy w wymiarze logistycznym – jako *hub* militarny i humanitarny. Szacuje się, że około 60% wszystkich cyberincydentów zgłoszonych na całym świecie od początku pełnowymiarowej rosyjskiej inwazji na Ukrainę zostało przeprowadzonych przez podmioty powiązane bezpośrednio lub pośrednio z Kremlm. W początkowym okresie dominujące były ataki sprowadzające się do kradzieży danych, *phishingu*, szpiegostwa, kampanii wpływu oraz włamań, a następnie ataki typu DDoS, których celem było również wspieranie kradzieży danych oraz cyberszpiegostwa¹⁶⁸⁴.

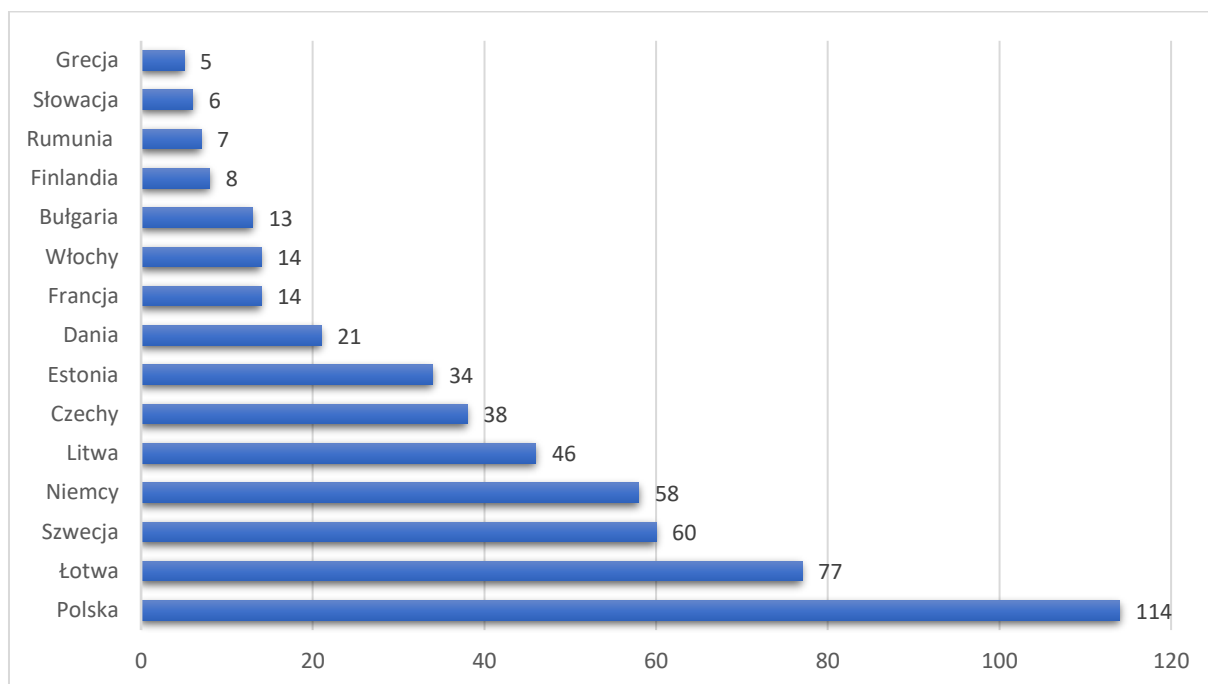
Wreszcie należy wspomnieć o kampanii szpiegowskiej przeprowadzonej przez podmioty powiązane z rosyjskimi służbami specjalnymi – między innymi grupę APT-29. Jej działania były ukierunkowane na pozyskiwanie informacji z resortów spraw zagranicznych oraz placów dyplomatycznych większości państw należących do NATO oraz Unii Europejskiej. Cyberatak polegał na wykorzystaniu techniki *spear phishingu*, która sprowadzała się do rozsyłania do wybranych pracowników resortów wiadomości e-mail w których podszywano się pod ambasadę innych państw europejskich. W ich treści lub w załączniku umieszczano link z rzekomym odniesieniem do kalendarza ambasadora (przedstawiciela dyplomatycznego), a po kliknięciu następowało przekierowanie na stronę ze złośliwym oprogramowaniem i zainfekowanie urządzenia. W dacie publikacji komunikatu przez SKW i CERT Polska kampania była nadal realizowana w związku z czym nie jest możliwe wskazanie jej ostatecznych skutków¹⁶⁸⁵.

Na poniższych wykresach przedstawiono rozkład cyberataków związanych z wojną rosyjsko-ukraińską (2022) na przykładzie wybranych państw Unii Europejskiej, rozkład cyberataków typu DDoS związanych z wojną rosyjsko-ukraińską (2022) na przykładzie wybranych państw, liczbę incydentów obsłużonych ręcznie przez Zespół CERT Polska w latach 2020-2022, liczbę zgłoszonych oraz faktycznych incydentów odnotowanych przez Zespół CSIRT GOV w latach 2020-2022, rozkład procentowy ataków z Federacji Rosyjskiej na monitorowane przez system ARAKIS sieci w latach 2020-2022 pod kątem liczby generowanych przepływów, liczbę zarejestrowanych przez system ARAKIS w latach 2020-2022, rozkład przepływów w sieciach teleinformatycznych uczestniczących w projekcie ARAKIS w latach 2020-2022.

¹⁶⁸⁴ Thales: *From Ukraine to the whole of Europe: cyber conflict reaches a turning point*. https://www.thalesgroup.com/en/worldwide/security/press_release/ukraine-whole-europe-cyber-conflict-reaches-turning-point (dostęp: 25.05.2023).

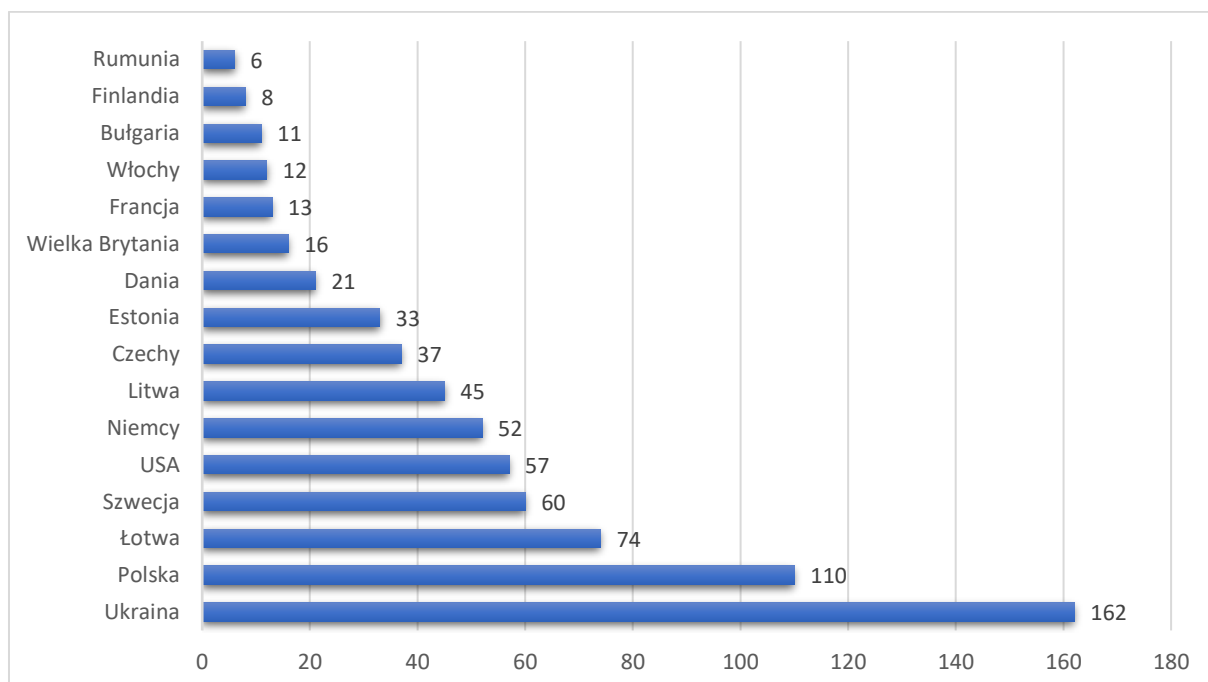
¹⁶⁸⁵ gov.pl: *Kampania szpiegowska wiązana z rosyjskimi służbami specjalnymi*. <https://www.gov.pl/web/baza-wiedzy/kampania-szpiegowska-wiazana-z-rosyjskimi-sluzbami> (dostęp: 25.05.2023).

Wykres 16. Rozkład cyberataków związanych z wojną rosyjsko-ukraińską (2022) na przykładzie wybranych państw członkowskich Unii Europejskiej.



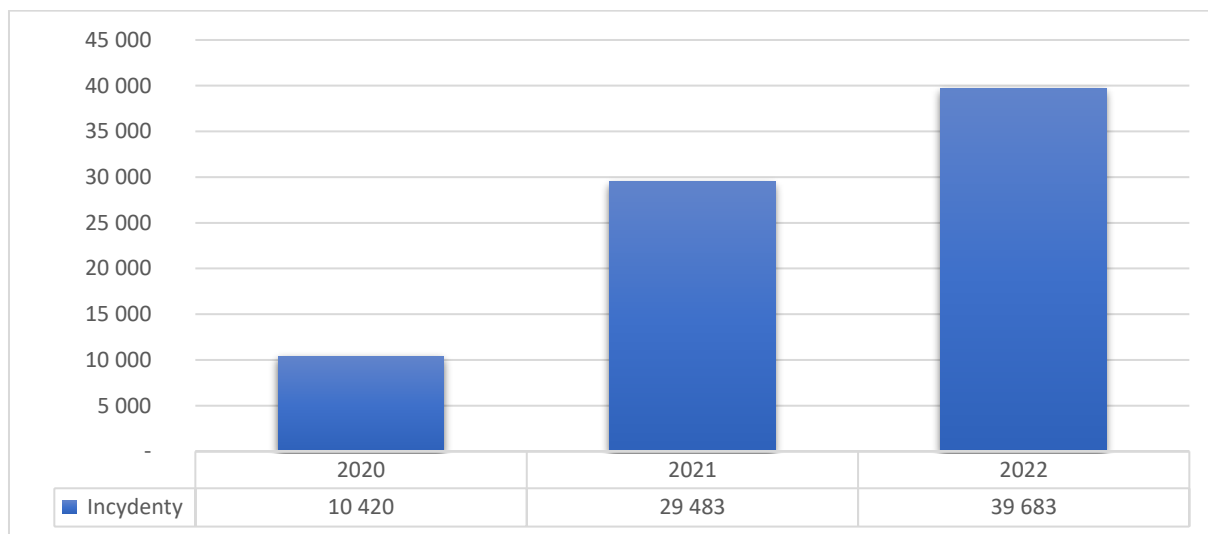
Źródło: Opracowanie własne na podstawie raportu Cyber Solutions by Thales. 2022-2023: A year of Cyber Conflict in Ukraine. Summary of extensive analysis from the Thales Cyber Threat Intelligence Team.

Wykres 17. Rozkład cyberataków typu DDoS związanych z wojną rosyjsko-ukraińską (2022) na przykładzie wybranych państw.



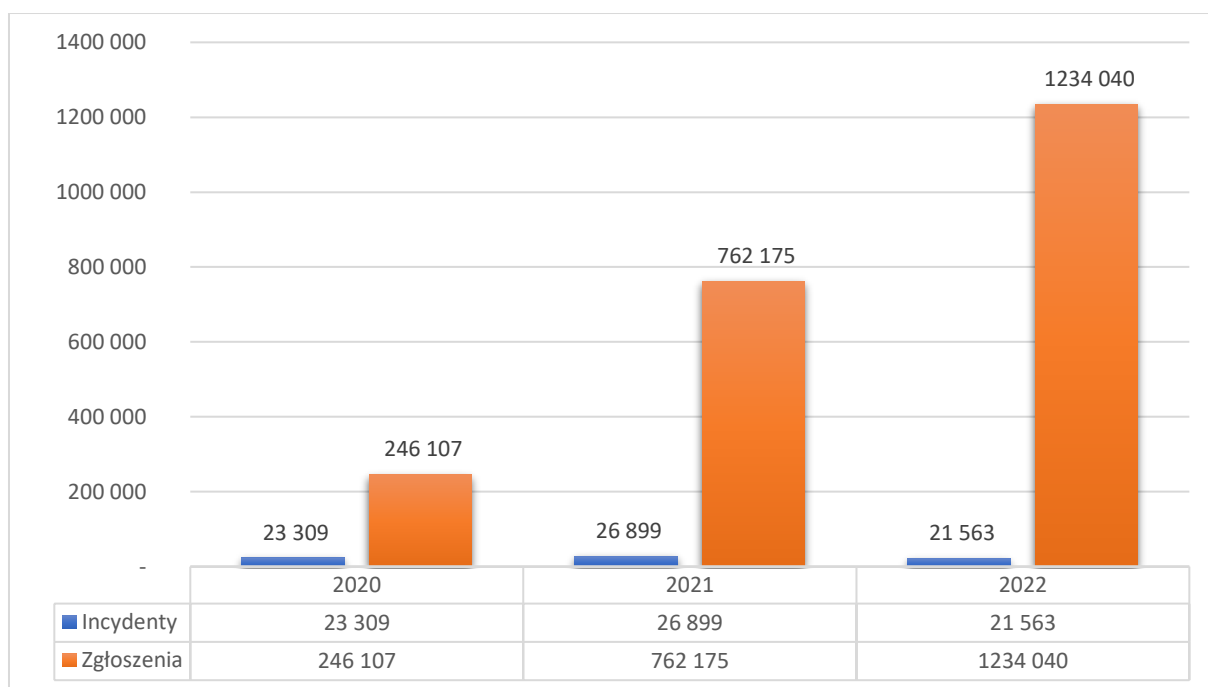
Źródło: Opracowanie własne na podstawie raportu Cyber Solutions by Thales. 2022-2023: A year of Cyber Conflict in Ukraine. Summary of extensive analysis from the Thales Cyber Threat Intelligence Team.

Wykres 18. Liczba incydentów obsługiwanych ręcznie¹⁶⁸⁶ przez Zespół CERT Polska w latach 2020-2022.



Źródło: Opracowanie własne na podstawie raportów rocznych Zespołu CERT Polska za lata 2020-2022.

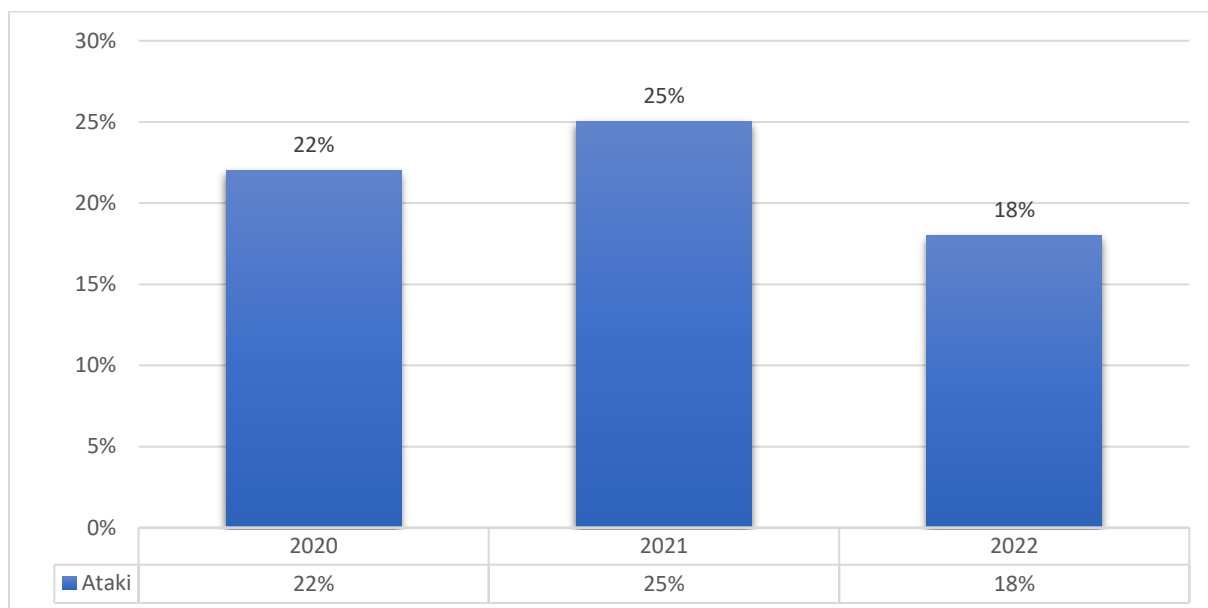
Wykres 19. Liczba zgłoszonych oraz faktycznych incydentów odnotowanych przez Zespół CSIRT GOV w latach 2020-2022.



Źródło: Opracowanie własne na podstawie raportów rocznych Zespołu CSIRT GOV za lata 2020-2022.

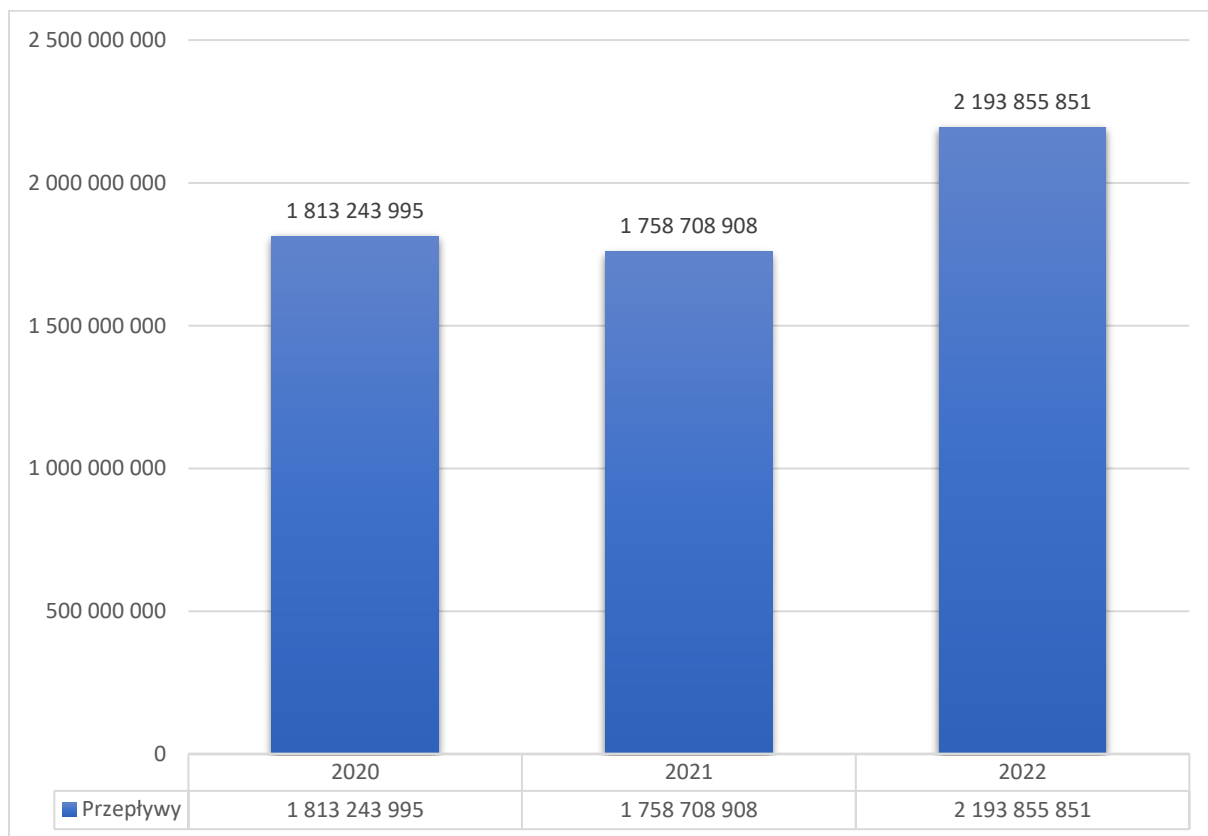
¹⁶⁸⁶ Incydenty obsługiwane ręcznie to incydenty, które zostały zarejestrowane oraz wymagają bezpośredniego działania przez członka Zespołu.

Wykres 20. Rozkład procentowy ataków z Federacji Rosyjskiej na monitorowane przez system ARAKIS sieci w latach 2020-2022 pod kątem liczby generowanych przepływów.



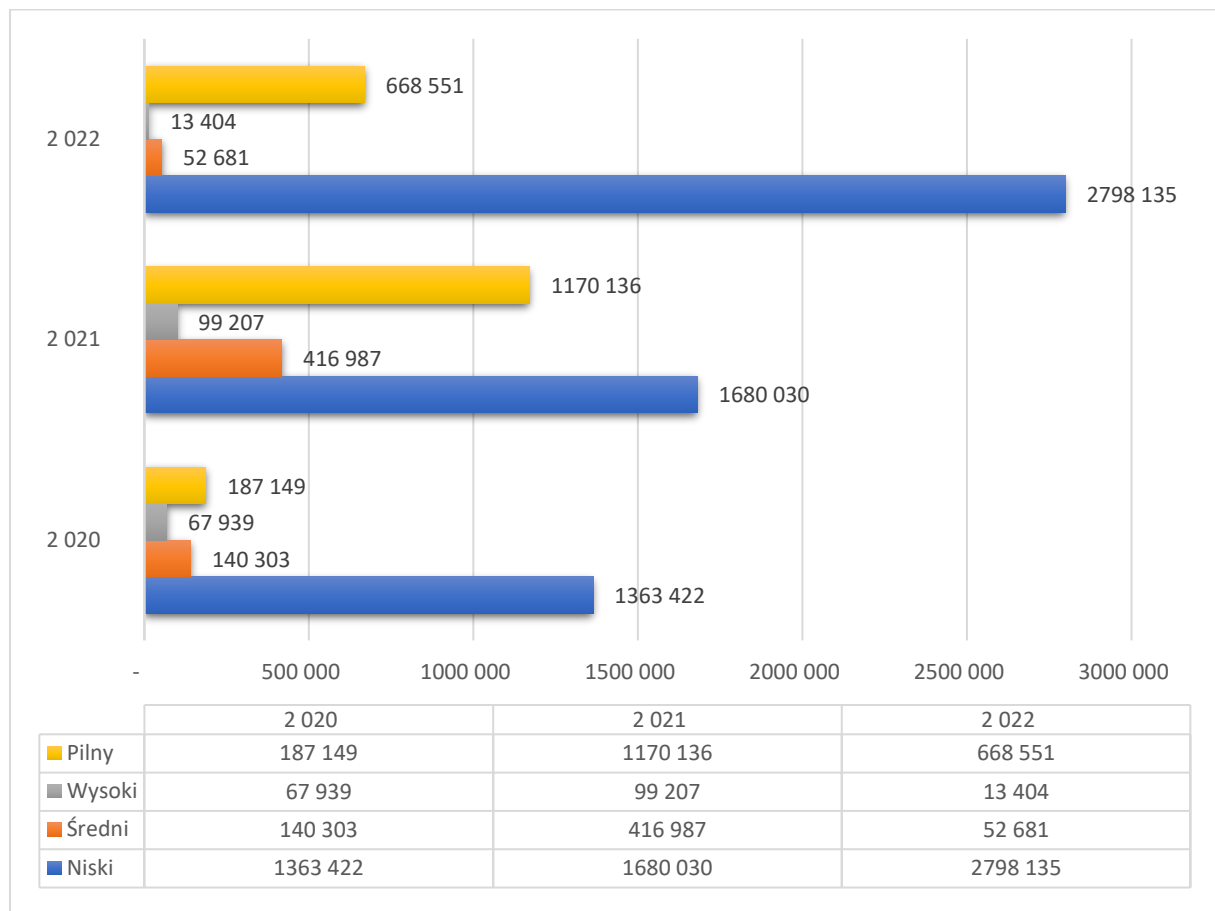
Źródło: Opracowanie własne na podstawie raportów rocznych Zespołu CSIRT GOV za lata 2020-2022.

Wykres 21. Rozkład przepływów w sieciach teleinformatycznych uczestniczących w projekcie ARAKIS w latach 2020-2022.



Źródło: Opracowanie własne na podstawie raportów rocznych Zespołu CSIRT GOV za lata 2020-2022.

Wykres 22. Liczba zarejestrowanych alarmów (z podziałem na priorytety¹⁶⁸⁷) przez system ARAKIS w latach 2020-2022.

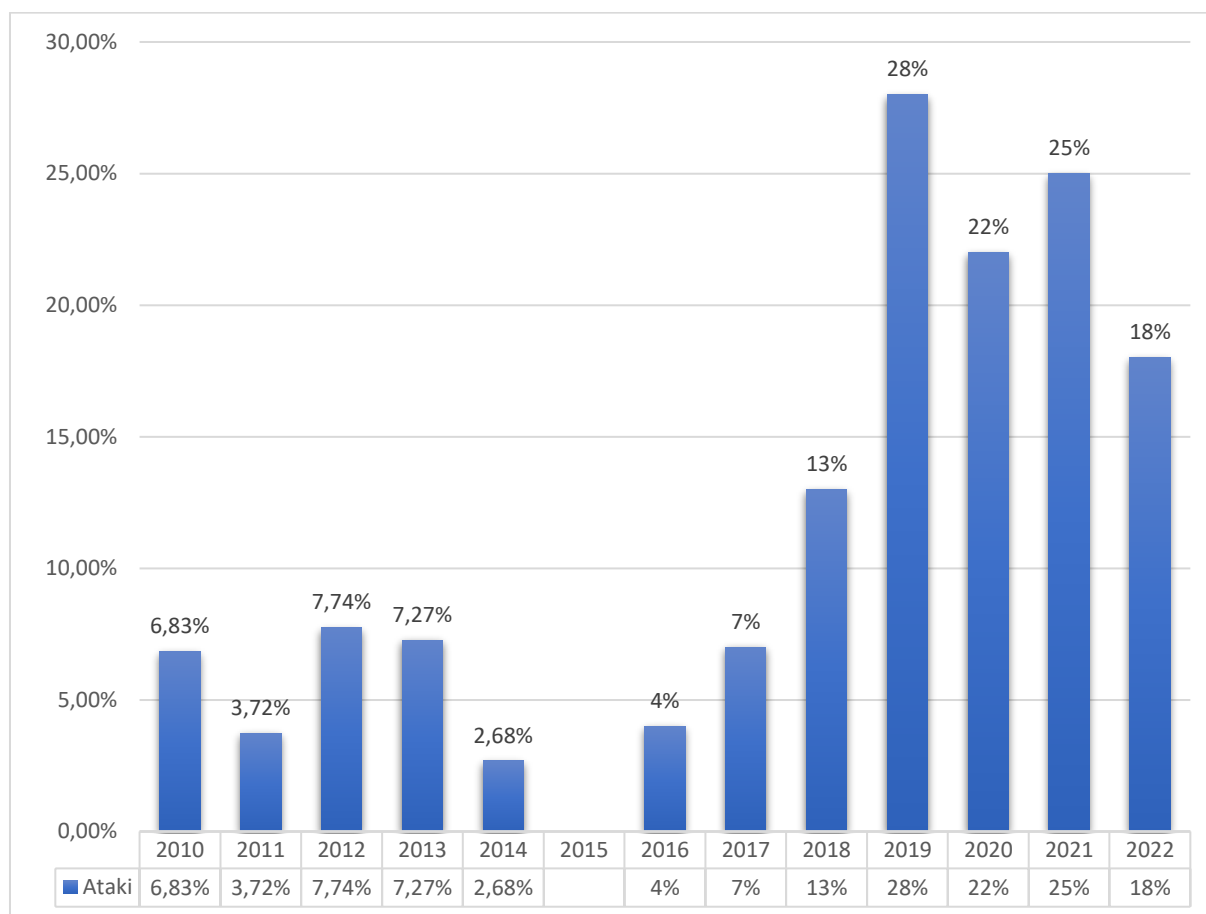


Źródło: Opracowanie własne na podstawie raportów rocznych Zespołu CSIRT GOV za lata 2020-2022.

Reasumując powyższe kwestie należy wskazać na następujące wnioski. Przede wszystkim omawiany okres, pomimo iż krótki, był szczególny w stosunkach polsko-rosyjskich, na co składała się przede wszystkim pandemia COVID-19 oraz rozpoczęcie przez Federację Rosyjską pełnowymiarowej wojny na Ukrainie. Konsekwencją tego było niespotykane dotąd zwiększenie zainteresowania Kremla polską infrastrukturą teleinformatyczną, ale również innych państw, co było szczególnie widoczne w raportach opublikowanych przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa. Rosja posiada zasoby oraz zdolności do realizowania wrogich operacji w cyberprzestrzeni, które wykorzystuje w ramach prowadzonej polityki zagranicznej. Ma to miejsce między innymi w stosunku do Polski, która stała się (szczególnie w ostatnich latach) jednym z celów ataku dla Kremla.

¹⁶⁸⁷ Raporty roczne Zespołu CSIRT GOV w zakresie analizy alarmów w sieci Internet na podstawie danych z systemu ARAKIS obejmują podział ich priorytetów na: niski, średni, wysoki, pilny.

Wykres 23. Rozkład procentowy ataków z Federacji Rosyjskiej na monitorowane przez system ARAKIS sieci w latach 2010-2022 pod kątem liczby generowanych przepływów.



Źródło: Opracowanie własne na podstawie raportów rocznych Zespołu CSIRT GOV za lata 2010-2022¹⁶⁸⁸.

Na przestrzeni lat 2010-2022 zauważalny jest postępujący wzrost zainteresowania polską infrastrukturą teleinformatyczną ze strony Kremla. Choć jego obecność zawsze była widoczna, to jednak ostatnie lata – przede wszystkim aktywność wobec sieci monitorowanych przez system ARAKIS (między innymi infrastruktury krytycznej) – pokazują, jak ważnym instrumentem w jego polityce zagranicznej jest działalność w cyberprzestrzeni. Ataki teleinformatyczne których źródłem była Rosja miały niezwykle zróżnicowanych charakter. Należy przez to rozumieć, że ich celem było nie tylko pozyskiwanie danych czy też zakłócanie

¹⁶⁸⁸ W wykresie nie zawarto danych za 2015 rok. W 2015 roku Federacja Rosyjska nie została uwzględniona w raporcie CSIRT GOV (nie znalazła się w pierwszej dziesiątce państw objętych zestawieniem). Należy jednak uwzględnić stosunkowo wysoki odsetek źródeł ataków określonych jako nieznany (2 miejsce – 21,5%), czyli z wykorzystaniem adresów IP, które nie są przypisane do żadnego podmiotu. Oznacza to, iż dokonano podmiiany prawdziwego źródłowego adresu IP. Pod takim adresem IP mogły zostać przeprowadzone cyberataki przez Federację Rosyjską, co jest wysoce prawdopodobne biorąc pod uwagę fakt, że Rosja rokrocznie znajdowała się w omawianym zestawieniu dziesięciu państw z których dokonywanych jest najwięcej cyberataków na monitorowane przez system ARAKIS sieci.

funkcjonowania infrastruktury państwa, ale również kooperowanie z prowadzonymi równolegle działaniami propagandowymi. Najważniejszymi sektorami, które stały się przedmiotem rosyjskich ataków wobec Polski w cyberprzestrzeni były w omawianym okresie administracja publiczna, infrastruktura krytyczna, przedsiębiorstwa, instytucje badawcze i edukacyjne, ale również społeczeństwo i media¹⁶⁸⁹.

Wojna informacyjna prowadzona przez Federację Rosyjską przeciwko Polsce jest zatem realizowana zarówno w oparciu o dokonywanie ataków w cyberprzestrzeni, jak i w oparciu o kampanie oddziaływania informacyjnego na odbiorców w Internecie, przy czym działania te są wobec siebie komplementarne. Rozpoczęcie przez Rosję pełnowymiarowej inwazji na Ukrainę w 2022 roku oraz wsparcie jakie zostało udzielone Kijowowi przez rząd w Warszawie, doprowadziły do nasilenia ataków przeprowadzanych przez Kreml wobec Polski w cyberprzestrzeni. Wskazuje się, że: „każdy atak w cyberprzestrzeni ma złożone cele i ma różne implikacje – społeczne, polityczne czy finansowe. Coraz częściej cyberataki wykorzystywane są w celu szerzenia rosyjskiej dezinformacji oraz służą rosyjskim służbom specjalnym do gromadzenia danych i wrażliwych informacji”¹⁶⁹⁰. W 2022 roku, poza Ukrainą, Polska była jednym z głównych celów rosyjskich cyberataków, zarówno tych o charakterze szpiegowskim jak i dezinformacyjnym¹⁶⁹¹. Warto odnotować, że omawiane incydenty w „cyberprzestrzeni to typowe dla Rosji działania odwetowe, które są odpowiedzią na niekorzystne i niewygodne dla Federacji Rosyjskiej działania innych państw. Grupy hakerskie powiązane z Kremlem wykorzystują oprogramowanie *ransomware*, DDoS i ataki *phishingowe*, a cel wrogich działań pokrywa się z celami ataku hybrydowego: destabilizacją, zastraszeniem i sianiem chaosu”¹⁶⁹². Skala zagrożenia w tych obszarach znacząco wzrasta, a w kolejnych latach należy spodziewać się nasilenia omawianych zjawisk.

Wrogie działania realizowane przez Kreml wobec Polski w cyberprzestrzeni wiążą się z kwestiami spornymi występującymi w stosunkach bilateralnych, jak również celami polityki zagranicznej Federacji Rosyjskiej. Przykładowo, rozkład procentowy ataków dokonanych z terytorium Rosji na sieci monitorowane przez system ARAKIS, poza rekordowym 2019 rokiem, był w okresie 2020-2022 nieporównywalnie większy względem lat ubiegłych¹⁶⁹³.

¹⁶⁸⁹ gov.pl: *Russian cyberattacks*. <https://www.gov.pl/web/special-services/russian-cyberattacks> (dostęp: 25.05.2023).

¹⁶⁹⁰ Ibidem.

¹⁶⁹¹ Council on Foreign Relations: *Polish Cyber Defenses and the Russia-Ukraine War*. <https://www.cfr.org/blog/polish-cyber-defenses-and-russia-ukraine-war> (dostęp: 25.05.2023).

¹⁶⁹² gov.pl: *Russian cyberattacks*. <https://www.gov.pl/web/special-services/russian-cyberattacks> (dostęp: 25.05.2023).

¹⁶⁹³ Warto odnotować, że stan ten utrzymał się w 2023 roku na poziomie 18%, a więc na takim samym jak w 2022 roku. Źródło: Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV: *Raport o stanie*

Działania Federacji Rosyjskiej intensyfikowały się wobec występujących napięć i sporów w relacjach dwustronnych, przede wszystkim dotyczących polityki bezpieczeństwa w Europie Środkowo-Wschodniej (w kontekście wojny rosyjsko-ukraińskiej¹⁶⁹⁴) oraz polityki bezpieczeństwa NATO (w kontekście wzmacniania wschodniej flanki Sojuszu oraz zwiększania obecności wojsk amerykańskich w Polsce). Rosja traktowała więc cyberprzestrzeń jako sferę rywalizacji z Polską oraz realizacji celów swojej polityki zagranicznej.

bezpieczeństwa cyberprzestrzeni RP w 2023 roku. <https://csirt.gov.pl/download/3/220/RaportostaniebezpieczenstwacyberprzestrzeniRPw2023.pdf> (dostęp: 06.02.2025), s. 83.

¹⁶⁹⁴ Warty odnotowania w omawianym kontekście jest działalność rosyjskiej grupy Killnet, która od rozpoczęcia przez Rosję pełnowymiarowej inwazji na Ukrainę w 2022 roku przeprowadziła szereg ataków na Polskę w cyberprzestrzeni. Do ich przykładów można zaliczyć atak na rządowy portal eZamówienia, Senat RP, Grupę Azoty, Centrum Zdrowia Matki Polki w Łodzi oraz strony internetowe sądów, w tym stronę Naczelnego Sądu Administracyjnego.

Rozdział 7. Portale informacyjne jako instrument wojny informacyjnej Federacji Rosyjskiej wobec Polski w latach 2010-2022

7.1. Portal informacyjny Sputnik News International jako narzędzie wojny informacyjnej Federacji Rosyjskiej wobec Polski

7.1.1. Charakterystyka portalu informacyjnego Sputnik News International

Sputnik News International¹⁶⁹⁵ to rosyjski portal informacyjny publikujący wiadomości w języku angielskim. Portal pod marką Sputnik został uruchomiony dnia 10 listopada 2014 roku¹⁶⁹⁶ przez grupę multimedialną Rossiya Segodnya¹⁶⁹⁷. Sputnik News powstał jako część wysiłków Rosji, aby zrównoważyć dominację amerykańskich i zachodnich mediów globalnych takich jak BBC, CNN, czy Reuters. Agencja miała stanowić alternatywę do zachodnich narracji i przedstawiać wydarzenia z perspektywy rosyjskiej. Nazwa *Sputnik* nawiązuje do historycznego wystrzelenia przez ZSRR pierwszego satelity sztucznego w 1957 roku, co miało symbolizować przełomową działalność Federacji Rosyjskiej w sferze technologii i komunikacji.

Jak wskazano na stronie internetowej w zakładce *About Us*, „Sputnik to nowoczesna agencja informacyjna, której produktami są kanały informacyjne, strony internetowe, sieci społecznościowe, aplikacje mobilne, audycje radiowe i multimedialne centra prasowe”¹⁶⁹⁸. Siedziba portalu zlokalizowana jest w Moskwie, jednakże w wielu miejscach na świecie znajdują się jego biura, między innymi w USA, Chinach, Francji, Niemczech, Egipcie oraz Wielkiej Brytanii. Serwisy informacyjne działają przez całą dobę, publikując wiadomości w ponad 30 językach, między innymi w angielskim, hiszpańskim, francuskim, niemieckim, arabskim i chińskim. Ponadto w językach obowiązujących w byłych państwach Związku Radzieckiego, ale również w krajach Europy Środkowo-Wschodniej¹⁶⁹⁹.

¹⁶⁹⁵ Sputnik News International. <https://sputnikglobe.com/>; <https://sputniknews.com/> (dostęp: 26.05.2023).

¹⁶⁹⁶ Choć wskazano, że portal rozpoczął swoje funkcjonowanie w 2014 roku to dla przykładu wiadomości dotyczące Polski są datowane również na lata wcześniejsze (między innymi na lata 2010-2013).

¹⁶⁹⁷ Rossiya Segodnya to grupa medialna, której właścicielem jest rząd Federacji Rosyjskiej. Dawniej Rossiya Segodnya działała pod nazwą RIA Nowosti, która była rosyjską krajową agencją informacyjną. Została zlikwidowana w 2013 roku na mocy dekretu wydanego przez Prezydenta Federacji Rosyjskiej W. Putina. Źródło: RIA: Международное агентство "Россия сегодня" создается на базе РИА Новости. <https://ria.ru/20131209/982905485.html> (dostęp: 08.03.2023).

¹⁶⁹⁸ Sputnik News International: *About Us*. <https://sputniknews.com/docs/index.html> (dostęp: 08.03.2023).

¹⁶⁹⁹ Z uwagi na zmianę struktury strony internetowej portalu, dostęp do wielu jego wersji językowych w latach 2022-2024 został ograniczony bądź zablokowany.

Agencja Sputnik posiada własną bazę zdjęć, prowadząc sprzedaż materiałów foto i wideo – Sputnik Images¹⁷⁰⁰. Jest też właścicielem przedsiębiorstwa zajmującego się badaniami opinii publicznej – Sputnik.Polls¹⁷⁰¹. Poprzednikiem Sputnik News International była państwowa agencja informacyjna RIA Novosti¹⁷⁰² oraz radio Voice of Russia¹⁷⁰³, które zostały rozwiązane w 2013 roku¹⁷⁰⁴.

Sputnik News International, będąc podmiotem zależnym od rządu Federacji Rosyjskiej¹⁷⁰⁵, publikuje treści zgodne z oficjalnym przekazem propagandowym płynącym z Kremla. Poruszane treści obejmują niezwykle szeroką tematykę, między innymi polityczną, militarną, gospodarczą, społeczną czy kulturalną. Treści publikowane przez portal mają wymiar krajowy, regionalny oraz globalny, komentując i odnosząc się w zasadzie do wszystkich państw na świecie¹⁷⁰⁶.

Portal publikuje stosunkowo dużą liczbę wiadomości dotyczących lub odnoszących się do Polski. Przy użyciu wyszukiwarki znajdującej się na witrynie portalu oraz na podstawie słowa *Poland* ustalono, iż w latach 2010-2022 opublikowano łącznie 10.734 artykuły, które dotyczyły bezpośrednio lub pośrednio Polski. Dla porównania po przeprowadzeniu wyszukiwaniu w analogiczny sposób, przy czym na podstawie wyrazu *Ukraine*, wyodrębniono 43.553 artykuły, przy użyciu wyrazu *Germany* 38.557 artykułów, a słowa *France* 37.931 artykułów. Zdecydowanie najwięcej artykułów można wyodrębnić za pomocą sformułowania *United States*, gdyż aż 123.936¹⁷⁰⁷. Powyższe może oznaczać, że Polska nie zajmuje istotnego miejsca, jeśli chodzi o działalność portalu i poruszaną tematykę, niemniej jednak liczba opublikowanych artykułów nadal jest znacząca.

Portal Sputnik News International, jako podmiot związany z Kremlen i od niego zależny, został zaklasyfikowany jako podmiot kolportujący propagandę¹⁷⁰⁸. Stało się to przyczyną objęcia go sankcjami przez kraje członkowskie Unii Europejskiej w skutek których

¹⁷⁰⁰ Sputnik Images. <https://sputnikmediabank.com/> (dostęp: 08.03.2023).

¹⁷⁰¹ Sputnik.Polls. https://sputniknews.com/sputnik_polls_2016/ (dostęp: 08.03.2023).

¹⁷⁰² W 2014 roku marka RIA Nowosti została ponownie zarejestrowana w Federacji Rosyjskiej, stając się częścią agencji (grupy medialnej) Rossiya Segodnya. Publikowane treści są kierowane do odbiorców rosyjskojęzycznych. Źródło: RIA Nowosti. <https://ria.ru/> (dostęp: 08.03.2023).

¹⁷⁰³ Voice of Russia został zastąpiony przez Radio Sputnik, które stanowi część portalu Sputnik News International, zarządzanego przez właściciela – agencję Rossiya Segodnya. Źródło: Radio Sputnik. <https://radiosputnik.ria.ru/> (dostęp: 08.03.2023).

¹⁷⁰⁴ Sputnik News International: *About Us*. <https://sputniknews.com/docs/index.html> (dostęp: 08.03.2023).

¹⁷⁰⁵ Właścicielem marki Sputnik jest agencja Rossiya Segodnya, której to właścicielem jest rząd Federacji Rosyjskiej.

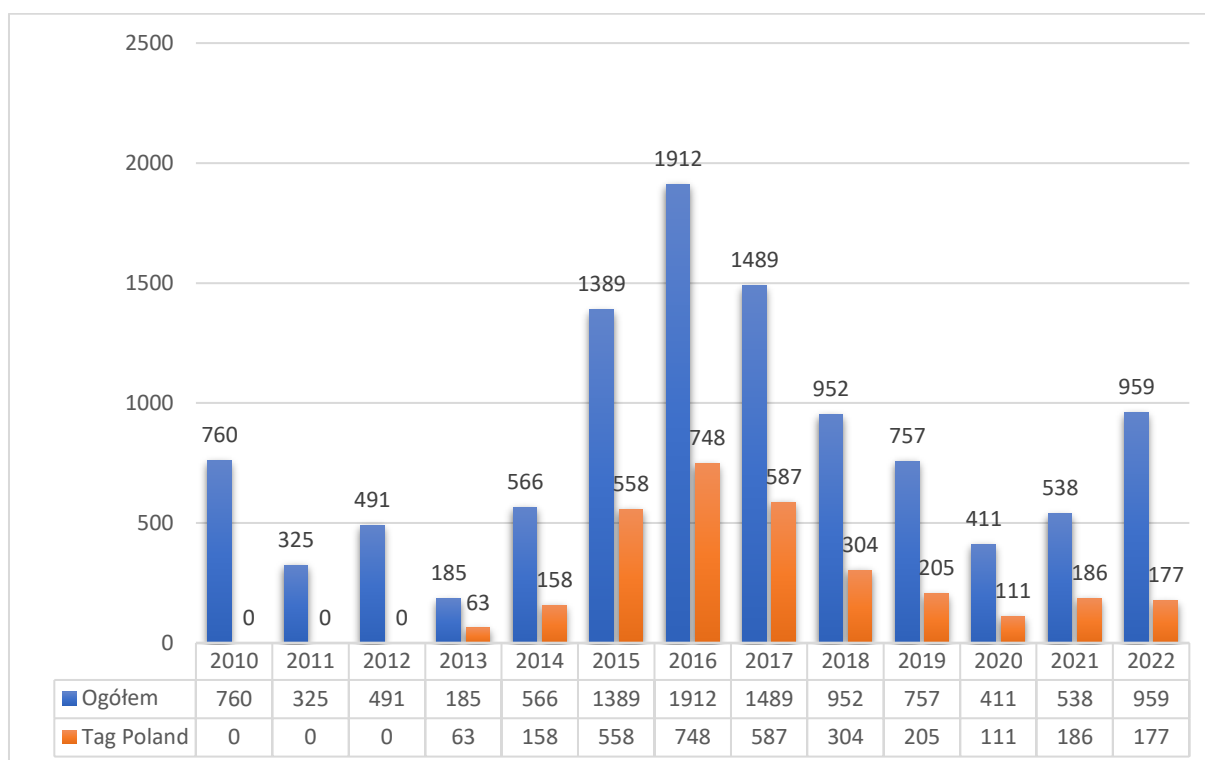
¹⁷⁰⁶ Sputnik News International. <https://sputniknews.com/> (dostęp: 08.03.2023).

¹⁷⁰⁷ Sputnik News International: *Search*. <https://sputniknews.com/search/?query=> (dostęp: 07.03.2023).

¹⁷⁰⁸ U.S. Department of State: *Report: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem*. <https://www.state.gov/report-rt-and-sputniks-role-in-russias-disinformation-and-propaganda-ecosystem/> (dostęp: 24.05.2023).

nałożono blokadę na dystrybucję publikowanych przez niego treści. Sankcje miały swój bezpośredni związek z rosyjską pełnowymiarową agresją na Ukrainę, do której doszło w 2022 roku¹⁷⁰⁹.

Wykres 24. Liczba indywidualnych wiadomości (artykułów) na portalu informacyjnym Sputnik News International wyodrębnionych przy użyciu wyszukiwarki witryny na podstawie słowa *Poland* z podziałem na zawierające tag o nazwie *Poland* oraz ogółem w latach 2010-2022.



Źródło: Opracowanie własne na podstawie wyników uzyskanych z wyszukiwarki przy użyciu wyrazu *Poland* na portalu informacyjnym Sputnik News International¹⁷¹⁰.

Analizując powyższy wykres można zauważyć, że koreluje on ze stanem stosunków polsko-rosyjskich na przestrzeni lat 2010-2022. W 2010 roku miała miejsce katastrofa smoleńska, co w sposób oczywisty spowodowało zwiększone występowanie tematyki dotyczącej Polski. Następnie w kolejnych latach liczba artykułów waha się w przedziale od

¹⁷⁰⁹ European Council, Council of the European Union: *EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU*. <https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rt-russia-today-and-sputnik-s-broadcasting-in-the-eu/> (dostęp: 08.03.2023); CyberDefence24: *RT i Sputnik oficjalnie zablokowane w UE. Za wdrożenie sankcji odpowiedzialne kraje członkowskie*. <https://cyberdefence24.pl/polityka-i-prawo/rt-i-sputnik-oficjalnie-zablokowane-w-ue-za-wdrozenie-sankcji-odpowiedzialne-kraje-czlonkowskie> (dostęp: 08.03.2023).

¹⁷¹⁰ Sputnik News International: *Search*. <https://sputniknews.com/search/?query=Poland> (dostęp: 10.03.2023).

około 200 do około 500. Od 2014 roku, a więc od aneksji Półwyspu Krymskiego liczba artykułów systematycznie wzrasta, by osiągnąć apogeum w 2016 roku, kiedy to miał miejsce szczyt NATO w Warszawie. Następnie liczba publikowanych artykułów z roku na rok maleje, by w 2022 roku widocznie wzrosnąć, co z kolei ma związek z rozpoczętą wojną rosyjsko-ukraińską. We wszystkich wskazanych wyżej wydarzeniach ścierały się interesy polityki zagranicznej Federacji Rosyjskiej z interesami Polski. To z kolei doprowadziło do zwiększenia liczby publikowanych artykułów, które odnosiły się do tej tematyki.

Warto odnotować, że w związku z ograniczeniem dostępności (na obszarze państw członkowskich Unii Europejskiej) portalu Sputnik News International działającego pod domeną sputniknews.com, uruchomiono bliźniaczą wersję serwisu pod domeną sputnikglobe.com celem uniknięcia blokady wskutek nałożonych sankcji. Od 2023 roku portal funkcjonuje wyłącznie pod drugą ze wskazanych domen¹⁷¹¹. Warto również odnotować, iż od 2023 roku można zaobserwować zmiany w strukturze witryny oraz jej działaniu. Przejawiają się one przede wszystkim w wyłączeniu znacznej części witryn publikujących wiadomości w językach państw Europy Środkowo-Wschodniej, w tym Polski (Sputnik News Polska¹⁷¹²). Może to wskazywać na trudności portalu w omijaniu nałożonych sankcji i w konsekwencji publikowaniu treści, ale również na możliwą zmianę kanałów oddziaływania informacyjnego. Skoro bowiem państwa europejskie, w tym Polska, podjęły intensywne działania zmierzające do całkowitego zablokowania dostępności portalu, to prawdopodobne jest, że Federacja Rosyjska dokona zmian w zakresie realizowanych kampanii informacyjnych.

7.1.2. Typy publikowanych treści na portalu informacyjnym Sputnik News International

Zgodnie z przyjętymi założeniami metodologicznymi zrealizowano badania, które obejmowały 358 wyodrębnionych artykułów, opublikowanych na portalu Sputnik News International na przestrzeni lat 2010-2022. Przyjęte do badań artykuły wyodrębniono w oparciu o wyraz *Poland*, spośród 10.734 ogólnej ich liczby (zawierających wyraz *Ponad*)¹⁷¹³.

Z przeprowadzonych badań wynika, że dominującymi typami treści które są publikowane na portalu informacyjnym Sputnik News International, są treści o charakterze politycznym, militarnym oraz społecznym. Pierwsze z nich wyróżniają się w sposób szczególny, gdyż wystąpiły w aż 311 artykułach spośród 358 wyodrębnionych do badań, co

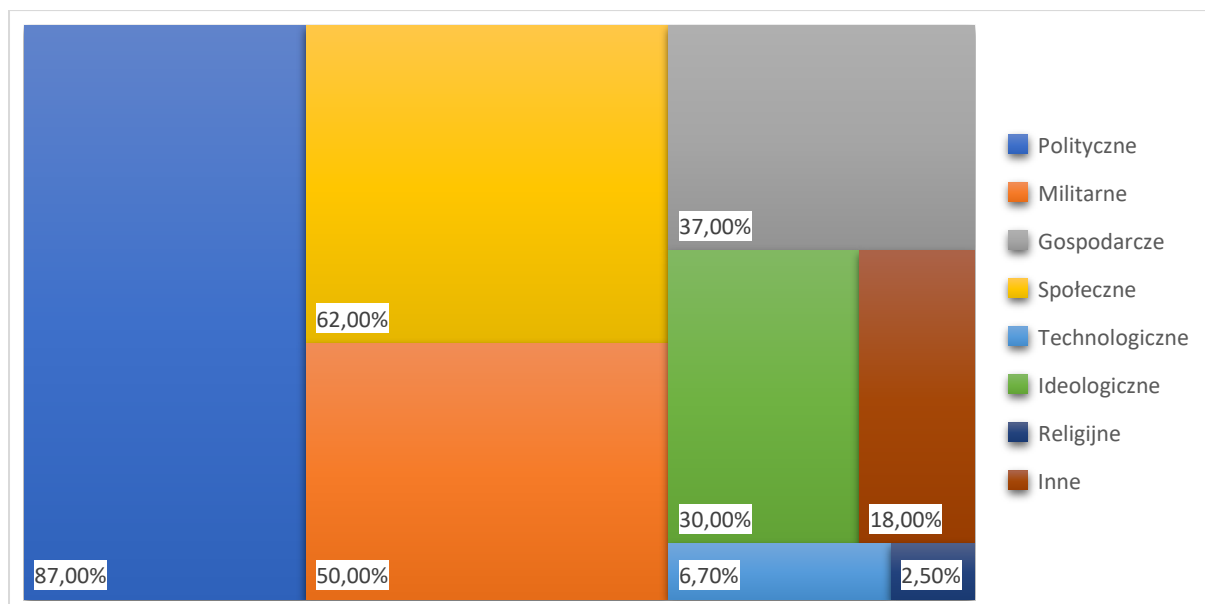
¹⁷¹¹ Sputnik News International. <https://sputnikglobe.com/> (dostęp: 26.05.2023).

¹⁷¹² Sputnik News Polska. <https://pl.sputniknews.com/> (dostęp: 01.02.2022).

¹⁷¹³ Szczegółowe założenia w zakresie przeprowadzonych badań zawarto w rozdziale metodologicznym.

stanowi prawie 87% tej liczby. Treści o charakterze politycznym występowały najczęściej wspólnie z treściami o charakterze społecznym, które pojawiły się 192 razy (około 62%) oraz treściami militarnymi, które zidentyfikowano 179 razy (50%). Zauważalne były również treści o charakterze gospodarczym, które zaobserwowano w przypadku 131 artykułów (około 37%) oraz ideologiczne w przypadku 106 artykułów (około 30%). Najrzadziej występowały treści technologiczne, tj. w 24 artykułach (6,7%) oraz religijne w 9 artykułach (około 2,5%). Wyraźnie zauważalne były treści niemieszczące się w żadnej z powyższych kategorii, tj. inne, które wystąpiły 64 razy, a więc w około 18% artykułów. Dotyczyły one takich zagadnień jak: prawo międzynarodowe publiczne, polskie oraz unijne (14 razy), sport (11 razy), szpiegostwo (9 razy), EURO 2012 (9 razy), kultura (7 razy), historia¹⁷¹⁴ (5 razy), propaganda (3 razy), media (3 razy) oraz zdrowie (2 razy). Ponadto odnotowano jednostkowe przypadki treści dotyczących niemieckiego złotego pociągu w województwie dolnośląskim, powodzi, pomoru świń w Polsce oraz dzikich zwierząt, które wtargnęły na płytę lotniska. Co ciekawe, w latach 2020-2021 treści dotyczące pandemii wywołanej wirusem SARS-CoV-2, występowały w publikowanych artykułach w stopniu marginalnym.

Wykres 25. Procentowe występowanie poszczególnych typów treści w artykułach opublikowanych na portalu informacyjnym Sputnik News International w latach 2010-2022.



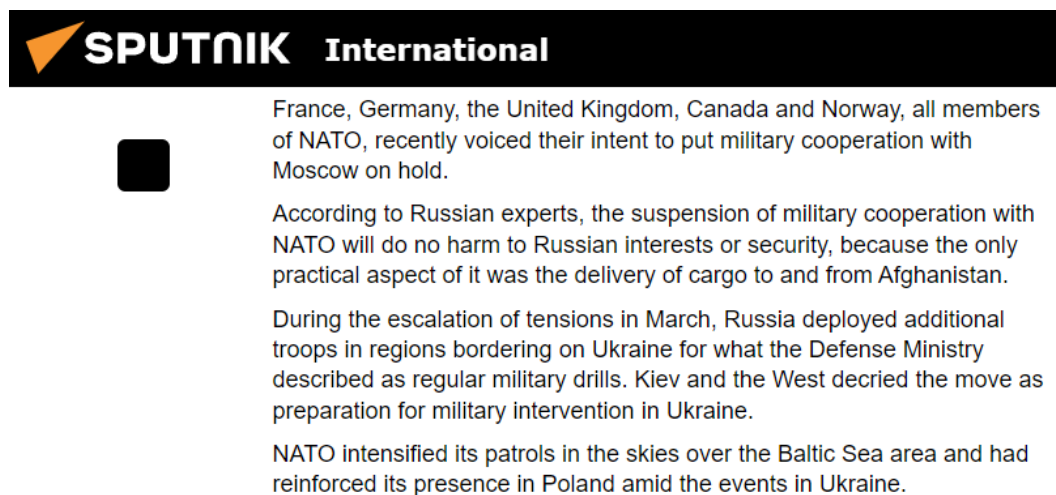
Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

¹⁷¹⁴ Tematyka historyczna nie dotycząca stosunków polsko-rosyjskich.

Nasycenie artykułów poszczególnymi typami treści w badanym okresie było zmienne, lecz nie korespondowało ze stanem stosunków polsko-rosyjskich, jaki występował w danym czasie. Oznacza to, że artykuły w których zidentyfikowano jeden bądź dwa typy treści, jak również cztery bądź pięć typów treści, występowały przez cały badany okres, z podobnym natężeniem. Nie można wyróżnić więc okresu, w którym treści o konkretnym typie występowały szczególnie często bądź rzadko. Treści o charakterze politycznym, z wyjątkiem kilku przypadków, występowały w zasadzie zawsze wraz z innymi typami treści, głównie typem militarnym, gospodarczym, społecznym lub ideologicznym. Jeśli w danym artykule treści polityczne nie występowały, to bardzo często taki artykuł był klasyfikowany w kategorii *inne*.

Z przeprowadzonych badań można wyprowadzić wniosek, że treści publikowane przez portal Sputnik News International są skoncentrowane głównie na polityce, przede wszystkim międzynarodowej, a w widocznie mniejszej części na polityce wewnętrznej. Jeśli natomiast dany artykuł poruszał już treści o charakterze wewnątrzpaństwowym, to dotyczyły one co do zasady wydarzeń budzących ożywioną debatę w Polsce. Zauważalne było również to, że treści dotyczące stosunków międzynarodowych odnosiły się przede wszystkim do wydarzeń, których uczestnikiem w sposób bezpośredni bądź pośredni, była lub jest Federacja Rosyjska.

Zdjęcie 1.



Źródło: Sputnik News International¹⁷¹⁵.

¹⁷¹⁵ Sputnik News International: *NATO Suspends All Practical Cooperation with Russia – Statement*. <https://sputnikglobe.com/20140402/NATO-Suspends-All-Practical-Coooperation-with-Russia---Statement-188973288.html> (dostęp: 02.12.2024). Tłumaczenie własne: Francja, Niemcy, Wielka Brytania, Kanada i Norwegia, wszyscy członkowie NATO, niedawno wyrazili zamiar zawieszenia współpracy wojskowej z Moskwą. Według rosyjskich ekspertów, zawieszenie współpracy wojskowej z NATO nie zaszkodzi rosyjskim interesom ani bezpieczeństwu, ponieważ jedynym praktycznym aspektem tej współpracy był transport ładunków

Zdjęcie 2.



Stoltenberg requested a meeting with the US President "well in advance," the expert underscored. Obama's move could only be considered as an obvious slight to Jens Stoltenberg: the US President is one of a few Western leaders who have yet to meet with the NATO chief, who assumed the position almost six months ago.

However, Obama has demonstrated disinterest in the US' European allies many times before. For instance, in November 2009, Barack Obama opted out of holding a meeting with European Union leaders at the White House sparking speculations that British Prime Minister Gordon Brown and French President Nicolas Sarkozy, one of the most pro-American French leaders, felt like they were being ignored.

Remarkably, a year later the American President once again missed a summit with the EU leaders.

In September 2009, during a so-called "reset" of relations with Moscow, Barack Obama changed his plans of deploying a missile defense system in Poland and the Czech Republic, but did not bother to inform his eastern European counterparts about his decision.

David J. Karl cited a top Polish security official who said that Warsaw heard Obama had shifted the plan though the media.

Źródło: Sputnik News International¹⁷¹⁶.

Treści o charakterze społecznym odznaczały się również niezwykle dużym zainteresowaniem autorów artykułów publikowanych na portalu Sputnik News International. Prezentowały przede wszystkim problemy i konflikty natury społecznej występujące w Polsce,

do i z Afganistanu. Podczas eskalacji napięć w marcu, Rosja rozmieszczała dodatkowe wojska w regionach graniczących z Ukrainą, co Ministerstwo Obrony określiło jako regularne ćwiczenia wojskowe. Kijów i Zachód potępiły ten ruch jako przygotowania do interwencji wojskowej na Ukrainie. NATO zintensyfikowało patrolowanie przestrzeni powietrznej nad obszarem Morza Bałtyckiego i wzmocniło swoją obecność w Polsce w związku z wydarzeniami na Ukrainie.

¹⁷¹⁶ Sputnik News International: *US-EU 'Transatlantic Renaissance' Plan Falling Apart at Seams*. <https://sputnikglobe.com/20150402/1020387992.html> (dostęp: 01.12.2024). Tłumaczenie własne: Stoltenberg z wyprzedzeniem poprosił o spotkanie z prezydentem USA, podkreślił ekspert. Działanie Obamy można uznać za oczywiste lekceważenie Jensa Stoltenberga: prezydent USA jest jednym z niewielu zachodnich przywódców, którzy jeszcze nie spotkali się z szefem NATO, który objął stanowisko prawie sześć miesięcy temu. Jednak Obama wielokrotnie wykazywał brak zainteresowania europejskimi sojusznikami USA. Na przykład w listopadzie 2009 roku Barack Obama zrezygnował z organizacji spotkania z przywódcami Unii Europejskiej w Białym Domu, co wywołało spekulacje, że premier Wielkiej Brytanii Gordon Brown i prezydent Francji Nicolas Sarkozy, jeden z najbardziej proamerykańskich francuskich przywódców, czuli się ignorowani. Co ciekawe, rok później amerykański prezydent ponownie opuścił szczyt z przywódcami UE. We wrześniu 2009 roku, podczas tzw. "resetu" stosunków z Moskwą, Barack Obama zmienił plany dotyczące rozmieszczenia systemu obrony przeciwrakietowej w Polsce i Czechach, ale nie zadał sobie trudu, aby poinformować o swojej decyzji wschodnioeuropejskich partnerów. David J. Karl przytoczył wypowiedź wysokiego rangą polskiego urzędnika ds. bezpieczeństwa, który powiedział, że Warszawa dowiedziała się o zmianie planów Obamy za pośrednictwem mediów.

ale i w innych państwach w Europie. Znakomita ich część odnosiła się do zjawiska migracji, z którym to problemem boryka się od 2015 roku Unia Europejska.

Treści militarne, które w następnej kolejności pojawiały się najczęściej w publikowanych artykułach, sprowadzały się przede wszystkim do omawiania programów zbrojeniowych w poszczególnych państwach, doktryn militarnych, relacji na linii Waszyngton-Kreml, bezpieczeństwa militarnego Europy Środkowo-Wschodniej, polityki bezpieczeństwa NATO oraz aneksji Półwyspu Krymskiego (2014) oraz pełnowymiarowej inwazji Rosji na Ukrainę (2022).

Poniższe zdjęcie przedstawia przykład podważania suwerenności Ukrainy oraz negowania w związku z tym możliwości jej członkostwa w Sojuszu Północnoatlantyckim. Autentyczność i waga tego stanowiska jest legitymizowana przez autorów artykułu faktem, że sformułowanie to zostało wypowiedziane przez jednego z deputowanych niemieckiego parlamentu – Bundestagu.

Zdjęcie 3.



Źródło: Sputnik News International¹⁷¹⁷.

Treści gospodarcze odnosiły się w przeważającej części do zagadnień dotyczących dostaw surowców energetycznych z Federacji Rosyjskiej do Polski oraz innych krajów członkowskich Unii Europejskiej, jak i problemów z tym związanych. Zauważalne były tutaj liczne nawiązania do budowy gazociągów Nord Stream I oraz Nord Stream II. Ponadto, kwestie dotyczące problemów z dostawami surowców energetycznych do Polski i innych państw bardzo często przedstawiano w kontekście Ukrainy, tj. poprzez obwinianie za ów stan rzeczy rządu w Kijowie i prowadzonej przez niego polityki.

¹⁷¹⁷ Sputnik News International: *Ukraine's Membership in NATO is Impossible – German Media*. <https://sputnikglobe.com/20150424/1021324562.html> (dostęp: 02.12.2024). Tłumaczenie własne: Ukraina nie może zostać członkiem NATO w obecnych warunkach, ponieważ jej suwerenność jest ograniczona. Członkostwo Ukrainy w NATO jest niemożliwe w obecnych warunkach – powiedział deputowany Bundestagu Roder Kiesewetter w rozmowie z Deutsche Welle.

Zdjęcie 4.



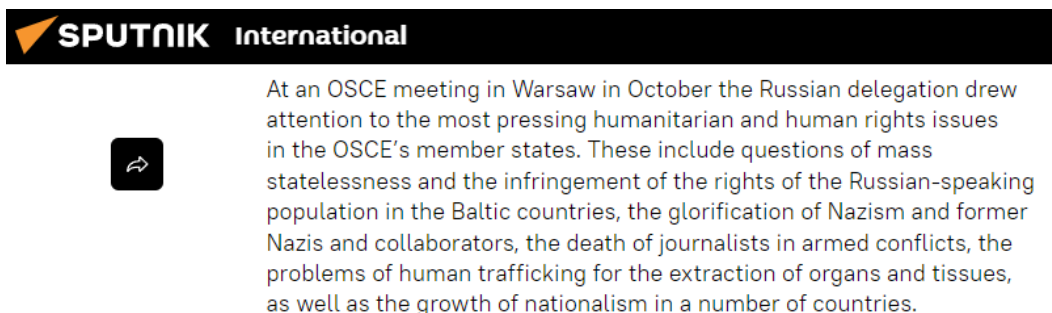
Źródło: Sputnik News International¹⁷¹⁸.

Treści ideologiczne pojawiły się w około 1/3 zbadanych artykułów. Co ciekawe, nie dotyczyły one ideologii komunistycznej (radzieckiej), będącej dla Federacji Rosyjskiej spuścizną po Związku Socjalistycznych Republik Radzieckich, lecz sprowadzały się do krytykowania wartości i ideologii zachodnich. Nacisk kładziono więc na ich krytykę, a nie na propagowanie własnych ideologii. Wielokrotnie pojawiały się wzmianki informujące o łamaniu przez państwa zachodnie (w tym Polskę) praw człowieka, które jednocześnie są przez nie tak powszechnie propagowane. Wskazywano również na występujące na Zachodzie nurty neonazistowskie i neofaszystowskie z którymi walczy Federacja Rosyjska i co też czynił Związek Radziecki podczas II wojny światowej. Ponadto nawiązywano do współpracy rządów zachodnich z rządem w Kijowie, który określano mianem faszystowskiego lub nazistowskiego. Można zauważyć, że narracja ta ma uzasadnić rosyjską operację realizowaną na Ukrainie i ukazać ją jako słuszną, jak również skojarzyć z działaniami podejmowanymi przez ZSRR wobec III Rzeszy podczas II wojny światowej (Wielką wojną ojczyźnianą¹⁷¹⁹). Podkreślano również występowanie w państwach członkowskich NATO i Unii Europejskiej postawy antyrosyjskiej, a nawet rusofobicznej, która może przejawiać się w niechęci do wszelkiej współpracy z Rosją, a także w negatywnym postrzeganiu jej działań na arenie międzynarodowej.

¹⁷¹⁸ Sputnik News International: *Russian Gas More Profitable Than US LNG, Ex-Austrian Envoy Says as Denmark Hampers Nord Stream 2*. <https://sputnikglobe.com/20191026/russian-gas-nord-stream-2-project-1077157248.html> (dostęp: 02.12.2024). Tłumaczenie własne: Były ambasador Austrii w Rosji Friedrich Bauer ostrzegł, że kraje UE mogą zapłacić cenę za porzucenie projektu gazociągu Nord Stream 2 na „obecnym etapie”. Według niego dostawy gazu ziemnego z Rosji są o wiele bardziej opłacalne niż amerykański skroplony gaz ziemny (LNG), biorąc pod uwagę, że blok musiałby zbudować w pełni rozwiniętą infrastrukturę dla dostaw z USA. Bauer zauważył, że rosyjski gaz jest tańszy i lepszy pod względem jakości i że jest „wystarczająco czysty”.

¹⁷¹⁹ Znaczenie tego wydarzenia w polityce zagranicznej Federacji Rosyjskiej zostało omówione we wcześniejszych częściach rozprawy.

Zdjęcie 5.



Źródło: Sputnik News International¹⁷²⁰.

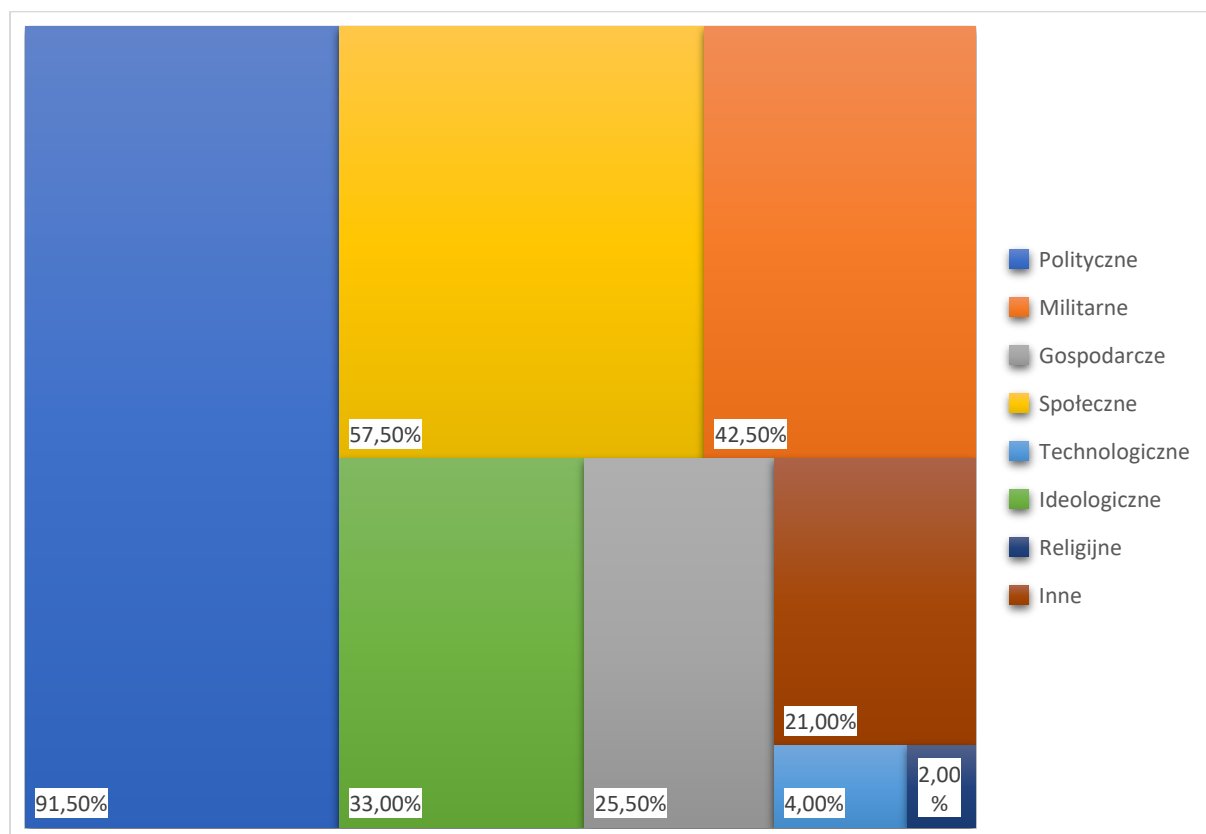
Wreszcie należy wskazać, że nie wszystkie spośród wyodrębnionych artykułów swoją treścią odnosiły się bezpośrednio do Polski. Bardzo często pojawiały się bowiem jedynie wzmianki o niej w kontekście relacji bilateralnych Federacji Rosyjskiej z innym podmiotem, przede wszystkim USA oraz Unią Europejską.

Spośród 358 artykułów przyjęty do badań, 106 z nich zostało oznaczonych przez ich autorów *tagiem* o nazwie *Poland*. Jako, że takie działanie nie jest z pewnością przypadkowe, warto zawęzić w tym kierunku wyniki badań. I tak ze wskazanej liczby 106 artykułów, 97 dotyczyło treści o charakterze politycznym (91,5%), 61 treści społecznych (57,5%), 45 treści militarnych (42,5%), 35 treści ideologicznych (33%), 27 treści gospodarczych (25,5%), 4 treści technologicznych (około 4%) oraz 2 treści religijnych (około 2%). Ponadto 22 artykuły (około 21%) dotyczyły innych treści niż wskazane powyżej. Odnosiły się one do prawa (9 razy), historii (4 razy), mediów (3 razy), szpiegostwa (2 razy), sportu (2 razy) oraz jednokrotnie do kwestii środowiskowych i zdrowotnych oraz *niemieckiego złotego pociągu z czasów II wojny światowej*, rzekomo odnalezionego na Dolnym Śląsku. Należy jednak zauważyć, że oznaczanie artykułów dotyczących Polski wskazanym powyżej *tagiem*, rozpoczęło się dopiero w 2013 roku i dotyczyło w tym czasie zaledwie dwóch artykułów, spośród wszystkich wyodrębnionych do badań. W 2014 roku było to już 7 artykułów, w 2015 roku oznaczono 21 artykułów, a w 2016 roku 25 z nich. Od 2017 roku liczba oznaczeń wskazanym *tagiem* zaczęła spadać wynosząc 16, następnie w 2018 roku 15, w 2019 roku 5, w 2020 roku 4, w 2021 roku 6 oraz w 2022 roku

¹⁷²⁰ Sputnik News International: *No Need for OSCE Monitoring of Entire Russian-Ukrainian Border: Moscow*. <https://sputnikglobe.com/20141202/1015394575.html> (dostęp: 01.12.2024). Tłumaczenie własne: Podczas spotkania OBWE w Warszawie w październiku rosyjska delegacja zwróciła uwagę na najpilniejsze kwestie humanitarne i dotyczące praw człowieka w państwach członkowskich OBWE. Obejmują one zagadnienia masowego bezpieczeństwa oraz naruszania praw ludności rosyjskojęzycznej w krajach bałtyckich, gloryfikacji nazizmu oraz byłych nazistów i kolaborantów, śmierci dziennikarzy w konfliktach zbrojnych, problemów handlu ludźmi w celu pozyskiwania organów i tkanek, a także wzrostu nacjonalizmu w wielu krajach.

5 razy. Częstotliwość oznaczania artykułów *tagiem Poland*, nie koreluje więc z wydarzeniami mającymi miejsce ówczesnie w stosunkach polsko-rosyjskich.

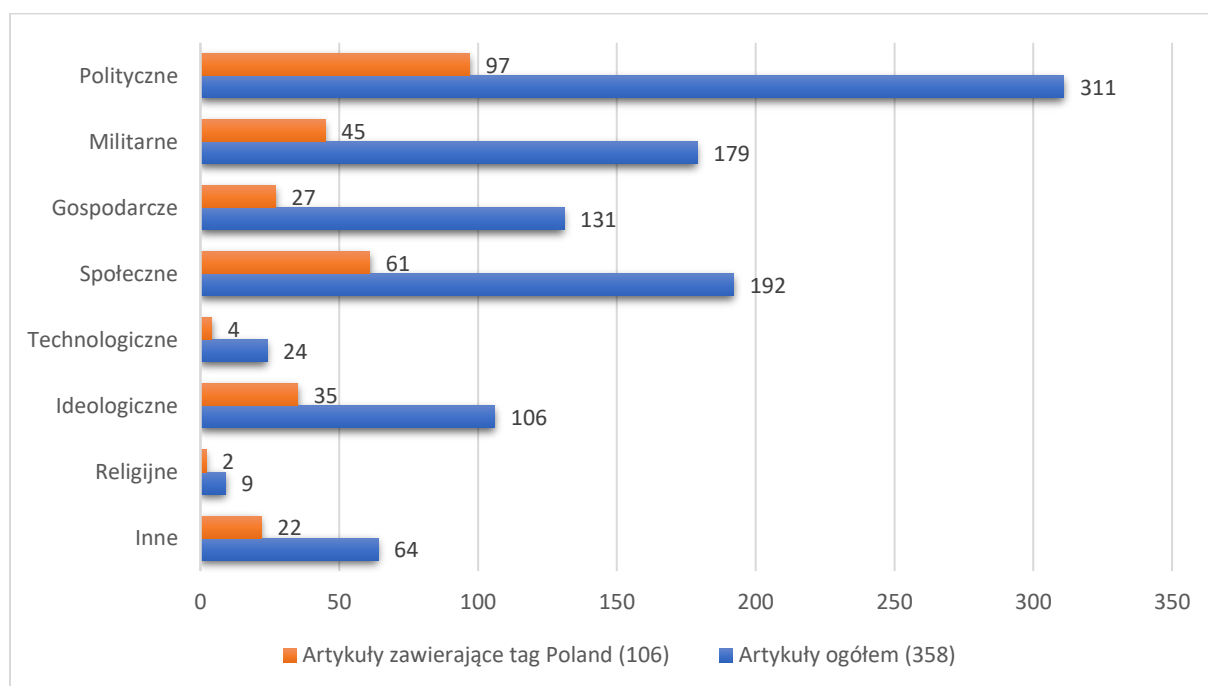
Wykres 26. Procentowe występowanie poszczególnych typów treści w artykułach zawierających tag o nazwie *Poland* opublikowanych na portalu informacyjnym Sputnik News International w latach 2010-2022.



Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

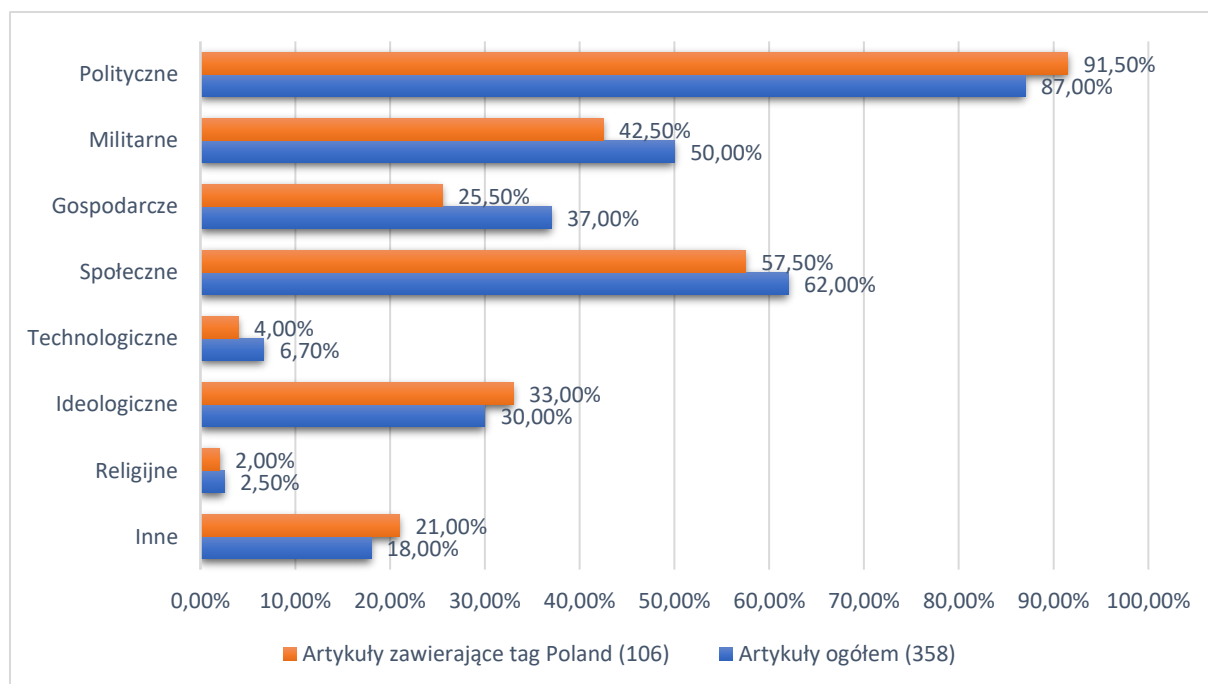
Poniżej przedstawiono wykres przedstawiający liczbę zidentyfikowanych typów treści w 358 wyodrębnionych do badań artykułach. W ramach wykresu uwzględniono również artykuły, które zawierają się w powyższej liczbie, lecz zostały oznaczone dodatkowo *tagiem* o nazwie *Poland*, przez ich autorów. Z badań wynika, że częstotliwość występowania w nich poszczególnych typów treści, co do zasady, nie uległa zmianie. Nadal najczęściej występującymi treściami są treści polityczne, następnie treści społeczne, później militarne i kolejno ideologiczne, gospodarcze, technologiczne oraz religijne. Jedynym wyjątkiem są treści ideologiczne, które wystąpiły częściej, niż treści gospodarcze.

Wykres 27. Typy treści w artykułach opublikowanych na portalu informacyjnym Sputnik News International w latach 2010-2022.



Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

Wykres 28. Procentowe występowanie poszczególnych typów treści w artykułach opublikowanych na portalu informacyjnym Sputnik News International w latach 2010-2022.



Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

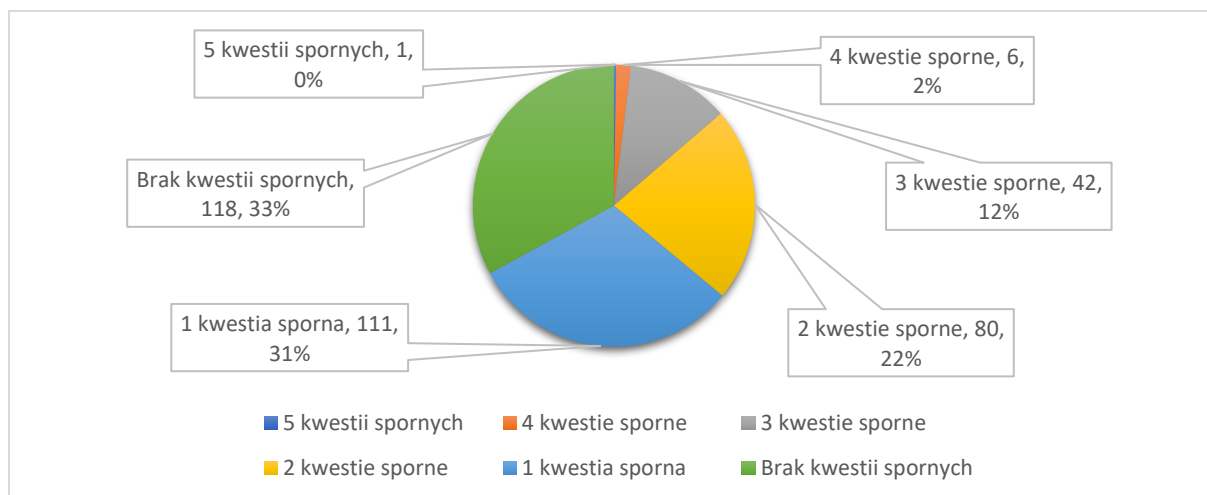
Konkludując należy zauważyć, że artykuły publikowane przez portal informacyjny Sputnik News International korelują z polityką zagraniczną Federacji Rosyjskiej wobec Polski. Zamieszczane na nim treści mają przede wszystkim charakter polityczny, który wielokrotnie nawiązuje do stosunków bilateralnych na linii Warszawa-Moskwa. W zainteresowaniu autorów artykułów znajdują się również treści o charakterze militarnym oraz społecznym, które niezwykle często współwystępowały z tymi o charakterze politycznym. W mniejszym stopniu publikowane są treści o charakterze gospodarczym i ideologicznym. Można również zauważyć, że typy publikowanych treści w artykułach ogółem (358) pokrywają się co do zasady z artykułami, które zawierają *tag* o nazwie *Poland* (106). Niemniej jednak więcej jest tu treści o charakterze politycznym i ideologicznym względem ogółu artykułów. Najważniejszym wnioskiem jest, iż publikowane treści pokrywają się ze stanowiskiem jakie na określone sprawy prezentuje Kreml w realizowanej przez siebie polityce zagranicznej. Sputnik News International jest więc ukierunkowany w swojej działalności na prezentowanie przede wszystkim rosyjskiego punktu widzenia. Wniosek ten potwierdza fakt, iż portal jest zależny od rosyjskiego rządu, na co wskazano w poprzednim podrozdziale. Podkreślić również należy, że publikowane materiały w wielu przypadkach nie dotyczyły bezpośrednio Polski, i stosunków polsko-rosyjskich, lecz były zestawiane ze sprawami odnoszącymi się do Unii Europejskiej, NATO, państw europejskich oraz Stanów Zjednoczonych Ameryki.

7.1.3. Polsko-rosyjskie kwestie sporne w treściach publikowanych na portalu informacyjnym Sputnik News International

W ramach założeń metodologicznych przyjęto następujące kwestie sporne występujące w stosunkach polsko-rosyjskich, takie jak: polityka historyczna, dywersyfikacja źródeł energii, polityka bezpieczeństwa w Europie Środkowo-Wschodniej, polityka bezpieczeństwa NATO, katastrofa samolotu rządowego z Prezydentem Rzeczypospolitej Polskiej w Smoleńsku, aneksja Półwyspu Krymskiego i wojna w Ukrainie oraz program Partnerstwa Wschodniego¹⁷²¹. Spośród 358 poddanych badaniom artykułów opublikowanych na portalu informacyjnym Sputnik News International, aż 118 z nich nie poruszało żadnej ze wskazanych wyżej kwestii spornych. 111 artykułów poruszało jedną kwestię sporną, 80 artykułów dwie kwestie sporne, 42 artykuły trzy kwestie sporne, 6 artykułów cztery kwestie sporne, a pięć kwestii spornych poruszał tylko 1 artykuł.

¹⁷²¹ Zobacz szerzej w rozdziale metodologicznym.

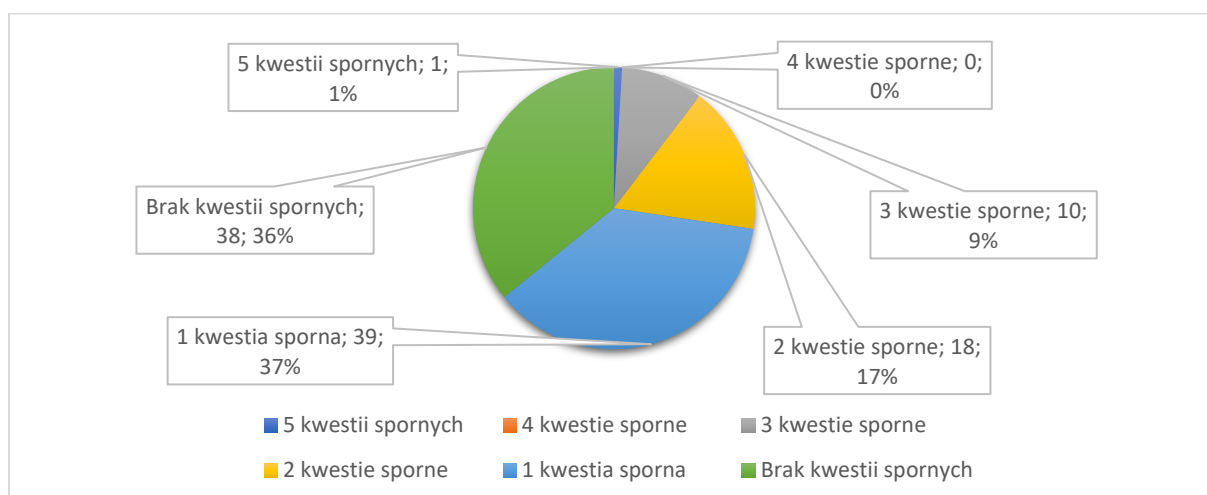
Wykres 29. Liczba zidentyfikowanych kwestii spornych w stosunkach polsko-rosyjskich w artykułach opublikowanych na portalu informacyjnym „Sputnik News International” w latach 2010-2022.



Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

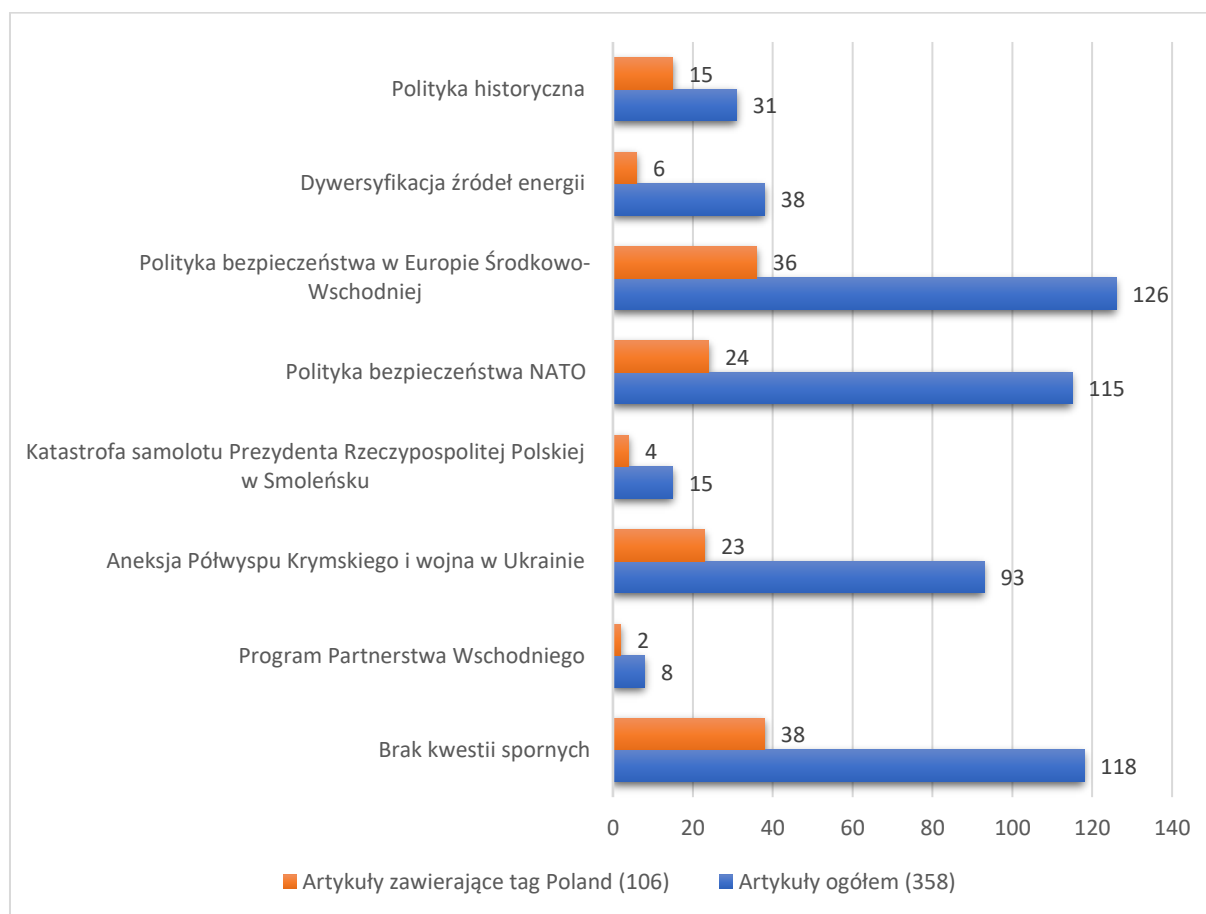
Podobne wyniki otrzymano w przypadku badań nad artykułami, zawierającymi *tag* o nazwie *Poland*, gdzie żadna kwestia sporna nie wystąpiła w przypadku 38 artykułów, 39 odniosło się tylko do jednej, 18 do dwóch, 10 do trzech, do czterech nie odniósł się żaden artykuł, a do pięciu wyłącznie 1.

Wykres 30. Liczba zidentyfikowanych kwestii spornych w stosunkach polsko-rosyjskich w artykułach zawierających *tag* o nazwie *Poland* opublikowanych na portalu informacyjnym Sputnik News International w latach 2010-2022.



Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

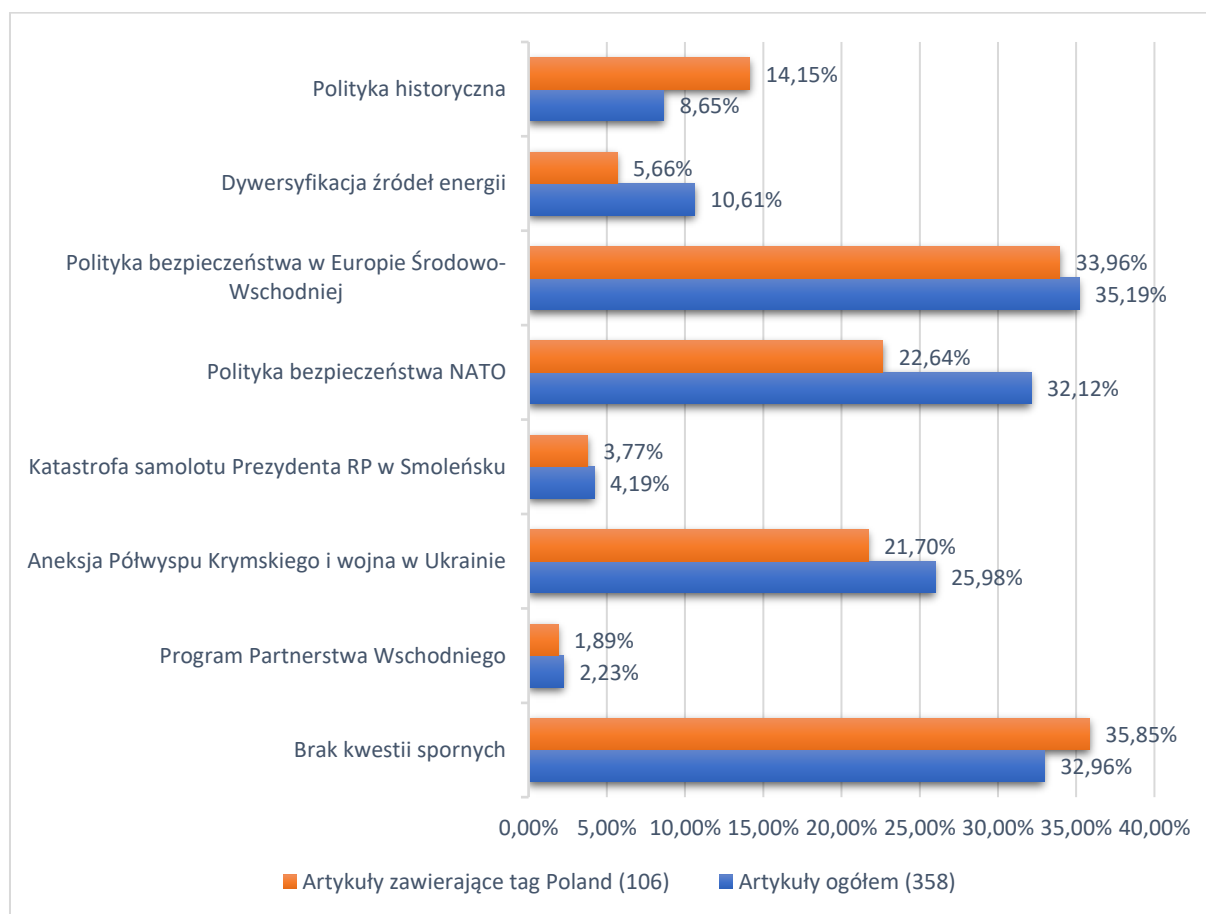
Wykres 31. Liczba zidentyfikowanych kwestii spornych w stosunkach polsko-rosyjskich w artykułach opublikowanych na portalu informacyjnym Sputnik News International w latach 2010-2022.



Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

Analizując powyższy wykres można zauważyć, że Rosjanie priorytetowo traktują kwestie dotyczące polityki bezpieczeństwa w Europie Środkowo-Wschodniej, polityki bezpieczeństwa NATO oraz aneksji Półwyspu Krymskiego i wojny na Ukrainie. Na tych tematach koncentrują swoją działalność z zakresu oddziaływania informacyjnego na odbiorców w Internecie. Taki wniosek potwierdza fakt, że wymienione kwestie pojawiają się stosunkowo często w wypowiedziach decydentów politycznych na Kremlu. Pozostają zatem w ścisłym związku z realizowaną przez Federację Rosyjską polityką zagraniczną. W interesie Moskwy jest bowiem kształtowanie określonej narracji oraz wizji na wskazane kwestie sporne występujące w stosunkach polsko-rosyjskich.

Wykres 32. Procentowe występowanie poszczególnych kwestii spornych w stosunkach polsko-rosyjskich w artykułach opublikowanych na portalu informacyjnym Sputnik News International w latach 2010-2022.



Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

Artykuły w których nie poruszono żadnej kwestii spornej, czy to oznaczone *tagiem Poland*, czy też nim nieoznaczone, dotyczyły takich zagadnień jak historia (z wyłączeniem stosunków polsko-rosyjskich), migracja, polityka wewnętrzna w Polsce, prawo, Brexit oraz szpiegostwo. Tak liczne występowanie artykułów w których nie zidentyfikowano żadnej kwestii spornej niekoniecznie musi wynikać z niewielkiego zainteresowania ich autorów Polską. Jak już bowiem wskazano, wiele z wyodrębnionych do badań artykułów zgodnie z przyjętym doborem próby badawczej jedynie wspominało o Polsce czasem wyłącznie jednym zdaniem. Oznacza to, że Polska pojawia się w publikowanych treściach, jednak nie dotyczą jej one zawsze bezpośrednio. Co więcej, występowanie określonej liczby kwestii spornych w danym artykule (bądź ich braku), zasadniczo nie korelowało z nasileniem stosowania przez autorów artykułów technik propagandowych. Z kolei z przeprowadzonych badań można już

wyprowadzić wniosek, że poruszane w danym czasie kwestie sporne, korelowały z aktualnymi wydarzeniami występującymi w ramach stosunków polsko-rosyjskich.

Najczęściej pojawiającą się kwestią sporną w publikowanych artykułach była polityka bezpieczeństwa w Europie Środkowo-Wschodniej, która wystąpiła w nich 126 razy. Wielokrotnie występowała ona łącznie z drugą i trzecią najczęściej występującą kwestią sporną. Pierwsza z nich to polityka bezpieczeństwa NATO, która pojawiła się w artykułach 115 razy, natomiast druga to aneksja Półwyspu Krymskiego i wojna na Ukrainie, którą zidentyfikowano 93 razy. Bardzo często poruszanym tematem, w ramach kwestii spornych w stosunkach polsko-rosyjskich, dotyczących polityki bezpieczeństwa w Europie Środkowo-Wschodniej oraz polityki bezpieczeństwa NATO, była budowa w Polsce elementów amerykańskiej tarczy antyrakietowej. Pomimo, iż ówczesny prezydent USA B. Obama zrezygnował z planów jej budowy w 2009 roku, to kwestia ta nadal pozostawała obecna w rosyjskim przekazie przede wszystkim w kontekście braku gwarancji dla Moskwy, iż system ten nie będzie skierowany przeciwko Federacji Rosyjskiej. Można było wręcz odnieść wrażenie, że Rosja postrzegała stanowisko USA w tym zakresie jako chwilowe, które w niedalekiej przyszłości ulegnie zmianie. Być może dlatego uznano, że dalsze kolportowanie tych treści jest konieczne.

Zdjęcie 6.



Źródło: Sputnik News International¹⁷²².

¹⁷²² Sputnik News International: *NATO Forces in Eastern Europe May Lead to Endless War, Hostilities – Expert*. <https://sputnikglobe.com/20140828/NATO-Forces-in-Eastern-Europe-May-Lead-to-Endless-War-192413930.html> (dostęp: 01.12.2024). Tłumaczenie własne: Siły NATO w Europie Wschodniej mogą prowadzić do niekończącej się wojny i działań wojennych - Ekspert. Rozmieszczenie sił NATO w nowych bazach w Europie Wschodniej otwiera nowe możliwości niekończącej się wojny i działań wojennych, powiedziała RIA Novosti nowojorska dyrektorka Nuclear Age Peace Foundation (NAPF) Alice Slater.

W 2014 roku, w którym doszło do aneksji Półwyspu Krymskiego przez Federację Rosyjską, publikowane artykuły dotyczyły w dużej części zwiększania obecności NATO, głównie USA, na wschodniej flance Sojuszu. Takie działania postrzegano i prezentowano jako powiększanie przez Sojusz swojej strefy wpływów kosztem Federacji Rosyjskiej. Wzrost zainteresowania polityką bezpieczeństwa NATO nastąpił po raz kolejny w 2016 roku wraz ze zorganizowanym w tym czasie szczytem Sojuszu w Warszawie. Od tego momentu można zaobserwować stałą i postępującą w kolejnych latach intensyfikację występowania w publikowanych treściach tej kwestii spornej. W odniesieniu do Ukrainy, tematyka z nią związana pojawiała się zasadniczo przez cały badany okres, lecz intensywnie dopiero od 2014 roku, przy czym w 2022 roku można było zaobserwować jej kumulację, co miało związek z rozpoczętą w tym czasie pełnowymiarową inwazją Federacji Rosyjskiej na to państwo.

Zdjęcie 7.



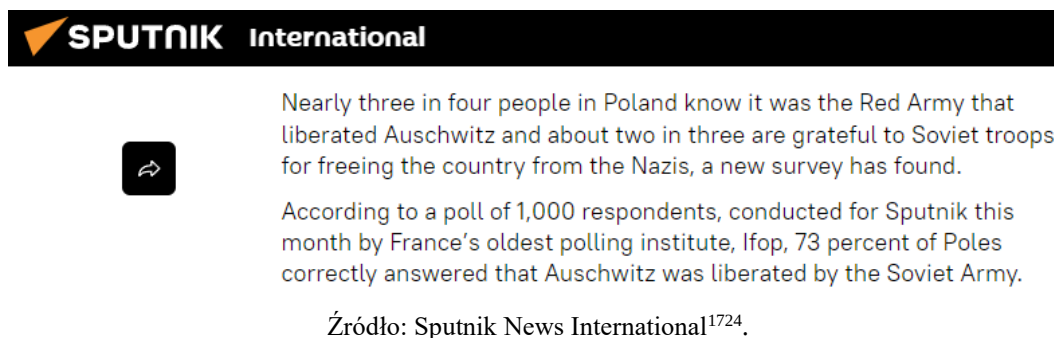
Źródło: Sputnik News International¹⁷²³.

W odniesieniu do polityki historycznej można wskazać na ciekawy wniosek, iż w wyodrębnionych do badań artykułach pojawiła się ona zaledwie 31 razy, co stanowi niecałe 10% spośród wszystkich 358 artykułów poddanych badaniom. Wskazana kwestia sporna pojawiała się w pierwszych latach badanego okresu oraz cyklicznie przy okazji ważniejszych wydarzeń (rocznie) związanych z II wojną światową. Publikowane treści przede wszystkim oskarżały polski rząd o fałszowanie historii poprzez przypisywanie ZSRR współodpowiedzialności, wraz z III Rzeszą, za rozpoczęcie konfliktu oraz prowadzenie działań zmierzających do usunięcia z terytorium Polski miejsc pamięci odwołujących się do bohaterskiej walki Armii Czerwonej. Widoczne były również artykuły nie dotyczące

¹⁷²³ Sputnik News International: *Defense or Delusion? The Hidden Motives Behind NATO's East European Buildup*. <https://sputnikglobe.com/20160517/nato-eastern-europe-buildup-political-show-1039748414.html> (dostęp: 01.02.2024). Tłumaczenie własne: Nadchodzący szczyt NATO w lipcu w Warszawie z pewnością zatwierdzi rozmieszczenie dodatkowego kontyngentu elitarnych wojsk NATO w Europie Wschodniej. Jednak wszyscy zdają się doskonale rozumieć, że siły wysokiej gotowości NATO to nic więcej niż symboliczna jednostka „bańki mydlanej”, która pęknie natychmiast po wybuchu działań wojennych.

bezpośrednio polityki historycznej Polski oraz Rosji, lecz wspominające o roli Niemiec w konflikcie oraz sporach historycznych pomiędzy Warszawą a Berlinem, które były inicjowane przede wszystkim przez Polskę (sprawa reparacji wojennych).

Zdjęcie 8.



Zdjęcie 9.



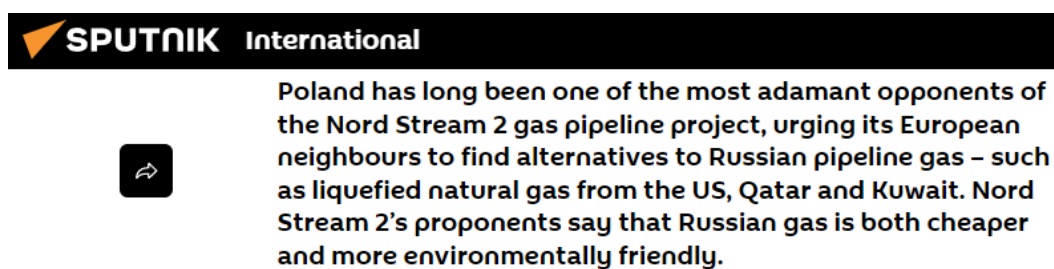
Kwestia sporna dotycząca dywersyfikacji źródeł energii na przestrzeni lat 2010-2022 koncentrowała się przede wszystkim na imporcie surowców energetycznych z Federacji Rosyjskiej do Polski oraz innych państw członkowskich Unii Europejskiej rurociągami biegnącymi przez terytorium Ukrainy, jak również przedsięwzięciem dotyczącym budowy gazociągów Nord Stream I i Nord Stream II. Omawiana kwestia sporna w poddanych badaniom

¹⁷²⁴ Sputnik News International: *Three in Four Poles Know Soviet Troops Liberated Auschwitz, New Poll Shows*. <https://sputnikglobe.com/20200221/auschwitz-most-ipoles-know-well-soviet-army-liberated-nazis-biggest-death-camp-1078365690.html> (dostęp: 01.02.2024). Tłumaczenie własne: Prawie trzy na cztery osoby w Polsce wiedzą, że to Armia Czerwona wyzwoliła Auschwitz, a około dwie na trzy są wdzięczne wojskom radzieckim za wyzwolenie kraju spod okupacji nazistowskiej, jak wynika z nowego sondażu. Według sondażu przeprowadzonego w tym miesiącu dla Sputnika przez najstarszy francuski instytut sondażowy Ifop, wśród 1000 respondentów, 73 procent Polaków prawidłowo odpowiedziało, że Auschwitz zostało wyzwolone przez Armię Radziecką.

¹⁷²⁵ Sputnik News International: *WWII History Falsification Among Europe's Most Pressing Political Issues - Russian Envoy*. <https://sputnikglobe.com/20200129/wwii-history-falsification-among-europes-most-pressing-political-issues---russian-envoy-1078175428.html> (dostęp: 01.02.2024). Tłumaczenie własne: PARYŻ (Sputnik) - Dążenie Kijowa i Warszawy do przepisania historii II wojny światowej jest jednym z najpoważniejszych problemów politycznych współczesnej Europy, powiedział w środę w Rosyjskim Centrum Nauki i Kultury w Paryżu Aleksander Kuzniecowa, stały delegat Rosji przy UNESCO.

artykułach pojawiała się relatywnie rzadko, podobnie jak polityka historyczna. W badanym okresie wystąpiła bowiem zaledwie 38 razy. Trzeba podkreślić, że niezwykle często problemy związane z dostawami surowców energetycznych z Rosji do innych państw (w tym Polski), były zestawiane z działalnością rządu w Kijowie, którego rzekoma wroga polityka wobec Moskwy miała być zasadniczym powodem związanych tym trudności oraz wszelkich negatywnych następstw. W istocie narracja ta sprowadzała się niejednokrotnie do stwierdzenia, że za wszelkie problemy związane z dostawą surowców energetycznych odpowiada Kijów, a nie Moskwa. Kwestie dotyczące problemów z dostawami surowców energetycznych (ropa naftowa i gaz ziemny) przez terytorium ukraińskie są również omawiane na kanwie stosunków polsko-ukraińskich, co ma na celu przede wszystkim ich antagonizację w sferze społeczno-politycznej.

Zdjęcie 10.



Źródło: Sputnik News International¹⁷²⁶.

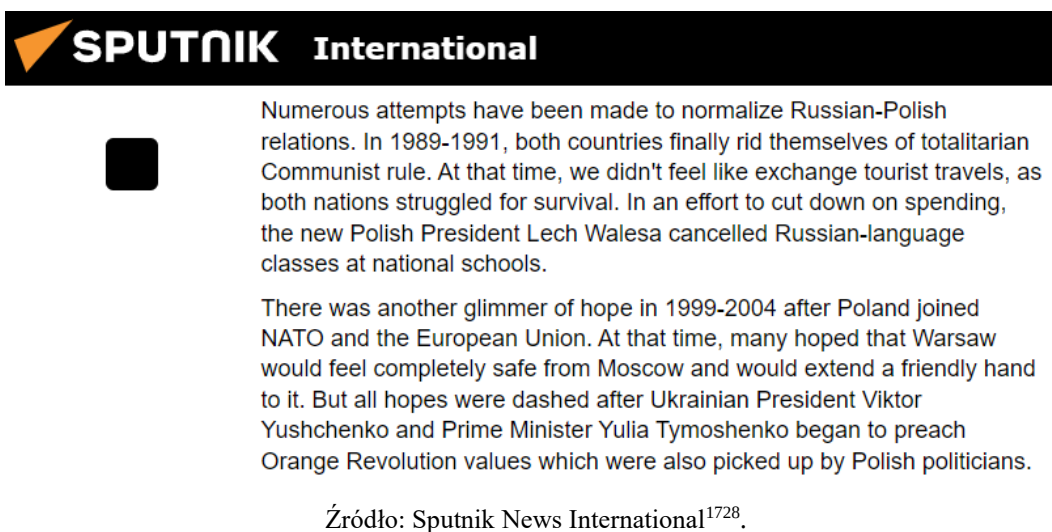
Dokonując analizy treści artykułów dotyczących katastrofy samolotu rządowego z Prezydentem Rzeczypospolitej Polskiej w Smoleńsku w 2010 roku, można dostrzec stonowaną rosyjską narrację, która nie koresponduje z ówczesnymi poglądami wielu badaczy i publicystów, wieszczącymi nowe otwarcie i reset w relacjach na linii Kreml-Warszawa. Z czasem, wobec pojawiających się napięć w stosunkach polsko-rosyjskich dotyczących tej kwestii spornej, narracja zmieniła się, skupiając na kreowaniu wizerunku Polski jako państwa winnego katastrofie oraz obwinianiu polskiego rządu za zmarnowanie szansy na poprawę relacji bilateralnych.

¹⁷²⁶ Sputnik News International: *Russian Embassy in Berlin Brushes Off Polish Envoy's Claim Nord Stream 2 Will Fund Russian Army*. <https://sputnikglobe.com/20210327/russian-embassy-in-berlin-brushes-off-polish-envoys-claim-nord-stream-2-will-fund-russian-army-1082466992.html> (dostęp: 01.02.2024). Tłumaczenie własne: Polska od dawna jest jednym z najbardziej zagorzałych przeciwników projektu gazociągu Nord Stream 2, zachęcając swoich europejskich sąsiadów do poszukiwania alternatyw dla rosyjskiego gazu rurociągowego – takich jak skroplony gaz ziemny z USA, Kataru i Kuwejtu. Zwolennicy Nord Stream 2 twierdzą, że rosyjski gaz jest zarówno tańszy, jak i bardziej przyjazny dla środowiska.

Zdjęcie 11.



Zdjęcie 12.



Ciekawym wnioskiem z przeprowadzonych badań jest stopień zainteresowania autorów artykułów na portalu Sputnik News International katastrofą smoleńską, a w zasadzie jego brak. Na przestrzeni bowiem 13 lat oraz w 358 wyodrębnionych do badań artykułach temat ten pojawił się łącznie zaledwie 15 razy, z czego 7 razy w 2010 roku i 4 razy w 2011 roku.

¹⁷²⁷ Sputnik News International: *A new page in Russian-Polish relations after a dark epilogue*. <https://sputnikglobe.com/20100412/158544992.html> (dostęp: 01.12.2024). Tłumaczenie własne: Komorowski, dysydent i krytyk rosyjskich przywódców, w ciągu ostatnich kilku lat prezentował realistyczne stanowisko, podczas gdy członkowie Sejmu, którzy wykazywali najmniej uległości w stosunku do Rosji, ostatnio stracili swoje stanowiska. Tradycyjnie centralnym elementem polskiego systemu politycznego jest Sejm, a nie Prezydent. Mijamy więc nadzieję, że w przeciwieństwie do lat 90. i 2000. Rosja i Polska nawiążą teraz bardziej udane relacje.

¹⁷²⁸ Ibidem. Tłumaczenie własne: Podejmowano liczne próby normalizacji stosunków rosyjsko-polskich. W latach 1989-1991 oba kraje ostatecznie uwolniły się od totalitarnych rządów komunistycznych. W tym czasie nie czuliśmy się jak turyści na wymianie, ponieważ oba narody walczyły o przetrwanie. W celu ograniczenia wydatków nowy prezydent Polski Lech Wałęsa odwołał zajęcia z języka rosyjskiego w szkołach państwowych. Kolejny promyk nadziei pojawił się w latach 1999-2004, po przystąpieniu Polski do NATO i Unii Europejskiej. W tym czasie wielu miało nadzieję, że Warszawa poczuje się całkowicie bezpieczna przed Moskwą i wyciągnie do niej przyjazną dłoń. Ale wszystkie nadzieje legły w gruzach, gdy prezydent Ukrainy Wiktor Juszczenko i premier Julia Tymoszenko zaczęli głosić wartości pomarańczowej rewolucji, które podchwycili również polscy politycy.

Następnie dopiero w 2015 roku 2 razy oraz jednokrotnie w 2016 i 2017 roku. W kolejnych latach, tj. aż do 2022 roku, w artykułach wyodrębnionych do badań, katastrofa polskiego samolotu z Prezydentem Rzeczypospolitej Polskiej na pokładzie pozostaje w zasadzie niezauważalna. Co jeszcze ciekawsze, w latach 2010-2022 zainteresowanie powyższym zdarzeniem było na porównywalnym poziomie jak zainteresowanie tematyką sportową. Sport w publikowanych treściach w badanym okresie pojawił się 13 razy, z czego w 9 przypadkach dotyczył on odbywającego się w 2012 roku turnieju piłkarskiego Euro w Polsce i na Ukrainie¹⁷²⁹. Nie wydaje się możliwe, aby Rosjanie, mając świadomość skali podziałów polityczno-społecznych wywoływanych w Polsce przez omawiane zdarzenie, zrezygnowali z jego wykorzystania w ramach realizowanych kampanii z zakresu oddziaływania informacyjnego. W ocenie autora czynią to, lecz prawdopodobnie z wykorzystaniem innych kanałów lub technik oddziaływania na odbiorców, co wydaje się dużo bardziej prawdopodobne, mając również na względzie dotychczas przeprowadzone badania w poprzednich rozdziałach niniejszej rozprawy.

Najrzadziej poruszaną kwestią sporną w stosunkach polsko-rosyjskich spośród przyjętych do badań był Program Partnerstwa Wschodniego. Został on zidentyfikowany tylko 8 razy, co stanowi około 2% spośród łącznej liczby przyjętych do badań artykułów. Można więc wyprowadzić wniosek, że Program Partnerstwa Wschodniego ma marginalne znaczenie dla Federacji Rosyjskiej, która koncentrowała się przede wszystkim na kwestiach spornych o podłożu militarnym. Program Partnerstwa Wschodniego pojawił się w artykułach opublikowanych w latach 2010-2016 oraz jeden raz pośrednio, w kontekście wojny na Ukrainie w 2022 roku. Dodatkowo analizując treść artykułów w których owa kwestia sporna się pojawiła, można wskazać, że nie stanowiła ona jego głównego tematu, a raczej występowała w charakterze drobnej wzmianki.

Na koniec należy również zauważyć, że Polska w publikowanych artykułach była niezwykle często identyfikowana nie jako pojedyncze państwo, lecz kraj członkowski takich organizacji międzynarodowych jak Unia Europejska oraz Sojusz Północnoatlantycki. Oznacza to, że problematyka relacji bilateralnych na linii Warszawa-Moskwa była wpisywana w szerszy kontekst, obejmując swym zakresem stosunki Kremla ze wskazanymi organizacjami międzynarodowymi. Taka perspektywa pokazuje, że polityka zagraniczna Rosji wobec Polski

¹⁷²⁹ Duże zainteresowanie turniejem Euro 2012 organizowanym w Polsce i Ukrainie nie wydaje się być zaskakujące, biorąc pod uwagę fakt, że cztery lata wcześniej, reprezentacja piłkarska Federacji Rosyjskiej zajęła trzecie miejsce na Euro 2008. Wynik ten z pewnością wzbudził emocje i zainteresowanie piłką nożną w Rosji, co przełożyło się z kolei na częstsze publikacje na ten temat.

nie jest już tylko kwestią relacji dwustronnych, lecz częścią bardziej złożonych procesów decyzyjnych na poziomie europejskim i transatlantyckim.

Mając na względzie powyższe należy wskazać na następujące wnioski. Bardzo duża część, bo aż $\frac{2}{3}$ z wyodrębnionych do badań artykułów, odnosiła się w swojej treści do co najmniej jednej kwestii spornej występujących w stosunkach polsko-rosyjskich. Pozwala to na wyprowadzenie twierdzenia, że portal Sputnik News International jest zaangażowany w działalność Kremla nakierowaną na Polskę, co należy powiązać z zależnością portalu od rosyjskiej władzy. Najczęściej występujące kwestie sporne to polityka bezpieczeństwa w Europie Środkowo-Wschodniej, polityka bezpieczeństwa NATO oraz aneksja Półwyspu Krymskiego i wojna na Ukrainie. Wskazane tematy przez cały badany okres pozostawały w żywotnym zainteresowaniu Federacji Rosyjskiej w zakresie realizowanej przez nią polityki zagranicznej, a więc ich liczne występowanie w treściach publikowanych przez portal stanowi potwierdzenie tego faktu. Polska pozostaje ważnym aktorem w ramach wszystkich wskazanych wyżej kwestii spornych, stąd też nie powinno dziwić ich nasilone występowanie w wyodrębnionych do badań artykułach.

Podobnie bowiem ma to miejsce w przypadku artykułów oznaczonych *tagiem Poland* w których występowanie powyższych kwestii było na podobnym poziomie. Zauważyć jednak należy, że poza wskazanymi tematami zauważalnie większą wagę przykładano do polityki historycznej, która wystąpiła w przypadku około 14% artykułów, natomiast w ich ogóle (358) było to już około 8%. Zmalało z kolei zainteresowanie kwestią dywersyfikacji źródeł energii, które w ogóle artykułów wyniosło około 10%, natomiast w przypadku artykułów z *tagiem Poland* już tylko około 5%. Katastrofa samolotu rządowego z Prezydentem Rzeczypospolitej Polskiej w Smoleńsku oraz Program Partnerstwa Wschodniego pozostawały na tym samym poziomie. Należy jednak zauważyć, że w przypadku pierwszego ze wskazanych wydarzeń, było ono stosunkowo rzadko poruszane w ramach publikowanych treści, gdyż wystąpiło tylko w około 4% z nich. Może to wskazywać na małe znaczenie tej kwestii spornej w stosunkach bilateralnych. Wydaje się, że taki wniosek jest prawidłowy, gdyż katastrofa smoleńska jest wydarzeniem kontestowanym zdecydowanie częściej w ramach polityki wewnętrznej Polski, aniżeli zewnętrznej w kontekście stosunków polsko-rosyjskich. Ciekawym jest również fakt, niezwykle rzadkiego występowania kwestii dotyczącej Programu Partnerstwa Wschodniego, który jest skierowany do państw znajdujących się w bezpośredniej strefie wpływów Federacji Rosyjskiej. Wydaje się więc, że Kreml nie postrzega działań Unii Europejskiej w tym zakresie jako zagrożenia.

7.1.4. *Framing* treści na portalu informacyjnym Sputnik News International

Na potrzeby badań przyjęto następujące rodzaje *framingu*, tj. pozytywny, neutralny oraz negatywny¹⁷³⁰. Spośród wszystkich zbadanych artykułów, w 11 z nich zidentyfikowano *framing* pozytywny, w 209 neutralny, a w 138 negatywny. Można więc wyprowadzić wniosek, że Polska nie jest prezentowana w publikacjach na portalu Sputnik News International, jak by się mogło wydawać, jednoznacznie w sposób negatywny, gdyż ponad połowa spośród 358 artykułów cechuje się neutralnym wydźwiękiem. Należy jednak zauważyć, że jak już wspomniano, w wielu z ogółu wyodrębnionych do badań artykułach Polska była jedynie wzmiankowana. W związku z tym w wielu takich artykułach nie zauważono używania słów wartościowanych pozytywnie albo negatywnie i na tej podstawie klasyfikowano takie treści jako neutralne.

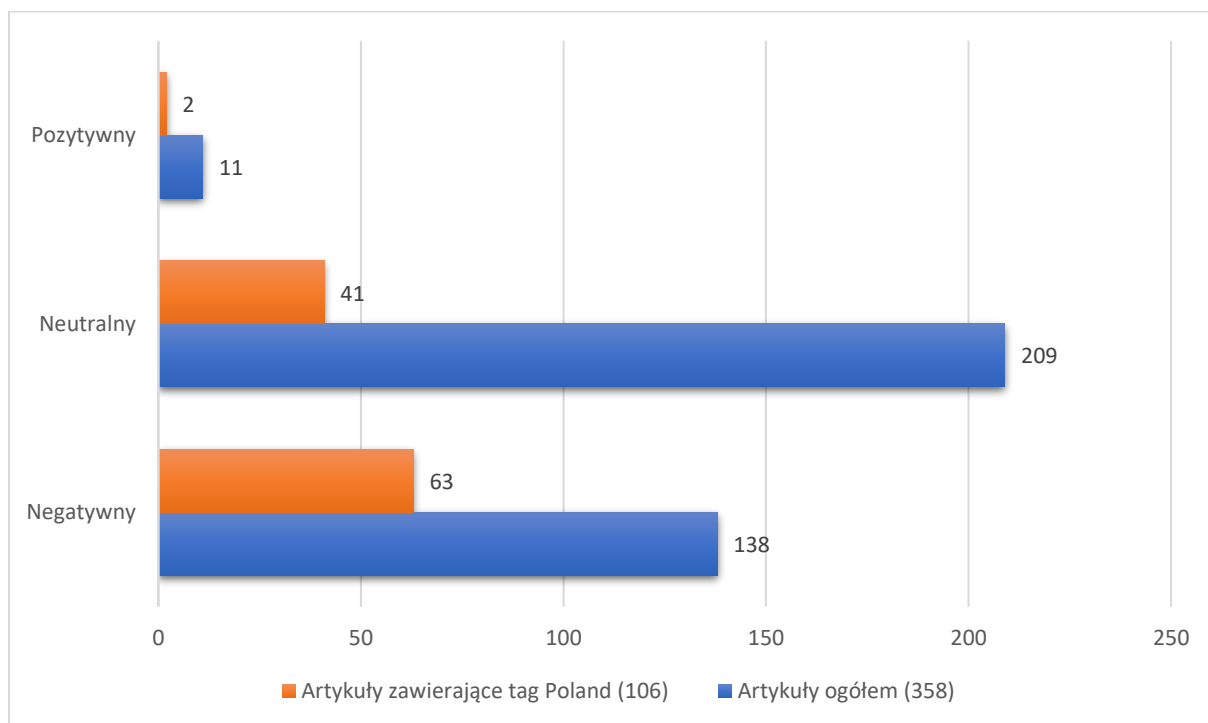
Jednakże zdecydowanie odmienne wyniki otrzymano, gdy spośród 358 artykułów poddano badaniom wyłącznie 106 zawierających *tag* o nazwie *Poland*. W ich przypadku już tylko 2 z nich kształtowały wizerunek Polski w sposób pozytywny, 41 w sposób neutralny, a aż 63 w sposób negatywny. Widoczna jest więc jednoznaczna tendencja do pejoratywnego przedstawiania wizerunku Polski w publikowanych artykułach – szczególnie w tych w których autorzy artykułów dokonali ich oznaczenia wskazanym *tagiem*.

Co więcej, należy już w tym momencie zaznaczyć, że powyższe wyniki badań są co do zasady analogiczne wobec tych przeprowadzonych w zakresie artykułów opublikowanych na witrynie agencji informacyjnej TASS. Zgodnie z nimi żaden artykuł nie kształtował wizerunku Polski pozytywnie, 34 robiły to w sposób neutralny, a 57 w sposób negatywny (wyniki omówiono szczegółowo w dalszej części pracy).

Kształtowanie w powyższy sposób wizerunku Polski w artykułach publikowanych przez Sputnik News International koreluje z polityką zagraniczną Kremla prowadzoną wobec Warszawy, jak również z kwestiami spornymi występującymi w stosunkach bilateralnych. Polska w ocenie Rosji nie jest postrzegana jako państwo jej przyjazne, co znajduje swoje odzwierciedlenie w publikowanych treściach.

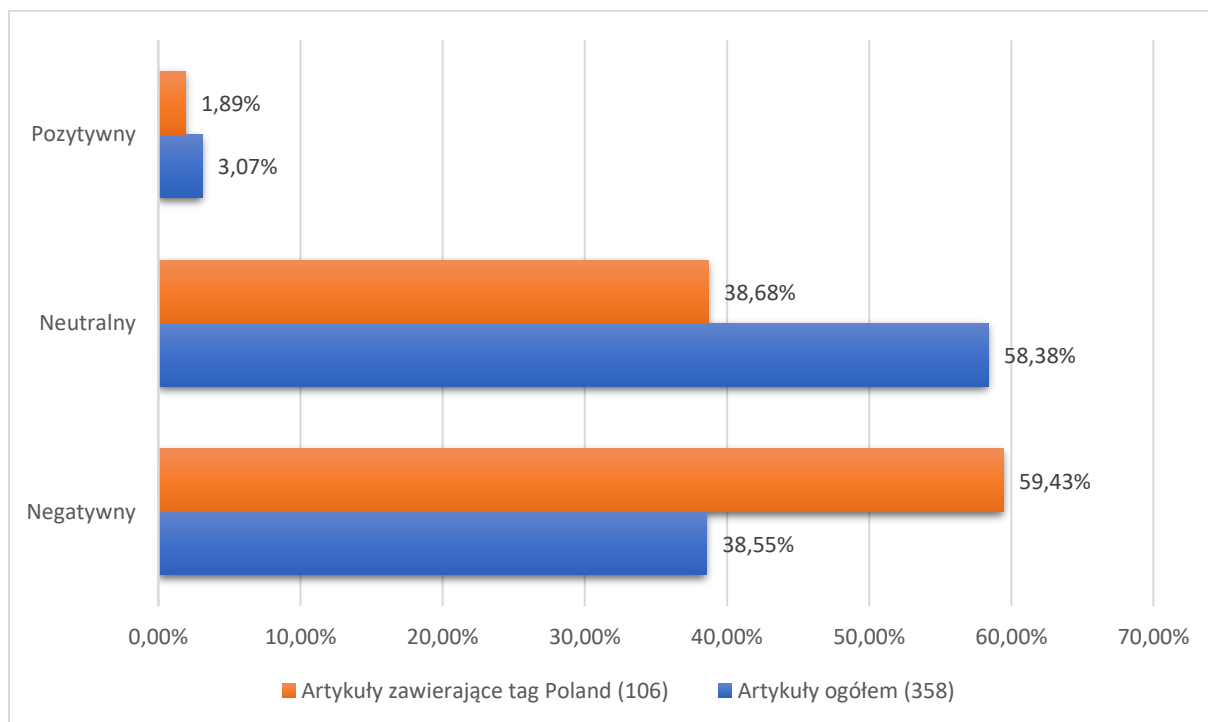
¹⁷³⁰ Zobacz szerzej w rozdziale metodologicznym.

Wykres 33. Rodzaj *framingu* treści na portalu informacyjnym Sputnik News International w latach 2010-2022.



Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

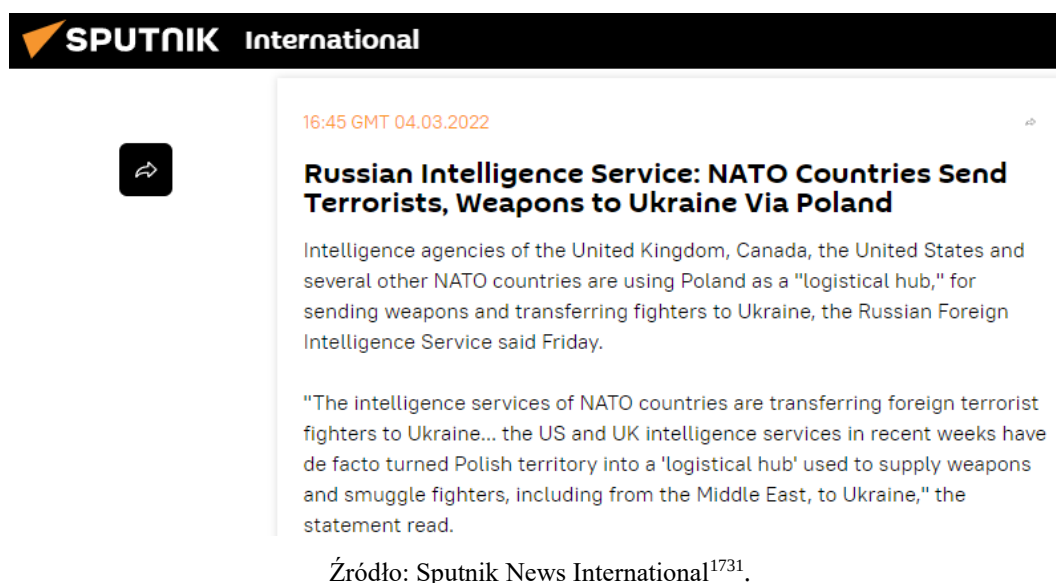
Wykres 34. Procentowe występowanie rodzajów *framingu* treści na portalu informacyjnym Sputnik News International w latach 2010-2022.



Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

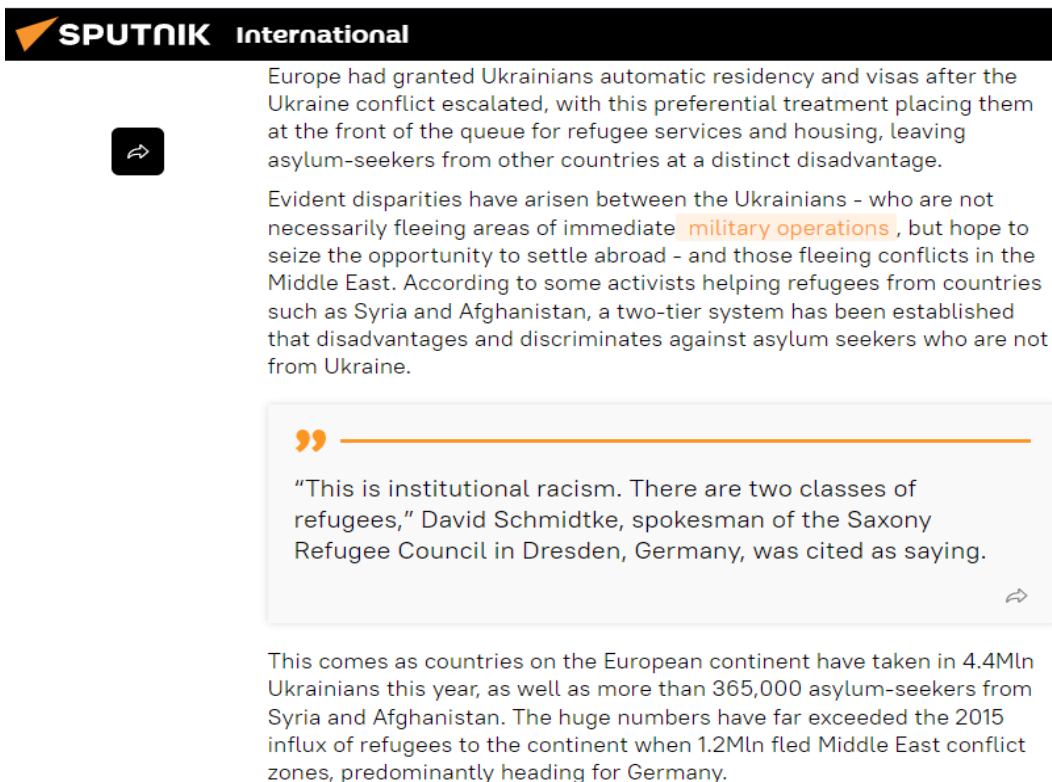
Można również zauważyć, że publikowane na portalu Sputnik News International artykuły mają często charakter informacyjny, tj. nie zawierają oceny danego wydarzenia bądź wydarzeń. Sprowadzają się więc do prezentowania punktu widzenia Polski oraz punktu widzenia Federacji Rosyjskiej, bez jednoczesnego wskazania, które stanowisko jest prawidłowe, a które błędne. Co więcej, *framing* treści w publikowanych artykułach jest w wielu przypadkach wyjątkowo subtelny. Trudno bowiem zidentyfikować w nich słowa jednoznacznie postrzegane jako wartościowane negatywnie w kontekście prezentowania wizerunku Polski. Zdarzało się również, że w odniesieniu do Polski używane są zwroty jednoznacznie neutralne, lecz występują one w artykule, który co do zasady wypowiada się krytycznie o polityce Unii Europejskiej (np. w kontekście migracji) lub NATO (np. w kontekście rozmieszczania wojsk na wschodniej flance NATO), a których to organizacji Polska jest członkiem.

Zdjęcie 13.



¹⁷³¹ Sputnik News International: *LIVE UPDATES: Ukrainian Nationalists Blow Up Bridge to Town of Schastye Near Lugansk*. <https://sputnikglobe.com/20220531/live-updates-two-people-killed-and-24-wounded-in-lpr-by-ukraines-shelling-over-past-day-1095888448.html> (dostęp: 01.12.2024). Tłumaczenie własne: Rosyjskie służby wywiadowcze: Kraje NATO wysyłają terrorystów i broń na Ukrainę przez Polskę Agencje wywiadowcze Wielkiej Brytanii, Kanady, Stanów Zjednoczonych i kilku innych krajów NATO wykorzystują Polskę jako „centrum logistyczne” do wysyłania broni i transferu bojowników na Ukrainę, poinformowała w piątek rosyjska Służba Wywiadu Zagranicznego. „Służby wywiadowcze państw NATO przetrzucają zagranicznych bojowników terrorystycznych na Ukrainę... Służby wywiadowcze USA i Wielkiej Brytanii w ostatnich tygodniach de facto przekształciły terytorium Polski w „centrum logistyczne”, służące do dostarczania broni i przemykania bojowników, w tym z Bliskiego Wschodu, na Ukrainę” – czytamy w oświadczeniu.

Zdjęcie 14.



Źródło: Sputnik News International¹⁷³².

Framing treści w publikowanych na portalu artykułach ulegał zmianie na przestrzeni lat. Przykładowo, artykuły prezentujące Polskę w pozytywnym świetle, których łącznie zidentyfikowano 11 w badanym okresie, w samym 2010 roku wystąpiły 5 razy, co koreluje z odwilżą jaka miała ówczesnie miejsce w stosunkach polsko-rosyjskich. Następnie dwa razy w 2015 roku, dwa razy w 2019 roku i dwa razy w 2021 roku. Artykuły te cechowały się niskim nasyceniem kwestii spornych występujących w stosunkach polsko-rosyjskich. W ponad

¹⁷³² Sputnik News International: *Preferential Treatment of Ukrainian Refugees in EU Stirs Anger Amid Claims of 'Institutional Racism'*. <https://sputnikglobe.com/20221104/preferential-treatment-of-ukrainian-refugees-in-eu-stirs-anger-amid-claims-of-institutional-racism-1103777096.html> (dostęp: 01.12.2024). Tłumaczenie własne: Europa przyznała Ukraińcom automatyczne prawo pobytu i wizy po eskalacji konfliktu na Ukrainie, a to preferencyjne traktowanie umieściło ich na początku kolejki do usług dla uchodźców i zakwaterowania, stawiając osoby ubiegające się o azyl z innych krajów w wyraźnie niekorzystnej sytuacji. Pojawiły się wyraźne dysproporcje między Ukraińcami – którzy niekoniecznie uciekają z obszarów natychmiastowych działań wojennych, ale mają nadzieję wykorzystać okazję do osiedlenia się za granicą – a tymi uciekającymi przed konfliktami na Bliskim Wschodzie. Według niektórych aktywistów pomagających uchodźcom z krajów takich jak Syria i Afganistan ustanowiono dwupoziomowy system, który dyskryminuje i stawia w niekorzystnej sytuacji osoby ubiegające się o azyl, które nie pochodzą z Ukrainy. „To jest rasizm instytucjonalny. Istnieją dwie klasy uchodźców” – powiedział David Schmidtke, rzecznik Saksońskiej Rady ds. Uchodźców w Dreźnie w Niemczech. Stało się tak, ponieważ kraje na kontynencie europejskim przyjęły w tym roku 4,4 mln Ukraińców, a także ponad 365 000 osób ubiegających się o azyl z Syrii i Afganistanu. Ogromna liczba uchodźców znacznie przekroczyła napływ uchodźców na kontynent w 2015 r., kiedy to 1,2 mln osób uciekło z obszarów objętych konfliktem na Bliskim Wschodzie, kierując się głównie do Niemiec.

połowie nie występowały one bowiem w ogóle, w dwóch przypadkach wystąpiła jedna kwestia sporna, w takiej samej liczbie dwie kwestie sporne i tylko w jednym przypadku trzy kwestie sporne.

W latach 2010-2013 Polska była prezentowana wyraźnie w sposób neutralny. Dopiero od 2014 roku można zaobserwować tendencję do kształtowania wizerunku Polski w sposób negatywny, co ma z pewnością związek z aneksją Półwyspu Krymskiego przez Rosję (2014) i jednoznacznym potępieniem tego działania przez Polskę oraz wsparciem rządu w Kijowie. W kolejnych latach nie można wyodrębnić okresów, w których *framing* treści byłby jednoznacznie neutralny albo negatywny. Inaczej sytuacja kształtuje się biorąc pod uwagę wyłącznie artykuły zawierające *tag* o nazwie *Poland*. W ich przypadku widoczne jest nasilenie się kształtowania wizerunku Polski w sposób negatywny od 2017/2018 roku, co może mieć swój związek z realizacją postanowień szczytu NATO w Warszawie (2016), podczas którego podjęto decyzję o zwiększeniu obecności amerykańskich sił zbrojnych w Polsce. Można również zaobserwować, że wzrost występowania w danym tekście kwestii spornych w stosunkach polsko-rosyjskich, korelował z częstszym występowaniem negatywnego *framingu* wobec Polski.

Reasumując powyższe rozważania należy zwrócić uwagę na rozbieżności w zakresie otrzymanych wyników badań, których przedmiotem były wyodrębnione artykuły w ogóle (358) oraz artykuły, które zawierały *tag* o nazwie *Poland* (106). Taka rozbieżność nie występowała bowiem w przypadku żadnej z pozostałych kategorii kodowych. Z przeprowadzonych badań wynika, że 209 artykułów (około 59%) prezentowało Polskę w sposób neutralny, 138 (około 38%) w sposób negatywny a 11 (około 3%) w sposób pozytywny. Jeśli jednak uwzględnić tylko te artykuły, które zawierały *tag* o nazwie *Poland*, to struktura wyników badań kształtuje się w sposób odmienny. 63 artykuły prezentowały Polskę w sposób negatywny (około 59%), 41 neutralny (około 39%), a 2 pozytywny (około 2%). Choć pierwsze z zaprezentowanych wyników badań mogłyby być zaskoczeniem w stosunku do relacji bilateralnych Polski oraz Rosji na przestrzeni lat 2010-2022, to już analiza wyłącznie artykułów zawierających *tag Poland* w sposób jednoznaczny wpisuje *framing* publikowanych treści w stosunki polsko-rosyjskie. Cezura czasowa przyjęta w ramach rozprawy była okresem, który co do zasady cechował się niezwykle trudnymi oraz napiętymi relacjami na linii Warszawa-Moskwa, co znalazło swój wydzźwięk sposobie prezentowania Polski w artykułach opublikowanych na portalu informacyjnym Sputnik News International.

Zdjęcie 15.



PARIS (Sputnik) - Kiev's and Warsaw's pursuit to rewrite the history of World War II is among the most serious political problem of modern Europe, Russian Permanent Delegate to UNESCO Alexander Kuznetsov said on Wednesday in the Russian Centre for Science and Culture in Paris.

Kuznetsov voiced his concerns during an opening ceremony of an exhibition dedicated to the role played by Soviet Jews in WWII. The exhibition will be open to visitors from 30 January to 10 April.

"Let's face the truth: since the end of the second world war, there have never been such explicit, arrogant and shameless attempts to rewrite the history of the second world war", Kuznetsov said.

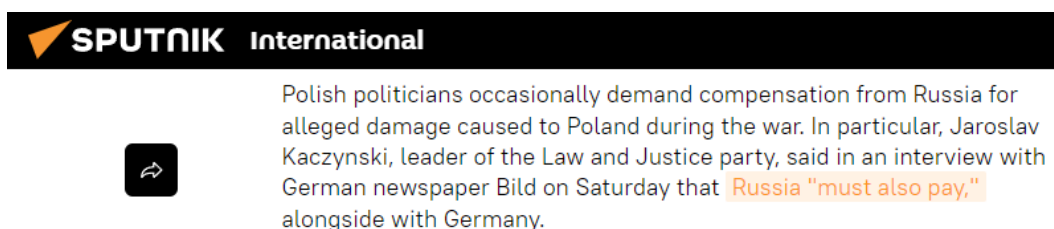
He then proceeded to provide examples of such attempts - Warsaw's demands for compensation from Moscow and Kiev's accusations that Soviet Union had a role to play in starting WWII.

"It turns out that the interpretation of the history of World War II without exaggeration has become one of the most critical political problems in modern Europe", the Russian envoy said.

Źródło: Sputnik News International¹⁷³³.

¹⁷³³ Sputnik News International: *WWII History Falsification Among Europe's Most Pressing Political Issues - Russian Envoy*. <https://sputnikglobe.com/20200129/wwii-history-falsification-among-europes-most-pressing-political-issues---russian-envoy-1078175428.html> (dostęp: 01.12.2024). Tłumaczenie własne: PARYŻ (Sputnik) - Dążenie Kijowa i Warszawy do przepisania historii II wojny światowej należy do najpoważniejszych problemów politycznych współczesnej Europy, powiedział w środę w Rosyjskim Centrum Nauki i Kultury w Paryżu stały delegat Rosji przy UNESCO Aleksander Kuzniecowa. Kuzniecowa wyraził swoje obawy podczas ceremonii otwarcia wystawy poświęconej roli, jaką odegrali radzieccy Żydzi w II wojnie światowej. Wystawa będzie otwarta dla zwiedzających od 30 stycznia do 10 kwietnia. „Spójrzmy prawdzie w oczy: od zakończenia II wojny światowej nigdy nie było tak jawnych, aroganckich i bezwstydných prób przepisania historii II wojny światowej” — powiedział Kuzniecowa. Następnie podał przykłady takich prób — żądania od Moskwy odszkodowania ze strony Warszawy i oskarżenia Kijowa, że Związek Radziecki odegrał rolę w rozpoczęciu II wojny światowej. „Okazuje się, że interpretacja historii II wojny światowej bez przesady stała się jednym z najpoważniejszych problemów politycznych we współczesnej Europie” — powiedział rosyjski wysłannik.

Zdjęcie 16.



Źródło: Sputnik News International¹⁷³⁴.

7.1.5. Techniki propagandowe stosowane przez portal informacyjny Sputnik News International

Istotnym wnioskiem z badań na który należy wskazać w pierwszej kolejności jest to, że artykuły publikowane na portalu informacyjnym Sputnik News International są co do zasady zdecydowanie bardziej obszerne, niż artykuły publikowane na witrynie agencji informacyjnej TASS. Zawierają one obszerne opinie badaczy i ekspertów, jak również liczne informacje przedstawiające stanowiska poszczególnych stron. Tym samym artykuły zawierały zdecydowanie więcej technik propagandowych. Drugim nasuwającym się wnioskiem jest stwierdzenie, że propaganda występująca w publikowanych treściach nie cechuje się topornością i prostotą, a wręcz przeciwnie jest niezwykle wyrafinowana.

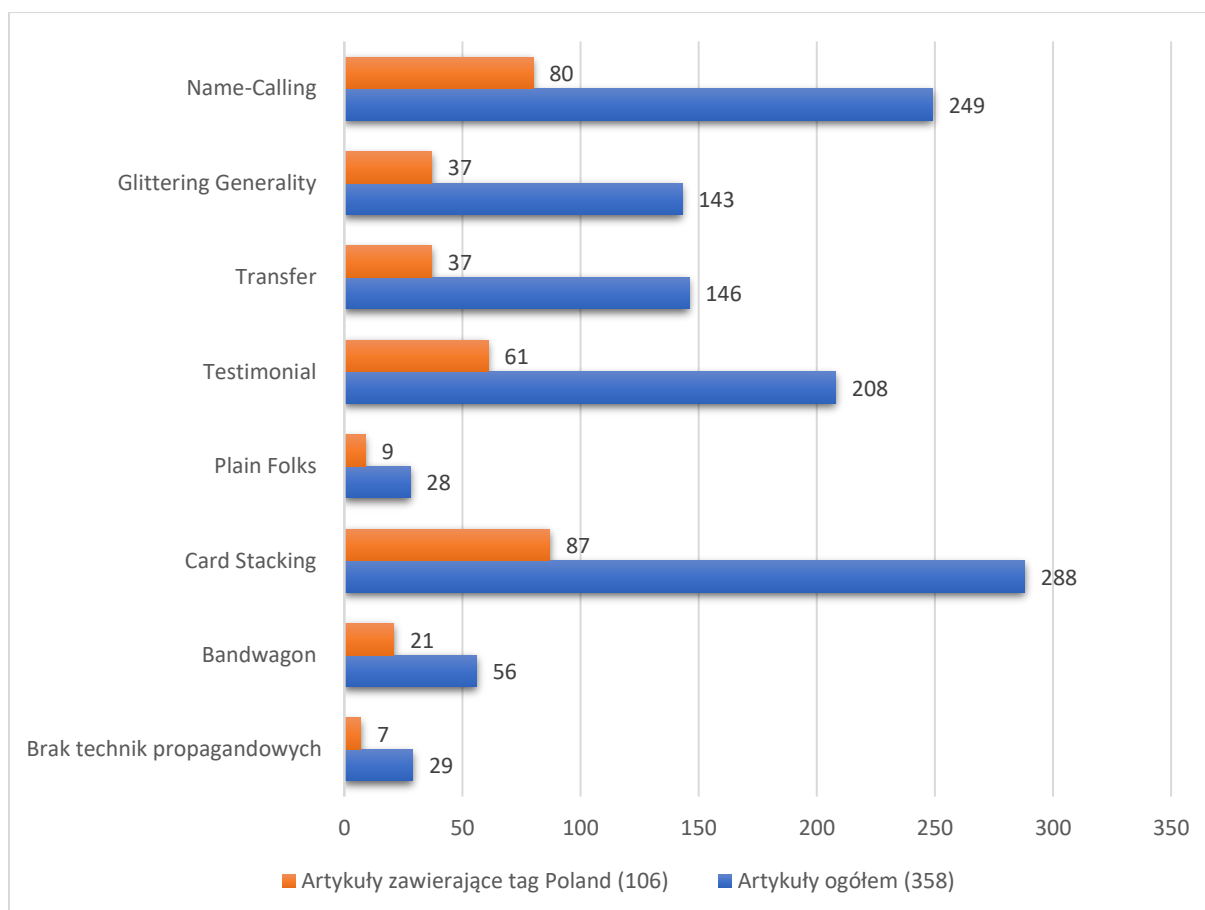
Najczęściej identyfikowaną w artykułach była technika propagandowa o nazwie *Card Stacking*, którą wyodrębniono w 288 artykułach (spośród 358 przyjętych do badań), co stanowi ponad 80% ogólnej ich liczby. Drugą w kolejności była technika *Name-Calling*, którą zaobserwowano w przypadku 249 artykułów (prawie 70%), a trzecią technika *Testimonial* w liczbie 208 (około 58%). Następnymi w kolejności była technika *Transfer*, która pojawiła się 146 razy (około 40%) oraz *Glittering Generalities*, zidentyfikowana 143 razy (niecałe 40%). Najrzadziej występowały techniki *Bandwagon* w liczbie 56 razy (około 16%) oraz *Plain Folks*, zaledwie 28 razy (około 8%).

Podobny trend jest widoczny w przypadku 106 spośród 358 wyodrębnionych artykułów, które zawierają *tag* o nazwie *Poland*. W ich przypadku najczęściej występującymi technikami propagandowymi były kolejno: *Card Stacking* (87 razy – około 82%), *Name-Calling* (80 razy – około 75%), *Testimonial* (61 razy – około 57%), *Transfer* (37 razy – około 35%), *Glittering*

¹⁷³⁴ Ibidem. Tłumaczenie własne: Polscy politycy czasami domagają się od Rosji odszkodowania za rzekome szkody wyrządzone Polsce podczas wojny. W szczególności Jarosław Kaczyński, lider partii Prawo i Sprawiedliwość, powiedział w wywiadzie dla niemieckiej gazety Bild w sobotę, że Rosja „również musi zapłacić”, razem z Niemcami.

Generalities (37 razy – około 35%), *Bandwagon* (21 razy – około 20%) oraz *Plain Folks* (9 razy – około 8%).

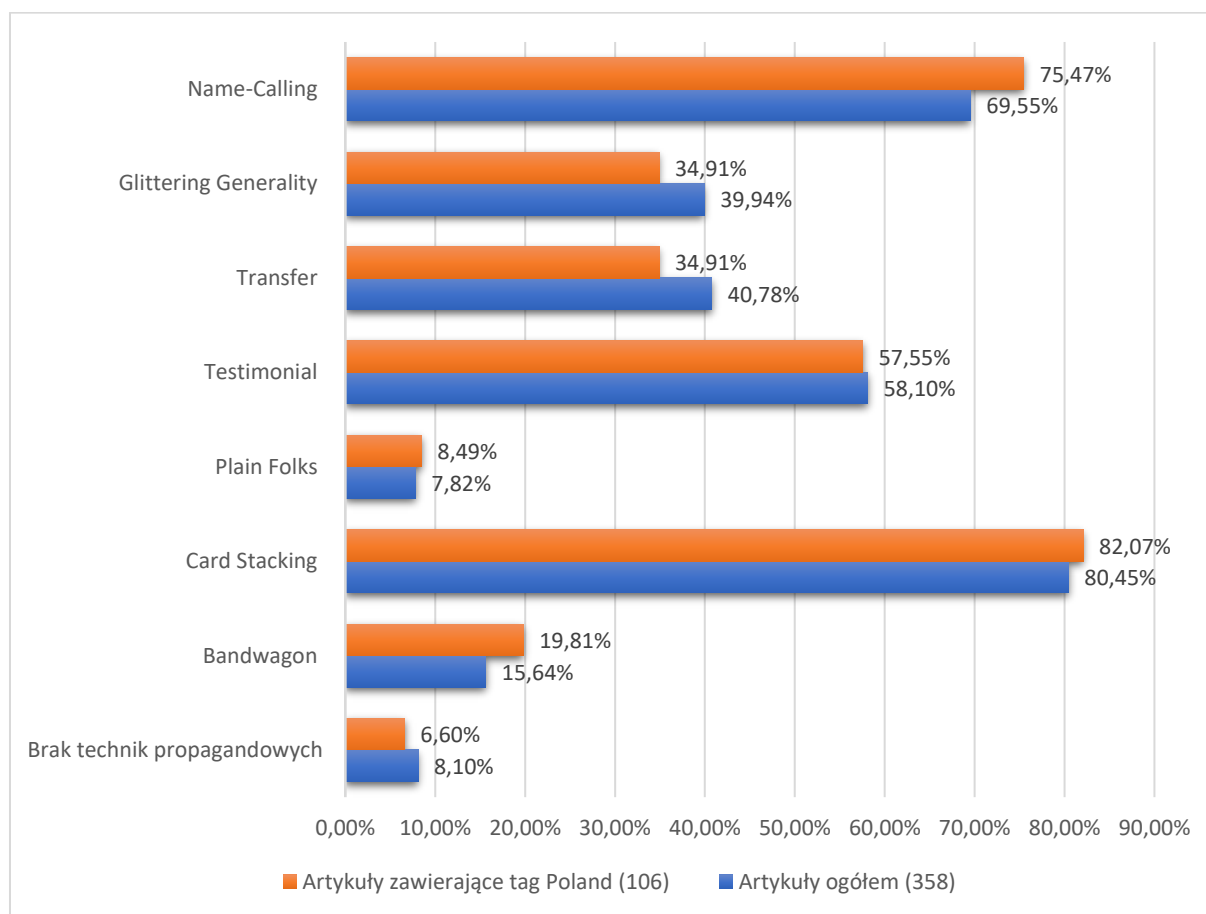
Wykres 35. Zastosowane techniki propagandowe w artykułach opublikowanych na portalu informacyjnym Sputnik News International w latach 2010-2022.



Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

Z powyższego zestawienia wynika więc, że zarówno częstotliwość występowania jak i stosunek procentowy do ogólnej liczby artykułów jest bardzo zbliżony, zarówno w przypadku wszystkich wyodrębnionych do badań artykułów (358), jak i wyłącznie tych zawierających *tag* o nazwie *Poland* (106). Może to prowadzić do wniosku, że kampanie oddziaływania informacyjnego w zakresie wykorzystywanych do tego technik propagandowych są do siebie niezwykle podobne, niezależnie od tego wobec jakiego podmiotu są kierowane.

Wykres 36. Procentowe występowanie technik propagandowych w artykułach opublikowanych na portalu informacyjnym Sputnik News International w latach 2010-2022.



Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

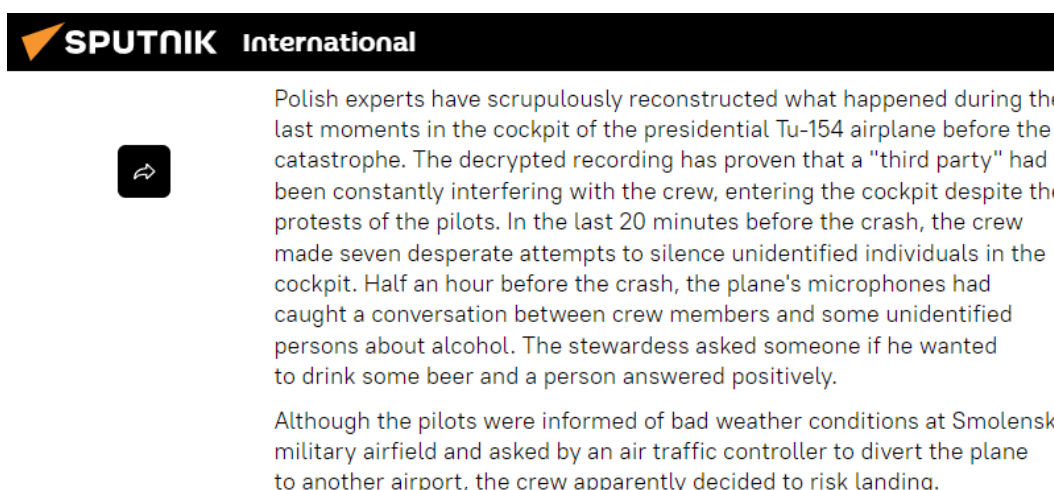
Z powyższego zestawienia wynika więc, że zarówno częstotliwość występowania, jak i stosunek procentowy do ogólnej liczby artykułów jest bardzo zbliżony, zarówno w przypadku wszystkich wyodrębnionych do badań artykułów (358), jak i wyłącznie tych zawierających *tag* o nazwie *Poland* (106). Może to prowadzić do wniosku, że kampanie oddziaływania informacyjnego w zakresie wykorzystywanych do tego technik propagandowych są do siebie niezwykle podobne, niezależnie od tego wobec jakiego podmiotu są kierowane.

Nie stanowi zaskoczenia bardzo wysokie nasycenie publikowanych treści technikami propagandowymi o nazwie *Card Stacking* oraz *Name-Calling*. Są to bowiem proste techniki, które w przypadku pierwszej z wymienionych realizują przede wszystkim zadania z zakresu wspierania oddziaływania propagandowego za pomocą odpowiedniej selekcji informacji na dany temat. W przypadku drugiej z technik jest to etykietowanie treści, a więc za pomocą

odpowiednich słów oceniających nadawanie im konkretnego znaczenia, zgodnego z założeniami dysponenta propagandy.

Interesujące było natomiast zidentyfikowanie wyjątkowo częstego występowania w tekstach techniki *Testimonial*. Była ona wykorzystywana przede wszystkim do uzasadniania poprawności określonych poglądów poprzez prezentowanie ich przez konkretne osoby, przedstawiane jako eksperci w danej dziedzinie. Były to zarówno osoby, które na podstawie imienia, nazwiska oraz zajmowanej funkcji można było zidentyfikować jako Rosjan, jak i w dużej mierze eksperci zachodni, głównie z Niemiec i Wielkiej Brytanii. Ekspert z Zachodu prezentowali Rosję w pozytywnym świetle, tworząc wrażenie, że działania Moskwy są prawidłowe i akceptowane. Nie brakowało również uzasadniania słuszności określonych poglądów, odwołując się do poglądów głównych decydentów politycznych na Kremlu.

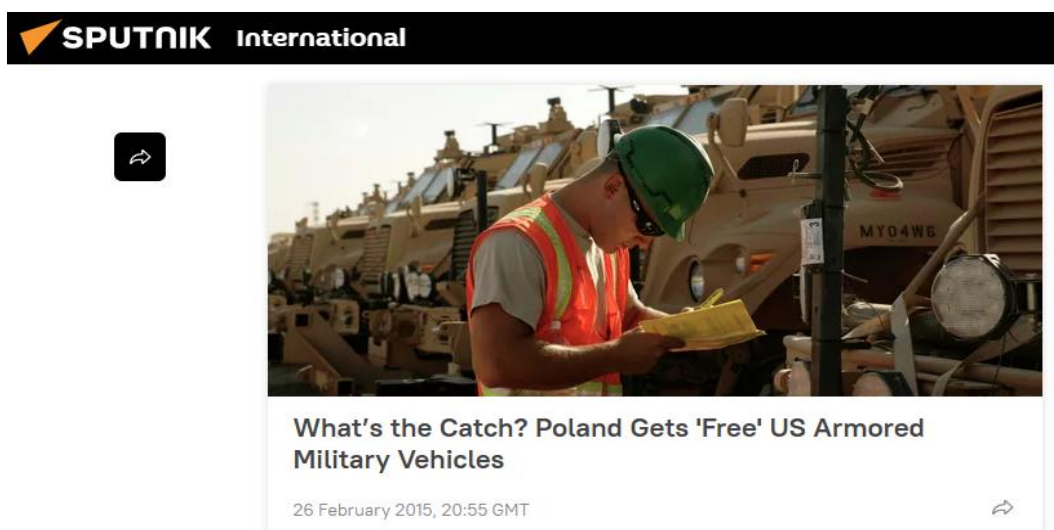
Zdjęcie 17.



Źródło: Sputnik News International¹⁷³⁵.

¹⁷³⁵Sputnik News International: *Shocking Facts of Poland's Kaczynski Plane Crash Revealed*. <https://sputnikglobe.com/20150407/1020580333.html> (dostęp: 01.12.2024). Tłumaczenie własne: Polscy eksperci skrupulatnie zrekonstruowali to, co wydarzyło się w ostatnich chwilach w kokpicie prezydenckiego samolotu Tu-154 przed katastrofą. Odszyfrowane nagranie udowodniło, że „osoba trzecia” stale ingerowała w pracę załogi, wchodząc do kokpitu pomimo protestów pilotów. W ciągu ostatnich 20 minut przed katastrofą załoga podjęła siedem desperackich prób uciszenia niezidentyfikowanych osób w kokpicie. Pół godziny przed katastrofą mikrofony samolotu wychwyciły rozmowę członków załogi z kilkoma niezidentyfikowanymi osobami na temat alkoholu. Stewardesa zapytała kogoś, czy chce napić się piwa, a osoba odpowiedziała twierdząco. Chociaż piloci zostali poinformowani o złych warunkach pogodowych na lotnisku wojskowym w Smoleńsku i poproszeni przez kontrolera ruchu lotniczego o skierowanie samolotu na inne lotnisko, załoga najwyraźniej zdecydowała się zaryzykować lądowanie.

Zdjęcie 18.



Źródło: Sputnik News International¹⁷³⁶.

Przykładowo, na powyższym zdjęciu podjęto próbę podważenia stosunków polsko-amerykańskich. Autor poddał bowiem w wątpliwość fakt darmowego przekazania pojazdów wojskowych przez USA sugerując, że nie jest to działanie bezinteresowne.

Zdjęcie 19.



Źródło: Sputnik News International¹⁷³⁷.

¹⁷³⁶ Sputnik News International: *Poland Prepares for 'Hybrid War' Through Shady Diplomacy, Arms Buildup*. <https://sputnikglobe.com/20150311/1019352561.html> (dostęp: 02.12.2024). Tłumaczenie własne: Gdzie jest haczyk? Polska otrzymuje „darmowe” amerykańskie pojazdy opancerzone.

¹⁷³⁷ Sputnik News International: *EU Cuts Military Aid to Ukraine as Arms Dry Up, Kiev on Verge of Losing Conflict, Expert Says*. <https://sputnikglobe.com/20220818/eu-cuts-military-aid-to-ukraine-as-arms-dry-up-ki-ev-on-verge-of-losing-conflict-expert-says-1099739940.html> (dostęp: 01.12.2024). Tłumaczenie własne: „Rządy zachodnie mogą ponieść ciężkie konsekwencje sankcji nałożonych na Rosję tylko wtedy, gdy konflikt będzie miał jakiś sens; a dla rządów europejskich oczekiwanym sensem jest zwycięstwo Ukrainy. Nie ma szans, aby Ukraina wygrała, więc jesteśmy świadkami szaleńczego napływu propagandy” – powiedział Moreau dla Sputnika.

Zdjęcie 20.



Therefore, he suggested, “our protests against the ‘annexation of Crimea’, which Polish governments [have vowed to] ‘never recognise’, look pathetic and resemble the complaints of a child who has been deceived.”

Bad Deals

Modzelewski complained that the Poles were made to look like fools in Warsaw’s arms deals with the US. “We, as always, made ourselves to be idiots, spending billions on some decommissioned weapons from the Americans, who usually humiliate their clients,” he wrote.

“Today there are also those who profit off of our foolishness, scaring us with the ‘threat’ [of] ‘Putin’s Russia’. Russia ‘threatens’ us, which means we need to arm ourselves. We can’t produce the weapons ourselves, so we need to buy them from our good friends (after all, friendship requires sacrifices). But it would be interesting to know who among our politicians are truly paralysed with fear by Moscow, and who among them fears Russia for a material reward?” Modzelewski asked.

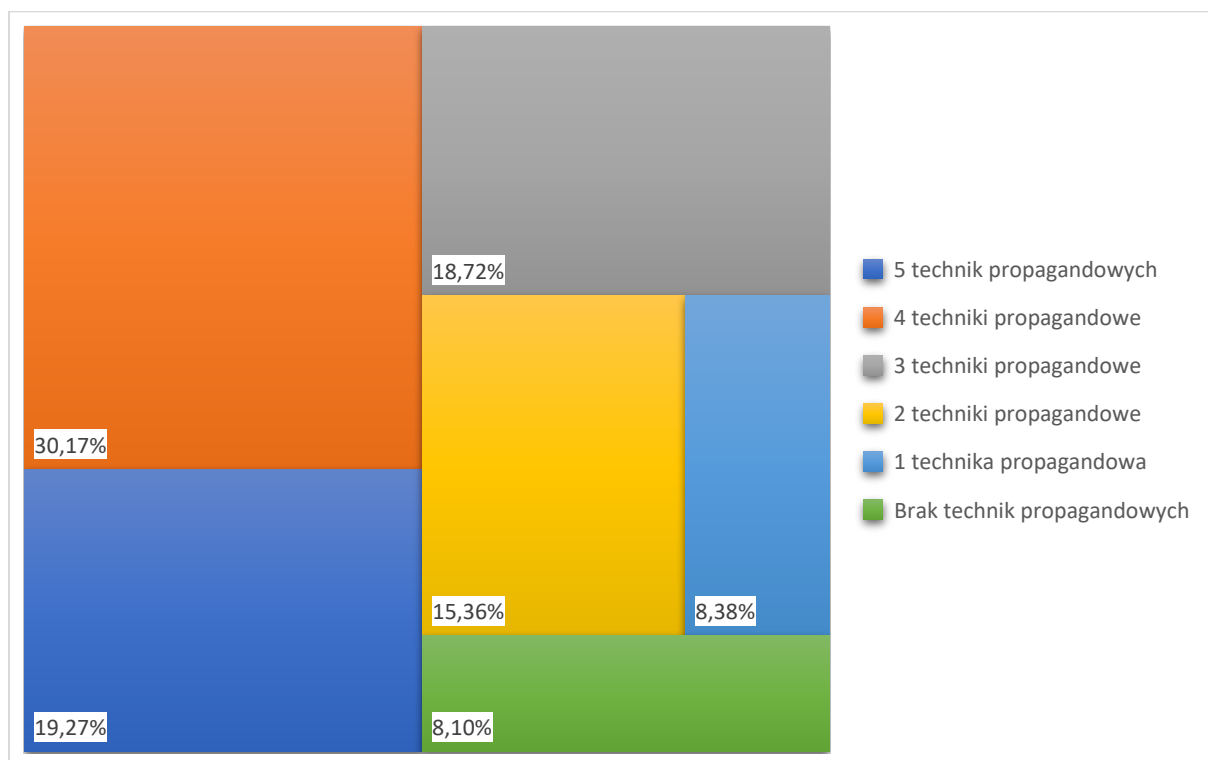
Źródło: Sputnik News International¹⁷³⁸.

Należy również odnieść się do nasycenia występowania poszczególnych technik propagandowych w danym artykule (liczby). I tak przyjmując, że kodowanie technik propagandowych ograniczono do maksymalnie 5 można wskazać, że maksymalna ich liczba wystąpiła w przypadku 69 artykułów, co stanowi około 19%. 4 techniki występowały najczęściej, bo aż w przypadku 108 artykułów, co przekłada się na około 30% ogólnej ich liczby. Następnie kolejno 3 techniki pojawiły się w przypadku 67 artykułów (około 19%),

¹⁷³⁸ Sputnik News International: *EU Polish Presidential Advisor Calls US ‘Simpletons’, Blasts Gov’t for Spending Billions on Old US Arms*. <https://sputnikglobe.com/20191221/polish-presidential-advisor-calls-us-simpletons-blasts-govt-for-spending-billions-on-old-us-arms-1077706457.html> (dostęp: 01.12.2024). Tłumaczenie własne: Dlatego zasugerował, że „nasze protesty przeciwko 'aneksji Krymu', której polskie rządy 'nigdy nie uznają', wyglądają żałośnie i przypominają skargi dziecka, które zostało oszukane”. Złe interesy. Modzelewski narzekał, że Polacy zostali przedstawieni jako głupcy w umowach zbrojeniowych Warszawy z USA. „My, jak zawsze, zrobiliśmy z siebie idiotów, wydając miliardy na jakąś wycofaną broń od Amerykanów, którzy zazwyczaj upokarzają swoich klientów” – napisał. „Dziś są też tacy, którzy czerpią zyski z naszej głupoty, strasząc nas 'groźbą' [ze strony] 'Rosji Putina'. Rosja 'zagroża' nam, co oznacza, że musimy się uzbroić. Nie możemy sami wyprodukować broni, więc musimy ją kupić od naszych dobrych przyjaciół (w końcu przyjaźń wymaga poświęceń). Ale byłoby interesujące wiedzieć, kto wśród naszych polityków jest naprawdę sparaliżowany strachem przed Moskwą, a kto z nich boi się Rosji dla korzyści materialnych?” – pytał Modzelewski.

2 techniki w przypadku 55 artykułów (około 15%) oraz 1 technika w 30 artykułach (około 8%), z kolei w 29 artykułach nie wystąpiła żadna technika propagandowa (około 8%).

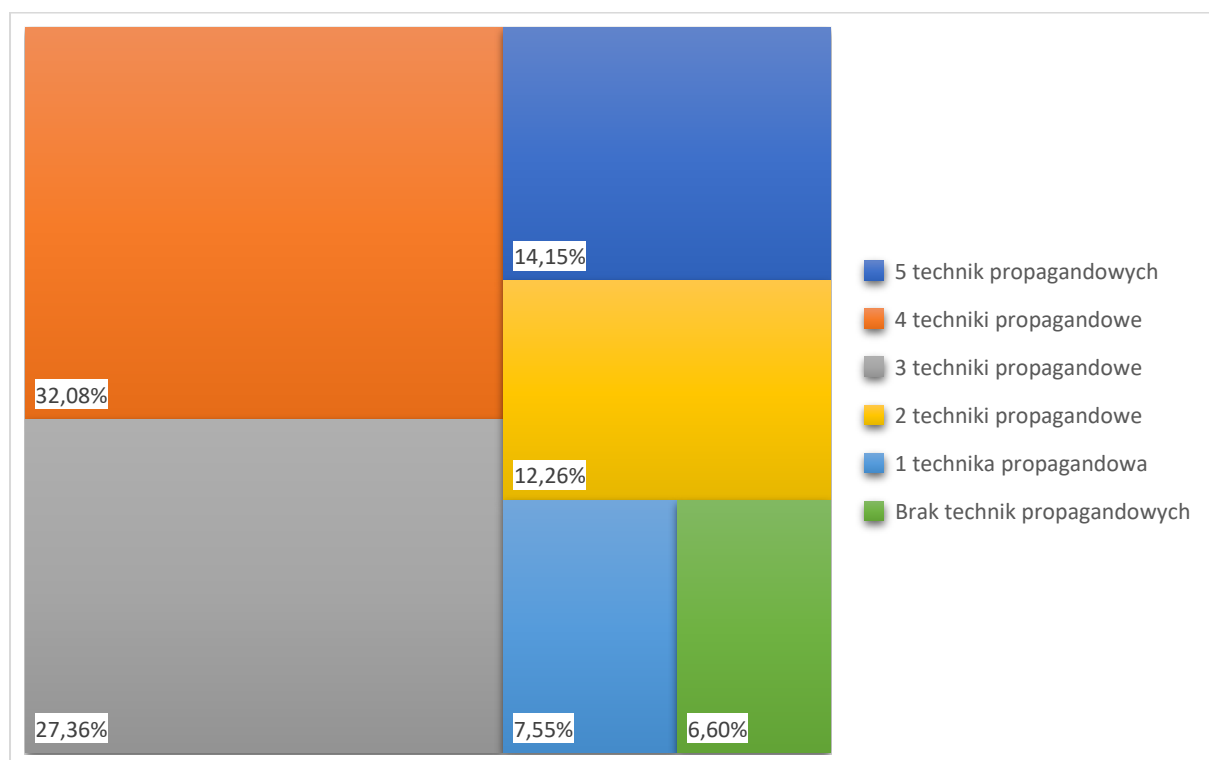
Wykres 37. Procentowe występowanie (nasycenie) technik propagandowych w artykułach opublikowanych na portalu informacyjnym Sputnik News International w latach 2010-2022.



Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

Dokonując analizy wyłącznie artykułów zawierających *tag* o nazwie *Poland*, liczba zidentyfikowanych w jednym artykule technik propagandowych kształtuje się w sposób następujący: 5 razy – 15 artykułów (około 14%), 4 razy – 34 artykuły (32%), 3 razy – 29 artykułów (około 27%), 2 razy – 13 artykułów (około 12%), 1 raz – 8 artykułów (około 7%), 0 razy – 7 artykułów (około 6%). Nasycenie technik propagandowych w artykułach zawierających wskazany *tag* kształtuje się podobnie, jak w przypadku ogólnej liczby poddanych badaniom artykułów, jednakże z zauważalnym wzrostem artykułów zawierających trzy techniki propagandowe.

Wykres 38. Procentowe występowanie (nasycenie) technik propagandowych w artykułach zawierających tag o nazwie *Poland* opublikowanych na portalu informacyjnym Sputnik News International w latach 2010-2022.



Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

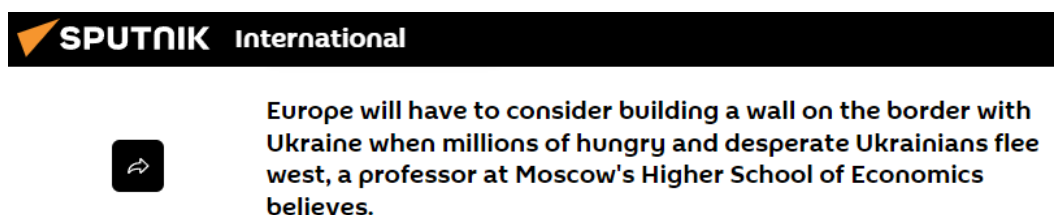
Dostrzegalna jest prawidłowość, zgodnie z którą w artykułach niezawierających odniesień do kwestii spornych występujących w stosunkach polsko-rosyjskich, zazwyczaj nie występowały techniki propagandowe lub ich nasilenie było stosunkowo niewielkie. Podobnie, w artykułach, w których względem Polski zidentyfikowano *framing* negatywny, liczba występujących technik propagandowych była zazwyczaj wyższa niż w przypadku artykułów o neutralnym *framingu*.

Należy podkreślić, że publikowane artykuły miały często charakter informacyjny, co oznacza, że nie dokonywały oceny danych zagadnień. Przykładem mogą być informacje o wydarzeniach wewnętrznych w poszczególnych państwach (w tym również o wydarzeniach nie dotyczących polityki), czy doniesienia o ćwiczeniach wojskowych organizowanych przez NATO. Warto zaznaczyć, że pojawienie się zagadnienia dotyczącego, na przykład, polityki bezpieczeństwa NATO (które według Federacji Rosyjskiej stanowi dla niej zagrożenie), nie implikowało automatycznie większego nasycenia tekstów technikami propagandowymi. Nie zaobserwowano również istotnych zmian w nasyceniu technikami propagandowymi artykułów oblikowanych w latach 2010-2022. W całym badanym okresie można bowiem zauważyć

zarówno artykuły o wyższym, jak i o niższym wskaźniku ich występowania. Oznacza to, że wydarzenia w stosunkach polsko-rosyjskich w latach 2010-2022 nie miały wpływu na intensyfikację stosowania technik propagandowych w tekstach publikowanych na portalu. Wyjątkiem była pełnowymiarowa inwazja Federacji Rosyjskiej na Ukrainę w 2022 roku, która spowodowała zauważalną intensyfikację stosowania wielu technik propagandowych w artykułach na badanym portalu.

Wyodrębnione do badań artykuły cechowały się wysokim nasyceniem technik propagandowych. Ich wykorzystanie w publikowanych tekstach korelowało z polityką zagraniczną Federacji Rosyjskiej wobec Polski, co należy rozpatrywać na dwóch płaszczyznach. Po pierwsze, stosowane techniki miały na celu odpowiednie prezentowanie postawy Rosji na arenie międzynarodowej, w tym wobec Polski. Chodziło więc o wspieranie realizowanej przez Kreml polityki zagranicznej oraz przedstawianie przede wszystkim rosyjskiego punktu widzenia na określone tematy. Po drugie, techniki propagandowe wykorzystywano do deprecjonowania Polski na arenie międzynarodowej. Należy przez to rozumieć podważanie jej wiarygodności jako sojusznika w Sojuszu Północnoatlantyckim oraz państwa członkowskiego Unii Europejskiej. Polska była prezentowana jako kraj antyrosyjski, a wręcz rusofobiczny. W odniesieniu do nasycenia technik propagandowych w artykułach ogółem oraz tych, które zawierały *tag* o nazwie *Poland*, to nie można wskazać, aby występowały one częściej bądź rzadziej, gdyż utrzymywały się one na w miarę jednakowym poziomie.

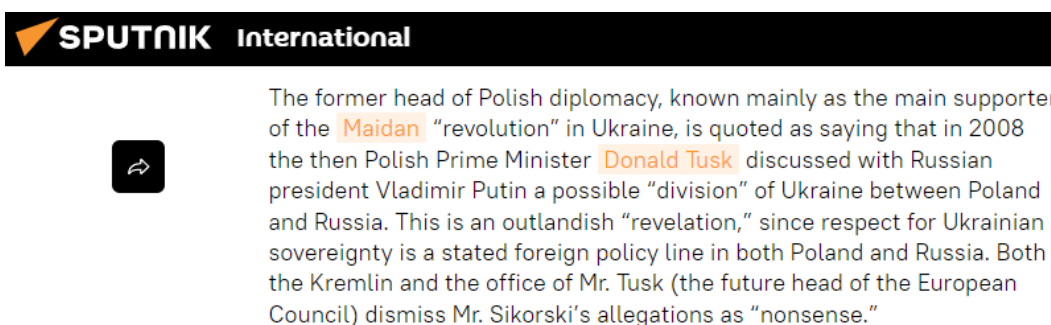
Zdjęcie 21.



Źródło: Sputnik News International¹⁷³⁹.

¹⁷³⁹ Sputnik News International: *EU Policy in Ukraine Could Result in Mass Exodus to Europe*. <https://sputnikglobe.com/20150128/1017467778.html> (dostęp: 01.12.2024). Tłumaczenie własne: Europa będzie musiała rozważyć budowę muru na granicy z Ukrainą, gdy miliony głodnych i zdesperowanych Ukraińców uciekną na zachód, uważa profesor Wyższej Szkoły Ekonomicznej w Moskwie.

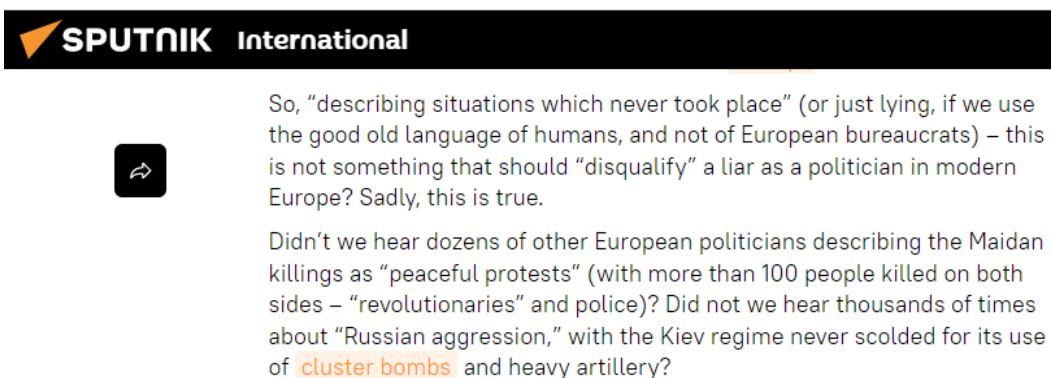
Zdjęcie 22.



Źródło: Sputnik News International¹⁷⁴⁰.

Na powyższym zdjęciu autor tekstu podjął próbę podważenia stosunków polsko-rosyjskich, wskazując na rzekomą rozmowę do jakiej miało dojść między D. Tuskiem a W. Putinem. Tematem rozmowy miał być podział Ukrainy pomiędzy Polskę i Rosję. Jednocześnie nazwano R. Sikorskiego zwolennikiem rewolucji na Majdanie, co ma zdecydowanie negatywny wydźwięk.

Zdjęcie 23.



Źródło: Sputnik News International¹⁷⁴¹.

¹⁷⁴⁰ Sputnik News International: *Radoslaw Sikorski Is Testing the Limits of Lies*. <https://sputnikglobe.com/20141023/Radoslaw-Sikorski-Is-Testing-the-Limits-of-Lies-194478671.html> (dostęp: 01.12.2024). Tłumaczenie własne: Były szef polskiej dyplomacji, znany głównie jako główny zwolennik „rewolucji” Majdanu na Ukrainie, został zacytowany, gdy powiedział, że w 2008 r. ówczesny polski premier Donald Tusk rozmawiał z prezydentem Rosji Władimirem Putinem o możliwym „podziale” Ukrainy między Polską a Rosją. Jest to absurdalne „objawienie”, ponieważ szacunek dla suwerenności Ukrainy jest deklarowaną linią polityki zagranicznej zarówno w Polsce, jak i w Rosji. Zarówno Kreml, jak i biuro pana Tuska (przyszłego szefa Rady Europejskiej) odrzucają oskarżenia pana Sikorskiego jako „bzdury”.

¹⁷⁴¹ Ibidem. Tłumaczenie własne: Tak więc „opisywanie sytuacji, które nigdy nie miały miejsca” (lub po prostu kłamanie, jeśli użyjemy dobrego, starego języka ludzi, a nie europejskich biurokratów) – to nie jest coś, co powinno „dyskwalifikować” kłamcę jako polityka we współczesnej Europie? Niestety, to prawda. Czy nie słyszeliśmy dziesiątek innych europejskich polityków opisujących zabójstwa na Majdanie jako „pokoju protesty” (z ponad 100 zabitymi po obu stronach – „rewolucjonistami” i policją)? Czy nie słyszeliśmy tysiące razy o „rosyjskiej agresji”, a reżim w Kijowie nigdy nie został zrugany za użycie bomb kasetowych i ciężkiej artylerii?

Zdjęcie 24.



Participating in the annual pilgrimage to the Josna Gora Monastery in Czestochowa, southern Poland, which marks the traditional opening of the motorcycle season in the country, 'Katyn Rally' commander Wiktor Wegrzyn called on local bikers to adopt a resolution to ensure that the Russians receive "security and hospitality" on Polish territory.

"We, the Polish motorcyclists gathered at the 12th Rally to Jasna Gora named after Rev. Zdzislaw Peszkowski, reaffirm our solidarity with the bikers of the world, and ensure security and hospitality on Polish territory," Wegrzyn noted.

"Today, when functionaries from Polish newspapers and television, using misinformation, have unleashed the baiting our Russian motorcyclist guests hitherto unprecedented in Polish tradition, factually calling on the use of physical violence against them, we declare: The Russian motorcyclists will travel safely through Poland," Wegrzyn declared.

The Katyn Raid Motocross commander emphasized that a "boycott," or worse, "an attack on the Russian bikers, is something against our culture, against Polish morals."

Źródło: Sputnik News International¹⁷⁴².

W powyższym tekście władze Polski zostały oskarżone o wrogą działalność wobec Federacji Rosyjskiej oraz przedstawione w tym kontekście pejoratywnie. Autor artykułu w tym celu posłużył się odwołaniem do pielgrzymki na Jasną Górę w Częstochowie (miejsca ważnego dla Polaków) oraz zbrodni katyńskiej (co stanowi nawiązanie do kwestii spornej dotyczącej polityki historycznej).

¹⁷⁴² Sputnik News International: *Polish Bikers Resolve to Ensure Safe Passage for Russia's Night Wolves*. <https://sputnikglobe.com/20150420/1021125256.html> (dostęp: 01.12.2024). Tłumaczenie własne: Uczestnicząc w corocznej pielgrzymce do klasztoru Jasna Góra w Częstochowie, na południu Polski, która tradycyjnie otwiera sezon motocyklowy w kraju, dowódca „Rajdu Katyńskiego” Wiktor Węgrzyn wezwał lokalnych motocyklistów do przyjęcia rezolucji, która zapewni Rosjanom „bezpieczeństwo i gościnność” na terytorium Polski. „My, polscy motocykliści zebrani na 12. Rajdzie na Jasną Górę im. ks. Zdzisława Peszkowskiego, potwierdzamy naszą solidarność z motocyklistami na całym świecie i zapewniamy bezpieczeństwo i gościnność na terytorium Polski” - zauważył Węgrzyn. „Dziś, gdy funkcjonariusze polskich gazet i telewizji, wykorzystując dezinformację, rozpętali nękanie naszych rosyjskich gości motocyklistów, dotychczas niespotykane w polskiej tradycji, faktycznie wzywając do użycia wobec nich przemocy fizycznej, oświadczamy: Rosyjscy motocykliści będą bezpiecznie podróżować przez Polskę” — oświadczył Węgrzyn. Dowódca rajdu motocrossowego w Katyniu podkreślił, że „bojkot” lub, co gorsza, „atak na rosyjskich motocyklistów jest czymś przeciwko naszej kulturze, przeciwko polskiej moralności”.

Zdjęcie 25.



Zdjęcie 26.



¹⁷⁴³ Sputnik News International: *Experts reject criticism of Russian probe into Kaczynski crash*. <https://sputnikglobe.com/20110121/162240457.html> (dostęp: 01.12.2024). Tłumaczenie własne: „Jestem przekonany, że nasza [polska] strona jest winna większości przyczyn katastrofy smoleńskiej” – powiedział w wywiadzie dla kanału TVN24 specjalny wysłannik Polski do MAK, Edmund Klich. „Jakiegokolwiek błędy ze strony Rosji powinny zostać wykluczone”. Klich powiedział, że katastrofa była spowodowana „błędami w szkoleniu pilotów”. „Dobra załoga sprawnego samolotu – a nie mamy informacji, że Tu-154 miał problemy techniczne – po prostu nie wykona lądowania w taki sposób. Nawet jeśli tak poleciła im kontrola ruchu lotniczego” – powiedział.

¹⁷⁴⁴ Sputnik News International: *NATO Unveils New Headquarters Inspired by the Nazi SS Lightning Bolts?* <https://sputnikglobe.com/20160627/nato-nazi-ss-brussels-hitler-1042050232.html> (dostęp: 01.12.2024). Tłumaczenie własne: To, co prawdopodobnie jest niefortunnym błędem projektowym, jest jednak niepokojące w obliczu dużego nagromadzenia sił koalicji wojskowej wzdłuż granicy z Rosją, kierowanej przez wojska niemieckie. Organizacja Traktatu Północnoatlantyckiego (NATO) wywołała poruszenie w ostatnich tygodniach, ogłaszając swoją nowo wybudowaną siedzibę „dla was i przyszłych pokoleń”. Budynek ma wzór projektu niepokojąco przypominający pioruny nazistowskich „SS”. Nazistowskie obrazy podążają śladami Niemiec, które przewodziły wielkim Anaconda War Games. Ćwiczenia, w których bierze udział ponad 30 000 żołnierzy NATO, odbędą się w Polsce w 75. rocznicę niemieckiej inwazji na Związek Radziecki.

Zdjęcie 27.



Źródło: Sputnik News International¹⁷⁴⁵.

7.2. Agencja informacyjna TASS jako narzędzie wojny informacyjnej Federacji Rosyjskiej wobec Polski

7.2.1. Charakterystyka agencji informacyjnej TASS

Rozważania w przedmiotowym zakresie należy rozpocząć od podkreślenia, że TASS różni się od Sputnik News International tym, że nie jest portalem informacyjnym, lecz rządową agencją informacyjną. Historia agencji informacyjnej TASS¹⁷⁴⁶ rozpoczęła się już w 1904 roku, kiedy to powstała pierwsza informacyjna agencja Rosji, tj. Petersburska Agencja Telegraficzna. W kolejnych latach doszło do zmiany nazwy agencji na Piotrogradzką Agencję Telegraficzną (1914), a następnie na Rosyjską Agencję Telegraficzną (1918). Kilka lat po przemianach ustrojowych w carskiej Rosji i powstaniu Związku Socjalistycznych Republik Radzieckich w 1925 roku przekształcono ją w Agencję Telegraficzną Związku Radzieckiego, w skrócie TASS. W 1992 roku, po samorozwiązaniu ZSRR i powstaniu Federacji Rosyjskiej, agencja otrzymała nazwę Informacyjna Telegraficzna Agencja Rosji (ITAR-TASS), z kolei w 2014 roku nastąpił powrót do dawnej sowieckiej nazwy, czyli Rosyjskiej Agencji Informacyjnej TASS¹⁷⁴⁷.

TASS jest największą rządową agencją informacyjną w Rosji. To za jej pośrednictwem kolportowane są przekazy informacyjne, formułowane przez decydentów politycznych na Kremlu. Jej siedziba mieści się w Moskwie, lecz agencja działa również za pośrednictwem około 70 biur w różnych regionach Rosji oraz około 60 biur w wielu państwach na całym

¹⁷⁴⁵ Sputnik News International: *LIVE UPDATES: Kiev Ready to Blow Up Krivorozhskaya Thermal Power Plant to Blame Russian Forces – MoD*. <https://sputnikglobe.com/20220627/live-updates-ukrainian-forces-fire-20-shells-overnight-at-village-in-dpr-donetsk-says-1096686158.html> (dostęp: 01.12.2024). Tłumaczenie własne: W lutym Rosja rozpoczęła operację wojskową na Ukrainie po apelach o pomoc ze strony separatystycznych republik Doniecka i Ługańska. Kraje zachodnie odpowiedziały, nakładając kompleksowe sankcje na Rosję, a także zwiększając wsparcie wojskowe dla Ukrainy.

¹⁷⁴⁶ TASS. <https://tass.com> (dostęp: 27.07.2024).

¹⁷⁴⁷ TASS: *TASS history*. <https://tass.com/history> (dostęp: 27.07.2024).

świecie. Ciekawostką jest, że TASS posiada swoje biuro informacyjne nawet w kosmosie na Międzynarodowej Stacji Kosmicznej. Według TASS, agencja jest najczęściej cytowaną spośród wszystkich działających w Rosji, publikując codziennie około 3000 wiadomości i 700 zdjęć oraz filmów pochodzących od korespondentów z całego świata. Agencja publikuje wiadomości we wszystkich oficjalnych językach Organizacji Narodów Zjednoczonych, a więc po angielsku, arabsku, hiszpańsku, chińsku, francusku i rosyjsku.

Na stronie internetowej TASS można znaleźć informacje o bliskich związkach agencji z rządem Federacji Rosyjskiej, co prowadzi do wniosku, że jest to podmiot całkowicie zależny od Kremla. Wynika to nie tylko z faktu finansowania agencji przez Moskwę, ale również z organizacji licznych wydarzeń na które są zapraszani rosyjscy politycy, jak i patronowaniu licznym akcjom, konkursom i konferencjom, które są organizowane przez rząd federalny. Nie budzi więc wątpliwości, że TASS jest klasyfikowana jako podmiot szerzący rosyjską propagandę¹⁷⁴⁸.

Stronę internetową tass.com odwiedza miesięcznie około 1,8 miliona użytkowników przede wszystkim z USA, Wielkiej Brytanii, Francji, Niemiec, Kanady oraz Polski¹⁷⁴⁹. Co ciekawe, w odróżnieniu od Sputnik News International, strona internetowa agencji nie została zablokowana w państwach członkowskich Unii Europejskiej w wyniku nałożonych sankcji po rozpoczęciu przez Kreml pełnowymiarowej inwazji na Ukrainę w 2022 roku. Nie jest jednak wśród badaczy zachodnich kwestią sporną, że TASS realizuje operacje z zakresu oddziaływania informacyjnego na swoich odbiorców. Działania te są szczególnie widoczne wobec rozpoczętej w 2014 roku wojny rosyjsko-ukraińskiej oraz jej intensyfikacji w 2022 roku¹⁷⁵⁰.

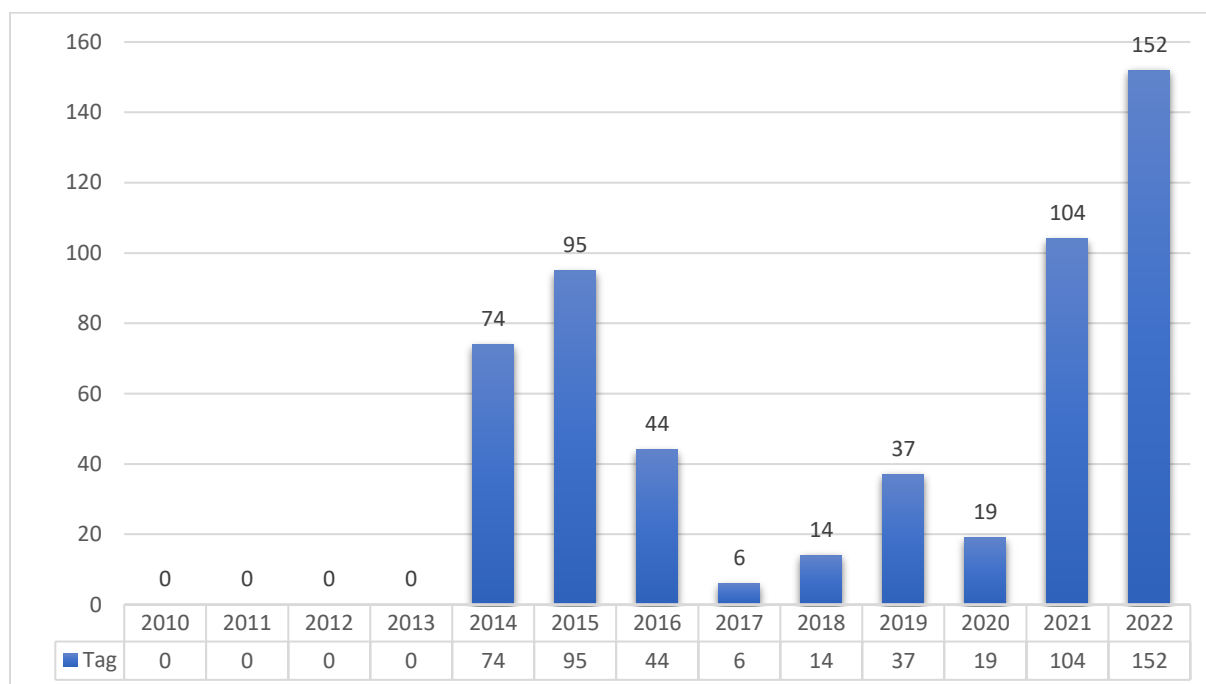
Agencja, wykorzystując swoją pozycję medialną na arenie międzynarodowej, a przede wszystkim fakt bycia agencją rządową której zablokowanie nie jest tak proste ani oczywiste jak w przypadku Sputnik News International, cieszy się pewnym rodzajem przyzwolenia i tolerancji na prowadzenie działań dezinformacyjnych. Dzięki posiadaniu statusu rządowej agencji informacyjnej, TASS może operować w medialnej przestrzeni międzynarodowej często z mniejszą reakcją ze strony organów regulacyjnych, co pozwala agencji na skuteczniejsze rozprzestrzenianie treści zgodnych z interesami Kremla.

¹⁷⁴⁸ TASS: *About TASS*. <https://tass.com/today> (dostęp: 27.07.2024).

¹⁷⁴⁹ SimilarWeb: *tass.com*. <https://www.similarweb.com/website/tass.com/#overview> (dostęp: 27.07.2024).

¹⁷⁵⁰ Zobacz szerzej: OECD: *Disinformation and Russia's war of aggression against Ukraine: Threats and governance responses*. https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/11/disinformation-and-russia-s-war-of-aggression-against-ukraine_8b596425/37186bde-en.pdf (dostęp: 28.07.2024).

Wykres 39. Liczba indywidualnych wiadomości (artykułów) na witrynie agencji informacyjnej TASS wyodrębnionych na podstawie tagu o nazwie *Poland* w latach 2010-2022.



Źródło: Opracowanie własne na podstawie wyników z wyszukiwania opartych o tag z wyrazem *Poland* na witrynie internetowej agencji informacyjnej TASS¹⁷⁵¹.

7.2.2. Typy publikowanych treści na witrynie internetowej agencji informacyjnej TASS

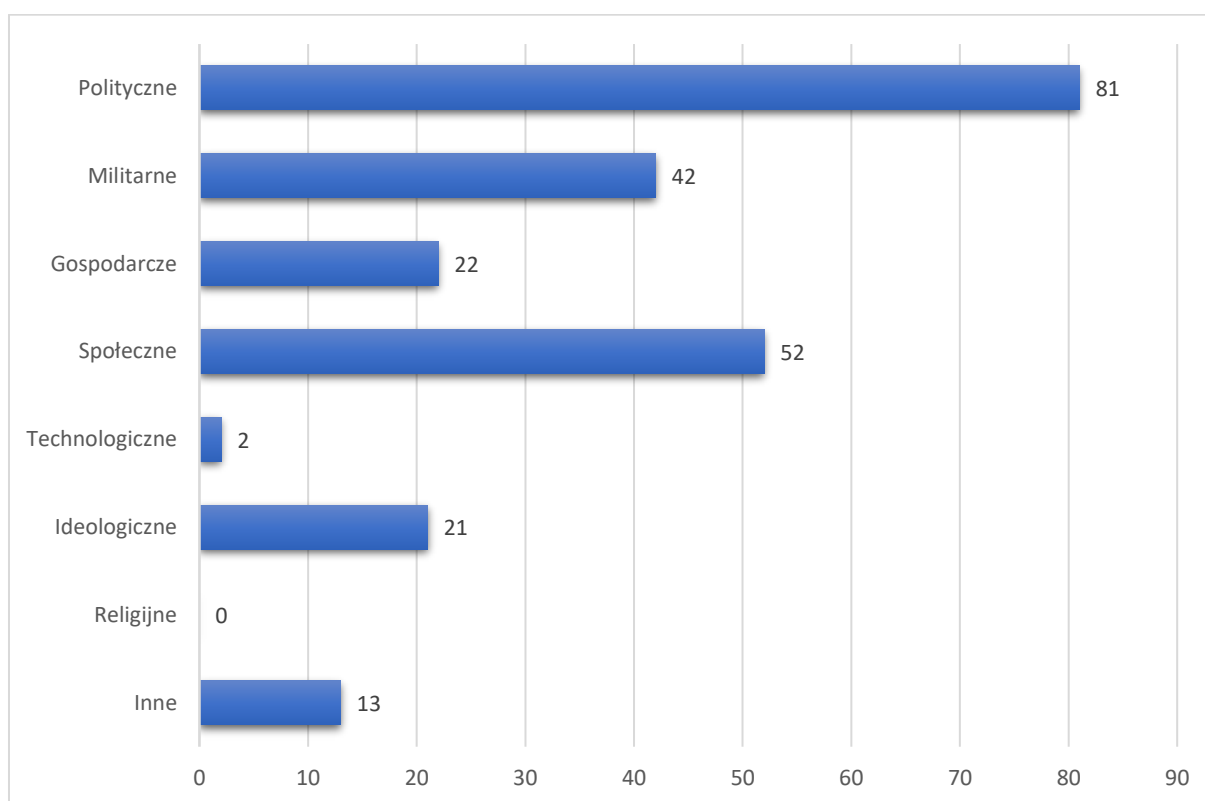
Rosyjska agencja informacyjna TASS jest podmiotem rządowym, który kolportuje treści zgodne z aktualną i oficjalną polityką zagraniczną Kremla. Prowadzi to do wniosku, że rodzaje publikowanych treści są silnie skorelowane z bieżącymi wydarzeniami na arenie międzynarodowej, które dotyczą pośrednio bądź bezpośrednio interesów Federacji Rosyjskiej, w tym tych w kontekście stosunków polsko-rosyjskich.

Z przeprowadzonych badań wynika, że najczęstszym typem treści jaki pojawia się w materiałach publikowanych na witrynie, są te o charakterze politycznym. Spośród 91 zbadanych artykułów wystąpiły one w aż 81 z nich, co stanowi ponad 89%. Treści polityczne niezwykle często były zestawiane z treściami militarnymi oraz społecznymi. Są to drugie w kolejności najczęściej pojawiające się typy treści, tj. treści militarne – 42 razy oraz treści społeczne – 52 razy. Widoczne były również treści gospodarcze oraz ideologiczne. Pierwszy ze wskazanych typów pojawił się 22 razy oraz dotyczył w przeważającej mierze kwestii

¹⁷⁵¹ TASS: *Poland*. <https://tass.com/tag/poland> (dostęp: 08.08.2024).

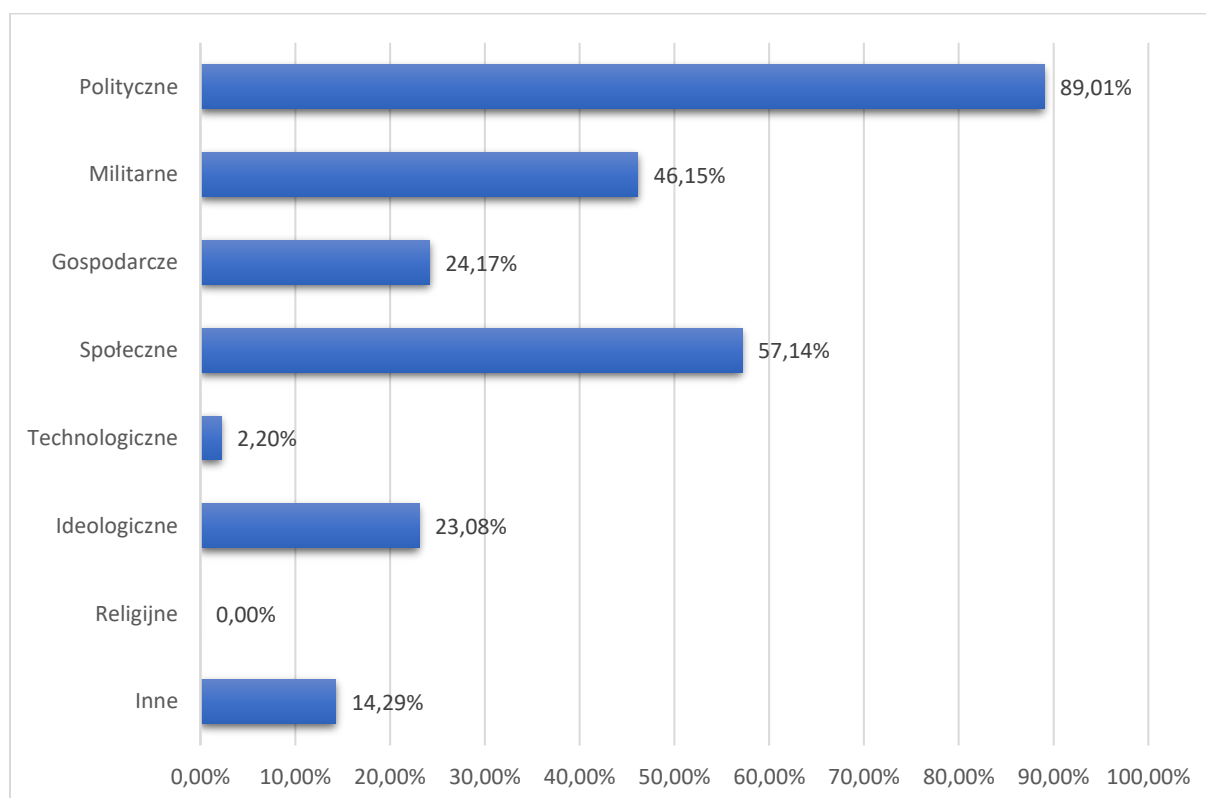
związanej z dostawami surowców energetycznych do Polski, a więc odnosił się do kwestii spornej w stosunkach polsko-rosyjskich jaką jest dywersyfikacja źródeł energii. Drugi typ, tj. treści ideologiczne występowały w odniesieniu do problemów dotyczących postrzegania wspólnej historii przez Polskę oraz Rosję. Dotyczyło to głównie kwestii związanych z II wojną światową, a precyzyjniej (w ocenie Kremla) z wyzwolenczą rolą Armii Czerwonej oraz niszczeniem pomników i cmentarzy (miejsc pamięci) w Polsce, przez władze w Warszawie. Zauważalne było również poruszanie treści o charakterze ideologicznym w kontekście kryzysu migracyjnego na granicy polsko-białoruskiej, który rozpoczął się w 2021 roku. Spośród wszystkich zbadanych artykułów w żadnym nie pojawiły się treści o charakterze religijnym, a w zaledwie dwóch przypadkach poruszono tematy związane z technologią. Warto również zwrócić uwagę, że poza powyższymi rodzajami treści, w artykułach publikowanych na portalu w 13 przypadkach poruszono inne ich typy. Były to przede wszystkim treści dotyczące prawa (5 razy), historii (1 raz), szpiegostwa (1 raz), sportu (3 razy), środowiska (1 raz), koronawirusa (1 raz) oraz współpracy międzynarodowej (1 raz).

Wykres 40. Typy treści w artykułach opublikowanych na witrynie internetowej agencji informacyjnej TASS w latach 2010-2022.



Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

Wykres 41. Procentowe występowanie typów treści w artykułach opublikowanych na witrynie internetowej agencji informacyjnej TASS w latach 2010-2022.



Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

W odniesieniu do poszczególnych rodzajów wydarzeń na arenie międzynarodowej, na portalu agencji informacyjnej TASS omawiano przede wszystkim aneksję Półwyspu Krymskiego i wojnę we wschodniej Ukrainie (2014), pełnowymiarową wojnę rosyjsko-ukraińską (2022), współpracę wojskową Polski w ramach NATO (szczególnie z USA), kryzys migracyjny na granicy polsko-białoruskiej (2021), eksplozję rakiety (incydent) w Przewodowie (2021) oraz dostawy surowców energetycznych do Polski z Federacji Rosyjskiej (stosunki biznesowe polskiego PGNiG oraz rosyjskiego Gazpromu). Ponadto, w swoich materiałach TASS regularnie poruszał temat niszczenia pomników żołnierzy Armii Czerwonej w Polsce, krytykując działania polskich władz w zakresie dekomunizacji przestrzeni publicznej, przedstawiając je jako element wrogiej polityki historycznej wymierzonej przeciwko Rosji. Omawiana była również katastrofa samolotu rządowego z Prezydentem Rzeczypospolitej Polskiej w Smoleńsku (2010), szczególnie w kontekście różnic w narracji strony polskiej i rosyjskiej dotyczącej przyczyn tragedii.

Zdjęcie 28.



RUSSIAN NEWS AGENCY

EU ignoring Poland's, Lithuania's cruelty to migrants — Russian diplomat

Polish and Lithuanian border guards are violating "all possible international conventions and norms of civilized behavior," Dmitry Polyansky pointed out

UNITED NATIONS, November 23. /TASS/. It is inhumane of the European Union to ignore Poland's and Lithuania's cruelty to migrants at the border with Belarus, Russian First Deputy Permanent Representative to the United Nations Dmitry Polyansky said on Tuesday.

Źródło: TASS¹⁷⁵².

Zdjęcie 29.



RUSSIAN NEWS AGENCY

Medvedev blasts Poland's 'talentless politicians puppeteered by US' who fuel Russophobia

The Deputy Chairman of the Russian Security Council expressed confidence that people in Poland "will understand sooner or later that hatred toward Russia doesn't promote social cohesion, well-being or peace"

Źródło: TASS¹⁷⁵³.

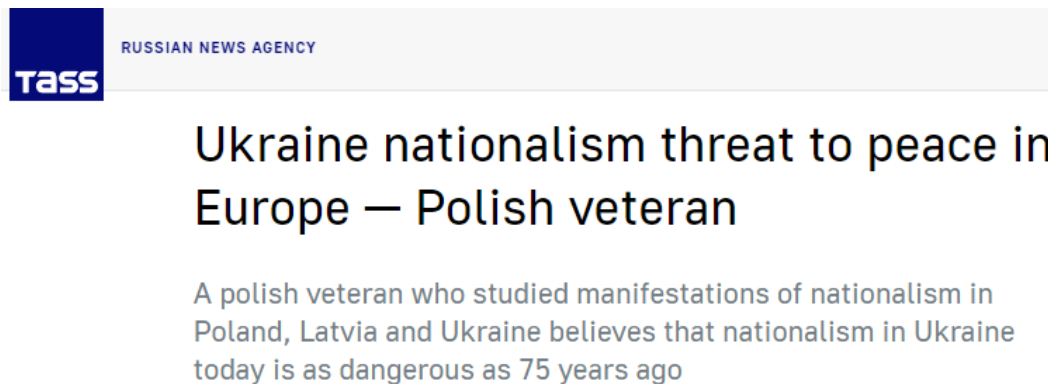
¹⁷⁵² TASS: *EU ignoring Poland's, Lithuania's cruelty to migrants — Russian diplomat*. <https://tass.com/world/1365325> (dostęp: 03.11.2024). Tłumaczenie własne: UE ignoruje okrucieństwo Polski i Litwy wobec migrantów - rosyjski dyplomata. Polscy i litewscy strażnicy graniczni naruszają „wszystkie możliwe międzynarodowe konwencje i normy cywilizowanego zachowania” – zauważył Dmitrij Polanski. NOWY JORK, 23 listopada. /TASS/. To nieludzkie, że Unia Europejska ignoruje okrucieństwo Polski i Litwy wobec migrantów na granicy z Białorusią – powiedział we wtorek pierwszy zastępca stałego przedstawiciela Rosji przy ONZ, Dmitrij Polanski.

¹⁷⁵³ TASS: *Medvedev blasts Poland's 'talentless politicians puppeteered by US' who fuel Russophobia*. <https://tass.com/politics/1425035> (dostęp: 03.11.2024). Tłumaczenie własne: Miedwiediew krytykuje Polskę za „beztalencie polityków sterowanych przez USA”, którzy podsycają rusofobię. Zastępca przewodniczącego Rady Bezpieczeństwa Rosji wyraził przekonanie, że ludzie w Polsce „prędzej czy później zrozumieją, że nienawiść do Rosji nie sprzyja spójności społecznej, dobrobytowi ani pokojowi”.

W publikowanych artykułach wyraźnie dominują treści dotyczące Ukrainy, lecz nie tylko w kontekście aneksji Półwyspu Krymskiego przez Rosję oraz rozpoczętej przez Kreml w 2022 roku pełnoskalowej inwazji na to państwo, ale również takie które sugerują, że działania polskiego rządu zmierzają do rozpadu Ukrainy oraz przejęcia przez Polskę części jej terytorium. Treści te w sposób jednoznaczny mają na celu antagonizowanie relacji polsko-ukraińskich, wskazując na wrogie zamiary Polski, ale również podkreślając niechęć Ukraińców do Polaków.

Należy również zasygnalizować, iż w artykułach publikowanych przez TASS bardzo często pojawiają się odniesienia do Białorusi w kontekście stosunków polsko-białoruskich oraz polsko-rosyjskich. Szczególna intensyfikacja treści o tej tematyce miała miejsce w 2021 i 2022 roku, co miało związek z kryzysem migracyjnym na granicy polsko-białoruskiej, a później rosyjskiej inwazji na Ukrainę. W przypadku kryzysu migracyjnego, artykuły publikowane przez TASS w 2021 roku odnosiły się co do zasady wyłącznie do jego tematyki. W samym 2021 roku opublikowano kilkanaście wiadomości prezentujących sytuację na granicy polsko-białoruskiej.

Zdjęcie 30.



Źródło: TASS¹⁷⁵⁴.

¹⁷⁵⁴ TASS: *Ukraine nationalism threat to peace in Europe — Polish veteran*. <https://tass.com/world/783246> (dostęp: 03.11.2024). Tłumaczenie własne: Ukraiński nacjonalizm zagrożeniem dla pokoju w Europie — polski weteran. Polski weteran, który badał przejawy nacjonalizmu w Polsce, na Łotwie i Ukrainie, uważa, że nacjonalizm na Ukrainie jest dziś tak samo niebezpieczny, jak 75 lat temu.

Zdjęcie 31.



RUSSIAN NEWS AGENCY

Kremlin aide certain Poland will "snatch" Ukraine's western regions if given half a chance

Vladimir Medinsky mentioned a historical precedent set by Poland's similar actions

MOSCOW, May 18. /TASS/. Poland will not hesitate to seize lands in western Ukraine should such an opportunity offer itself, Russian Presidential Aide Vladimir Medinsky said on Wednesday.

Źródło: TASS¹⁷⁵⁵.

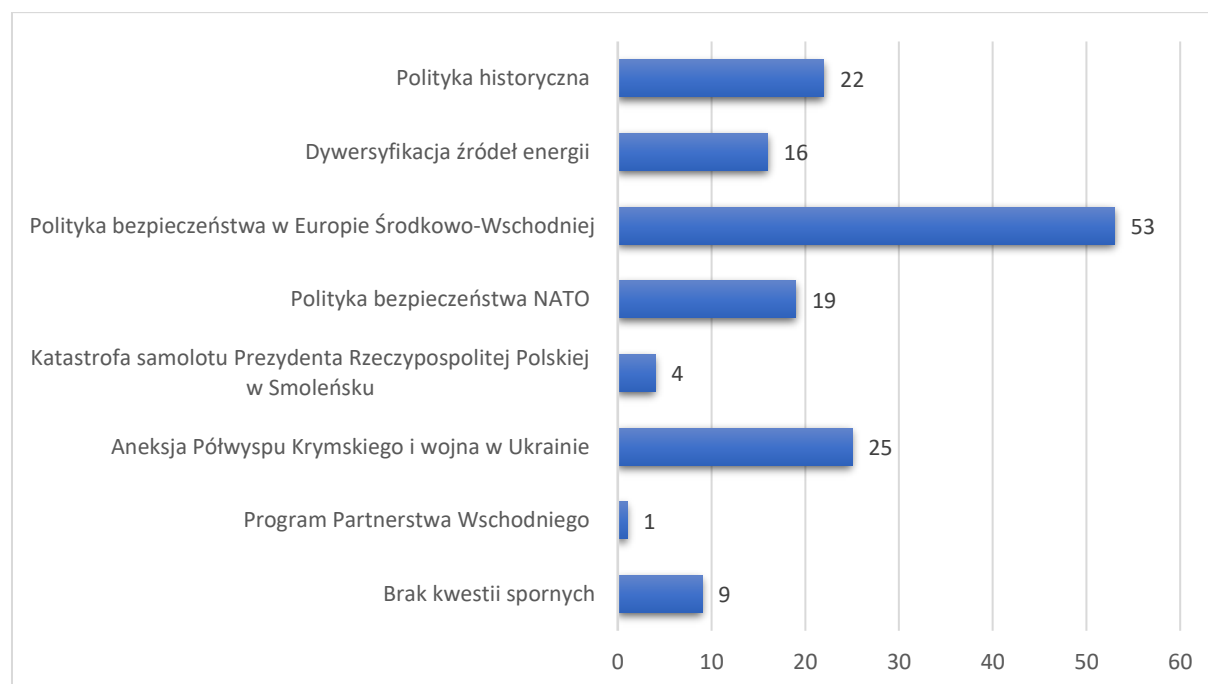
Typy treści publikowane przez portal internetowy agencji informacyjnej TASS odnosiły się przede wszystkim do tematyki politycznej, społecznej oraz militarnej. W mniejszym stopniu do gospodarczej oraz ideologicznej. Treści technologiczne występowały marginalnie, a religijnych nie zidentyfikowano w ogóle. Publikowane materiały korelowały z aktualnymi wydarzeniami w stosunkach polsko-rosyjskich, jak i stałymi kwestiami spornymi które w ramach nich występują. Publikowane artykuły odnosiły się do spraw istotnych w danym czasie dla Kremla, wspierając i promując rosyjski punkt widzenia. Nie wydaje się być szczególnym zaskoczeniem (mając na względzie charakter badanego podmiotu), że TASS będąc rządową agencją informacyjną *de facto* kolportował treści formułowane przez Kreml. Można więc wyprowadzić ogólne stwierdzenie, że tematyka poruszana w ramach relacji bilateralnych znajdowała swoje odzwierciedlenie w treściach zamieszczanych na stronie internetowej agencji.

¹⁷⁵⁵ TASS: *Kremlin aide certain Poland will "snatch" Ukraine's western regions if given half a Chance*. <https://tass.com/world/1452849> (dostęp: 03.11.2024). Tłumaczenie własne: Kremlowski doradca pewny, że Polska „zagarnie” zachodnie regiony Ukrainy, jeśli tylko nadarzy się okazja. Władimir Medinski wspominał o historycznym precedensie związanym z podobnymi działaniami Polski. MOSKWA, 18 maja. /TASS/. Polska nie zawaha się przejąć ziem w zachodniej Ukrainie, jeśli nadarzy się taka okazja – powiedział w środę doradca prezydenta Rosji, Władimir Medinski.

7.2.3. Polsko-rosyjskie kwestie sporne w treściach publikowanych na witrynie internetowej agencji informacyjnej TASS

W ramach założeń metodologicznych poczynionych na potrzeby badań przyjęto następujące kwestie sporne występujące w stosunkach polsko-rosyjskich: polityka historyczna, dywersyfikacja źródeł energii, polityka bezpieczeństwa w Europie Środkowo-Wschodniej, polityka bezpieczeństwa NATO, katastrofa samolotu rządowego z Prezydentem Rzeczypospolitej Polskiej w Smoleńsku, aneksja Półwyspu Krymskiego i wojna w Ukrainie oraz program Partnerstwa Wschodniego¹⁷⁵⁶. Z przeprowadzonych badań wynika, że w 82 spośród 91 zbadanych artykułów występowała co najmniej jedna z przyjętych kwestii spornych. W przypadku 9 artykułów nie pojawiła się żadna z nich, a od 2020 roku w zasadzie każdy z opublikowanych materiałów odnosił się do jakiegokolwiek kwestii spornej. Początkowo w artykułach zaobserwowano treści dotyczące jednej bądź dwóch kwestii spornych, z kolei od 2020 roku zauważalne było odnoszenie się do nawet trzech czy czterech kwestii spornych występujących w stosunkach bilateralnych.

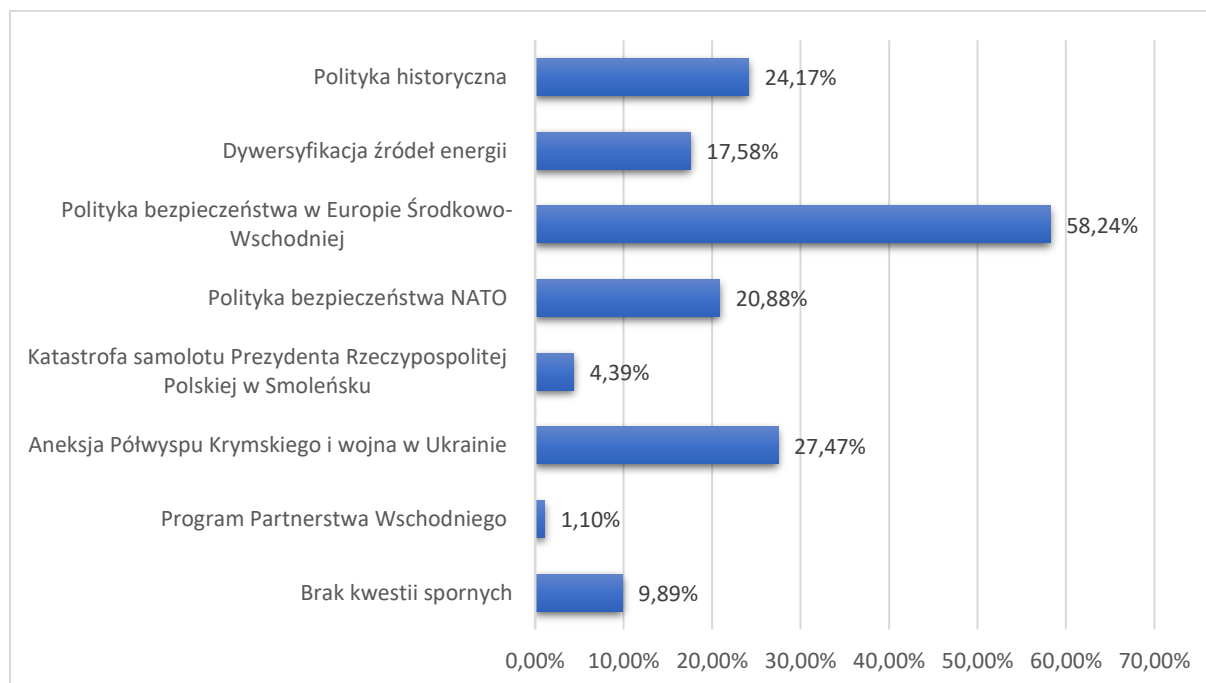
Wykres 42. Liczba zidentyfikowanych kwestii spornych w stosunkach polsko-rosyjskich w artykułach opublikowanych na witrynie internetowej agencji informacyjnej TASS w latach 2010-2022.



Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

¹⁷⁵⁶ Zobacz szerzej w rozdziale metodologicznym.

Wykres 43. Procentowe występowanie zidentyfikowanych kwestii spornych w stosunkach polsko-rosyjskich w artykułach opublikowanych na witrynie internetowej agencji informacyjnej TASS w latach 2010-2022.



Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

Spośród opublikowanych przez TASS artykułów najwięcej, bo aż 53, dotyczyło kwestii spornej związanej z polityką bezpieczeństwa w Europie Środkowo-Wschodniej. Zagadnienie to było często łączone z dywersyfikacją źródeł energii, która wystąpiła w publikacjach agencji informacyjnej TASS 16 razy, polityką bezpieczeństwa NATO, która pojawiła się 19 razy oraz aneksją Półwyspu Krymskiego i wojną w Ukrainie, do której odnosiło się 25 opublikowanych materiałów.

Początkowo, artykuły publikowane w latach 2014-2015 skupiały się na kwestiach historycznych dotyczących II wojny światowej (problemach w interpretacji wydarzeń przez Polskę i Federację Rosyjską) oraz dywersyfikacji źródeł energii, co jest szczególnie ciekawe w kontekście trwających ówczesnie napięć międzynarodowych związanych z rosyjską aneksją Półwyspu Krymskiego oraz wojną we wschodniej Ukrainie. Wydarzenia dotyczące tego zagadnienia na przestrzeni lat 2014-2021 pojawiły się w publikowanych materiałach zaledwie 8 razy. Dla porównania, w samym 2022 roku nawiązania do wojny na Ukrainie wystąpiły 17 razy.



RUSSIAN NEWS AGENCY

NORD STREAM GAS LEAK INVESTIGATION 28 SEP 2022, 03:19

Former Polish Foreign Minister Sikorski thanks US for damaging Nord Stream

According to Radoslaw Sikorsky, it limits Russia's room for maneuver

WARSAW, September 28. /TASS/. Radoslaw Sikorski, a European Parliament member and a former Polish foreign minister, has thanked the US for damaging the Nord Stream.

"A small thing, but so much joy," he said on Twitter, posting a photo of the accident site to accompany the tweet and assigning it the hashtag #Nordstream.

"Thank you, USA," he said in the following tweet, with the same picture.

Źródło: TASS¹⁷⁵⁷.

Powyższe zdjęcie przedstawia tekst nawiązujący do wpisu na Twitterze R. Sikorskiego, w którym podziękował on USA za zniszczenie gazociągu Nord Stream II po inwazji Rosji na Ukrainę w 2022 roku. Ostatecznie wpis zniknął z konta polityka, jednak szybko został podchwycony przez rosyjskie media propagandowe. Opisano go w kontekście przyznania się Zachodu do realizowania działań o charakterze terrorystycznym przeciwko Federacji Rosyjskiej. Przykładowo D. Poljański, pierwszy zastępca stałego przedstawiciela Rosji przy ONZ, napisał: „Dziękujemy, Radosławie Sikorski, za wyjaśnienie, kto stoi za tym terrorystycznym atakiem na infrastrukturę cywilną”¹⁷⁵⁸.

¹⁷⁵⁷ TASS: *Former Polish Foreign Minister Sikorski thanks US for damaging Nord Stream*. <https://tass.com/world/1514367> (dostęp: 03.11.2024). Tłumaczenie własne: Były szef MSZ Polski Sikorski dziękuje USA za uszkodzenie Nord Stream. Według Radosława Sikorskiego ogranicza to pole manewru Rosji. WARSZAWA, 28 września. /TASS/. Radosław Sikorski, poseł do Parlamentu Europejskiego i były minister spraw zagranicznych Polski, podziękował USA za uszkodzenie Nord Stream. „Mała rzecz, a cieszy” – napisał na Twitterze, dodając zdjęcie miejsca awarii i oznaczając je hasztagiem #Nordstream. „Dziękuję, USA” – dodał w kolejnym tweecie, używając tego samego zdjęcia.

¹⁷⁵⁸ Rzeczpospolita: *Kontrowersyjny wpis o wycieku z Nord Stream zniknął z konta Sikorskiego*. <https://www.rp.pl/polityka/art37145071-kontrowersyjny-wpis-o-wycieku-z-nord-stream-zniknal-z-konta-sikorskiego> (dostęp: 02.11.2024).

Zdjęcie 33.



RUSSIAN NEWS AGENCY

MILITARY OPERATION IN UKRAINE 29 APR 2022, 11:37

Poland sends to Ukraine over 200 T-72 tanks, several dozen infantry carriers — radio

It is reported that this number of tanks is enough to form two brigades

WARSAW, April 29. /TASS/. Polish authorities sent to Ukraine more than 200 T-72 tanks and several dozen armored infantry carriers, Polskie Radio reported on Friday.

Źródło: TASS¹⁷⁵⁹.

Jak wskazano wcześniej, w latach 2014-2015 można było zaobserwować intensyfikację w zakresie publikacji materiałów dotyczących historii w stosunkach polsko-rosyjskich. Niezmiennie treści historyczne odnosiły się do dwóch zagadnień. Po pierwsze, do roli Armii Czerwonej jako wyzwoliciela Europy spod okupacji nazistowskich Niemiec, oraz po drugie, do prowadzenia przez Polskę działań mających na celu umniejszanie pamięci o roli ZSRR, jaką odegrał podczas II wojny światowej. Miało mieć to miejsce poprzez niszczenie miejsc pamięci w Polsce – demontaż pomników oraz dewastację cmentarzy czerwonoarmistów. Narracja ta była kontynuowana w 2016 roku oraz pojawiała się niezmiennie na przestrzeni kolejnych lat. Łącznie zagadnienia dotyczące polityki historycznej pojawiły się 25 razy (na 91 artykułów), co pokazuje, jak istotną rolę Kreml przywiązuje do tych tematów. Szczególną intensyfikację poruszania tych zagadnień należy wiązać z siedemdziesiątą rocznicą zakończenia II wojny światowej, która miała miejsce w 2015 roku oraz z uchwaleniem przez polski parlament w 2016 roku ustawy o zakazie propagowania komunizmu lub innego ustroju totalitarnego przez nazwy jednostek organizacyjnych, jednostek pomocniczych gminy, budowli, obiektów i urządzeń użyteczności publicznej oraz pomniki. Przyjęty akt prawny spowodował masową zmianę nazw

¹⁷⁵⁹ TASS: *Poland sends to Ukraine over 200 T-72 tanks, several dozen infantry carriers — radio*. <https://tass.com/defense/1445261> (dostęp: 02.11.2024). Tłumaczenie własne: Polska wysłała do Ukrainy ponad 200 czołgów T-72 i kilkadziesiąt transporterów piechoty — radio. Podano, że taka liczba czołgów wystarczy do sformowania dwóch brygad. WARSZAWA, 29 kwietnia. /TASS/. Polskie władze wysłały na Ukrainę ponad 200 czołgów T-72 oraz kilkadziesiąt opancerzonych transporterów piechoty – poinformowało w piątek Polskie Radio.

ulic, placów oraz sposobów eksponowania pomników (miejsc pamięci), co skutkowało stanowczym sprzeciwem ze strony Kremla.

Zdjęcie 34.



RUSSIAN NEWS AGENCY

"Attempts are being made to eradicate the memory of the Soviet soldier-liberators from the minds of the Europeans since the earliest days, both at home and at school. They are being told a distorted version of World War II history, with traces of whitewashing for which they should be ashamed. As a consequence, the number of acts of vandalism against Soviet memorials abroad is on the rise," he said.

Bogdanov noted that, in many countries, the destruction of war memorials is not only approved officially, but is also considered patriotism of a sort. Even more, the authorities of some countries effectively ignore international agreements, with Poland being the most egregious example.

"The Polish authorities came up with the concept of so-called symbolic memorials, which must be de-communized, despite it contradicting the agreements between our countries on burials and places of memory of the heroes of war and victims of repressions, signed on February 22, 1994," the senior diplomat underscored.

He added that Polish authorities also violate the list of memorials of the Soviet defenders of the Homeland who are laid to rest on Polish territory.

"This paper used to include 561 objects. Currently, by March 31 this year, according to our embassy in Warsaw, only 112 of these objects remain in this foreign state," Bogdanov said. "In violation of agreements, 449 Soviet memorials, installed outside burial sites, were eliminated."

TAGS

Poland

Źródło: TASS¹⁷⁶⁰.

¹⁷⁶⁰ TASS: *Vandalism against memorials to Soviet warriors on the rise abroad, says diplomat*. <https://tass.com/world/1292073> (dostęp: 02.11.2024). Tłumaczenie własne: „Od najwcześniejszych lat podejmowane są próby wykorzenia z umysłów Europejczyków pamięci o sowieckich żołnierzach-wyzwolicielach, zarówno w domu, jak i w szkole. Przekazywana jest im zniekształcona wersja historii II wojny światowej, wybielona w sposób, za który powinni się wstydzić. W konsekwencji rośnie liczba aktów wandalizmu wobec sowieckich pomników za granicą” – powiedział. Bogdanow zauważył, że w wielu krajach niszczenie pomników wojennych jest nie tylko oficjalnie aprobowane, ale wręcz uważane za pewną formę patriotyzmu. Co więcej, władze niektórych państw skutecznie ignorują międzynarodowe porozumienia, a najbardziej rażącym przykładem jest Polska. „Polskie władze wymyśliły koncepcję tzw. symbolicznych pomników, które muszą zostać zdekomunizowane, mimo że stoi to w sprzeczności z umowami między naszymi krajami dotyczącymi pochówków oraz miejsc pamięci bohaterów wojny i ofiar represji, podpisanymi 22 lutego 1994 roku” – podkreślił wysoki rangą dyplomata. Dodał, że polskie władze naruszają także listę pomników sowieckich obrońców Ojczyzny, którzy spoczywają na terytorium Polski. „Dokument ten obejmował kiedyś 561 obiektów. Obecnie, według informacji naszej ambasady na Warszawie na dzień 31 marca tego roku, w tym obcym państwie pozostało jedynie 112 z tych obiektów” – powiedział Bogdanow. „Wbrew umowom zlikwidowano 449 sowieckich pomników znajdujących się poza miejscami pochówku”.

Zdecydowanie marginalne znaczenie w publikowanych przez TASS materiałach miała katastrofa samolotu rządowego z Prezydentem Rzeczypospolitej Polskiej w Smoleńsku, która pojawiła się zaledwie 4 razy, tj. 1 raz w 2022 roku oraz 3 razy w 2016 roku. Należy jednak zaznaczyć, że wyodrębnione do badań artykuły zostały opublikowane w latach 2014-2022, co może tłumaczyć tak niewielkie występowanie tego zagadnienia¹⁷⁶¹. Trzeba bowiem wziąć pod uwagę, że katastrofa miała miejsce w 2010 roku, a więc z pewnością to właśnie w tamtym czasie skupiano się na relacjonowaniu tego wydarzenia. Podobnie, zainteresowanie Programem Partnerstwa Wschodniego również było znikome, gdyż temat ten został poruszony tylko raz w jednym z artykułów opublikowanych w 2019 roku. Program ten choć o znaczącej roli w polityce europejskiej, miał w publikowanych materiałach marginalne znaczenie.

Kluczową kwestią sporną poruszaną w publikowanych przez TASS artykułach była polityka bezpieczeństwa w Europie Środkowo-Wschodniej, która dominowała na tle innych przyjętych na potrzeby badań. Jest to zagadnienie, które przez cały badany okres stanowiło jeden z głównych problemów w relacjach bilateralnych, czym należy uzasadnić tak częste jego występowanie. Widoczne były również (choć zauważalnie rzadziej) takie kwestie jak polityka historyczna, dywersyfikacja źródeł energii, polityka bezpieczeństwa NATO oraz aneksja Półwyspu Krymskiego i wojna na Ukrainie. Można stwierdzić, że kwestie sporne zdominowały publikowane przez TASS treści, gdyż tylko w przypadku 9 artykułów spośród 91 zbadanych, nie zidentyfikowano żadnej z nich. Stanowi to niecałe 10% ogólnej liczby artykułów. Warto przypomnieć, że w przypadku portalu informacyjnego Sputnik News International liczba artykułów, w których nie zidentyfikowano żadnej kwestii spornej wynosiła 118 ogólnej ich liczby, co przekłada się na niecałe 33%. W przypadku artykułów zawierających *tag Poland* było to 38 artykułów (około 36%). Widać więc w sposób zauważalny, że tematyka problemów występujących w stosunkach polsko-rosyjskich jest poruszana zdecydowanie częściej, niż w przypadku omówionego wcześniej portalu informacyjnego. Może to być spowodowane faktem, że w przeciwieństwie do Sputnik News International, TASS jest rządową agencją informacyjną, kolportującą treści pochodzące bezpośrednio z Kremla i na jego polecenie.

¹⁷⁶¹ Zobacz szerzej w rozdziale metodologicznym.

Zdjęcie 35.



RUSSIAN NEWS AGENCY

RUSSIA'S DEFENSE INDUSTRY 4 MAY 2015, 13:37

Poland's president signs law on establishing Polish-Lithuanian-Ukrainian military brigade

The brigade will be formed as part of the European Union's combat groups with an aim to participate in operations under the UN, NATO and EU aegis

Źródło: TASS¹⁷⁶².

Zdjęcie 36.



RUSSIAN NEWS AGENCY

29 NOV 2021, 11:32

West uses migrants against Belarus in case of Russia-Ukraine conflict — Lukashenko

As the Belarusian president noted, the West was aware that should Ukraine try to start a conflict with Russia, Belarus would not remain an idle spectator

MINSK, November 29. /TASS/. Belarusian President Alexander Lukashenko believes that the West is using migrants as a means to distract the Belarusian army in case of a Russia-Ukraine conflict.

Źródło: TASS¹⁷⁶³.

¹⁷⁶² TASS: *Poland's president signs law on establishing Polish-Lithuanian-Ukrainian military brigade*. <https://tass.com/world/792931> (dostęp: 02.11.2024). Tłumaczenie własne: Prezydent Polski podpisuje ustawę o utworzeniu polsko-litewsko-ukraińskiej brygady wojskowej. Brygada zostanie sformowana w ramach grup bojowych Unii Europejskiej z zamiarem udziału w operacjach pod auspicjami ONZ, NATO i UE.

¹⁷⁶³ TASS: *West uses migrants against Belarus in case of Russia-Ukraine conflict — Lukashenko*. <https://tass.com/world/1367773> (dostęp: 03.11.2024). Tłumaczenie własne: Zachód wykorzystuje migrantów przeciwko Białorusi w przypadku konfliktu Rosja-Ukraina — Łukaszenko. Jak zauważył prezydent Białorusi, Zachód był świadomy, że jeśli Ukraina spróbuje rozpocząć konflikt z Rosją, Białoruś nie pozostanie biernym obserwatorem. MINSK, 29 listopada. /TASS/. Prezydent Białorusi Aleksander Łukaszenko uważa, że Zachód wykorzystuje migrantów jako środek do odwrócenia uwagi białoruskiej armii w przypadku konfliktu Rosja-Ukraina.

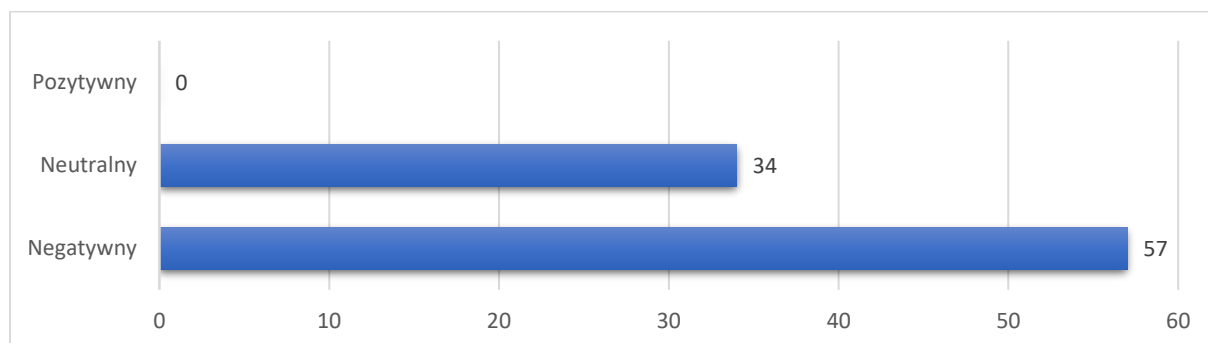
7.2.4. *Framing* treści na witrynie internetowej agencji informacyjnej TASS

Na potrzeby badań przyjęto następujące rodzaje *framingu*, tj. pozytywny, neutralny oraz negatywny¹⁷⁶⁴. Spośród wszystkich 91 wyodrębnionych do badań artykułów, żaden nie kształtował wizerunku Polski w sposób pozytywny, 34 z nich kształtowały go w sposób neutralny, a aż 57 w sposób negatywny.

Zaobserwowano, że w latach 2014-2015 nie można było wskazać jednoznacznie w jaki sposób publikowane treści prezentują Polskę, tzn. około połowa artykułów przedstawiała Polskę neutralnie (13 artykułów), a druga połowa negatywnie (15 artykułów). Zmiana w tym zakresie nastąpiła w 2016 roku i od tego momentu wizerunek Polski był prezentowany przede wszystkim w sposób negatywny, incydentalnie w sposób neutralny. Powodem tego może być szczyt NATO zorganizowany we wskazanym roku w Warszawie, podczas którego podjęto decyzję o zwiększeniu zaangażowania Sojuszu na jego wschodniej flance. O wysłanie do Polski i innych państw regionu dodatkowych wojsk NATO w sposób szczególny zabiegała Warszawa, co z kolei Kreml postrzegał jako zagrożenie dla bezpieczeństwa Federacji Rosyjskiej i ingerencję Zachodu w obszar będący w bezpośredniej bliskości jego strefy wpływów. Nie powinien dziwić natomiast fakt, że żaden z artykułów opublikowanych przez TASS, nie kształtował wizerunku Polski w sposób pozytywny. Liczba oraz znaczenie kwestii spornych w stosunkach bilateralnych, ale również kierunki prowadzonej przez Warszawę i Moskwę polityki zagranicznej sprawiają, że Polska jest dla Federacji Rosyjskiej raczej przeciwnikiem niż partnerem – co zostało szczegółowo omówione w poprzednich częściach pracy. Ponadto, nawet jeśli konkretne działania Polski omawiane w ramach publikowanych przez TASS treści, można by uznać co do zasady za pozytywne, to i tak były one prezentowane raczej neutralnie, poprzez wskazywanie konkretnych faktów, bez nadawania im określonego charakteru. Nie zamieszczano więc ocen danych faktów, a jedynie o nich informowano, w szerszym bądź węższym zakresie.

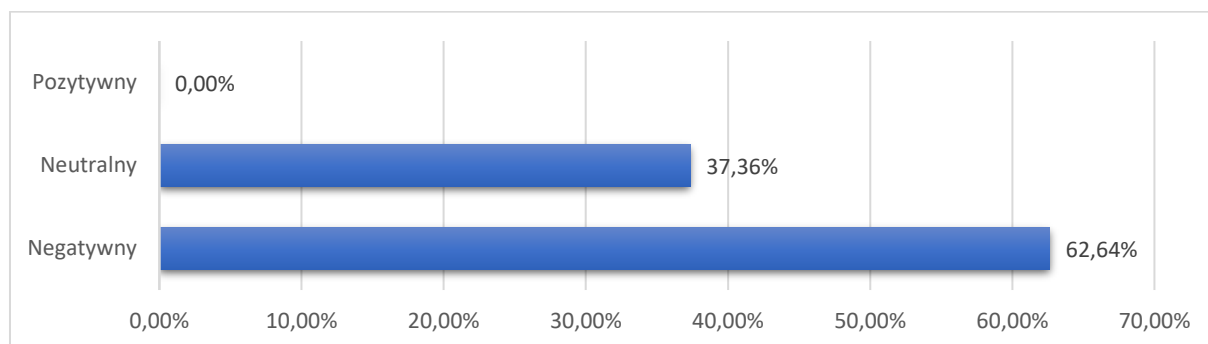
¹⁷⁶⁴ Zobacz szerzej w rozdziale metodologicznym.

Wykres 44. Rodzaj *framingu* treści na witrynie internetowej agencji informacyjnej TASS w latach 2010-2022.



Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

Wykres 45. Procentowe występowanie rodzajów *framingu* treści na witrynie internetowej agencji informacyjnej TASS w latach 2010-2022.



Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

Analizując sposób kreowania wizerunku Polski można zaobserwować, że jest on formułowany negatywnie, co do zasady zawsze, gdy poruszana jest kwestia sporna dotycząca polityki historycznej. Chodzi więc przede wszystkim o wydarzenia odnoszące się do II wojny światowej oraz roli ZSRR i Armii Czerwonej w jej zakończeniu, jak również dotyczące upamiętniania tych wydarzeń (miejsca pamięci w postaci pomników i cmentarzy). Podobnie wizerunek Polski jest kształtowany przede wszystkim w sposób negatywny, gdy poruszane są zagadnienia dotyczące polityki bezpieczeństwa w Europie Środkowo-Wschodniej, polityki bezpieczeństwa NATO oraz aneksji Półwyspu Krymskiego i wojny na Ukrainie. Polityka rządu w Warszawie jest przedstawiana jako konfrontacyjna wobec Federacji Rosyjskiej, skrajnie rusofobiczna, zmierzająca do destabilizacji pokoju i bezpieczeństwa w regionie, jak również dążąca do wykorzenienia pamięci o pozytywnej roli jaką zdaniem Moskwy odegrał ZSRR podczas II wojny światowej w pokonaniu nazistowskich Niemiec.

Zdjęcie 37.



RUSSIAN NEWS AGENCY

MOSCOW, December 22. /TASS/. Polish authorities have undermined relations with Moscow for many years as well as the work of experts seeking to study challenging issues of the two countries' history, Russian Foreign Ministry Spokeswoman Maria Zakharova told TASS on Sunday.

"Warsaw's representatives for many years have undermined the work of experts and bilateral relations," Zakharova said commenting on the Polish Foreign Ministry's statement in connection with Russian President Vladimir Putin's remark on World War II. "Aggressive rhetoric and the demolition of monuments to fighters against fascism and playing the first fiddle in imposing the EU's anti-Russian sanctions are the direct evidence of this."

During his annual news conference on December 19, Putin recalled that the USSR was the last country in Europe, which signed the treaty on non-aggression with Germany, known as the Molotov-Ribbentrop Pact. Putin noted that the Soviet forces entered Poland in line with protocols under this pact, but earlier Poland had taken part in dividing Czechoslovakia. By the moment when the Soviet troops entered the territory, the Polish government had lost control over the armed forces and fled the country. As the Russian president said, "there was no one to talk to."

In response, the Polish Foreign Ministry voiced concerns over Putin's remark. In its statement, the ministry noted that Putin's words "represented a wrong picture of events" and aroused concerns and mistrust.

Russian-Polish experts are working as part of a commission on challenging historic issues in bilateral relations, set up to overcome contradictions over different viewpoints on the events of the past.

Źródło: TASS¹⁷⁶⁵.

¹⁷⁶⁵ TASS: *Russian diplomat says Poland has undermined bilateral ties for years.* <https://tass.com/politics/1102165> (dostęp: 03.11.2024). Tłumaczenie własne: MOSKWA, 22 grudnia. /TASS/. Władze Polski przez wiele lat podważały relacje z Moskwą, a także pracę ekspertów próbujących badać trudne kwestie związane z historią obu krajów – powiedziała w niedzielę rzeczniczka Ministerstwa Spraw Zagranicznych Rosji Maria Zacharowa w rozmowie z TASS. „Przedstawiciele Warszawy przez wiele lat podważyli pracę ekspertów i dwustronne relacje” – powiedziała Zacharowa, komentując oświadczenie Ministerstwa Spraw Zagranicznych Polski w związku z uwagami prezydenta Rosji Władimira Putina na temat II wojny światowej. „Agresywna retoryka, burzenie pomników bojowników przeciwko faszyzmowi oraz odgrywanie głównej roli w nakładaniu unijnych sankcji antyrosyjskich są bezpośrednim dowodem na to.” Podczas swojej corocznej konferencji prasowej 19 grudnia Putin przypomniał, że ZSRR było ostatnim krajem w Europie, który podpisał pakt o nieagresji z Niemcami, znany jako pakt Ribbentrop-Mołotow. Putin zaznaczył, że wojska radzieckie wkroczyły do Polski zgodnie z protokołami tego paktu, ale wcześniej Polska brała udział w podziale Czechosłowacji. W momencie, gdy wojska radzieckie wkroczyły na terytorium Polski, rząd polski stracił kontrolę nad siłami zbrojnymi i opuścił kraj. Jak stwierdził prezydent Rosji, „nie było z kim rozmawiać. „W odpowiedzi Ministerstwo Spraw Zagranicznych Polski wyraziło zaniepokojenie uwagami Putina. W swoim oświadczeniu ministerstwo zaznaczyło, że słowa Putina „stanowiły błędny obraz wydarzeń” i wywołały zaniepokojenie oraz brak zaufania. Rosyjsko-polscy eksperci pracują w ramach komisji ds. trudnych kwestii historycznych w relacjach dwustronnych, powołanej w celu przezwyciężenia sprzeczności wynikających z różnych punktów widzenia na wydarzenia z przeszłości.



RUSSIAN NEWS AGENCY

Orlen signs oil supply contract with Rosneft

Orlen refineries are currently supplied with oil on the basis of long-term contracts with suppliers from Saudi Arabia and Russia and on the spot basis from the Northern Sea region

WARSAW, March 16. /TASS/. Orlen signed a new contract with the Russian oil major Rosneft, stipulating reduction of oil supplies in 2022-2023 from 5.4-6.6 to 3.6 mln tonnes per year; the largest oil refining company in Poland says on Tuesday.

"The contract between Orlen and Rosneft in effect by January 31 of this year provided for oil supplies at the level of 5.4-6.6 mln tonnes per year. The new two-year contract stipulates that deliveries to Orlen refineries will amount to 3.6 mln tonnes per year," Orlen says.

"Monthly supplies under the contract will total 300,000 tonnes of feedstock. It corresponds to terms agreed during negotiations with the Russian side. The limitation of volumes does not affect security of deliveries to Orlen group refineries," the company says.

Orlen refineries are currently supplied with oil on the basis of long-term contracts with suppliers from Saudi Arabia and Russia and on the spot basis from the Northern Sea region. Early in March, Orlen signed a contract with ExxonMobil, stipulating deliveries of about 1 mln tonnes of feedstock per year in total for needs of Orlen refineries.

Źródło: TASS¹⁷⁶⁶.

¹⁷⁶⁶ TASS: *Orlen signs oil supply contract with Rosneft*. <https://tass.com/economy/1266603> (dostęp: 03.11.2024). Tłumaczenie własne: Orlen podpisuje umowę na dostawy ropy z Rosnieftem. Rafinerie Orlenu są obecnie zaopatrywane w ropę na podstawie długoterminowych umów z dostawcami z Arabii Saudyjskiej i Rosji oraz na miejscu z regionu Morza Północnego. WARSZAWA, 16 marca. /TASS/. Orlen podpisał nową umowę z rosyjskim gigantem naftowym Rosnieftem, przewidującą redukcję dostaw ropy w latach 2022-2023 z 5,4-6,6 do 3,6 mln ton rocznie, poinformowała we wtorek największa firma rafineryjna w Polsce. „Umowa między Orlenem a Rosnieftem, obowiązująca do 31 stycznia br., przewidywała dostawy ropy na poziomie 5,4-6,6 mln ton rocznie. Nowa dwuletnia umowa przewiduje, że dostawy do rafinerii Orlenu wyniosą 3,6 mln ton rocznie” – informuje Orlen. „Miesięczne dostawy w ramach umowy wyniosą łącznie 300 000 ton surowca. Odpowiada to warunkom ustalonym podczas negocjacji ze stroną rosyjską. Ograniczenie wolumenów nie wpływa na bezpieczeństwo dostaw do rafinerii grupy Orlen” – podaje spółka. Rafinerie Orlenu są obecnie zaopatrywane w ropę na podstawie długoterminowych umów z dostawcami z Arabii Saudyjskiej i Rosji oraz na zasadzie spot z regionu Morza Północnego. Na początku marca Orlen podpisał umowę z ExxonMobil, która przewiduje dostawy łącznie ok. 1 mln ton surowca rocznie na potrzeby rafinerii Orlenu.



RUSSIAN NEWS AGENCY

Medvedev blasts Poland's 'talentless politicians puppeteered by US' who fuel Russophobia

The Deputy Chairman of the Russian Security Council expressed confidence that people in Poland "will understand sooner or later that hatred toward Russia doesn't promote social cohesion, well-being or peace"

MOSCOW, March 21. /TASS/. The interests of Polish citizens are now being sacrificed on the altar of Russophobia by "talentless politicians" and their string-pullers "from across the ocean," Deputy Chairman of the Russian Security Council Dmitry Medvedev said in a post on Telegram in response to Warsaw's actions.

Źródło: TASS¹⁷⁶⁷.

W przypadku kwestii spornej dotyczącej dywersyfikacji źródeł energii, Polska jest przedstawiana raczej w sposób neutralny, sprowadzając prezentowane treści do omówienia punktów widzenia poszczególnych stron, bez jednoczesnego dokonania oceny każdego z nich. W przypadku Programu Partnerstwa Wschodniego Polska została przedstawiona negatywnie, natomiast w odniesieniu do katastrofy samolotu rządowego z Prezydentem Rzeczypospolitej Polskiej w Smoleńsku trzykrotnie neutralnie oraz jednokrotnie negatywnie. Co więcej, wyraźnie dostrzegalna jest prawidłowość, zgodnie z którą w sytuacji, gdy w danym artykule zawarte są cytaty poszczególnych osób (czy to polityków zachodnich czy kremlowskich), to mają one charakter raczej neutralny. Z kolei w sytuacji, gdy w danym artykule formułowana jest opinia samego autora, to wydzźwięk formułowanych treści staje się zdecydowanie bardziej negatywny.

¹⁷⁶⁷ TASS: *Medvedev blasts Poland's 'talentless politicians puppeteered by US' who fuel Russophobia*. <https://tass.com/politics/1425035> (dostęp: 03.11.2024). Tłumaczenie własne: Miedwiediew ostro krytykuje polskich „beztalencie polityków sterowanych przez USA”, którzy podsycają rusofobię. Wiceprzewodniczący Rady Bezpieczeństwa Rosji wyraził przekonanie, że ludzie w Polsce „wcześniej czy później zrozumieją, że nienawiść do Rosji nie sprzyja spójności społecznej, dobrobytowi ani pokojowi” MOSKWA, 21 marca. /TASS/. Interesy obywateli Polski są teraz składane w ofierze na ołtarzu rusofobii przez „beztalencie polityków” i ich „pociągaczy zza oceanu” — powiedział wiceprzewodniczący Rady Bezpieczeństwa Rosji Dmitrij Miedwiediew w poście na Telegramie w odpowiedzi na działania Warszawy.

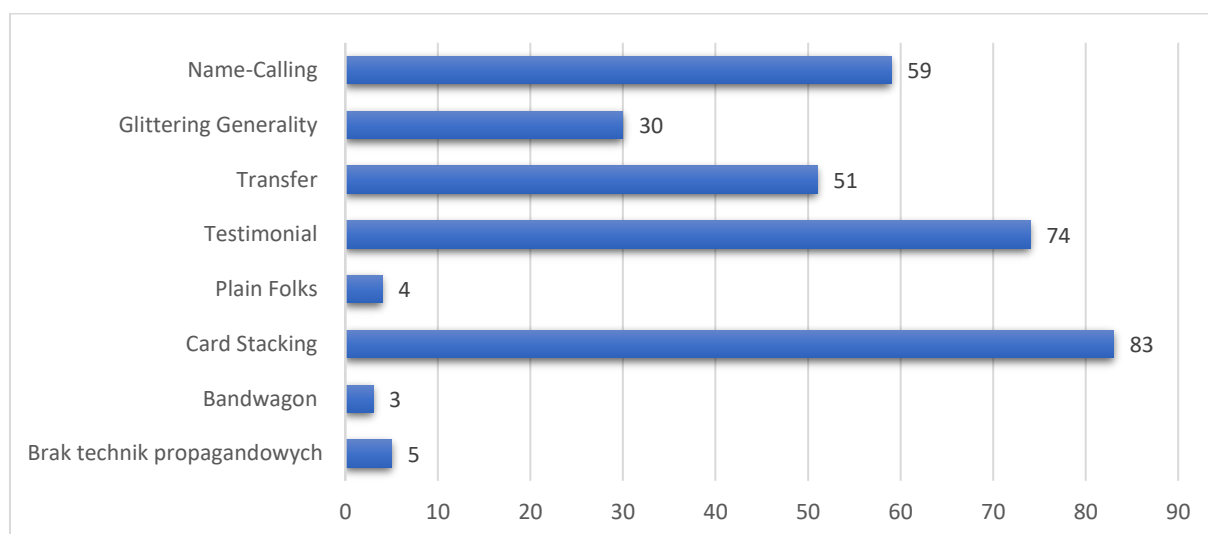
7.2.5. Techniki propagandowe stosowane na witrynie internetowej agencji informacyjnej TASS

Z przeprowadzonych badań wynika, że w treściach publikowanych na witrynie agencji informacyjnej TASS występują techniki propagandowe w typologii stworzonej przez The Institute for Propaganda Analysis, tj. *Name-Calling* (etykietowanie), *Glittering Generalities* (błyskotliwe ogólniki), *Transfer* (transfer), *Testimonial* (świadectwo autorytetu), *Plain Folks* (prosty człowiek), *Card Stacking* (tasowanie kart), *Bandwagon* (owczy pęd)¹⁷⁶⁸. Spośród 91 poddanych badaniom artykułów tylko 5 z nich nie zawierało żadnej techniki propagandowej z wyżej wymienionych.

Najczęściej występującymi technikami w publikowanych artykułach były *Name-Calling*, *Transfer*, *Testimonial* oraz *Card Stacking*. Ostatnia z wymienionych została użyta najwięcej razy, co pozwoliło na jej zidentyfikowanie w aż 83 materiałach (ponad 91%). Jej stosowanie służy do bieżącego wspierania oddziaływania propagandy na odbiorców, a w przypadku treści publikowanych przez TASS polegało przede wszystkim na odpowiedniej selekcji argumentów oraz prezentowania określonych wydarzeń bez jednoczesnego osadzenia ich w należytych kontekście. Najczęściej było to więc formułowanie półprawd lub fałszu w celu przedstawienia danej idei czy problemu. Drugą najczęściej stosowaną techniką była *Testimonial*, która została zidentyfikowana 74 razy (ponad 81%). Z kolei technika *Name-Calling* wystąpiła w przypadku 59 artykułów (około 65%), natomiast *Transfer* w 51 (około 56%). Technika *Name-Calling* opierała się na wykorzystywaniu sformułowań wartościujących dane zjawisko lub zagadnienie w sposób negatywny, takich jak: rusofobia, konfrontacja, prowokacja, agresja czy destabilizacja. Technika ta była bardzo często łączona z techniką *Transfer*, w przypadku której starano się przerzucać odpowiedzialność za określone działania Rosji, poprzez wykazanie, że analogiczne, podobne, bądź związane z tym działania podejmowały inne państwa, przede wszystkim Polska oraz kraje zachodnie. Kolejną techniką która wystąpiła 30 razy (około 33%) była *Glittering Generalities*, z kolei najrzadziej identyfikowane były takie techniki jak *Plain Folks* (4 razy – około 4%) oraz *Bandwagon* (3 razy – około 3%).

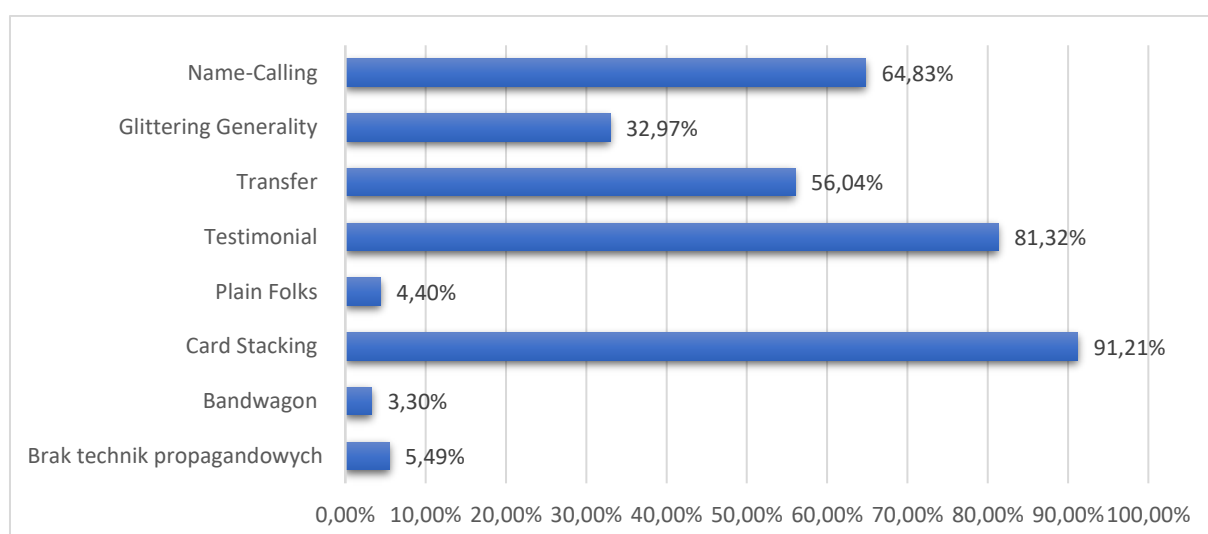
¹⁷⁶⁸ Zobacz szerzej w rozdziale metodologicznym.

Wykres 46. Zastosowane techniki propagandowe w artykułach opublikowanych na witrynie internetowej agencji informacyjnej TASS w latach 2010-2022.



Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

Wykres 47. Procentowe występowanie technik propagandowych w artykułach opublikowanych na witrynie internetowej agencji informacyjnej TASS w latach 2010-2022.

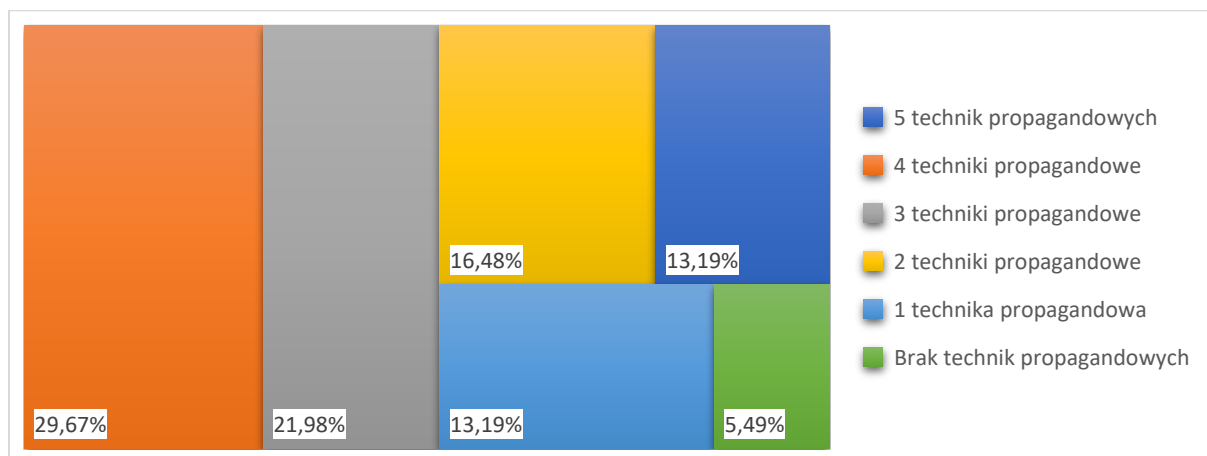


Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

Na podstawie przeprowadzonych badań nie można jednoznacznie wskazać, aby jakieś określone rodzaje technik propagandowych występowały w przypadku określonych treści, poruszających konkretne kwestie sporne. Nie można więc wskazać, aby wybrane techniki były wykorzystywane do prezentowania wybranych zagadnień z zakresu stosunków polsko-rosyjskich. Można jednak zauważyć, że liczba stosowanych technik propagandowych

w publikowanych treściach z roku na rok wzrastała. I o ile w latach 2014-2015 liczba wykorzystanych w danym tekście technik wynosiła co do zasady jedną lub dwie, tak w kolejnych latach były to przeważnie trzy bądź cztery techniki, ale również pięć. W 91 poddanych badaniom artykułach, pięć technik propagandowych zastosowano w przypadku 12 z nich, cztery techniki propagandowe wykorzystano w 27 z nich, trzy techniki w 20, dwie techniki w 15, jedną technikę w 12 oraz jak już wskazano w 5 artykułach nie zidentyfikowano żadnej.

Wykres 48. Procentowe występowanie (nasycenie) technik propagandowych w artykułach opublikowanych na witrynie internetowej agencji informacyjnej TASS w latach 2010-2022.



Źródło: Opracowanie własne na podstawie otrzymanych wyników badań.

W powyższym kontekście warto zauważyć, że artykuły publikowane w latach 2014-2015 charakteryzują się często bardzo krótką formą, ograniczając się niemal wyłącznie do kilku zdań które przekazują ogólną informację na dany temat. W kolejnych latach zauważalna jest jednak wyraźna zmiana – objętość tekstów stopniowo rośnie, a artykuły stają się bardziej rozbudowane, zawierając szerszy kontekst, szczegółowe analizy oraz głębsze omówienie poruszanych zagadnień. Takie zmiany wskazują na ewolucję podejścia do tematyki kwestii spornych występujących w stosunkach polsko-rosyjskich oraz modyfikowania sposobu oddziaływania informacyjnego na odbiorców portalu.



RUSSIAN NEWS AGENCY

28 OCT 2022, 20:07

Medvedev advises Warsaw to never forget multibillion-dollar Soviet aid

It is reported that one more option is an adamant refusal to take into account Warsaw's demands

MOSCOW, October 28. /TASS/. Deputy Chairman of Russia's Security Council Dmitry Medvedev has suggested replying with a firm refusal or a counter-claim to Warsaw's demands for compensating for "war damage," allegedly caused to Poland by the Soviet Union during World War II.

In a post uploaded to his Telegram channel on Friday, he said that such demands "can be responded to in two ways."

"It might be possible to put forward a counter-claim, a bill for everything that the Soviet Union shared with Poland during the period of socialism. That's hundreds of billions of dollars," Medvedev said about one proposed option.

Or, he continued, there can be another one - an adamant refusal to take into account Warsaw's demands.

TAGS

Foreign policy Poland

Źródło: TASS¹⁷⁶⁹.

¹⁷⁶⁹ TASS: *Medvedev advises Warsaw to never forget multibillion-dollar Soviet aid.* <https://tass.com/politics/1529445> (dostęp: 02.11.2024). Tłumaczenie własne: Medwediew radzi Warszawie, aby nigdy nie zapomniała o wielomiliardowej pomocy radzieckiej. Podaje się, że inną opcją jest stanowcza odmowa uwzględnienia żądań Warszawy. MOSKWA, 28 października. /TASS/. Wiceprzewodniczący Rady Bezpieczeństwa Rosji Dmitrij Miedwediew zasugerował odpowiedź stanowczą odmową lub kontrpozewem na żądania Warszawy dotyczące rekompensaty za „szkody wojenne”, rzekomo wyrządzone Polsce przez Związek Radziecki podczas II wojny światowej. We wpisie opublikowanym na swoim kanale Telegram w piątek powiedział, że na takie żądania „można odpowiedzieć na dwa sposoby”. „Można by wysunąć kontrpozew, rachunek za wszystko, czym Związek Radziecki dzielił się z Polską w okresie socjalizmu. To setki miliardów dolarów” — powiedział Medwediew o jednej z proponowanych opcji. Albo, kontynuował, może być inna — stanowcza odmowa uwzględnienia żądań Warszawy.



RUSSIAN NEWS AGENCY

Poland's lower house votes to brand Russia 'state sponsor of terrorism'

The resolution was adopted with 231 votes for, while 226 parliamentarians abstained from voting

WARSAW, December 15. /TASS/. The lower house of Poland's parliament, the Sejm, voted on Wednesday night to declare Russia a country that supports terrorism.

The resolution was adopted with 231 votes in favor of the initiative, while 226 legislators abstained.

"The Sejm of the Republic of Poland recognizes the Russian Federation as a country that supports terrorism and a state that uses means of terrorism," the lower house said in a statement.

According to the resolution, Russia bears "direct responsibility" for the MH17 crash in July 2014 and the crash of a Polish government delegation flight near Smolensk in April 2010.

Poland's lawmakers adopted the resolution in their second bid. Last week, no voting was held due to a protest by the opposition.

The Sejm's resolution is symbolic and non-binding. It serves as an opinion expressed on current domestic or foreign affairs, and is not a legal act. As a rule, such resolutions are meant either to support actions by the government or to shine the official spotlight on a certain problem.

TAGS
Poland

Źródło: TASS¹⁷⁷⁰.

¹⁷⁷⁰ TASS: *Poland's lower house votes to brand Russia 'state sponsor of terrorism'*. <https://tass.com/world/1550711> (dostęp: 03.11.2024). Tłumaczenie własne: Izba niższa polskiego parlamentu głosuje za uznaniem Rosji za „państwo sponsorujące terroryzm”. Rezolucja została przyjęta 231 głosami za, podczas gdy 226 parlamentarzystów wstrzymało się od głosu. WARSZAWA, 15 grudnia. /TASS/. Sejm, izba niższa polskiego parlamentu, zagłosował w środę wieczorem za uznaniem Rosji za kraj wspierający terroryzm. Rezolucja została przyjęta 231 głosami za inicjatywą, podczas gdy 226 parlamentarzystów wstrzymało się od głosu. „Sejm Rzeczypospolitej Polskiej uznaje Federację Rosyjską za kraj wspierający terroryzm i państwo stosujące środki terrorystyczne” – stwierdziła izba niższa w oświadczeniu. Zgodnie z rezolucją Rosja ponosi „bezpośrednią odpowiedzialność” za katastrofę lotu MH17 w lipcu 2014 r. i katastrofę samolotu polskiej delegacji rządowej pod Smoleńskiem w kwietniu 2010 r. polscy ustawodawcy przyjęli rezolucję w swoim drugim głosowaniu. W zeszłym tygodniu nie odbyło się głosowanie z powodu protestu opozycji. Uchwała Sejmu ma charakter symboliczny i niewiążący. Stanowi opinię wyrażoną na temat bieżących spraw krajowych lub

Analizując otrzymane wyniki badań w kontekście zastosowanych technik propagandowych, należy uwzględnić charakter działalności podmiotu który je stosuje. Warto bowiem zauważyć, że TASS nie jest zwykłym portalem informacyjnym kolportującym rosyjską propagandę, lecz rządową agencją informacyjną, której treści często odzwierciedlają oficjalne stanowisko Kremla w danej sprawie. Co więcej, materiały publikowane przez TASS jako rządową agencję informacyjną, są często wykorzystywane przez media na całym świecie we własnych przekazach. Powoduje to, że mają one znaczny wpływ na globalną przestrzeń medialną oraz znaczenie w kształtowaniu opinii publicznej, zarówno w wymiarze narodowym, jak i międzynarodowym. Oznacza to, że wizerunek Polski który jest kształtowany w określony sposób w publikowanych artykułach (najczęściej negatywny), dociera do większości państw na świecie. W konsekwencji, działalność TASS realizuje cele polityki zagranicznej Federacji Rosyjskiej wobec Polski, podważając jej pozycję na arenie międzynarodowej oraz prezentując jako państwo niestabilne i niegodne zaufania.

Z przeprowadzonych badań wynika, że wiadomości publikowane na stronie TASS nie cechują się jawną i bezpośrednią propagandą – takie przypadki są raczej rzadkie. W treściach publikowanych przez TASS przedstawiane jest bowiem nie tylko stanowisko Moskwy, ale również innych państw, których dotyczą omawiane zagadnienia. Często stosowana jest konstrukcja komunikatu, w ramach której najpierw podawane jest stanowisko państwa trzeciego, a następnie punkt widzenia Kremla w którym wskazuje się, dlaczego opinia tego państwa jest błędna lub nieprawdziwa. Taki sposób prezentowania treści ma na celu ukazanie, że stanowisko Federacji Rosyjskiej jest jedynym słusznym, a inne opinie są nieuzasadnione. Szczególnie widoczne było to w przypadku artykułów dotyczących eksplozji rakiety w Przewodowie w Polsce w 2022 roku, gdzie najpierw przedstawiano stanowiska innych państw, a na końcu zamieszczano komunikat Ministerstwa Obrony Federacji Rosyjskiej, który je dementował. Ponadto powielano narrację, że Rosja nie ma nic wspólnego z tą sytuacją i nie ponosi za nią odpowiedzialności, a odmienne poglądy określano jako umyślną i celową prowokację.

zagranicznych i nie jest aktem prawnym. Z reguły takie uchwały mają na celu albo wsparcie działań rządu, albo zwrócenie uwagi opinii publicznej na pewien problem.



RUSSIAN NEWS AGENCY

Washington, Warsaw work jointly to gather info on blast in east Poland — White House

"We've seen these reports out of Poland and are working with the Polish government to gather more information," National Security Council Spokesperson Adrienne Watson has said

WASHINGTON, November 16. /TASS/. The United States is working with the government of Poland to gather additional information about blasts in the east of the country, National Security Council Spokesperson Adrienne Watson has said.

"We've seen these reports out of Poland and are working with the Polish government to gather more information. We cannot confirm the reports or any of the details at this time. We will determine what happened and what the appropriate next steps would be," she wrote on Twitter on Tuesday.

Poland's Radio Zet reported on Tuesday with reference to unofficial sources that two missiles hit grain dryers in the village of Przewodów in eastern Poland's Lublin Voivodeship, close to the border with Ukraine. According to the report, two people were killed in the incident. The report makes no mention of the origin of those missiles.

The Russian Defense Ministry dismissed as a "deliberate provocation" Polish media reports about the alleged fall of Russian missiles in Poland on Tuesday, adding that the Russian military has performed no strikes targeting the Ukrainian-Polish border zone. "The wreckage published by Polish mass media from the scene in Przewodów have no relation to Russian firepower," the ministry said in a statement.

Źródło: TASS¹⁷⁷¹.

¹⁷⁷¹ TASS: *Washington, Warsaw work jointly to gather info on blast in east Poland — White House*. <https://tass.com/world/1537277> (dostęp: 03.11.2024). Tłumaczenie własne: Waszyngton, Warszawa współpracują w celu zebrania informacji o wybuchu we wschodniej Polsce — Biały Dom. „Widzieliśmy te raporty z Polski i współpracujemy z polskim rządem w celu zebrania większej ilości informacji” — powiedziała rzeczniczka Rady Bezpieczeństwa Narodowego Adrienne Watson. WASZYNGTON, 16 listopada. /TASS/. Stany Zjednoczone współpracują z polskim rządem w celu zebrania dodatkowych informacji o wybuchach na wschodzie kraju, powiedziała rzeczniczka Rady Bezpieczeństwa Narodowego Adrienne Watson. „Widzieliśmy te raporty z Polski i współpracujemy z polskim rządem w celu zebrania większej ilości informacji. Nie możemy potwierdzić tych raportów ani żadnych szczegółów w tej chwili. Ustalimy, co się stało i jakie będą odpowiednie następne kroki” - napisała we wtorek na Twitterze. Radio Zet poinformowało we wtorek, powołując się na nieoficjalne źródła, że dwa pociski uderzyły w suszarnie zbożowe we wsi Przewodów w województwie lubelskim we wschodniej Polsce, blisko granicy z Ukrainą. Według doniesień w incydencie zginęły dwie osoby. W raporcie nie wspomniano o pochodzeniu tych pocisków. Rosyjskie Ministerstwo Obrony odrzuciło jako „celową prowokację” doniesienia polskich mediów o rzekomym upadku rosyjskich pocisków w Polsce we wtorek, dodając, że rosyjskie wojsko nie

Co ciekawe, TASS nie unika cytowania polityków czy publicystów z państw zachodnich, a wręcz przeciwnie. Wielokrotnie można było zidentyfikować pierwszoplanowych decydentów politycznych, jak na przykład Prezydent USA, Prezydent Polski, Minister Spraw Zagranicznych Polski, Sekretarz Generalny NATO, Przedstawiciele Unii Europejskiej oraz Organizacji Narodów Zjednoczonych, jak również ekspertów z zakresu wojskowości. Niemniej jednak cytaty powyższych osób były wielokrotnie kontrastowane z wypowiedziami przeciwnymi D. Miedwiediewa (były Prezydent oraz Premier Federacji Rosyjskiej), A. Łukaszenki (Prezydenta Republiki Białorusi), M. Zacharowej (Rzeczniczki Ministerstwa Spraw Zagranicznych Federacji Rosyjskiej), D. Pieskowa (Rzecznika Prezydenta Federacji Rosyjskiej) czy S. Andriejewa (Ambasadora Federacji Rosyjskiej w Polsce). Należy również podkreślić, że wypowiedzi polityków państw zachodnich nie były prezentowane w sposób obiektywny, gdyż zdarzało się, iż były wyrywane z kontekstu w celu nadania im pożądanego wydźwięku.

Przykładem opisanego wyżej schematu działania był artykuł poświęcony byłemu Prezydentowi Polski, L. Wałęsie, w którym wskazywał on rzekomych polskich sprawców katastrofy smoleńskiej, jednocześnie pomijając okoliczności niekorzystne dla strony rosyjskiej. W artykule tym próbowano nadać jego słowom określoną interpretację, pomijając kontekst, w jakim zostały one wypowiedziane. Sformułowanie, że odpowiedzialność za katastrofę ponosi Polska (a więc w domyśle nie ponosi jej Federacja Rosyjska), wypowiedziane przez L. Wałęsę, laureata Pokojowej Nagrody Nobla, miała poprzez jego autorytet i uznanie na arenie międzynarodowej legitymizować prawdziwość tej tezy. Początek artykułu, którego fragment został przedstawiony poniżej brzmiał „Były prezydent Polski i laureat Pokojowej Nagrody Nobla Lech Wałęsa obarczył winą za katastrofę polskiego samolotu prezydenckiego pod Smoleńskiem 10 kwietnia 2010 r. braci Kaczyńskich”¹⁷⁷².

przeprowadziło żadnych ataków na ukraińsko-polską strefę graniczną. „Wrak opublikowany przez polskie media masowego przekazu z miejsca zdarzenia w Przewodzie nie ma nic wspólnego z rosyjską siłą ognia” – stwierdziło ministerstwo w oświadczeniu.

¹⁷⁷² TASS: *Polish ex-president blames Kaczynski brothers for Tu-154M plane near Smolensk*. <https://tass.com/world/868868> (dostęp: 02.11.2024).

Zdjęcie 43.



RUSSIAN NEWS AGENCY

WARSAW, April 11 /TASS/. Poland's former president and Nobel Peace Prize winner Lech Valenca has put the blame for the April 10, 2010 Polish presidential plane crash near Smolensk on the Kaczynski brothers.

READ ALSO

Poland's DefMin may ask NATO for assistance in Tu-154M jet fragments transfer case



"If the truth wins, I shall bet that the Kaczynski brothers will turn out to be responsible for the tragedy near Smolensk," Valenca, the leader of Poland's famous Solidarity trade union, wrote on his page in Facebook on Monday. The crash came as a consequence of irresponsible decisions, "a desire to use the Katyn theme in the election race and for plenty of other reasons," Valenca explained.

On April 10, 2010, an official Polish delegation led by the then Polish President Lech Kaczynski flew onboard of a TU-154M government plane to Katyn, a village near the Russian city of Smolensk, to attend the commemorations of the Katyn massacre - a mass execution of Polish officers in the Katyn forest in 1940. The pilots decided to land the plane in conditions of bad visibility and the absence of visual contact with the Earth. The plane

Źródło: TASS¹⁷⁷³.

Konkludując, można wyprowadzić jeszcze jeden wniosek, zgodnie z którym techniki propagandowe stosowane przez autorów artykułów na stronie internetowej agencji informacyjnej TASS nie zawsze były od razu dostrzegalne już po pierwszej, pobieżnej analizie tekstu. Propaganda w tym przypadku była bowiem bardzo subtelna, delikatna, a momentami wręcz zakamuflowana. Z pełną pewnością można stwierdzić, że publikowane treści są starannie sformułowane i skrupulatnie przemyślane. Oczywiście w tekstach zamieszczonych na portalu można odnaleźć fragmenty które stanowią jawną propagandę, niemniej jednak są to wyjątki, a nie reguła. Podobnie jak w przypadku portalu informacyjnego Sputnik News International stosowane techniki propagandowe służyły wspieraniu stanowiska Federacji Rosyjskiej,

¹⁷⁷³ Ibidem. Tłumaczenie własne: WARSZAWA, 11 kwietnia /TASS/. Były prezydent Polski i laureat Pokojowej Nagrody Nobla Lech Wałęsa zrzucił winę za katastrofę polskiego samolotu prezydenckiego 10 kwietnia 2010 r. pod Smoleńskiem na braci Kaczyńskich. „Jeśli prawda zwycięży, obstawiam, że bracia Kaczyńscy okażą się odpowiedzialni za tragedię pod Smoleńskiem” – napisał Wałęsa, lider słynnego polskiego związku zawodowego Solidarność, na swojej stronie na Facebooku w poniedziałek. Katastrofa była konsekwencją nieodpowiedzialnych decyzji, „chęci wykorzystania tematu Katynia w wyścigu wyborczym i z wielu innych powodów” – wyjaśnił Wałęsa. 10 kwietnia 2010 r. oficjalna polska delegacja pod przewodnictwem ówczesnego prezydenta Polski Lecha Kaczyńskiego poleciała na pokładzie rządowego samolotu TU-154M do Katynia, wsi niedaleko rosyjskiego miasta Smoleńsk, aby wziąć udział w obchodach upamiętniających zbrodnię katyńską - masową egzekucję polskich oficerów w lesie katyńskim w 1940 r. Piloci zdecydowali się wylądować samolotem w warunkach złej widoczności i braku kontaktu wzrokowego z Ziemią. Samolot (...).

formułowanego w ramach kwestii spornych występujących w relacjach bilateralnych. Ich celem było również prezentowanie Polski jako państwa niewiarygodnego i antyrosyjskiego. Publikowane treści stanowiły więc odzwierciedlenie stanowiska Kremla.

Zdjęcie 44.



RUSSIAN NEWS AGENCY

MOSCOW, June 30. /TASS/. The director of Russia's foreign intelligence service SVR, Sergey Naryshkin, has said that, according to SVR sources the Polish leadership has begun to work on scenarios of dismembering Ukraine, the SVR's press-bureau told TASS on Thursday.

"Warsaw has analyzed the situation to arrive at a painful conclusion that it will be impossible, contrary to statements by the Western politicians and military, to prevent the forces of Russia, the DPR and the LPR from coping with the tasks of the special operation and to prevent Russia's victory on the battlefield. In this connection the Poles see the prospects for the Zelensky regime's political survival as 'disappointing.' In the emerging 'critical' circumstances Warsaw tends to go beyond the previously planned deployment of a Polish 'peacekeeping contingent' in western Ukraine," the press-bureau says, citing the SVR director's statement.

"One of the options on the agenda is creating on the Kresy Wschodnie (Eastern Borderlands) a Poland-controlled proxy state 'under the protection' of the Polish armed forces. Alongside this a plan is being considered for converting Ukraine's central regions into a buffer zone, which, Poland hopes, will help it avoid an extremely undesirable direct clash with Russia," Naryshkin said.

According to the Russian foreign intelligence, the Polish authorities are certain that the United States and Britain will be forced to support this plan. "Warsaw believes that as Russian troops advance deep into Ukrainian territory, Washington and London will have no choice other than to display 'unconditional solidarity' with an ally who is ready to 'resolutely defend the interests of the West in Ukraine'," the SVR said.

TAGS

Ukraine United States United Kingdom Poland

Źródło: TASS¹⁷⁷⁴.

¹⁷⁷⁴ TASS: *Polish leadership begins work on scenarios of dismembering Ukraine — Russian intelligence*. <https://tass.com/world/1473919> (dostęp: 02.11.2024). Tłumaczenie własne: MOSKWA, 30 czerwca. /TASS/. Dyrektor rosyjskiej służby wywiadu zagranicznego SVR, Siergiej Naryszkin, powiedział, że według źródeł w SVR polskie kierownictwo zaczęło pracować nad scenariuszami rozczłonkowania Ukrainy, poinformowało biuro prasowe SVR w czwartek TASS. „Warszawa przeanalizowała sytuację i doszła do bolesnego wniosku, że wbrew oświadczeniom zachodnich polityków i wojskowych nie będzie można powstrzymać sił Rosji, DRL i ŁRL przed wykonaniem zadań operacji specjalnej i zapobiec zwycięstwu Rosji na polu bitwy. W związku z tym Polacy postrzegają perspektywę politycznego przetrwania reżimu Zelenskiego jako „rozczarowujące”. W pojawiających się „krytycznych” okolicznościach Warszawa ma tendencję do wykraczania poza wcześniej zaplanowane rozmieszczenie polskiego „kontyngentu sił pokojowych” na zachodniej Ukrainie”, mówi biuro prasowe, cytując oświadczenie dyrektora SVR. „Jedną z opcji na porządku dziennym jest utworzenie na Kresach Wschodnich kontrolowanego przez Polskę państwa zastępczego „pod ochroną” polskich sił zbrojnych. Jednocześnie rozważany jest plan przekształcenia centralnych regionów Ukrainy w strefę buforową, co, jak ma nadzieję Polska, pomoże jej uniknąć wyjątkowo niepożądanego bezpośredniego starcia z Rosją” – powiedział Naryszkin. Według

Kwestie sporne występujące w stosunkach polsko-rosyjskich korelują z treściami publikowanymi przez agencję informacyjną TASS. W artykułach zamieszczonych na witrynie występują techniki propagandowe, które nadają treściom odpowiednie brzmienie, zbieżne z celami rosyjskiej polityki zagranicznej wobec Polski. Treści te kształtują negatywny wizerunek Polski na arenie międzynarodowej, jako państwa prowadzącego politykę antyrosyjską i rusofobiczną. Działania rządu w Warszawie są prezentowane jako wrogie wobec Federacji Rosyjskiej, a sam rząd jako niegodny zaufania. Zauważalna pozostaje więc spójność w zakresie publikowanych przez TASS treści z polityką zagraniczną Rosji wobec Polski w latach 2010-2022.

rosyjskiego wywiadu zagranicznego polskie władze są pewne, że Stany Zjednoczone i Wielka Brytania zostaną zmuszone do poparcia tego planu. „Warszawa uważa, że gdy wojska rosyjskie wkroczą głęboko na terytorium Ukrainy, Waszyngton i Londyn nie będą miały innego wyboru, jak tylko okazać „bezwartunkową solidarność” sojusznikowi, który jest gotowy „zdecydowanie bronić interesów Zachodu na Ukrainie” – powiedział SWR.

Zakończenie

Federacja Rosyjska postrzegała i postrzega wojnę informacyjną jako kluczowy instrument swojej polityki zagranicznej. Zrozumienie roli informacji jako broni oraz umiejętność efektywnego wykorzystywania nowych technologii w działaniach informacyjnych pozwala Rosji na realizację przyjętych celów polityki zagranicznej. Istotny z tego punktu widzenia jest występujący w Federacji Rosyjskiej tzw. syndrom oblężonej twierdzy, który zakłada, że państwo pozostaje w nieustannym stanie zagrożenia ze strony podmiotów zewnętrznych. Uzasadnia to po stronie decydentów politycznych na Kremlu konieczność podejmowania działań, mających na celu przeciwdziałanie związanym z tym zagrożeniom. W tym kontekście jako niebezpieczeństwo Kreml postrzega w jego ocenie wrogą polską politykę zagraniczną, realizowaną nie tylko na kanwie stosunków na linii Warszawa-Moskwa, ale również w ramach członkostwa Polski w Unii Europejskiej i Sojuszu Północnoatlantyckim. W związku z tym Rosja musi korzystać z pełnego spektrum posiadanych przez siebie narzędzi realizacji polityki zagranicznej, a więc również z tych właściwych dla zjawiska wojny informacyjnej.

Wykorzystanie przez Federację Rosyjską narzędzi z zakresu wojny informacyjnej jest wszechstronne i nieograniczone. Obejmuje bowiem zarówno czas pokoju, jak i czas wojny, co udowodniły wydarzenia z poprzednich lat, tj. przykład Gruzji w 2008 roku czy Ukrainy w 2014 i 2022 roku. Rosyjska wojna informacyjna jest wielodomenowa, przez co należy rozumieć, że sprowadza się zarówno do działań ofensywnych w cyberprzestrzeni, jak i oddziaływania informacyjnego na odbiorców w świecie cyfrowym, które obejmuje różnorodne narzędzia propagandowe. Należy zauważyć, że wojna informacyjna w ujęciu rosyjskim może być prowadzona zarówno środkami wojskowymi i cywilnymi oraz w przestrzeni politycznej, społecznej, militarnej, gospodarczej, cybernetycznej, dyplomatycznej, psychologicznej i tym podobnych. Ponadto narzędzia właściwe dla rosyjskiej wojny informacyjnej mają na celu oddziaływanie o charakterze negatywnym.

Rozważania zawarte w niniejszej rozprawie pozwalają stwierdzić, że wojna informacyjna stanowiła istotny instrument polityki zagranicznej Federacji Rosyjskiej również wobec Polski w latach 2010-2022. W badanym okresie była prowadzona w sposób wszechstronny i nieograniczony. Rosyjska wojna informacyjna wobec Polski była ściśle związana z kluczowymi kwestiami spornymi w stosunkach dwustronnych. Działania te miały na celu destabilizację wewnętrzną Polski oraz osłabianie jej pozycji na arenie międzynarodowej. Wykorzystując różnice w interpretacji historii, kwestie dotyczące

dywersyfikacji źródeł energii, politykę bezpieczeństwa NATO, politykę bezpieczeństwa w Europie Środkowo-Wschodniej, katastrofę samolotu rządowego z Prezydentem RP pod Smoleńskiem, aneksję Półwyspu Krymskiego i wojnę we wschodniej Ukrainie oraz Program Partnerstwa Wschodniego, Federacja Rosyjska starała się wpływać na postawy społeczno-polityczne w Polsce i realizować swoje interesy, ale również kreować negatywny wizerunek Polski na świecie jako państwa niestabilnego i niewiarygodnego. Zrealizowanie badań w przedmiotowym zakresie z perspektywy rosyjskich koncepcji wojny informacyjnej, umożliwiło oddanie ich pełnego spektrum oraz zrozumienie charakteru, uwarunkowań i implikacji, jako narzędzia wykorzystywanego w ramach polityki zagranicznej. Z kolei przyjęcie długiej cezury czasowej pozwoliło lepiej zrozumieć naturę zachodzących procesów w ramach stosunków bilateralnych.

[HG] Przeprowadzone w ramach rozprawy badania pozwoliły potwierdzić główną hipotezę badawczą pracy. Polska, z uwagi na swoje geograficzne położenie oraz charakter prowadzonej polityki zagranicznej na kierunku wschodnim, pozostawała w szczególnym zainteresowaniu decydentów politycznych na Kremlu w badanym okresie, tj. w latach 2010-2022. Niezwykle trudne stosunki polsko-rosyjskie charakteryzowały się licznymi kwestiami spornymi, co wpływało negatywnie na relacje bilateralne. To z kolei spowodowało, że Federacja Rosyjska prowadziła z reguły wrogą politykę zagraniczną wobec Polski i tak też postrzegała polską politykę zagraniczną, która była wobec niej realizowana. Federacja Rosyjska wykorzystywała narzędzia z zakresu wojny informacyjnej do prowadzenia polityki zagranicznej wobec Polski. Przedmiotowa działalność Kremla była zauważalna na przestrzeni całego badanego okresu, przy czym z roku na rok ulegała co do zasady intensyfikacji. Niemniej jednak wnioski z badań wskazują, iż miała ona miejsce jeszcze przed 2010 rokiem i z całkowitą pewnością również po 2022 roku.

Rosyjskie koncepcje wojny informacyjnej postrzegały ją wielopłaszczyznowo, a więc odmiennie niż ma to miejsce w przypadku koncepcji zachodnich. W ujęciu rosyjskim, wojna informacyjna sprowadzała się po pierwsze do organizowania i przeprowadzania kampanii z zakresu oddziaływania informacyjnego na odbiorców w Internecie z wykorzystaniem wielu rodzajów mediów, w tym stron internetowych portali oraz agencji informacyjnych. Po drugie, wojna informacyjna polegała na jednoczesnym dokonywaniu ataków w cyberprzestrzeni poprzez paraliżowanie infrastruktury teleinformatycznej przeciwnika. Oba przedstawione wyżej zjawiska były wobec siebie komplementarne. Oznacza to, że kampanie oddziaływania informacyjnego były wspierane przez dokonywane cyberataki i odwrotnie, cyberataki były wspierane kampaniami oddziaływania informacyjnego. Działania, które były prowadzone

w omawianym zakresie przez Kreml, służyły więc jako narzędzie realizowania przez Federację Rosyjską polityki zagranicznej wobec Polski. Zauważyć należy, że aktywność Moskwy, polegająca na wykorzystywaniu narzędzi właściwych dla wojny informacyjnej, pozostawała w związku z aktualnym stanem stosunków polsko-rosyjskich. Oznacza to, że zarówno kampanie oddziaływania informacyjnego na odbiorców w Internecie jak i dokonywane ataki w cyberprzestrzeni swoim charakterem (w tym treścią) nawiązywały bezpośrednio do kwestii spornych w relacjach bilateralnych, wspierając narrację Kremla. Przykładowo, można wskazać w przedmiotowym kontekście na dwa wydarzenia. Po pierwsze, w związku z aneksją Półwyspu Krymskiego oraz wojną we wschodniej Ukrainie wzrosła liczba artykułów publikowanych na temat Polski, zarówno w przypadku portalu Sputnik News International jak i agencji informacyjnej TASS. Podobnie miało to miejsce w odniesieniu do dokonywanych przez Rosję cyberataków, których liczba od wskazanego wydarzenia systematycznie, co do zasady, rosła przez cały badany okres. Po drugie, aktywność badanych portali zwiększyła się wraz ze wzrostem napięć w relacjach na linii Moskwa-Zachód, poprzedzających pełnoskalową wojnę na Ukrainie oraz w związku z samą inwazją, do której doszło w 2022 roku.

Głównymi celami polityki zagranicznej Rosji realizowanej wobec Polski w badanym okresie było osłabianie struktur wewnątrzpaństwowych, pogłębianie podziałów społecznych, marginalizowanie pozycji Polski na arenie międzynarodowej, kreowanie jej negatywnego wizerunku na arenie międzynarodowej oraz podważanie jej wiarygodności jako partnera i sojusznika w Unii Europejskiej oraz NATO. Wszystkie ze wskazanych celów były realizowane przy użyciu omawianych narzędzi z zakresu wojny informacyjnej. Poddane badaniom strony internetowe rosyjskich mediów publikowały treści, które wpisywały się w oficjalną narrację Kremla w kontekście stosunków polsko-rosyjskich. Podobnie miało to miejsce w przypadku cyberataków, które były dokonywane w stosunku do celów mających bezpośredni lub pośredni związek z kwestiami spornymi występującymi w relacjach polsko-rosyjskich.

Znaczący zakres działalności Federacji Rosyjskiej, przejawiający się w rokrocznym, permanentnym dokonywaniem ataków na Polskę w cyberprzestrzeni, jak i liczba oraz charakter materiałów publikowanych przez rosyjskie i prorosyjskie media, wreszcie zestawienie tych działań z aktualnym stanem stosunków polsko-rosyjskich dowodzi, że wojna informacyjna jest nie tylko istotnym, co stale wykorzystywanym narzędziem realizowanej przez Federację Rosyjską wobec Polski polityki zagranicznej.

Wskazać należy, że przeprowadzone badania potwierdzają wszystkie sformułowane w ramach pracy hipotezy szczegółowe, które stanowią rozwinięcie hipotezy głównej. Po

pierwsze, rewolucja cyfrowa oraz postępujące przemiany technologiczne, stworzyły warunki sprzyjające wykorzystywaniu narzędzi z zakresu wojny informacyjnej na niespotykaną dotąd skalę [HS1]. Państwa mają świadomość znaczenia przestrzeni informacyjnej, wykorzystując ją jako narzędzie realizacji własnych interesów na arenie międzynarodowej oraz prowadząc przy tym działania, które wykraczają poza tradycyjne metody o charakterze militarnym i dyplomatycznym. Wprowadzenie do przestrzeni publicznej nowych form komunikacji i technologii pozwala na szybkie przekazywanie informacji w czasie rzeczywistym, ale stwarza jednocześnie potencjalne zagrożenia. Powstanie społeczeństwa informacyjnego w XX wieku i jego intensywny rozwój w XXI wieku przyczyniły się do pojawienia nowych wyzwań w zakresie bezpieczeństwa teleinformatycznego, zarówno na poziomie krajowym, jak i międzynarodowym. Skuteczne zarządzanie bezpieczeństwem informacyjnym wymaga natomiast nie tylko zastosowania zaawansowanych technologii ochrony infrastruktury, ale również wypracowania kompleksowych działań w zakresie prewencji, edukacji społecznej i współpracy międzynarodowej. Wojna informacyjna stała się nieodłącznym elementem sporów i konfliktów międzynarodowych, natomiast jej skutki pośrednie i bezpośrednie mogą mieć daleko idące konsekwencje dla bezpieczeństwa państw oraz porządku międzynarodowego.

Po drugie, badania dotyczące rosyjskiej wojny informacyjnej wskazują, że jest ona głęboko zakorzeniona w kulturze strategicznej Kremla [HS2]. Jej geneza sięga czasów Związku Socjalistycznych Republik Radzieckich. W okresie zimnej wojny oraz rywalizacji z blokiem zachodnim, ZSRR dostrzegał znaczenie informacji oraz propagandy w kształtowaniu opinii publicznej innych państw, a w konsekwencji zdobywaniu przewagi nad przeciwnikiem. Po rozpadzie ZSRR, Federacja Rosyjska jako sukcesorka tego państwa kontynuowała rozwijanie tych założeń, dostosowując je do postępu technologicznego, w tym rewolucji cyfrowej. Federacja Rosyjska postrzega wojnę informacyjną jako kluczowy instrument swojej polityki zagranicznej. Zrozumienie roli informacji jako broni oraz umiejętność efektywnego wykorzystywania nowych technologii w działaniach informacyjnych pozwala Rosji na realizację przyjętych celów polityki zagranicznej. Przeprowadzone badania pokazują, że Federacja Rosyjska skutecznie zaadaptowała się i adaptuje się do przemian technologicznych związanych z postępującą rewolucją informacyjną, wykorzystując nowoczesne technologie do prowadzenia wojny informacyjnej na niespotykaną dotąd skalę. Zaawansowana infrastruktura informacyjna Federacji Rosyjskiej umożliwia jej prowadzenie kampanii oddziaływania informacyjnego na poziomie globalnym – w zasadzie wobec każdego państwa. Do przykładów można zaliczyć anglojęzyczne media takie jak portal informacyjny Sputnik News International,

portal RT.com oraz agencja informacyjna TASS. W odniesieniu do działań realizowanych w cyberprzestrzeni są to wyspecjalizowane grupy APT, jak na przykład APT28, APT29, SandWorm czy Turla. To z kolei pozwala jej na kształtowanie opinii publicznej, destabilizowanie wewnętrzne innych państw oraz realizowanie własnych interesów na arenie międzynarodowej. Rosja doskonale rozumie znaczenie informacji jako kluczowego zasobu w sporach i konfliktach międzynarodowych, postrzegając narzędzia właściwe dla wojny informacyjnej jako narzędzie realizacji polityki zagranicznej. Potwierdzają to oficjalne dokumenty rządowe publikowane na przestrzeni wielu lat. Wynika z nich, że wojna informacyjna stanowi integralną część prowadzonej przez Rosję polityki zagranicznej. Jej celem jest wpływanie na procesy decyzyjne w innych państwach, budowanie własnego pozytywnego wizerunku na arenie międzynarodowej oraz zabezpieczanie interesów w swojej strefie wpływów.

Po trzecie, Polska ze względu na swoje położenie geograficzne w Europie Środkowo-Wschodniej znajduje się w zainteresowaniu Federacji Rosyjskiej podobnie jak wcześniej Związku Socjalistycznych Republik Radzieckich, a jeszcze wcześniej Imperium Rosyjskiego [HS3]. Istotnym aspektem z punktu widzenia relacji bilateralnych była w badanym okresie niezwykle duża asymetria na niekorzyść Polski, co wynikało z potencjału obu państw. Stosunki polsko-rosyjskie w całym badanym okresie miały zdecydowanie charakter sporny, co w ocenie Kremla wynikało z natury prowadzonej przez Warszawę polityki wschodniej, stojącej w opozycji do interesów rosyjskich w regionie Europy Środkowo-Wschodniej. Katastrofa samolotu rządowego z Prezydentem Rzeczypospolitej Polskiej pod Smoleńskiem do której doszło dnia 10 kwietnia 2010 roku paradoksalnie nie doprowadziła do normalizacji stosunków na linii Warszawa-Moskwa, lecz przeciwnie, stała się źródłem napięć i sporów. Stan ten utrzymywał się przez kolejne lata i definitywnie pogłębił w 2014 roku w związku z rosyjską aneksją Półwyspu Krymskiego oraz rozpoczęciem wojny we wschodniej Ukrainie. Ponadto, Polska jako członek Sojuszu Północnoatlantyckiego oraz Unii Europejskiej jest traktowana przez Kreml jako podmiot, który zagraża jego interesom, prowadząc działania antyrosyjskie. Sprowadza się to bowiem do postrzegania Polski jako ważnego uczestnika kreowania wrogiej polityki zagranicznej wskazanych wyżej organizacji wobec Federacji Rosyjskiej.

Na przestrzeni badanego okresu można wyróżnić wiele kwestii spornych w relacjach bilateralnych, między innymi takich, których początek miał miejsce jeszcze przed 2010 rokiem i takich, które trwały nadal po 2022 roku. Całokształt napięć oraz sporów prowadzi do wniosku, że problemy w stosunkach dwustronnych nie zostaną szybko zażegnane. W latach 2010-2022 dla Rosji najistotniejszymi kwestiami spornymi pozostawały polityka bezpieczeństwa

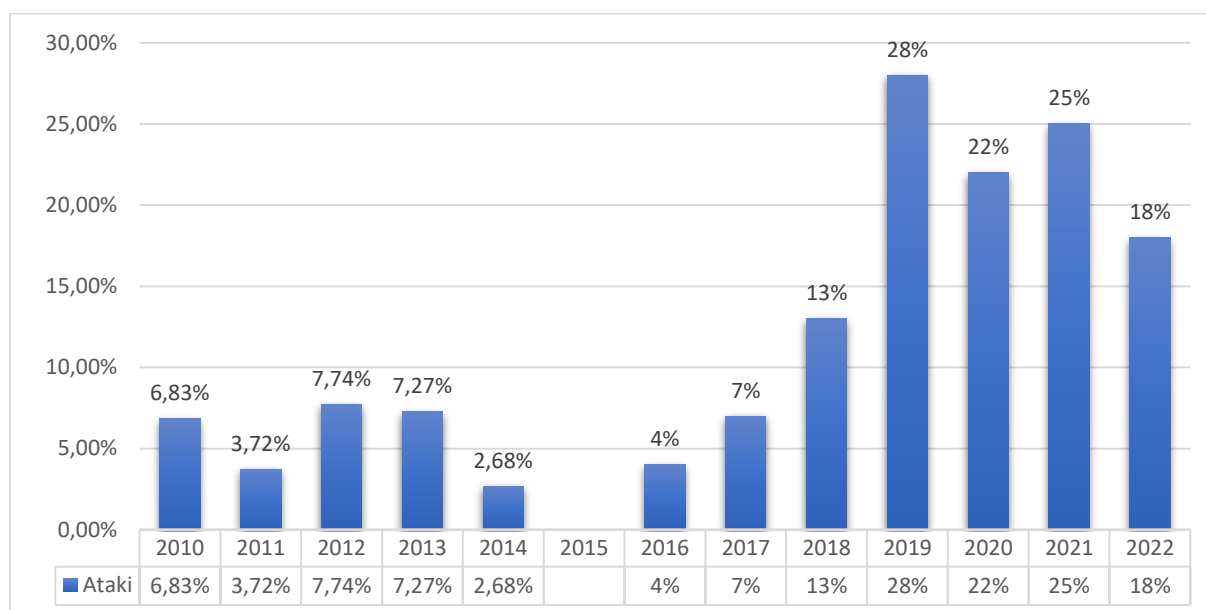
w Europie Środkowo-Wschodniej, polityka bezpieczeństwa NATO (w szczególności zwiększanie obecności wojsk Sojuszu na jego wschodniej flance) oraz aneksja Półwyspu Krymskiego i wojna we wschodniej Ukrainie (w tym wspieranie przez Polskę ukraińskiej polityki prozachodniej). W mniejszym stopniu była to polityka historyczna oraz polska dywersyfikacja źródeł energii.

Po czwarte, rosyjskie cyberataki były skierowane zarówno na sektor publiczny, jak i prywatny, a ich cele pozostawały zróżnicowane i dostosowane do specyfiki każdego z tych obszarów [HS4]. Sektor publiczny był w tym zakresie dominującym, a cyberataki miały na celu przeprowadzanie operacji wywiadowczych, które pozwalały na zdobywanie wrażliwych informacji oraz na atakowanie polskiej infrastruktury teleinformatycznej (również krytycznej¹⁷⁷⁵). Tego typu operacje były zaplanowane w taki sposób, aby w jak największym stopniu zakłócić funkcjonowanie kluczowych struktur państwowych i instytucji, w tym systemów zarządzania kryzysowego, energetycznego czy infrastrukturalnego. W tym kontekście bardzo istotne było realizowanie działań dążących do skompromitowania wizerunku Polski w wymiarze narodowym (wewnętrznym), jak i międzynarodowym (zewnętrznym). W sektorze prywatnym rosyjskie cyberataki były przede wszystkim narzędziem działalności przestępczej, w tym cyberszpiegowskiej. Dodatkowo, operacje te obejmowały niszczenie lub sabotowanie infrastruktury teleinformatycznej prywatnych przedsiębiorstw (szczególnie tych istotnych z punktu widzenia funkcjonowania państwa), co miało na celu destabilizowanie polskiej gospodarki, ale również zniechęcanie do dalszych inwestycji lub współpracy z zaatakowanymi podmiotami.

Analizując wyłącznie rozkład procentowy ataków z terytorium Federacji Rosyjskiej na monitorowane przez system ARAKIS sieci pod kątem liczby generowanych przepływów, można zauważyć, że w latach 2010-2017 udział Rosji kształtował się na poziomie kilku procent, z kolei w latach 2018-2022, a więc w czasie zaostrzenia się sporów na linii Warszawa-Moskwa, od kilkunastu do kilkadziesiąt procent. Tym samym można wyprowadzić wniosek, że rosyjska aktywność wobec Polski w cyberprzestrzeni korelowała z aktualnym stanem stosunków polsko-rosyjskich.

¹⁷⁷⁵ Do przykładów można zaliczyć cyberataki na: Ministerstwo Spraw Zagranicznych i Agencję Bezpieczeństwa Wewnętrznego w 2010 roku; Ministerstwo Obrony Narodowej w 2015 roku; gazociąg Baltic Pipe i Komisję Nadzoru Finansowego w 2017 roku; Policję, Narodowy Bank Polski, Sąd Najwyższy, kilka lotnisk oraz portal pasazer.gov.pl w 2022 roku. Zobacz szerzej: 6.2. *Charakterystyka, przebieg i implikacje rosyjskich ataków teleinformatycznych wobec Polski w cyberprzestrzeni w latach 2010-2022.*

Wykres 49. Rozkład procentowy ataków z Federacji Rosyjskiej na monitorowane przez system ARAKIS sieci w latach 2010-2022 pod kątem liczby generowanych przepływów.



Źródło: Opracowanie własne na podstawie raportów rocznych Zespołu CSIRT GOV za lata 2010-2022¹⁷⁷⁶.

Rosja przeprowadzała cyberataki wobec Polski wykorzystując do tego przede wszystkim grupy APT (ang. *advanced persistent threat*). W badanym okresie szczególnie wyróżniały się grupy o nazwach APT-28 i APT-29. Przeprowadzały one cyberataki różnego typu, które sprowadzały się przede wszystkim do zakłócania funkcjonowania polskiej infrastruktury teleinformatycznej oraz pozyskiwania z niej danych wrażliwych. Celem ataków były podmioty sektora publicznego w zasadzie każdego szczebla, tj. od pojedynczych gmin do ministerstw. Ataki polegały na blokowaniu dostępu do stron internetowych poprzez przeciążanie serwerów odpowiedzialnych za ich funkcjonowanie, podmienianie treści stron internetowych podmiotów publicznych poprzez zamieszczanie na nich przekazów zgodnych z propagandą Kremla, czy też podszywanie się pod określone podmioty celem pozyskania danych wrażliwych (przede wszystkim danych logowania). Działania te można zaobserwować przez cały badany okres, natomiast na przestrzeni lat ulegały one intensyfikacji. Operacje podejmowane przez Federację Rosyjską wobec Polski w cyberprzestrzeni korelowały

¹⁷⁷⁶ W 2015 roku Federacja Rosyjska nie została uwzględniona w raporcie CSIRT GOV (nie znalazła się w pierwszej dziesiątce państw objętych zestawieniem). Należy jednak uwzględnić stosunkowo wysoki odsetek źródeł ataków określonych jako nieznany (2 miejsce – 21,5%), czyli z wykorzystaniem adresów IP, które nie są przypisane do żadnego podmiotu. Oznacza to, iż dokonano podmiany prawdziwego źródłowego adresu IP. Pod takim adresem IP mogły zostać przeprowadzone cyberataki przez Federację Rosyjską, co jest wysoce prawdopodobne biorąc pod uwagę fakt, że Rosja rokrocznie znajdowała się w omawianym zestawieniu dziesięciu państw z których dokonywanych jest najwięcej cyberataków na monitorowane przez system ARAKIS sieci.

z aktualnym stanem stosunków polsko-rosyjskich, co wskazuje na to, iż były one traktowane jako narzędzie realizowanej przez Kreml polityki zagranicznej.

Przedstawiony powyżej wykres obrazuje rosyjskie ingerencje w sieci monitorowane przez system ARAKIS, a więc również takie, które są kluczowe dla funkcjonowania państwa. Widoczne jest, iż w początkowym okresie liczba przepływów oscylowała na poziomie kilku procent, co korelowało z okresem odwilży w stosunkach bilateralnych. Następnie, wobec eskalacji napięć doszło do stopniowego wzrostu aktywności Rosji w tym obszarze. Od 2014 roku, a więc od aneksji Półwyspu Krymskiego i rozpoczęcia wojny we wschodniej Ukrainie która stała się jedną z istotniejszych kwestii spornych w stosunkach dwustronnych, zaobserwować można rokroczne zwiększanie skali rosyjskiej aktywności.

Podczas dokonywanych cyberataków zauważalne było nawiązywanie do kwestii spornych. Przykładowo, sporne wydarzenia historyczne w stosunkach polsko-rosyjskich wykorzystywano do przeprowadzania cyberataków. W tym celu plikom ze złośliwym oprogramowaniem nadawano odpowiednią nazwę (np. *katyn*), zachęcając do kliknięcia w link bądź uruchomienia pliku. Cyberataki polegały również na atakowaniu podmiotów zaangażowanych w prowadzoną przez Polskę politykę dywersyfikacji źródeł energii. Sprowadzały się one do paraliżowania infrastruktury tych podmiotów bądź zamieszczaniu na ich stronach internetowych treści zgodnych z przekazem propagandowym Kremla, które negował podejmowane przez Polskę działania w tej materii.

Szczególnie widoczne było nawiązywanie do kwestii spornych dotyczących polityki bezpieczeństwa NATO, polityki bezpieczeństwa w Europie Środkowo-Wschodniej oraz do aneksji Półwyspu Krymskiego i wojny we wschodniej Ukrainie. Wielokrotnie dochodziło do cyberataków w wyniku których przeprowadzano włamania na strony internetowe określonych podmiotów, zamieszczając na nich treści propagandowe oskarżające Polskę oraz NATO o prowadzenie polityki antyrosyjskiej, wręcz rusofobicznej¹⁷⁷⁷. Ponadto zamieszczano treści podważające pozycję Polski na arenie międzynarodowej, ukazując ją w stosunku do NATO i Unii Europejskiej jako partnera niestabilnego oraz niegodnego zaufania. Omawiane w pracy przykłady cyberataków potwierdzają bardzo duże zaangażowanie Federacji Rosyjskiej w prowadzenie wrogiej działalności wobec Polski w cyberprzestrzeni. Należy więc wskazać, że Kreml uznaje cyberprzestrzeń za pole walki, na którym rywalizacja o dominację

¹⁷⁷⁷ Jako przykład można wskazać włamanie na stronę internetową Żagania oraz ponad stu innych gmin. Podczas powitania wojsk amerykańskich we wskazanej gminie doszło do cyberataku, w wyniku którego na stronie internetowej zamieszczono informacje sprzeciwiające się obecności wojsk NATO w Polsce, nazywając ich okupantami. Źródło: M. Frączek: *(Nie)bezpieczna cyberprzestrzeń* 2017. W: *Wsparcie teleinformatyczne i bezpieczeństwo cyberprzestrzeni w SZ RP*. Red. B. Biernacik, L. Kalman, G. Pilarski. Warszawa 2018, s. 221.

informacyjną jest równie istotna, jak tradycyjne formy wojny. Cyberataki realizowane przez Moskwę miały na celu nie tylko paraliżowanie polskiej infrastruktury teleinformatycznej, ale również dostarczanie cennych danych, które mogły być wykorzystane w ramach kampanii oddziaływania informacyjnego. Wnioski płynące z analizy tych działań wskazują na rosnące zagrożenie dla bezpieczeństwa Polski w wymiarze cybernetycznym. Cyberataki, prowadzone w ramach wojny informacyjnej, stanowią bowiem nie tylko bezpośrednie zagrożenie dla infrastruktury krytycznej, ale także dla stabilności politycznej i społecznej państwa.

Po piąte, ataki dokonywane wobec Polski w cyberprzestrzeni przez Federację Rosyjską są komplementarne wobec kampanii oddziaływania informacyjnego, które Kreml prowadzi między innymi za pośrednictwem portali informacyjnych [HS5]. W tym kontekście, cyberataki stanowią element strategii, w ramach której Rosja wykorzystuje je do wspierania oddziaływania informacyjnego. Federacja Rosyjska prowadzi wojnę informacyjną, wykorzystując do tego portale informacyjne, takie jak Sputnik News International oraz portal internetowy agencji informacyjnej TASS. Wyniki przeprowadzonych badań wskazują, że treści publikowane przez wskazane wyżej portale są zgodne z narracją formułowaną przez Kreml w ramach realizowanej wobec Polski polityki zagranicznej. Większość poddanych badaniom artykułów odnosiła się w swojej treści do tematyki politycznej¹⁷⁷⁸, współwystępując z tematyką natury militarnej, społecznej, gospodarczej i ideologicznej. W mniejszym stopniu występowały treści o charakterze technologicznym i religijnym. Trzeba podkreślić, że w publikowanych artykułach Polska była bardzo często przedstawiana w kontekście działań NATO oraz Unii Europejskiej. Należy przez to rozumieć, że Polska była postrzegana jako państwo, które bierze aktywny udział w kreowaniu polityki wskazanych organizacji wobec Rosji. Polityka ta w ocenie Moskwy jest konfrontacyjna oraz ingerująca w rosyjską strefę wpływów. Przykładowo można wskazać, że o przyczynę sporów na linii Kreml-NATO, Kreml-UE obwiniano Polskę.

W publikowanych artykułach występowały również wyodrębnione w ramach badań kwestie sporne. Najczęściej była to polityka bezpieczeństwa w Europie Środkowo-Wschodniej (Sputnik News International około 35%; TASS około 58%), polityka bezpieczeństwa NATO (Sputnik News International około 32%; TASS około 21%) i aneksja Półwyspu Krymskiego oraz wojna we wschodniej Ukrainie (Sputnik News International około 26%; TASS około

¹⁷⁷⁸ Około 87% w przypadku portalu Sputnik News International i około 89% w przypadku witryny agencji informacyjnej TASS. Zobacz szerzej: Wykres 28. Procentowe występowanie poszczególnych typów treści w artykułach opublikowanych na portalu informacyjnym „Sputnik News International” w latach 2010-2022 oraz Wykres 41. Procentowe występowanie typów treści w artykułach opublikowanych na witrynie internetowej agencji informacyjnej „TASS” w latach 2010-2022.

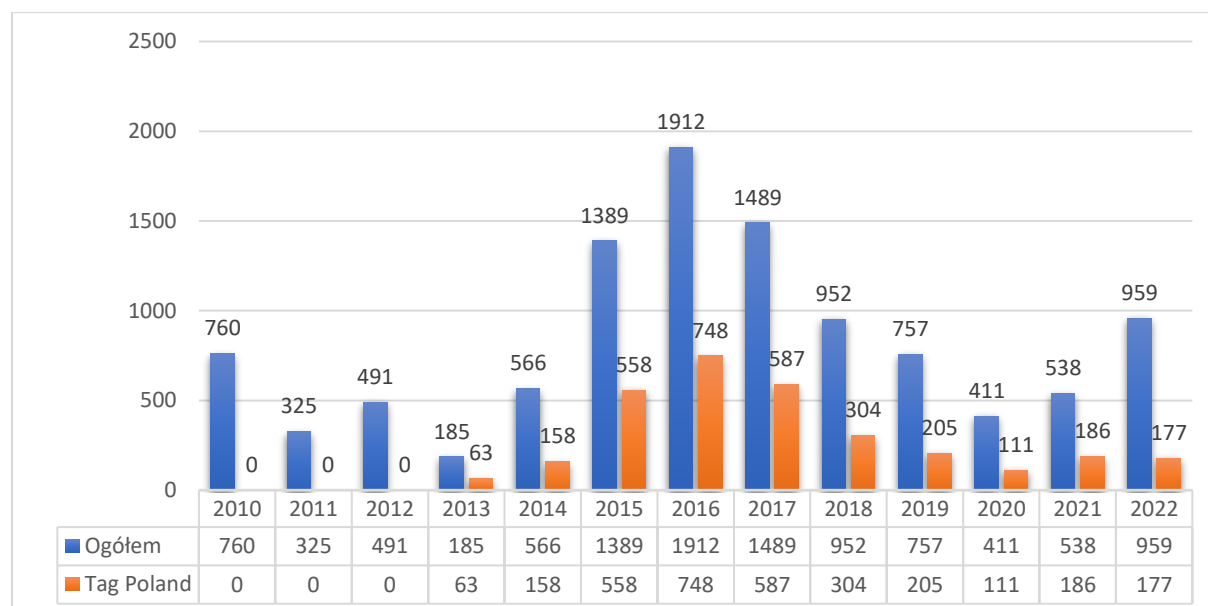
27%). W ich przypadkach Polska była przedstawiana jako państwo prowadzące politykę antyrosyjską wręcz rusofobiczną. W ocenie autorów poddanych badaniom artykułów to Polska odpowiada za antagonizowanie i podsycanie niepokojów w regionie, czemu przeciwstawia się Federacja Rosyjska. Takie prezentowanie Polski pozostaje spójne z twierdzeniami formułowanymi przez Kreml. Ponadto Polska, zarówno w publikowanych artykułach, jak i w oficjalnej narracji Moskwy jest prezentowana jako partner niegodny zaufania i niestabilny, co ma podważać relacje Warszawy z innymi państwami, a w szczególności z państwami będącymi członkami NATO oraz Unii Europejskiej. Na przestrzeni całego badanego okresu zidentyfikowano również kwestie sporne takie jak polityka historyczna oraz polska dywersyfikacja źródeł energii. Kwestie te występowały co do zasady z podobnym natężeniem w zasadzie przez cały badany okres. W najmniejszym stopniu zainteresowanie poświęcano katastrofie samolotu rządowego z Prezydentem RP pod Smoleńskiem oraz Programowi Partnerstwa Wschodniego.

Wyniki przeprowadzonych badań w zakresie *framingu* w sposób jednoznaczny wskazują, że wizerunek Polski był w badanym okresie kształtowany w przewarżającej mierze w sposób negatywny, rzadziej neutralny, a prawie w ogóle w sposób pozytywny. Otrzymane wyniki wpisują się w politykę zagraniczną Kremla, która nie postrzegała Polski jako państwa przyjaznego Moskwie. Przykładowo na portalu Sputnik News International w artykułach oznaczonych *tagiem Poland* około $\frac{2}{3}$ prezentowało Polskę w sposób negatywny, $\frac{1}{3}$ w sposób neutralny, a artykuły prezentujące ją w sposób pozytywny wystąpiły zaledwie kilka razy. Podobne wyniki badań otrzymano w przypadku witryny agencji informacyjnej TASS.

W celu osiągnięcia zamierzonych efektów w publikowanych artykułach, zarówno w przypadku portalu Sputnik News International, jak i agencji informacyjnej TASS, zidentyfikowano licznie występujące techniki propagandowe. Autorzy artykułów w sposób selektywny dobierali argumenty oraz stanowiska na temat określonych wydarzeń. Ponadto korzystali z autorytetów (niekoniecznie powszechnie uznanych), które prezentowały poglądy zgodne z wizją Kremla. Bardzo często w artykułach identyfikowano słowa mające względem Polski charakter pejoratywny. Nasycenie technikami propagandowymi było znaczące, gdyż w przypadku portalu Sputnik News International tylko w przypadku 8,10% nie zidentyfikowano żadnej techniki propagandowej, z kolei w przypadku agencji informacyjnej TASS było to 5,49%. Należy więc wskazać, że kampanie oddziaływania informacyjnego, które Federacja Rosyjska realizuje między innymi za pośrednictwem portalu informacyjnego Sputnik News International oraz witryny agencji informacyjnej TASS, to nic innego jak działalność propagandowa, która była nakierowana na Polskę. Zainteresowanie Polską w artykułach

publikowanych przez wskazane wyżej podmioty co do zasady korelowało ze stanem stosunków polsko-rosyjskich. Na poniższych wykresach zobrazowano liczbę indywidualnych wiadomości na portalu Sputnik News International oraz TASS w których pojawia się Polska. Widoczne jest, że w latach 2015-2017 na portalu Sputnik News International oraz w latach 2014-2016 na portalu agencji informacyjnej TASS artykuły odnoszące się do Polski były publikowane zdecydowanie częściej. Ową intensyfikację można powiązać z mającym miejsce w tym czasie kryzysem na Ukrainie spowodowanym aneksją Półwyspu Krymskiego i wojną we wschodniej części państwa oraz zmianą polityki NATO, zakładającą zwiększenie zaangażowania Sojuszu na jego flance wschodniej, w tym w Polsce. W kolejnych latach trudnych relacji bilateralnych zainteresowanie Polską malało, z kolei od roku 2020 w przypadku obu badanych podmiotów, widoczny jest jednoznaczny trend wzrostowy, co ponownie można powiązać z napięciami dotyczącymi polityki bezpieczeństwa NATO, a następnie pełnoskalową inwazją Rosji na Ukrainę. Polska w sposób zdecydowany sprzeciwiała się działaniom Kremla, co skutkowało odpowiedzią Moskwy.

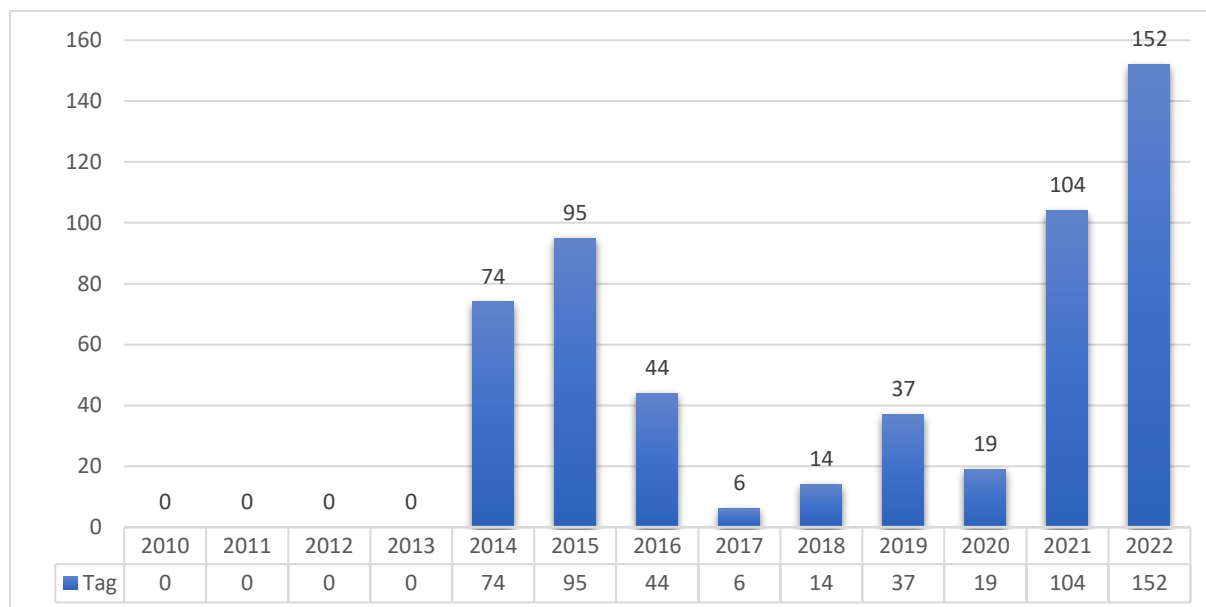
Wykres 50. Liczba indywidualnych wiadomości (artykułów) na portalu informacyjnym Sputnik News International wyodrębnionych przy użyciu wyszukiwarki witryny na podstawie słowa *Poland* z podziałem na zawierające tag o nazwie *Poland* oraz ogółem w latach 2010-2022.



Źródło: Opracowanie własne na podstawie wyników uzyskanych z wyszukiwarki przy użyciu wyrazu *Poland* na portalu informacyjnym Sputnik News International¹⁷⁷⁹.

¹⁷⁷⁹ Sputnik News International: Search. <https://sputniknews.com/search/?query=Poland> (dostęp: 10.03.2023).

Wykres 51. Liczba indywidualnych wiadomości (artykułów) na witrynie agencji informacyjnej TASS wyodrębnionych na podstawie *tagu* o nazwie *Poland* w latach 2010-2022.



Źródło: Opracowanie własne na podstawie wyników z wyszukiwania opartych o *tag* z wyrazem *Poland* na witrynie internetowej agencji informacyjnej TASS¹⁷⁸⁰.

Reasumując, do podstawowych celów polityki zagranicznej Federacji Rosyjskiej wobec Polski w badanym okresie należało dyskredytowanie Polski na arenie międzynarodowej, osłabianie relacji Polski z państwami sąsiednimi oraz partnerami międzynarodowymi, destabilizacja współpracy Polski w ramach NATO oraz Unii Europejskiej, kreowanie napięć między Polską a Stanami Zjednoczonymi. Ponadto, ośmieszanie i poniżanie Sił Zbrojnych RP, przedstawianie Polski jako państwa prześląkniętego nastrojami antyrosyjskimi oraz obwinianie Polski za pogorszenie stosunków między Rosją a Zachodem. Wszystkie ze wskazanych celów znajdują swoje odzwierciedlenie w dokonanych przez Federację Rosyjską cyberatakach wobec Polski oraz kampaniach oddziaływania informacyjnego realizowanych za pośrednictwem portalu informacyjnego Sputnik News International oraz witryny internetowej agencji informacyjnej TASS w latach 2010-2022. Występujące na przestrzeni wskazanych lat kwestie sporne w stosunkach polsko-rosyjskich, pojawiały się niezwykle często, zarówno w kontekście cyberataków dokonywanych wobec Polski, jak i działalności powyższych portali. Najczęściej odnoszono się do polityki bezpieczeństwa w Europie Środkowo-Wschodniej, polityki

¹⁷⁸⁰ TASS: *Poland*. <https://tass.com/tag/poland> (dostęp: 08.08.2024). W latach 2010-2013 nie opublikowano żadnego artykułu zawierającego *tag* o nazwie *Poland*.

bezpieczeństwa NATO oraz aneksji Półwyspu Krymskiego i wojny we wschodniej Ukrainie. Intensyfikacja sporów w zakresie wskazanych kwestii pociągała za sobą zwiększenie zainteresowania nimi w artykułach publikowanych przez Sputnik News International oraz TASS, ale również skutkowało ich częstszym występowaniem w ramach dokonywanych cyberataków. Przykładowo, w wyniku ustaleń podjętych podczas szczytu Sojuszu Północnoatlantyckiego w Warszawie w 2016 roku który doprowadził do zmiany polityki bezpieczeństwa NATO, w publikowanych przez powyższe portale artykułach pojawiły się treści informujące o konfrontacyjnej i destabilizującej polityce Polski wobec Rosji. Z kolei dokonywane w tamtym czasie cyberataki polegały między innymi na włamywaniu się na strony internetowe podmiotów publicznych i publikowaniu treści sprzeciwiających się obecności wojsk NATO w Polsce (jak w przypadku Gminy Żagań w 2017 roku, podczas powitania wojsk amerykańskich). Wskazany przykład dowodzi komplementarności rosyjskich cyberataków z kampaniami oddziaływania informacyjnego na odbiorców w Internecie, z kolei charakter działań nakazuje powiązać je z polityką zagraniczną Federacji Rosyjskiej prowadzoną wobec Polski.

W odpowiedzi na rosnące niebezpieczeństwo ze strony Rosji, zarówno w zakresie cyberataków, jak i oddziaływania informacyjnego, Polska podjęła szereg działań mających na celu przeciwdziałanie tym zagrożeniom. Analiza dokumentów rządowych wskazuje, iż polskie władze miały świadomość, że cyberprzestrzeń oraz przestrzeń informacyjna stanowią kluczowe obszary w których mogą ścierać się interesy państw, dlatego też priorytetowo traktowały kwestie dotyczące cyberbezpieczeństwa oraz ochrony przed działalnością propagandową¹⁷⁸¹. Polska zintensyfikowała działania na rzecz wzmocnienia swoich zdolności w zakresie cyberobrony, szczególnie w kontekście ochrony infrastruktury krytycznej oraz kluczowych sektorów gospodarki. W tym celu zwiększono zasoby poświęcone cyberobronie, rozbudowując krajowe instytucje odpowiedzialne za monitorowanie i reagowanie na zagrożenia, takie jak NASK oraz Wojska Obrony Cyberprzestrzeni¹⁷⁸². W odpowiedzi na cyberzagrożenia, Polska rozwijała również współpracę z sojusznikami z NATO oraz Unii Europejskiej, co pozwoliło na wymianę informacji oraz koordynację działań w obliczu zagrożeń¹⁷⁸³. Zwiększenie nakładów

¹⁷⁸¹ gov.pl: *Raport Zespołu ds. Dezinformacji Komisji ds. badania wpływów rosyjskich i białoruskich*. <https://www.gov.pl/web/sprawiedliwosc/raport-zespołu-ds-dezinformacji-komisji-ds-badania-wplywow-rosyjskich-i-bialoruskich> (dostęp: 12.03.2025).

¹⁷⁸² gov.pl: *W trosce o cyfrowe bezpieczeństwo Polski*. <https://www.gov.pl/web/cppc/w-trosce-o-cyfrowe-bezpieczenstwo-polski> (dostęp: 12.03.2025); Zobacz szerzej: 6.1.3. *Ewolucja systemu cyberbezpieczeństwa Polski w latach 2010-2022*.

¹⁷⁸³ gov.pl: *Współpraca międzynarodowa*. <https://www.gov.pl/web/cyfryzacja/wspolpraca-miedzynarodowa1> (dostęp: 12.03.2025).

na szkolenia z zakresu cyberbezpieczeństwa oraz rozwoju systemów wczesnego ostrzegania stanowiło istotny element tej polityki. Należy jednak zaznaczyć, że znaczna część tych działań była podejmowana w wyniku implementacji prawa unijnego, a nie wynikała natomiast z rodzimych rozważań w tym przedmiocie. W zakresie rosyjskiej propagandy Polska prowadziła działania polegające na edukacji społecznej, aby podnieść świadomość obywateli w rozpoznawaniu szeroko rozumianej dezinformacji. Kampanie edukacyjne oraz programy szkoleniowe mają na celu uświadomienie obywatelom, jak istotna jest weryfikacja informacji i rozwijanie krytycznego myślenia, co może zminimalizować skutki działań propagandowych stosowanych przez podmioty zewnętrzne, takie jak Federacja Rosyjska¹⁷⁸⁴.

Pomimo podjętych działań, Polska nadal narażona jest na szereg zagrożeń. Przede wszystkim państwo może stać się celem dalszych cyberataków, które mogą prowadzić do destabilizacji zarówno infrastruktury teleinformatycznej państwa, jak i dezinformacji społeczeństwa przy użyciu narzędzi propagandowych. Długotrwała wojna informacyjna prowadzona przez Rosję może prowadzić do pogłębiania polaryzacji społecznej, co stanowi zagrożenie dla wewnętrznej stabilności Polski. Manipulacje informacjami mogą wykorzystywać wrażliwe kwestie społeczne i polityczne, ale również destabilizować relacje Polski z sojusznikami, szczególnie w kontekście współpracy z Sojuszem Północnoatlantyckim i Unią Europejską. Niezbędne jest więc wypracowanie mechanizmów przeciwdziałających tym zagrożeniom, jak i nieustanne ich monitorowanie poprzez prowadzenie badań w tym przedmiocie.

Mimo, że cezura badań realizowanych w ramach niniejszej rozprawy obejmuje przedział czasowy od 2010 roku do 2022 roku, to nie sposób nie wspomnieć o wydarzeniach, które miały miejsce w ciągu kolejnych ponad dwóch lat. W tym czasie spory na linii Warszawa-Moskwa, w szczególności w kontekście wojny we wschodniej Ukrainie, polityki bezpieczeństwa NATO (wzmacniania wschodniej flanki Sojuszu) oraz polityki bezpieczeństwa w Europie Środkowo-Wschodniej uległy znaczącej intensyfikacji. Polska nadal była celem rosyjskich działań asymetrycznych, zarówno w przestrzeni informacyjnej, jak również w cyberprzestrzeni. Ponadto, zidentyfikowano kolejne próby destabilizacji wewnętrznej państwa Polskiego, tym razem polegające na dokonywaniu aktów dywersji (przede wszystkim

¹⁷⁸⁴ Kompetencje cyfrowe: *Ochrona przed dezinformacją*. <https://kompetencjegyfrowe.gov.pl/aktualnosci/wpis/ochrona-przed-dezinformacja> (dostęp: 12.03.2025); P. Pogorzelski: *Zagrożenia rosyjską dezinformacją w Polsce i formy przeciwdziałania*. <https://www.kew.org.pl/wp-content/uploads/2021/05/Piotr-Pogorzelski-Zagrozenie-rosyjska-dezinformacja-w-Polsce-i-formy-przeciwdzialania-1.pdf> (dostęp: 13.03.2025).

podpaleń)¹⁷⁸⁵. Niewątpliwie, objęcie z początkiem 2025 roku urzędu Prezydenta USA przez D. Trumpa, jego wizja działania NATO i USA w Europie oraz strategia zakończenia wojny rosyjsko-ukraińskiej będzie kluczowym wyzwaniem dla bezpieczeństwa Polski w najbliższych latach w kontekście stosunków polsko-rosyjskich.

¹⁷⁸⁵ gov.pl: *Komisja ds. badania wpływów rosyjskich i białoruskich powołana*. <https://www.gov.pl/web/premier/komisja-ds-badania-wplywow-rosyjskich-i-bialoruskich-powolana> (dostęp: 12.03.2025).

Summary

Information warfare is closely associated with Russian political culture and the foreign policy pursued by the Kremlin. It has enduring features developed over decades, which have been perpetuated in the political system of the Union of Soviet Socialist Republics and are now evolving in the system of the Russian Federation. The subject of the dissertation's research is the Russian Federation's use of information warfare as an instrument of its foreign policy towards Poland. The tools that Russia uses are asymmetrical in nature. With their help, it carries out actions on an unprecedented scale in the offline dimension, but above all in the online sphere. In this respect, they are based on information warfare, which involves simultaneously influencing online audiences with propaganda techniques and launching cyber-attacks on ICT infrastructure. The Kremlin's information warfare poses an increasing threat to Poland's security, both nationally and internationally.

The main research objective of the dissertation is to determine the conditions, nature and implications of the information war of the Russian Federation against Poland in the years 2010-2022. The dissertation seeks first of all to identify and characterise its conditions and the direct and indirect goals that the Russian Federation pursues through it. Furthermore, the dissertation aims to identify the instruments it uses for this purpose, as well as to indicate the most important implications of the above actions. It should also be noted that, within the framework of this dissertation, Russian information warfare is seen both as a propaganda impact on online audiences and as activities conducted in cyberspace by launching cyber attacks. Therefore, the purpose of the thesis is to discuss the propaganda tools and techniques that are used in pro-Russian information channels on the Internet, in messages concerning Poland and Polish-Russian relations, as well as to present the characteristics of Russian attacks on Poland in cyberspace.

Within the framework of the dissertation, the following main research hypothesis was verified. Information warfare as an instrument of foreign policy conducted by the Russian Federation is steadily gaining in importance, which should also be applied to Polish-Russian relations. In its information warfare against Poland, Russia employs propaganda techniques and tools to exert an informational influence on the recipient. These activities are undertaken through Russian information portals. The Russian Federation's information warfare against Poland also manifests through cyber-attacks on Poland in cyberspace. The activities undertaken within the framework of the indicated dimensions are complementary to each other. The objective of the operations undertaken by Russia is primarily to weaken internal state structures,

deepen social cleavages, marginalise Poland's position on the international arena, create a negative image of Poland on the international arena and, above all, pursue its own interests.

The time frame of the research covers the period from 2010 to 2022, owing to the key events in Polish-Russian relations, starting from the Smolensk catastrophe of 2010 to the full-scale invasion of Ukraine by the Russian Federation in 2022. The most important issues of contention during the period under review include, first and foremost, historical policy, diversification of energy sources, security policy in Central and Eastern Europe, NATO security policy, the crash of the government plane carrying the President of the Republic of Poland in Smolensk, the annexation of the Crimean Peninsula and the war in Ukraine, as well as the Eastern Partnership Programme.

The following methodological assumptions were made as within the scope of the dissertation. The Russian English-language news portal Sputnik News International and the website of the government news agency TASS were subjected to research. The research included: identifying the types of content published on the websites of the above entities, determining the frequency of contentious issues in Polish-Russian relations in the articles, identifying the content framing used and identifying the propaganda techniques used. With regard to the research on the activity of the Russian Federation towards Poland in cyberspace, an analysis of source materials was conducted, in particular the reports published by the CERT Polska Team and the CSIRT GOV Computer Security Incident Response Team. As a result, it was possible to characterise Russian activity undertaken against Polish ICT infrastructure.

The research indicates that the Russian Federation uses information warfare as an instrument of its foreign policy towards Poland. The Kremlin's activity boils down to an information influence campaign on the Internet through the Sputnik News International news portal and the TASS news agency website. The Russian Federation carries out hostile activity against Poland in cyberspace by undertaking attacks, primarily on the country's critical infrastructure. The actions taken by the Kremlin in the areas outlined above are complementary to each other. Information warfare in the Russian view is a comprehensive and unlimited instrument. Furthermore, the Kremlin's activities are part of the contentious issues in Polish-Russian relations, thus correlating with the current state of bilateral relations. Internally, the aim of the Russian Federation is to create and fuel socio-political disputes in Poland. In the external dimension, it is undermining Poland's image and presenting Poland as an anti-Russian, unstable and untrustworthy state, primarily in the context of Warsaw-NATO, Warsaw-EU relations. A long-lasting information warfare waged by Russia may lead to deepening social polarisation, which poses a threat to Poland's internal stability. Furthermore, it can destabilise

Poland's relations with its allies, especially in the context of cooperation with the North Atlantic Alliance and the European Union. It is therefore necessary to develop mechanisms to counteract these threats, as well as to continuously monitor them.

Bibliografia

Akty prawne, dokumenty państwowe i raporty

1. Air Force. Doctrine Center (1999). *Psychological operations. Air Force Doctrine Document 2-5.3 27 August 1999*. <https://apps.dtic.mil/sti/tr/pdf/ADA331241.pdf>
2. Bielizszczuk, B., Legucka, A. (2018). *Raport. Druga generacja elity władzy w Rosji*. <https://www.pism.pl/upload/images/artykuly/bb841e99-261b-4a02-a6f3-d60bb936de21//1576193576194.pdf>
3. Biuro Standaryzacji NATO. (2017). *Słownik terminów i definicji NATO AAP-6 (2017)*. <https://wcnjik.wp.mil.pl/u/AAP6PL.pdf>
4. Biuro Standaryzacji NATO. (2020). *Allied Joint Publication-3.20 Allied Joint Doctrine for Cyberspace Operations*. https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2be f137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf
5. BP, Centre for Energy Economics Research and Policy, Heriot-Watt University. (2021). *Statistical Review of World Energy 2021 70th edition*. <https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/energy-economics/statistical-review/bp-stats-review-2021-full-report.pdf>
6. Cabinet Office. (2011). *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world*. <https://assets.publishing.service.gov.uk/media/5a78a991ed915d04220645e2/uk-cyber-security-strategy-final.pdf>
7. Centrum Polsko-Rosyjskiego Dialogu i Porozumienia. (2020). *Raport ROSJA–POLSKA DIAGNOZA SPOŁECZNA 2020. Rosjanie na temat Polski i Polaków oraz stosunków rosyjsko-polskich. Warszawa*. http://cprdip.pl/assets/media/Wydawnictwa/Raporty/ROSJA_POLSKA_Diagnoza_spoleczna_2020.pdf
8. Chairman of the Joint Chiefs of Staff (2012). *Joint Publication 3-13. Information Operations*. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf
9. Commission on the Roles and Capabilities of the United States Intelligence Community. (1996). *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*. <https://www.govinfo.gov/app/details/GPO-INTELLIGENCE/context>
10. Congressional Research Service. (2021). *Cybersecurity: Selected Cyberattacks, 2012-2021*. <https://crsreports.congress.gov/product/pdf/R/R46974>

11. Cybersecurity and Infrastructure Security Agency. (2019). *A Guide to Critical Infrastructure Security and Resilience*. <https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf>
12. Dateportal. (2019). *Global Digital Report 2019*. <https://wearesocial.com/global-digital-report-2019>
13. Digital Poland, Microsoft. (2022). *Stan cyfryzacji Polski na tle regionu*. <https://digitalpoland.org/publikacje/pobierz?id=4ceb0166-6dd6-4c58-ab9a-cf77f56d7c20>
14. *Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej zatwierdzona 9 września 2000 roku*. Moskwa. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf
15. *Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej zatwierdzona 5 grudnia 2016 roku*. Moskwa. <http://kremlin.ru/acts/bank/41460>
16. *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej 2015*. Warszawa. <https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf>
17. *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii* (Dziennik Urzędowy Unii Europejskiej L 194/1).
18. European Commission. (2016). *Indeks gospodarki cyfrowej i społeczeństwa cyfrowego na 2016 r. Profil krajowy Polska*. https://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=14161
19. European Commission. (2022). *Digital Economy and Society Index (DESI) 2022*. <https://ec.europa.eu/newsroom/dae/redirection/document/88764>
20. European Commission. (2022). *Indeks gospodarki cyfrowej i społeczeństwa cyfrowego (DESI) na 2022 r. Polska*. <https://ec.europa.eu/newsroom/dae/redirection/document/88756>
21. European Union Agency for Cybersecurity. (2020). *Wyludzanie informacji (phishing)*. <https://www.enisa.europa.eu/publications/report-files/ETL-translations/pl/etl2020-phishing-ebook-en-pl.pdf>
22. European Union Agency for Cybersecurity. (2020). *Botnet*. <https://www.enisa.europa.eu/publications/report-files/ETL-translations/pl/etl2020-botnet-ebook-en-pl.pdf>
23. European Union Agency for Cybersecurity. *ENISA Threat Landscape 2015*. <https://www.enisa.europa.eu/publications/etl2015/@@download/fullReport>

24. European Union Agency for Cybersecurity. *ENISA Threat Landscape 2018*. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/@@download/fullReport>
25. European Union Agency for Cybersecurity. *ENISA Threat Landscape 2021*. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021/@@download/fullReport>
26. European Union Agency for Cybersecurity. *ENISA Threat Landscape 2022*. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport>
27. European Union Agency for Cybersecurity. *From January 2019 to April 2020. Malware ENISA Threat Landscape*. <https://www.enisa.europa.eu/publications/malware/@@download/fullReport>
28. European Union Agency for Cybersecurity. *Publications ENISA*. <https://www.enisa.europa.eu/publications>
29. Eurostat. (2011). *Archive: Produkcja i import energii*. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Energy_production_and_imports/pl&oldid=83395
30. Eurostat. (2019). *Energy, transport and environment statistics – 2019 edition*. <https://ec.europa.eu/eurostat/web/products-statistical-books/-/ks-dk-19-001>
31. Federal Communications Commission. *Consumer Guide. Caller ID Spoofing*. https://www.fcc.gov/sites/default/files/caller_id_spoofing.pdf
32. FireEye. (2014). *APT28: A window into Russia's cyber espionage operations?* <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf>
33. Giles, K., Seaboyer, A. (2019). *The Russian Information Warfare Construct*. Contract Report, Report number: DRDC-RDDC-2019-C241. Defence Research and Development. Ontario.
34. Główny Urząd Statystyczny. (2014). *Spółeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2010-2014*. Warszawa. https://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/5497/1/8/1/spoleczenstwo_informacyjne_w_polsce_2010-2014.pdf
35. Główny Urząd Statystyczny. (2020). *Spółeczeństwo informacyjne w Polsce w 2020 r. Warszawa, Szczecin*. https://stat.gov.pl/files/gfx/portalinformacyjny/pl/defaultaktualnosci/5497/2/10/1/spoleczenstwo_informacyjne_w_polsce_w_2020.pdf

36. Główny Urząd Statystyczny. (2022). *Ludność rezydująca – dane NSP 2021*. <https://stat.gov.pl/obszary-tematyczne/ludnosc/ludnosc/ludnosc-rezydujaca-dane-nsp-2021,44,1.html>
37. Główny Urząd Statystyczny. (2022). *Rocznik Demograficzny 2022*. Warszawa. https://stat.gov.pl/files/gfx/portalinformacyjny/pl/defaultaktualnosci/5515/3/16/1/polski_rocznik_demograficzny_2022.pdf
38. Główny Urząd Statystyczny. (2022). *Spółeczeństwo informacyjne w Polsce w 2022 r.* Warszawa, Szczecin. https://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/5497/2/12/1/spoleczenstwo_informacyjne_w_polsce_w_2022_r.pdf
39. Guerrero-Saade, J. A., Raiu, C., Moore, D., Rid, T. (2017). *Penquin's Moonlit Maze. The Dawn of Nation-State Digital Espionage*. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180251/Penguins_Moonlit_Maze_PDF_eng.pdf
40. IDC Analyze the Future. (2013). *The Dangerous World of Counterfeit and Pirated Software How Pirated Software Can Compromise the Cybersecurity of Consumers, Enterprises, and Nations ... and the Resultant Costs in Time and Money*. <https://news.microsoft.com/download/presskits/antipiracy/docs/IDC030513.pdf>
41. *Karta Narodów Zjednoczonych, Statut Międzynarodowego Trybunału Sprawiedliwości i Porozumienie ustanawiające Komisję Przygotowawczą Narodów Zjednoczonych* (Dz.U. 1947 nr 23 poz. 90).
42. Kaspersky Lab. (2013). *The evolution of phishing attacks: 2011-2013*. https://media.kaspersky.com/pdf/kaspersky_lab_ksn_report_the_evolution_of_phishing_attacks_2011-2013.pdf
43. *Koncepcja polityki zagranicznej Federacji Rosyjskiej zatwierdzona 28 czerwca 2000 roku*. Moskwa. <https://www.bits.de/EURA/russia052800.pdf>
44. *Koncepcja polityki zagranicznej Federacji Rosyjskiej zatwierdzona 15 lipca 2008 roku*. Moskwa. <http://kremlin.ru/acts/news/785>
45. *Koncepcja polityki zagranicznej Federacji Rosyjskiej zatwierdzona 12 lutego 2013 roku*. Moskwa. <http://www.pircenter.org/media/content/files/9/13617765900.pdf>
46. *Koncepcja polityki zagranicznej Federacji Rosyjskiej zatwierdzona 30 listopada 2016 roku*. Moskwa. <http://static.kremlin.ru/media/acts/files/0001201612010045.pdf>
47. *Konstytucja Federacji Rosyjskiej przyjęta w ogólnonarodowym referendum w dniu 12 grudnia 1993 roku*. <https://libr.sejm.gov.pl/tek01/txt/konst/rosja.html>
48. *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum*

- konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (Dz.U. 1997 nr 78 poz. 483).
49. *Konwencja wiedeńska o stosunkach dyplomatycznych, sporządzona w Wiedniu dnia 18 kwietnia 1961 roku* (Dz.U. 1965 nr 37 poz. 232), artykuł 3.
 50. Kowalska, M., Lelonek, A. (2017). *Jak budować odporność społeczną w przestrzeni informacyjnej i cyberprzestrzeni: przeciwdziałanie propagandzie i dezinformacji*. Raport Centrum Analiz Propagandy i Dezinformacji. Warszawa. https://capd.pl/images/dokumenty/Raport_CSEU_CAPD.pdf
 51. Lucas, E., Pomerantsev, P. (2016). *Winning the Information War. Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe*. A Report by CEPA's Information Warfare Project in Partnership with the Legatum Institute. Washington D.C. <https://www.lse.ac.uk/iga/assets/documents/arena/archives/winning-the-information-war-full-report-pdf.pdf>
 52. Marek, M. (2025). *Wojna informacyjna Federacji Rosyjskiej przeciwko Ukrainie, Polsce i NATO*. Warszawa.
 53. *Montevideo Convention on the Rights and Duties of States Signed at Montevideo, 26 December 1933 Entered into Force, 26 December 1934 Article 8 reaffirmed by Protocol, 23 December 1936*.
 54. Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni. (2022). *Podsumowanie programu CYBER.MIL.PL 2019-2021*. https://www.cyber.mil.pl/c/articles/atts/2022/2/CYBER.MIL.PL_2019-2021.pdf
 55. Narodowy Bank Polski. (2020). *Bilans Płatniczy Rzeczypospolitej Polskiej za IV kwartał 2019 r.* Warszawa. https://nbp.pl/wp-content/uploads/2022/09/bilans_platniczy2019_4.pdf
 56. National Cyber Security Centre. (2020). *Advisory: APT29 targets COVID-19 vaccine development*. <https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf>
 57. *Obwieszczenie Ministra Gospodarki i Pracy z dnia 1 lipca 2005 r. w sprawie polityki energetycznej państwa do 2025 r.* (Monitor Polski 2005 nr 42 poz. 562).
 58. *Obwieszczenie Ministra Klimatu i Środowiska z dnia 2 marca 2021 r. w sprawie polityki energetycznej państwa do 2040 r.* (Monitor Polski 2021 r. poz. 264).
 59. OECD. (2022). *Disinformation and Russia's war of aggression against Ukraine: Threats and governance responses*. <https://www.oecd.org/content/dam/oecd/en/publications/>

- reports/2022/11/disinformation-and-russia-s-war-of-aggression-against-ukraine_8b596425/37186bde-en.pdf
60. Parlament Europejski. (2023). *Cyberbezpieczeństwo: główne i nowe zagrożenia*. https://www.europarl.europa.eu/pdfs/news/expert/2022/1/story/20220120STO21428/20220120STO21428_pl.pdf
 61. Pełnomocnik Rządu ds. Cyberbezpieczeństwa. (2021). *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*. Warszawa. <https://www.gov.pl/attachment/48226cb6-29d4-49f9-860f-acd703072e60>
 62. *Podstawy polityki państwowej Federacji Rosyjskiej w dziedzinie międzynarodowego bezpieczeństwa informacyjnego zatwierdzone 12 kwietnia 2021 roku*. Moskwa. <http://www.kremlin.ru/acts/bank/46614>
 63. President of the United States. (2017). *National Security Strategy*. <https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf>
 64. *Priorytety Polskiej Polityki Zagranicznej 2012-2016*. Warszawa. <https://www.bbn.gov.pl/download/1/9620/prpol.pdf>
 65. *Rozporządzenie Rady Ministrów z dnia 28 marca 2007 r. w sprawie Planu Informatyzacji Państwa na lata 2007-2010* (Dz.U. 2007 nr 61 poz. 415).
 66. *Rządowy program ochrony cyberprzestrzeni RP na lata 2009 – 2011 – założenia*. <https://csirt.gov.pl/download/3/40/ZalozeniaRzadowyProgramOchronyCyberprzestrzeniRP2009-2011.pdf>
 67. *Rządowy program w zakresie ochrony cyberprzestrzeni RP na lata 2011 – 2016*. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf
 68. Sejm RP. 6 kadencja, 87 posiedzenie, 1 dzień (16-03-2011), 2 punkt porządku dziennego: *Informacja ministra spraw zagranicznych o założeniach polskiej polityki zagranicznej w 2011 roku*. <http://orka2.sejm.gov.pl/Debata6.nsf/main/42A5B0D0>
 69. Select Committee on Intelligence United States Senate. (2020). *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1: Russian Efforts Against Election Infrastructure with Additional Views*. <https://www.hsdl.org/?abstract&did=830205>
 70. Stockholm International Peace Research Institute. (2022). *SIPRI Yearbook 2022. Armaments, Disarmament and International Security. Summary*. Solna. https://www.sipri.org/sites/default/files/2022-06/yb22_summary_en_v2_0.pdf

71. Stockholm International Peace Research Institute. (2022). *Trends in World Military Expenditure 2021*. Stockholm. https://www.sipri.org/sites/default/files/2022-04/fs_2204_milex_2021_0.pdf
72. Stockholm International Peace Research Institute. (2022). *Trends in international arms transfers 2021*. Stockholm. https://www.sipri.org/sites/default/files/2022-03/fs_2203_at_2021.pdf
73. *Strategia Bezpieczeństwa Narodowego Federacji Rosyjskiej zatwierdzona 2 lipca 2021 roku*. Moskwa. <http://static.kremlin.ru/media/events/files/ru/QZw6hSk5z9gWq0plD1ZzmR5cER0g5tZC.pdf>
74. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2014*. <https://www.bbn.gov.pl/ftp/SBN%20RP.pdf>
75. *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022*. <https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022>
76. *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*. <https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024>
77. *Strategia energetyczna Federacji Rosyjskiej do 2035 roku zatwierdzona dekretem rządowym z dnia 9 czerwca 2020 roku numer 1523*. Moskwa. <https://www.climate-laws.org/geographies/russia/policies/energy-strategy-2035-approved-by-government-decree-1523-r-2020>
78. *Strategia Polskiej Polityki Zagranicznej 2017-2021*. Warszawa. <https://www.gov.pl/attachment/8196524f-687b-40e6-aca8-82c53ff8e6db>
79. *Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022*. https://www.bbn.gov.pl/ftp/dok/01/strategia_rozwoju_systemu_bezpieczenstwa_narodowego_rp_2022.pdf
80. Straż Graniczna. Komenda Główna Straży Granicznej. *Statystyki SG. Informacje statystyczne za lata 2017-2019*. <https://www.strazgraniczna.pl/pl/granica/statystyki-sg/2206,Statystyki-SG.html>
81. Symantec. (2012). *Norton Cybercrime Report 2012*. https://biz-file.com/f/1311/2012_Norton_Cybercrime_Report_.pdf
82. Thales. (2023). *From Ukraine to the whole of Europe: cyber conflict reaches a turning point*. https://www.thalesgroup.com/en/worldwide/security/press_release/ukraine-whole-europe-cyber-conflict-reaches-turning-point

83. The Congressional Research Service. (2022). *Russian Cyber Units (IF11718)*. <https://crsreports.congress.gov/product/details?prodcode=IF11718>
84. The Vice Chairman of the Joint Chiefs of Staff (2010). *Joint Terminology for Cyberspace Operations*. Washington D.C. <https://info.publicintelligence.net/DoD-JointCyberTerms.pdf>
85. *Traktat między Rzeczpospolitą Polską a Federacją Rosyjską o przyjaznej i dobrosąsiedzkiej współpracy, sporządzony w Moskwie dnia 22 maja 1992 r.* (Dz.U. 1993 nr 61 poz. 291).
86. U.S. Department of State. (2020). *GEC Special Report. Pillars of Russia's Disinformation and Propaganda Ecosystem*. Washington. https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia's-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf
87. U.S. Department of State. (2023). *Report: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem*. <https://www.state.gov/report-rt-and-sputniks-role-in-russias-disinformation-and-propaganda-ecosystem/>
88. *Uchwała Nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024.* (M.P. z 2019 r. poz. 1037).
89. *Uchwała Nr 67 Rady Ministrów z dnia 9 kwietnia 2013 r. w sprawie przyjęcia "Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022"* (M.P. 2013 poz. 377).
90. United Nations Educational, Scientific and Cultural Organization. (2018). *Journalism, 'Fake News' & Disinformation. Handbook for Journalism Education and Training*. Paris. <https://unesdoc.unesco.org/ark:/48223/pf0000265552>
91. United Nations. Department of Economic and Social Affairs. (2010). *E-Government Survey 2010. Leveraging e-government at a time of financial and economic crisis*. New York. <https://ifap.ru/library/book492.pdf>
92. United Nations. Department of Economic and Social Affairs. (2022). *E-Government Survey 2022. The Future of Digital Government*. New York. <https://desapublications.un.org/sites/default/files/publications/2022-09/Web%20version%20E-Government%202022.pdf>
93. United States Department of Defense. (2021). *DOD Dictionary of Military and Associated Terms*. https://www.supremecourt.gov/opinions/URLs_Cited/OT2021/21A477/21A477-1.pdf

94. *Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne.* (Dz.U. z 2021 r. poz. 2070).
95. *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* (Dz.U. 2016 poz. 904).
96. *Ustawa z dnia 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczenia Cyberprzestępczości* (Dz.U. 2021 poz. 2447).
97. *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* (Dz.U. 2007 nr 89 poz. 590).
98. *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (Dz.U. 2018 poz. 1560).
99. *Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny* (Dz.U. 1997 nr 88 poz. 553).
100. *Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (Dz.U. 2006 nr 104 poz. 709).
101. Verizon RISK Team. (2013). *2013 Data Breach Investigations Report*. <https://www.netsurion.com/eventtracker/media/eventtracker/files/collateral/verizon-data-breach-2013.pdf>
102. Weiss, M., Pomerantsev, P. (2014). *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. A Special Report presented by The Interpreter, a project of the Institute of Modern Russia. New York. <https://www.loc.gov/item/2015433465/>
103. WeLiveSecurity by ESET. (2018). *LoJax: First UEFI rootkit found in the wild, courtesy of the Sednit group*. <https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/>
104. Wóycicki K., Kowalska M., Lelonek A. (2017). *Raport Rosyjska wojna dezinformacyjna przeciwko Polsce*. Warszawa. <https://pulaski.pl/wp-content/uploads/2023/06/RAPORT-Rosyjska-wojna-dezinformacyjna-przeciwko-Polsce.pdf>
105. Zespół CERT Polska. *Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2005*. https://cert.pl/uploads/docs/Raport_CP_2005.pdf
106. Zespół CERT Polska. *Raport roczny z działalności CERT Polska 2010. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2010.pdf
107. Zespół CERT Polska. *Raport roczny z działalności CERT Polska 2011. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2011.pdf

108. Zespół CERT Polska. *Raport roczny z działalności CERT Polska 2012. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2012.pdf
109. Zespół CERT Polska. *Raport roczny z działalności CERT Polska 2013. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2013.pdf
110. Zespół CERT Polska. *Raport roczny z działalności CERT Polska 2014. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2014.pdf
111. Zespół CERT Polska. *Raport roczny z działalności CERT Polska 2015. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2015.pdf
112. Zespół CERT Polska. *Raport roczny z działalności CERT Polska 2016. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2016.pdf
113. Zespół CERT Polska. *Raport roczny z działalności CERT Polska 2017. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2017.pdf
114. Zespół CERT Polska. *Raport roczny z działalności CERT Polska 2018. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2018.pdf
115. Zespół CERT Polska. *Raport roczny z działalności CERT Polska 2019. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2019.pdf
116. Zespół CERT Polska. *Raport roczny z działalności CERT Polska 2020. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2020.pdf
117. Zespół CERT Polska. *Raport roczny z działalności CERT Polska 2021. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2021.pdf
118. Zespół CERT Polska. *Raport roczny z działalności CERT Polska 2022. Krajobraz bezpieczeństwa polskiego Internetu*. https://cert.pl/uploads/docs/Raport_CP_2022.pdf
119. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. *Raporty o stanie bezpieczeństwa cyberprzestrzeni RP*. <https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi>
120. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2010 roku*. <https://csirt.gov.pl/download/3/121/Analizaroczna2010.pdf>
121. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2011 roku*. <https://csirt.gov.pl/download/3/137/Raportroczny2011.pdf>
122. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2012 roku*. <https://csirt.gov.pl/download/3/158/RaportostaniebezpieczenstwacyberprzestrzeniRPw2012roku.pdf>

123. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013 roku.* <https://csirt.gov.pl/download/3/165/RaportostaniebezpieczenstwacyberprzestrzeniRPw2013roku.pdf>
124. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 roku.* <https://csirt.gov.pl/download/3/172/RaportostaniebezpieczenstwacyberprzestrzeniRPw2014roku.pdf>
125. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku.* <https://csirt.gov.pl/download/3/183/RaportostaniebezpieczenstwacyberprzesytrzeniRPw2015roku.pdf>
126. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2016 roku.* <https://csirt.gov.pl/download/3/185/RaportostaniebezpieczenstwacyberprzesytrzeniRPw2016roku.pdf>
127. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2017 roku.* <https://csirt.gov.pl/download/3/186/RaportostaniebezpieczenstwacyberprzesytrzeniRPw2017roku.pdf>
128. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 roku.* <https://csirt.gov.pl/download/3/191/RaportostaniebezpieczenstwacyberprzestrzeniRPw2018roku.pdf>
129. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 roku.* <https://csirt.gov.pl/download/3/199/raportostaniebezpieczenstwacyberprzestrzenirp2019.pdf>
130. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2020 roku.* <https://csirt.gov.pl/download/3/201/RaportostaniebezpieczenstwacyberprzestrzeniRPw2020.pdf>
131. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku.* <https://csirt.gov.pl/download/3/204/RaportostaniebezpieczenstwacyberprzestrzeniRPw2021compressed.pdf>
132. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku.* <https://csirt.gov.pl/download/3/213/RaportostaniebezpieczenstwacyberprzestrzeniRPw2022.pdf>
133. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku.* <https://csirt.gov.pl/download/3/220/RaportostaniebezpieczenstwacyberprzestrzeniRPw2023.pdf>

Monografie i prace zbiorowe

134. Aleksandrowicz, T. R. (2016). *Podstawy walki informacyjnej*. Warszawa.
135. Aleksandrowicz, T. R. (2021). *Zagrożenia dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym. Budowanie zdolności defensywnych i ofensywnych w infosferze*. Warszawa.
136. Aro, J. (2020). *Trolle Putina. Prawdziwe historie z frontów rosyjskiej wojny informacyjnej*. Kraków.
137. Arystoteles. (1953). *Polityka*. Wrocław.
138. Babbie, E. (2004). *Badania społeczne w praktyce*. Warszawa.
139. Bäcker, R., Czechowska, L., Gadomska, G., Gajda, J., Gawron-Tabor, K., Giedz, M., Kasprowicz, D., Mateja, M., Płotka, B., Rak, J., Seklecka, A., Szewczak, W., Winclawska, M., Wojciechowska, J. (2016). *Metodologia badań politologicznych*. Warszawa.
140. Banasik, M. (2021). *Rywalizacja presja i agresja Federacji Rosyjskiej. Konsekwencje dla bezpieczeństwa międzynarodowego*. Warszawa.
141. Bazyłow, L. (2005). *Historia Rosji*. Wrocław.
142. Bernays, E. L. (1928). *Propaganda*. New York.
143. Berridge, G. R. (2002). *Diplomacy: Theory and Practice*. Houndmills.
144. Bieleń, S. (2006). *Tożsamość międzynarodowa Federacji Rosyjskiej*. Warszawa.
145. Bieleń, S. (2010). *Polityka w stosunkach międzynarodowych*. Warszawa.
146. Bierzanek, R. (1980). *Współczesne stosunki międzynarodowe*. Warszawa.
147. Bierzanek, R., Symonides, J. (2005). *Prawo Międzynarodowe Publiczne*. Warszawa.
148. Bittner, J. R. (1989). *Mass Communication. And Introduction*. New Jersey.
149. Borecki, R. (1987). *Propaganda i polityka. (Zarys problematyki funkcjonowania środków masowego przekazu w systemach społeczno-politycznych)*. Warszawa.
150. Bryc, A. (2004). *Cele polityki zagranicznej Federacji Rosyjskiej*. Toruń.
151. Bryc, A. (2009). *Rosja w XXI wieku. Gracz światowy czy koniec ery?* Warszawa.
152. Brzezińska, A. B., Gawrycki, M. F. (2003). *Cyberterroryzm jako nowe zagrożenie dla bezpieczeństwa międzynarodowego w dobie globalizacji*. Warszawa.
153. Brzeziński, Z. (1998). *Wielka szachownica: Główne cele polityki amerykańskiej*. Warszawa.
154. Cappella, J. N., Jamieson, K. H. (1997). *Spiral of cynicism. The press and the public good*. New York.

155. Chałubińska-Jentkiewicz, K. (2019). *Cyberodpowiedzialność*. Toruń.
156. Cialdini, R. (2016). *Wywieranie wpływu na ludzi. Teoria i praktyka*. Sopot.
157. Ciborowski, L. (1999). *Walka informacyjna*. Toruń.
158. Columbus, T. A., Wolfe, J. H. (1986). *Introduction to International Relations: Power and Justice*. Englewood Cliffs.
159. Cooper, R. (2005). *Pękanie granic. Porządek i chaos w XXI wieku*. Poznań.
160. Cziomer, E., Zyblikiewicz, L. W. (2004). *Zarys współczesnych stosunków międzynarodowych*. Warszawa.
161. Denning, D. E. (2002). *Wojna Informacyjna i bezpieczeństwo informacji*. Warszawa.
162. Diec, J. (2015). *Geostrategiczny wybór Rosji u zarania trzeciego tysiąclecia. Tom 1 Doktryna rosyjskiej polityki zagranicznej. Partnerzy najbliżsi i najdalsi*. Kraków.
163. Dobek-Ostrowska, B. (2007). *Komunikowanie polityczne i publiczne. Podręcznik akademicki*. Warszawa.
164. Dobek-Ostrowska, B., Fras, J., Ociepka, B. (1997). *Teoria i praktyka propagandy*. Wrocław.
165. Dobroczyński, M., Stefanowicz, J. (1984). *Polityka zagraniczna*. Warszawa.
166. Dobrzycki, P. (2020). *Cywilne służby specjalne*. Warszawa.
167. Ellul, J. (1962). *Propagandes*. Paris.
168. Ellul, J. (1973). *Propaganda: The formation of mens attitudes*. New York.
169. Fedorowicz, K. (2011). *Polityka Polski wobec Rosji, Ukrainy i Białorusi w latach 1989-2010*. Poznań.
170. Frankel, J. (1963). *The Making of Foreign Policy*. London.
171. Frankel, J. (1970). *National Interest*. London.
172. Frankel, J. (1973). *Contemporary International Theory and the Behavior of States*. London.
173. Furnis, E., Snyder, R. C. (1955). *An Introduction to American Foreign Policy*. New York.
174. Geller, M. A. (2005). *Historia Imperium Rosyjskiego*. Warszawa.
175. Gerovitch, S. (2002). *From Newspeak to Cyberspeak, a history of Soviet Cybernetics*. Cambridge.
176. Giles, K. (2016). *Handbook of Russian Information Warfare. Fellowship Monograph Research Division NATO Defense College 9*. Rome.
177. Giles, K. (2016). *The Next Phase of Russian Information Warfare. NATO Strategic Communications Centre of Excellence*. Riga.
178. Gilpin, R. (1981). *War and Change in World Politics*. Cambridge.

179. Gitlin, T. (1980). *The Whole World is Watching: Mass Media in the Making and the Unmaking of the New Left*. Berkeley.
180. Goban-Klas, T., Sienkiewicz, P. (1999). *Spółeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*. Kraków.
181. Goffman, E. (1974). *Frame analysis. An essay on the organization of experience*. New York.
182. Golicyn, A. (2007). *Nowe kłamstwa w miejsce starych*. Warszawa.
183. Grzegorowski, Z. (2013). *Służby specjalne a bezpieczeństwo państwa Polskiego*. Toruń.
184. Grzybowski, K. (1969). *Historia doktryn politycznych i prawnych*. Warszawa.
185. Harrel, Y. (2015). *Rosyjska Cyber-strategia*. Warszawa.
186. Hartmann, F. (1962). *The Relations of Nations*. New York.
187. Heywood, A. (2009). *Teoria polityki. Wprowadzenie*. Warszawa.
188. Hoffmann, T. (2018). *Wybrane aspekty cyberbezpieczeństwa w Polsce*. Poznań.
189. Holsti, K. J. (1967). *International Politics: A Framework for Analysis*. Englewood Cliffs.
190. Jackson, R., Sorensen, G. (2003). *Introduction to International relations. Theories and Approaches*. New York.
191. Jean, C. (2003). *Geopolityka*. Wrocław.
192. Jelinek, G. (1921). *Nauka o państwie*. Warszawa.
193. Jowett, G. S., O'Donnell, V. (2012). *Propaganda and Persuasion*. Thousand Oaks.
194. Kisielewski, T. A. (2007). *Schylek Rosji*. Poznań.
195. Kolczyński, M. (2008). *Strategie komunikowania politycznego*. Katowice.
196. Kossecki, J. (1981). *Cybernetyka społeczna*. Warszawa.
197. Kossecki, J. (1997). *Totalna wojna informacyjna XX wieku a II RP*. Kielce.
198. Kostecki, W. (1988). *Polityka zagraniczna: teoretyczne podstawy badań*. Warszawa.
199. Kowalewski, J., Kowalewski, M. (2017). *Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm*. Warszawa.
200. Krasuski, J. (1990). *Europa Zachodnia po II wojnie światowej: dzieje polityczne*. Poznań.
201. Kudors, A. (2016). *Fortress Russia: Political, Economic, and Security Development in Russia Following the Annexation of Crimea and its Consequences for the Baltic States*. Riga.
202. Kukułka, J. (1978). *Problemy teorii stosunków międzynarodowych*. Warszawa.
203. Kukułka, J. (1982). *Międzynarodowe stosunki polityczne*. Warszawa.
204. Kula, H. M. (2005). *Propaganda współczesna. Istota – właściwość*. Warszawa.
205. Kulikowski, J. L. (1978). *Informacja i świat w którym żyjemy*. Warszawa.

206. Kuśmierski, S., Frydrychowicz, A. (1980). *Podstawy wiedzy o propagandzie*. Warszawa.
207. Kuźniar, R. (2012). *Bezpieczeństwo międzynarodowe*. Warszawa.
208. Lakomy, M. (2015). *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*. Katowice.
209. Laskowska, E. (1993). *Wartościowanie w języku potocznym*. Bydgoszcz.
210. Lerche, Ch. O., Said, A. A. (1963). *Concept of International Politics*. Englewood Cliffs.
211. Libicki, M. C. (1995). *What is information warfare?* Washington D.C.
212. Liderman, K. (2012). *Bezpieczeństwo informacyjne*. Warszawa.
213. Liedel, K., Piasecka, P., Aleksandrowicz, T. R. (2012). *Analiza informacji. Teoria i praktyka*. Warszawa.
214. Lisiakiewicz, R. (2011). *Polityka Rosji wobec Polski za prezydentury Władimira Putina (2000-2008)*. Toruń.
215. Lo, B. (2002). *Russian Foreign Policy in the Post-Soviet Era Reality, Illusion and Mythmaking*. New York.
216. Łoś-Nowak, T. (1999). *Wstęp do teorii stosunków międzynarodowych*. Poznań.
217. Łoś-Nowak, T. (2006). *Stosunki międzynarodowe. Teorie – systemy – uczestnicy*. Wrocław.
218. Macdonald, S. (2007). *Propaganda and Information Warfare in the Twenty-First Century. Altered images and deception operations*. Abingdon.
219. Maj, Cz. (1992). *Wartości polityczne w stosunkach międzynarodowych*. Lublin.
220. Markiewicz, M. (2002). *Historia Polski 1492-1795*. Kraków.
221. Marples, D. R. (2006). *Historia ZSRR: od rewolucji do rozpadu*. Wrocław.
222. Merle, M. (1974). *Sociologie des relations internationales*. Paris.
223. Messner, J. (2005). *Хочешь Мира, Победи Мятежевойну!* Москва.
224. Michałowska, G. (1986). *Międzynarodowe stosunki kulturalne*. Warszawa.
225. Michałowska, G. (1991). *Zmienność i instytucjonalizacja międzynarodowych stosunków kulturalnych*. Warszawa.
226. Modelski, G. (1963). *A Theory of Foreign Policy: An Analysis of Decision-Making*. London.
227. Morgenthau, H. (1954). *Politics among Nations*. New York.
228. Morgenthau, H. (1958). *Dilemmas of Politics*. Chicago.
229. Morgenthau, H. (2010). *Polityka między narodami. Walka o potęgę i pokój*. Warszawa.
230. Neuman, W. R., Just, M., Crigler, A. N. (1992). *Common knowledge. News and the construction of political meaning*. Chicago.

231. Nowak, A. (1999). *Jak rozbić rosyjskie imperium? Idee polskiej polityki wschodniej (1733-1921)*. Kraków.
232. O'Shaughnessy, N. (2004). *Politics and propaganda. Weapons of mass seduction*. Manchester.
233. Organski, A. F. K. (1958). *World Politics*. New York.
234. Pacek, B. (2018). *Wojna hybrydowa na Ukrainie*. Warszawa.
235. Panarin, I. (2012). *СМИ, пропаганда и информационные войны*. Москва.
236. Panek, B. (2015). *Polityka Federacji Rosyjskiej w regionie Europy, Azji i Pacyfiku*. Warszawa.
237. Pietraś, J. (1986). *Podstawy teorii stosunków międzynarodowych*. Lublin.
238. Pietraś, J. Z. (1989). *Pojęcie i klasyfikacja ról międzynarodowych*. Lublin.
239. Polska Agencja Inwestycji i Handlu. (2018). *Rosja. Przewodnik po rynku*. Warszawa.
240. Porzeżyński, M. (2021). *Cyberbezpieczeństwo dostawców usług cyfrowych*. Warszawa.
241. Potulski, J. (2005). *Rola i znaczenie tradycji w funkcjonowaniu współczesnych instytucji politycznych w Rosji*. Toruń.
242. Rajczyk, R. (2016). *Nowoczesne wojny informacyjne*. Warszawa.
243. Rajczyk, R. (2019). *Oblicza współczesnej propagandy. Przypadek chińsko-tajwańskiej wojny informacyjnej*. Katowice.
244. Raś, M. (2018). *Aktywność międzynarodowa regionów Federacji Rosyjskiej*. Warszawa.
245. Riasanovsky, N. V., Steinberg, M. D. (2009). *Historia Rosji*. Kraków.
246. Rid, T. (2022). *Wojna informacyjna*. Warszawa.
247. Rosenau, J. N. (1980). *The Scientific Study of Foreign Policy*. London.
248. Savranska, K. (2020). *Problematyka walki informacyjnej w relacjach Rosji z wybranymi państwami europejskimi. Perspektywa medioznawcza*. Gdańsk.
249. Schopenhauer, A. (2010). *Erystyka czyli sztuka prowadzenia sporów*. Warszawa.
250. Sienkiewicz, P. (1983). *Inżynieria systemów*. Warszawa.
251. Siudak, R. (2022). *Cyberbezpieczeństwo w Polsce. Od dyskursów do polityk publicznych*. Kraków.
252. Sprout, H., Sprout, M. (1956). *Man – Milieu Relationship Hypotheses in the Context of International Politics*. Princeton.
253. Sprout, H., Sprout, M. (1968). *An Ecological Paradigm for Study of International Politics*. Princeton.
254. Stoessinger, J. (1965). *The Might of Nations. World Politics in Our Time*. New York.

255. Stolarczyk, M. (2016). *Rosja w polityce zagranicznej Polski w latach 1992-2015*. Katowice.
256. Sun Tzu. (1994). *Sztuka wojny*. Warszawa.
257. Sutor, J. (1996). *Prawo dyplomatyczne i konsularne*. Warszawa.
258. Szczepański, W. J. (1979). *Europa myśli politycznej de Gaulle'a. Próby analizy systemowej*. Warszawa.
259. Szczur, S. (2002). *Historia Polski. Średniowiecze*. Kraków.
260. Sztumski, J. (1990). *Propaganda – jej problemy i metody*. Katowice.
261. Taras, A. (2015). *Anatomia nienawiści. Stosunki polsko-rosyjskie XVIII-XX w.* Warszawa.
262. Tokarski, R. (2013). *Światy za słowami. Wykłady z semantyki leksykalnej*. Lublin.
263. Topolski, I. (2013). *Polityka Federacji Rosyjskiej wobec państw Europy Wschodniej*. Lublin.
264. Topolski, J. (1968). *Metodologia Historii*. Warszawa.
265. Topolski, J. (2015). *Historia Polski*. Wydanie elektroniczne.
266. Ventre, D. (2016). *Information Warfare. 2nd Edition revised and Updated*. London – New York.
267. Volkoff, V. (1990). *Dezinformacja. Oręż wojny*. Warszawa.
268. Volkoff, V. (2022). *Krótką historia dezinformacji. Od konia trojańskiego do Internetu*. Bielany Wrocławskie – Kobierzyce.
269. Wallace, W. (1971). *Foreign Policy and Political Process*. London.
270. Waltz, K. (1979). *Theory of international politics*. Reading.
271. Webber, M., Smith, M. (2002). *Foreign Policy in a Transformed World*. Harlow.
272. Weber, M. (1998). *Polityka jako zawód i powołanie*. Kraków.
273. Webster, F. (2006). *Theories of the information society*. New York.
274. White, B. (2001). *Understanding European Foreign Policy*. Houndmills.
275. Wiatr, J. (1999). *Socjologia polityki*. Warszawa.
276. Wiatr, J. (2017). *Bezpieczeństwo narodowe Polski a stosunki polsko-rosyjskie*. Poznań.
277. Wielomski, A. (2007). *Nacjonalizm francuski 1886-1940. Geneza, przemianu i istota filozofii politycznej*. Warszawa.
278. Wiener, N. (1961). *Cybernetyka i społeczeństwo*. Warszawa.
279. Zięba, R. (2013). *Polityka zagraniczna Polski w strefie euroatlantyckiej*. Warszawa.
280. Ziółkowski, J. (2019). *Syndrom oblężonej twierdzy*. Warszawa.

281. Znyk, P. (2011). *Propaganda. Współczesne oblicza. Technologia zabójstwa medialnego*. Łódź.
282. Żebrowski, A. (2016). *Walka informacyjna w asymetrycznym środowisku bezpieczeństwa międzynarodowego. Wybrane problemy*. Kraków.

Artykuły naukowe i rozdziały w pracach zbiorowych

283. Adamczuk, M., Liedel, K. (2015). *Doktryna cyberbezpieczeństwa*. Przegląd Bezpieczeństwa Wewnętrznego, 12/7.
284. Adamowski, J. (2002). *Wizerunek Rosji w polskich środkach masowego przekazu (u progu nowego tysiąclecia)*. W: M. Zamarlik (Red.), *Polityka zagraniczna Rosji*. Kraków.
285. Alcaraz, C., Zeadally, S. (2015). *Critical Infrastructure Protection: Requirements and Challenges for the 21st Century*. International Journal of Critical Infrastructure Protection, 8.
286. Aldwairi, M., Alwahedi, A. (2018). *Detecting Fake News in Social Media Networks*. Procedia Computer Science, 141.
287. Aleksandrowicz, T. R. (2016). *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*. Przegląd bezpieczeństwa wewnętrznego, 15/16.
288. Aleksandrowicz, T. R. (2017). *Wywiad jako narzędzie w koncepcji nowych wojen. Casus konfliktu ukraińskiego*. Studia Politologiczne, 43.
289. Aleksandrowicz, T. R. (2018). *Bezpieczeństwo informacyjne państwa*. Studia Politologiczne, 49.
290. Antonovich, P. (2011). *Cyberwarfare: Nature and Content*. Military Thought, 20(3).
291. Bajor, P., Gruszczak, A. (2019). *Między wiedzą a władzą – o związkach między informacją, wiedzą i bezpieczeństwem*. W: P. Bajor, A. Gruszczak (Red.), *Między wiedzą a władzą. Bezpieczeństwo w erze informacji*. Kraków.
292. Banasik, M. (2019). *Interesy i cele strategiczne Federacji Rosyjskiej oraz ich konsekwencje dla bezpieczeństwa międzynarodowego*. W: M. Banasik (Red.), *Polityka Federacji Rosyjskiej i jej konsekwencje dla bezpieczeństwa międzynarodowego*. Warszawa.
293. Banasik, M. (2020). *Bezpieczeństwo Europy Środkowo-Wschodniej w aspekcie zagrożeń płynących z Federacji Rosyjskiej*. Środkowoeuropejskie Studia Polityczne, 2.
294. Banasik, M. (2021). *Teoria i praktyka wojny informacyjnej stosowanej przez Federację Rosyjską*. W: M. Banasik (Red.), *Informacja czynnikiem warunkującym bezpieczeństwo. Kontekst rosyjski*. Warszawa.
295. Baraniuk, K. (2016). *Mniejszości rosyjskojęzyczne w polityce zagranicznej Federacji Rosyjskiej – przykład Estonii*. Wschodnioznawstwo, 10.

296. Bartosiewicz, M. (2019). Teorie propagandy w obliczu algorytmizacji internetowego komunikowania społecznego. *Kultura Współczesna*, 1(104).
297. Bartoszewicz, M. (2017). *Walka Propagandowa na Facebooku. Analiza jakościowa zawartości postów opublikowanych przez Prawo i Sprawiedliwość oraz Platformę Obywatelską w okresie tzw. Czarnego Protestu*. W: T. Gackowski, K. Brylska, M. Patera (Red.), *Memy czyli życie społeczne w czasach kultury obrazu*. Warszawa.
298. Barynkin, A. (2022). *Kwestie polityki historycznej we współczesnych stosunkach polsko-rosyjskich*. W: K. A. Wojtaszczyk, I. N. Novikova (Red.), *Polska i Rosja w zmieniającej się Europie*. Warszawa.
299. Bebbler, R. (2016). *Information War and Rethinking Phase 0*. *Journal of Information Warfare*, 15(2).
300. Bieleń, S. (2002). *Polityka zagraniczna Rosji*. W: J. Adamowski, A. Skrzypek (Red.), *Federacja Rosyjska 1991-2001*. Warszawa.
301. Bieleń, S. (2008). *Identyfikacja Rosji w stosunkach międzynarodowych*. W: S. Bieleń, M. Raś (Red.), *Polityka zagraniczna Rosji*. Warszawa.
302. Bieleń, S. (2008). *Polityka Federacji Rosyjskiej wobec Stanów Zjednoczonych Ameryki*. W: S. Bieleń, M. Raś (Red.), *Polityka zagraniczna Rosji*. Warszawa.
303. Bieleń, S., Raś, M. (Red.). (2008). *Polityka zagraniczna Rosji*. Warszawa.
304. Bieleń, S., Skrzypek, A. (2015). *Wstęp*. W: S. Bieleń, A. Skrzypek (Red.), *Rosja. Rozważania imperiolologiczne*. Warszawa.
305. Bieleń, S., Skrzypek, A. (Red.). (2017). *Pamięć i polityka historyczna w stosunkach polsko-rosyjskich*. Warszawa.
306. Bodrov, A. (2022). *Bezpieczeństwo europejskie – wizja Rosji*. W: K. A. Wojtaszczyk, I. N. Novikova (Red.), *Polska i Rosja w zmieniającej się Europie*. Warszawa.
307. Bojarowicz, T., Jakubowski, W., Przastek, D. (2022). *Społeczeństwo i kultura – tradycja i współczesność*. W: K. A. Wojtaszczyk, I. N. Novikova (Red.), *Polska i Rosja w zmieniającej się Europie*. Warszawa.
308. Brangetto, P., Veenendaal, M. A. (2016). *Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations*. 8th International Conference on Cyber Conflict Cyber Power.
309. Brown, K. (2013). *Agitprop in Soviet Russia*. *Constructing the Past*, 1(1).
310. Bryc, A. (2008). *Stosunki Federacji Rosyjskiej z Sojuszem Północnoatlantyckim*. W: S. Bieleń, M. Raś (Red.), *Polityka zagraniczna Rosji*. Warszawa.

311. Bryc, A. (2010). *Mechanizm polityki zagranicznej Federacji Rosyjskiej*. W: L. Zybkiewicz, M. Czajkowski, P. Bajor (Red.), *Polityka zagraniczna Federacji Rosyjskiej. Wybrane aspekty stosunków z Polską, Ukrainą i Białorusią*. Kraków.
312. Bryc, A. (2014). *Ewolucja społeczności międzynarodowej w nowej dynamice stosunków międzynarodowych*. Kultura i Edukacja, 2(102).
313. Bryc, A. (2015). *Putinizm jako doktryna odbudowy imperium?* W: S. Bieleń, A. Skrzypek (Red.), *Rosja. Rozważania imperiologiczne*. Warszawa.
314. Bryła, J. (1996). *Czynniki kształtujące stosunki międzynarodowe*. W: W. Malendowski, Cz. Mojsiewicz (Red.), *Międzynarodowe stosunki polityczne*. Poznań.
315. Chaudhry, J. A., Chaudhry, S., Rittenhouse, R. G. (2016). *Phishing Attacks and Defenses*. International Journal of Security and its Applications, 10(1).
316. Chmielewski, J. M., Waćkowski, K. (2018). *Technologie teleinformatyczne – podstawy, rozwój i bezpieczeństwo systemów teleinformatycznych*. W: C. Banasiński (Red.), *Cyberbezpieczeństwo: zarys wykładu*. Warszawa.
317. Chmielewski, P. (1994). *Polityka zagraniczna Związku Radzieckiego na rzecz utrzymania pokoju i bezpieczeństwa międzynarodowego do II wojny światowej*. W: W. Materski (Red.), *Polityka zagraniczna Rosji i ZSRR*. Łódź.
318. Ciborowski, L. (2002). *Mechanizmy i przestrzenie walki informacyjnej*. W: G. Nowacki (Red.), *Informacja w walce zbrojnej*. Warszawa.
319. Clark, D. (2010). *Characterizing cyberspace: past, present and future*. ECIR Working Paper, 2010-3.
320. Courter, I. J. (2022). *Russian Preinvasion Influence Activities in the War with Ukraine*. Military Review, July Online Exclusive Article.
321. Cronin, B., Crawford, H. (1999). *Information Warfare: Its Application in Military and Civilian Contexts*. The Information Society, 15(4).
322. Cybulski, M. (2009). *Polacy i Rosjanie. Zarys narodzin stereotypów*. Acta Polono-Ruthenica, XIV.
323. Czajkowski, A. (2011). *Federacja Rosyjska: przywracanie utraconej wielkości*. W: T. Łoś-Nowak (Red.), *Polityka zagraniczna: aktorzy, potencjały, strategie*. Warszawa.
324. Czarnocki, A. (2007). *Czynniki międzynarodowych stosunków politycznych*. W: M. Pietraś (Red.), *Międzynarodowe stosunki polityczne*. Lublin.
325. Cziomer, E. (2008). *Przesłanki i istota kształtowania się konfliktu Wschód-Zachód*. W: E. Cziomer (Red.), *Międzynarodowe Stosunki Polityczne*. Kraków.

326. Daniluk, A. (2017). *Nowa koncepcja polityki zagranicznej Federacji Rosyjskiej z 2016 roku – analiza dokumentu w kontekście wydarzeń na arenie międzynarodowej*. Studia Wschodnioeuropejskie, 7.
327. Darczewska, J. (2015). *Wojna informacyjna Rosji z Zachodem. Nowe wyzwanie?* Przegląd Bezpieczeństwa Wewnętrznego, Wydanie Specjalne.
328. Darczewska, J. (2017). *Dezinformacja – rosyjska broń strategiczna*. Biuletyn Kwartalny Rządowego Centrum Bezpieczeństwa, 19.
329. Darczewska, J. (2019). „*Wojny pamięci*”: historia, polityka i służby specjalne Federacji Rosyjskiej. Przegląd Bezpieczeństwa Wewnętrznego, 20/19.
330. de Lazari, A. (2006). *Wzajemne uprzedzenia Polaków i Rosjan*. W: A. de Lazari (Red.), *Katalog wzajemnych uprzedzeń Polaków i Rosjan*. Warszawa.
331. Delong, M. (2020). „*Ruski mir*” jako narzędzie rosyjskiej ekspansji geopolitycznej na terytorium Ukrainy. Przegląd Geopolityczny, 33.
332. Donnert, E. (1994). *Walka Rosji o dostęp do Morza Bałtyckiego w II połowie XVI wieku*. W: W. Materski (Red.), *Polityka zagraniczna Rosji i ZSRR*. Łódź.
333. Duraczyński, E. (1987). *Układ Sikorski-Majski*. Dzieje najnowsze, XIX.
334. Dziemidok-Olszewska, B. (2019). *Pozycja ustrojowa prezydentów Polski i Rosji*. Wschód Europy, 5(1).
335. Eisenberg, T., Gries, D., Hartmanis, J., Holcomb, D., Lynn, M. S., Santoro, T. (1989). *The Cornell Commission: On Morris and the Worm*. Communications of the ACM, 32(6).
336. Elliot, D., Culver, C. (1992). *Defining and Analyzing Journalistic Deception*. Journal of Mass Media Ethics, 7.
337. Entman, R. M. (1993). *Framing: Toward Clarification of a Fractured Paradigm*. Journal of Communication, 43(4).
338. Falkowicz, S. (1997). *Polska i Polacy w wyobrażeniach Rosjan: refleksje ogólne*. Dzieje Najnowsze, 29(1).
339. Fedorowicz, K. (2003). *Polska w polityce zagranicznej Rosji w latach 1991-2001*. W: R. Paradowski, Sz. Ossowski (Red.), *Polska w Rosji – Rosja w Polsce. Stosunki Polityczne*. Poznań.
340. Fiszer, J. M. (2016). *Zadania i cele polityki zagranicznej Władimira Putina*. Myśl Ekonomiczna i Polityczna, 1(52).
341. Fiszer, J. M. (2018). *Stanowisko Rosji wobec aneksji Polski do NATO i Unii Europejskiej*. Myśl Ekonomiczna i Polityczna, 1(60).

342. Frączek, M. (2018). *(Nie)bezpieczna cyberprzestrzeń 2017*. W: B. Biernacik, L. Kalman, G. Pilarski (Red.), *Wsparcie teleinformatyczne i bezpieczeństwo cyberprzestrzeni w SZ RP*. Warszawa.
343. Gardocki, S. (2020). *Polityka zagraniczna Rosji. Determinanty, interesy i środki*. Studia Orientalne, 2(18).
344. Gardocki, S. (Red.). (2015). *Rosja i jej sąsiedzi. Studia i szkice*. Toruń.
345. Gardocki, S., Worona, H. (2020). *Wykorzystanie przez Rosję cyberprzestrzeni w konfliktach hybrydowych a rosyjska polityka cyberbezpieczeństwa*. Colloquium Pedagogika – Nauki o Polityce i Administracji, 2(38).
346. Goliński, M. (2015). *E-administracja w Polsce w świetle badań ONZ*. Roczniki Kolegium Analiz Ekonomicznych, 38.
347. Gonéc, V. (1994). *Kwestia koordynacji polityki zagranicznej republik radzieckich w okresie do utworzenia ZSRR*. W: W. Materski (Red.), *Polityka zagraniczna Rosji i ZSRR*. Łódź.
348. Górka M. (2018). *Cyberbezpieczeństwo jako wyzwanie dla współczesnego państwa i społeczeństwa*. W: T. Dębowski. (Red.), *Cyberbezpieczeństwo wyzwaniem XXI wieku*. Łódź-Wrocław.
349. Gruszczak, A. (2023). *Kilka uwag o strategicznym wymiarze wojny w Ukrainie*. W: A. Gruszczak (Red.), *THE WAR MUST GO ON: Dynamika wojny w Ukrainie i jej reperkusje dla bezpieczeństwa Polski*. Kraków.
350. Gupta, S. (2013). *Types of Malware and its Analysis*. International Journal of Scientific & Engineering Research, 4(1).
351. Haliżak, E., Pietraś, M. (Red.). (2013). *Poziomy analizy stosunków międzynarodowych*. Warszawa.
352. Hathaway, O. (2011). *The Law of Cyber-Attack*. California Law Review, 100.
353. Hoffmann, T. (2018). *Główni aktorzy cyberprzestrzeni i ich działalność*. W: T. Dębowski (Red.), *Cyberbezpieczeństwo wyzwaniem XXI wieku*. Łódź – Wrocław.
354. Holsti, O. R. (1995). *Theories of International Relations and Foreign Policy: Realism and Its Challengers*. W: Ch. W. Kegley (Red.), *Controversies in International relations Theory: Realism and the Neoliberal Challenge*. New York.
355. Ishiyama, J., Kennedy, R. (2001). *Superpresidentialism and Political Party Development in Russia, Ukraine, Armenia and Kyrgyzstan*. Europe-Asia Studies, 53(8).
356. Jach, A. (2015). *Rosyjska nostalgia imperialna*. W: S. Bieleń, A. Skrzypek (Red.), *Rosja. Rozważania imperiologiczne*. Warszawa.

357. Jastrzębska, O. (2018). *Prorosyjskie portale internetowe w Polsce i innych krajach Europy Środkowej jako istotny element kształtowania prowadzonej przez Rosję wojny informacyjnej*. Ante Portas – Studia nad Bezpieczeństwem, 2(11).
358. Jedliński, M. (2009). *Polityka zagraniczna Federacji Rosyjskiej w latach 90-tych. Kontekst historyczno-ideowy*. Środkowoeuropejskie studia polityczne, 3.
359. Jeż, P. (2023). *Współczesna aktywność dezinformacyjna Federacji Rosyjskiej i przykłady jej neutralizacji*. Res Politicae, 15.
360. Kaczmarek, J., Łepkowski, W., Zdrodowski, B. (Red.). (2008). *Słownik terminów z zakresu bezpieczeństwa narodowego*. Warszawa.
361. Kaczmarek, K. (2024). *Rosyjska dezinformacja jako element budowania wpływów w Europie: Analiza i perspektywy*. Roczniki Nauk Społecznych, 16(52), 1.
362. Kakareko, K. (2008). *Państwo Związkowe Białorusi i Rosji*. Środkowoeuropejskie Studia Polityczne, 1.
363. Kardaś, Sz. (2008). *Federacja Rosyjska w organizacjach międzynarodowych*. W: S. Bieleń, M. Raś (Red.), *Polityka zagraniczna Rosji*. Warszawa.
364. Kazimierczak, D. (2017). *Walka informacyjna we współczesnych konfliktach i jej społeczne konsekwencje*. Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate, 7.
365. Kiera, J. (2019). *Implikacje koncepcji wojen buntowniczych Jewgienija Messnera dla doktryny bezpieczeństwa Federacji Rosyjskiej w XXI wieku*. W: M. Banasik, A. Rogozińska (Red.), *Perspektywy zagrożeń dla bezpieczeństwa międzynarodowego kreowanych przez Federację Rosyjską*. Warszawa.
366. Kłaczyński, R. (2012). *Kultura strategiczna Federacji Rosyjskiej*. Nowa Polityka Wschodnia, 1(2).
367. Kłaczyński, R. (2017). *Rosyjsko-ukraiński konflikt 2014-2017 jako przykład wojny hybrydowej*. Geneza, Polityka, Gospodarka. Rocznik Bezpieczeństwa Międzynarodowego, 11(2).
368. Kmiecik, P. (2019). *Bezpieczeństwo informacyjne Rzeczypospolitej w dobie fake news – przykłady wykorzystania mediów cyfrowych w szerzeniu dezinformacji*. Bezpieczeństwo Obronność Socjologia, 11/12.
369. Kondrakiewicz, D. (2007). *Państwo*. W: M. Pietraś (Red.), *Międzynarodowe stosunki polityczne*. Lublin.

370. Kortunov, A. V., Wolodin, A. (1996). *Contemporary Russia: National interests and emerging foreign policy perceptions*. Berichte des Bundesinstituts für Ostwissenschaftliche und Internationale Studien, 33.
371. Kossecki, J. (1972). *Socjotechnika propagandy politycznej*. Zeszyty poznawcze, 3(3).
372. Koziej, S., Pietrzak, P. (2014). *Szczyt NATO w Newport*. Bezpieczeństwo Narodowe, 2014/III.
373. Kozłowski, A. (2021). *Działalność Rosji w cyberprzestrzeni zagrożeniem dla bezpieczeństwa państw regionu euroatlantyckiego*. W: M. Banasik (Red.), *Informacja czynnikiem warunkującym bezpieczeństwo. Kontekst rosyjski*. Warszawa.
374. Kruglashov, A., Shvydiuk, S. (2020). *Hybrydowe zagrożenia dla demokracji. Wybrane przykłady zewnętrznej ingerencji Rosji w wybory*. Wschód Europy, 6(2).
375. Krysiński, M., Miller, P., Pamuła, A. (2017). *Zagrożenia typu Distributed Denial of Service jako przykład ryzyka związanego z prowadzeniem działalności gospodarczej w Internecie*. Ekonomiczne Problemy Usług, 2(1).
376. Krztoń, W. (2015). *XXI wiek – Wiekiem Społeczeństwa Informacyjnego*. Modern Management Review, 22(3).
377. Kukułka, J. (1982). *Bezpieczeństwo a współpraca europejska: współzależność i sprzeczność interesów*. Sprawy międzynarodowe, 7.
378. Kukułka, J. (1988). *Polityka zagraniczna jako element procesu oddziaływań międzynarodowych*. W: J. Kukułka (Red.), *Zmienność i instytucjonalizacja stosunków międzynarodowych*. Warszawa.
379. Kukułka, J. (1992). *Polityka zagraniczna a polityka wewnętrzna*. W: J. Kukułka, R. Zięba (Red.), *Polityka zagraniczna państwa*. Warszawa.
380. Kukułka, J. (1992). *Postrzeganie międzynarodowe*. Stosunki międzynarodowe – International Relations, 16.
381. Kukułka, J. (1999). *Pojmowanie i istota tożsamości narodowej pod koniec XX wieku*. W: S. Bieleń, W. Góralski (Red.), *Nowa tożsamość Niemiec i Rosji w stosunkach międzynarodowych*. Warszawa.
382. Kukułka, J. (2006). *Zaspokajanie potrzeb i rozwiązywanie konfliktów w stosunkach międzynarodowych*. W: E. Haliżak, R. Kuźniar (Red.), *Stosunki międzynarodowe. Geneza, struktura, dynamika*. Warszawa.
383. Kuźniar, R. (2000). *Międzynarodowe stosunki polityczne*. W: E. Haliżak, R. Kuźniar (Red.), *Stosunki międzynarodowe – geneza, struktura, dynamika*. Warszawa.

384. Kuźniar, R. (2000). *Stosunki międzynarodowe – istota, uwarunkowania, badanie*. W: E. Haliżak, R. Kuźniar (Red.), *Stosunki międzynarodowe – geneza, struktura, dynamika*. Warszawa.
385. Lakomy, M. (2010). *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku*. *Stosunki Międzynarodowe*, Tom 42, Numer 3/4.
386. Lakomy, M. (2013). *Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek do typologii*. *Kwartalnik Naukowy OAP UW e-Politikon*, Numer 6.
387. Lakomy, M. (2014). *Polityka bezpieczeństwa teleinformatycznego Polski*. W: K. Czornik, M. Lakomy, M. Stolarczyk (Red.), *Dylematy polityki zagranicznej Polski na początku XXI wieku*. Katowice.
388. Lakomy, M. (2016). *Wymiar informacyjny i telekomunikacyjny bezpieczeństwa Polski*. W: M. Pietraś, K. A. Wojtaszczyk (Red.), *Polska w systemie bezpieczeństwa międzynarodowego*. Warszawa.
389. Lakomy, M. (2019). *Recruitment and Incitement to Violence in the Islamic State's Online Propaganda: Comparative Analysis of Dabiq and Rumiyah*. *Studies in Conflict & Terrorism*, 44(7).
390. Legucka, A. (2019). *Polityka zagraniczna Polski wobec Rosji po aneksji Krymu*. *Wschód Europy*, 5(1).
391. Legucka, A. (2019). *Rosja wobec Partnerstwa Wschodniego Unii Europejskiej*. *Rocznik Instytutu Europy Środkowo-Wschodniej*, 17(2).
392. Legucka, A. (2020). *Dezinformacja jako element wojny informacyjnej Federacji Rosyjskiej – założenia i efektywność*. *Sprawy Międzynarodowe*, 73(4).
393. Lelito, R. (2018). *Idea systemu cyberobronności państwa*. W: B. Biernacik, L. Kalman, G. Pilarski (Red.), *Wsparcie teleinformatyczne i bezpieczeństwo cyberprzestrzeni w SZ RP*. Warszawa.
394. Lelonek, A. (2016). *Wojna informacyjna, operacje informacyjne i psychologiczne: pojęcia, metody i zastosowanie*. W: A. Lelonek (Red.), *Potencjał słowa. Międzynarodowe stosunki i komunikacja: stan i perspektywy*. Warszawa – Lwów.
395. Lewandowski, P. (2023). *Rosyjska walka informacyjna z polską historią. Rzeczpospolita obojga narodów jako przedmiot rosyjskich działań dezinformacyjnych*. *Fides, Ratio et Patria. Studia Toruńskie*, 18.
396. Liedel, K. (2015). *Zdolność prowadzenia działań ofensywnych w cyberprzestrzeni warunkiem bezpieczeństwa państwa*. W: P. Sienkiewicz, H. Świeboda, E. Szczepaniuk (Red.), *Nie-bezpieczny świat. Systemy Informacja Bezpieczeństwo*. Warszawa.

397. Liedel, K., Piasecka, P. (2011). *Wojna cybernetyczna – wyzwanie XXI wieku*. Bezpieczeństwo narodowe, Numer I-2011/17.
398. Lukaseder, T., Stölzle, K., Kleber, S., Erb, B., Kargl, F. (2019). *An SDN-based Approach For Defending Against Reflective DDoS Attacks*. 2018 IEEE 43rd Conference on Local Computer Networks (LCN).
399. Łomanowski, A., Musiałowicz, B. (2006). *Kierunki rosyjskiej polityki zagranicznej*. Bezpieczeństwo Narodowe, II – 2006/2.
400. Łoś-Nowak, T. (2011). *Polityka zagraniczna – stałe i zmienne komponenty procesu formułowania i realizacji*. W: T. Łoś-Nowak (Red.), *Polityka zagraniczna: aktorzy, potencjały, strategie*. Warszawa.
401. Madden, A. D. (2000). *A definition of information*. Aslib Proceedings, 52(9).
402. Madej, M. (2009). *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państwa i systemu międzynarodowego*. W: M. Madej, M. Terlikowski (Red.), *Bezpieczeństwo Teleinformatyczne Państwa*. Warszawa.
403. Madej, M., Terlikowski, M. (Red.). (2009). *Bezpieczeństwo teleinformatyczne państwa*. Warszawa.
404. Małycha, J. (2016). *Cyberwojna. Obronność* – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej, Numer 4(20).
405. Marsh, D., Stoker, G. (Red.). (2006). *Teorie i metody w naukach politycznych*. Kraków.
406. McCombs, M. E., Guo, L. (2014). *Agenda-setting Influence of the Media in the Public Sphere*. W: R. S. Fortner, P. M. Fackler (Red.), *The Handbook of Media and Mass Communication Theory*. New York.
407. Milewski, J. (2016). *Identyfikacja infrastruktury krytycznej i jej zagrożeń*. Zeszyty naukowe AON, 4(105).
408. Modrzejewski, Z. (2018). *Dezinformacja w służbie walki informacyjnej*. W: T. W. Grabowski, M. Lakomy, K. Oświecimski (Red.), *Bezpieczeństwo informacyjne w dobie postprawdy*. Kraków.
409. Moliński, M. (2011). *Refleksje nad wzajemnym postrzeganiem stosunków Polska-Rosja*. W: A. Stępień-Kuczyńska, M. Potz, M. Słowikowski (Red.), *Dwie dekady transformacji w Europie Środkowej i Wschodniej 1989–2009*. Toruń.
410. Molo, B. (2008). *Systemy, zasady i formy międzynarodowej współpracy politycznej*. W: E. Cziomer (Red.), *Międzynarodowe stosunki polityczne*. Kraków.

411. Nowak, J. S. (2008). *Spółeczeństwo informacyjne – geneza i definicje*. W: P. Sienkiewicz, J. S. Nowak (Red.), *Spółeczeństwo informacyjne. Krok naprzód, dwa kroki wstecz*. Katowice.
412. Nowak-Far, A. (2022) *Gospodarka*. W: K. A. Wojtaszczyk, I. N. Novikova (Red.), *Polska i Rosja w zmieniającej się Europie*. Warszawa.
413. Nowiak, J. (1996). *Polityka zagraniczna*. W: W. Malendowski, Cz. Mojsiewicz (Red.), *Międzynarodowe stosunki polityczne*. Poznań.
414. Olędzka, J. (2017). *Russian Language as a Tool of Geopolitical Influence*. Yearbook of the Institute of East-Central Europe, 15(3).
415. Olszański, T. A. (1994). *Czym (nie) jest WNP? Wspólnota Niepodległych Państw w świetle własnych dokumentów*. EURAZJA, 1-2(1).
416. Pastusiak, L. (2017). *Teheran, Jałta, Poczdam: Wielka Trójka o zachodniej granicy Polski*. Niepodległość i Pamięć, 24(1).
417. Pawlikowski, G. (2016). *Mniejszość rosyjska jak instrument polityki zagranicznej Federacji Rosyjskiej po 1991 roku*. Wybrane aspekty. Przegląd Geopolityczny, 15.
418. Pietraś, Z. J. (1992). *Polityka zagraniczna państwa*. W: T. Łoś-Nowak (Red.), *Współczesne stosunki międzynarodowe*. Wrocław.
419. Pietrzak, H. (2011). *Wybrane zagadnienia mierzalności przestrzeni medialnej*. Nierówności Społeczne a Wzrost Gospodarczy, 22.
420. Pióro, T. (1990). *Wojsko – nasze wojsko?* Res Publica, 5.
421. Pomorski, J. (Red.). (1998). *Historia, metodologia, współczesność*. Lublin.
422. Popiuk-Rysinska, I. (2006). *Uczestnicy stosunków międzynarodowych, ich interesy i oddziaływania*. W: E. Halizak, R. Kuźniar (Red.), *Stosunki międzynarodowe. Geneza, struktura, dynamika*. Warszawa.
423. Pratkanis, A., Aronson, E. (2004). *Wiek propagandy. Używanie i nadużywanie perswazji na co dzień*. Warszawa; Francuz, P. *Strach i lęk w reklamie politycznej*. W: P. Francuz (Red.), *Psychologiczne aspekty komunikacji audiowizualnej*. Lublin.
424. Pronińska, K. (2009). *Strategie bezpieczeństwa energetycznego państwa na przykładzie wybranych krajów UE*. W: M. Sułek, J. Symonides (Red.), *Państwo w teorii i praktyce stosunków międzynarodowych*. Warszawa.
425. Pushkov, A. K. (1998). *Constitutional Reform as a Struggle for Power*. East European Constitutional Review, 7(4).
426. *Raport Niezależnej Międzynarodowej Misji Wyjaśniającej w sprawie Konfliktu w Gruzji*. (2010). Międzynarodowy Przegląd Polityczny, 1.

427. Raś, M. (2010). *Polityka Rosji wobec Europy Środkowo-Wschodniej*. Prace Instytutu Europy Środkowo-Wschodniej, 16.
428. Raś, M. (2020). *Cele oddziaływań politycznych Federacji Rosyjskiej*. W: T. Stępniewski (Red.), *Rosja wobec państw Europy Środkowej i Wschodniej: zagrożenia pozamilitarne*. Lublin.
429. Raś, M. (2022). *Polska w stosunkach międzynarodowych*. W: K. A. Wojtaszczyk, I. N. Novikova (Red.), *Polska i Rosja w zmieniającej się Europie*. Warszawa.
430. Rogozińska, A. (2020). *Analiza zagrożeń kreowanych w cyberprzestrzeni*. W: T. Stępniewski (Red.), *Rosja wobec państw Europy Środkowej i Wschodniej: zagrożenia pozamilitarne*. Lublin.
431. Rosenau, J. N. (1968). *Comparative Foreign Policy: Fad, Fantasy or Field?* International Studies Quarterly, 12.
432. Rot, A., Olszewski, B. (2017). *Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection*. Position papers of the Federated Conference on Computer Science and Information Systems, 13.
433. Sabat, M. (2010). *Stosunki polsko-rosyjskie. Rozbieżności interesów strategicznych*. W: L. Zyblikiewicz, M. Czajkowski, P. Bajor (Red.), *Polityka zagraniczna Federacji Rosyjskiej. Wybrane aspekty stosunków z Polską, Ukrainą i Białorusią*. Kraków.
434. Sadiku, M. N. O., Shadare, A. E., Musa, S. M. (2016). *Social Engineering: An Introduction*. The Journal of Scientific and Engineering Research, 3(3).
435. Sadowski, E. (1988). *Racja stanu w polityce zagranicznej współczesnego państwa*. W: J. Kukułka (Red.), *Zmienność i instytucjonalizacja stosunków międzynarodowych*. Warszawa.
436. Schmitt, M. N. (Red.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge.
437. Semetko, H. A., Valkenburg, P. M. (2000). *Framing European politics: a content analysis of press and television news*. Journal of Communication, 50(2).
438. Sienkiewicz, P. (2003). *Wizje i modele wojny informacyjnej*. W: L. H. Haber (Red.), *Spółeczeństwo informacyjne - wizja czy rzeczywistość?* Kraków.
439. Sienkiewicz, P. (2011). *Ewaluacja informacji w społeczeństwie informacyjnym*. Ekonomiczne Problemy Usług, 67.
440. Sienkiewicz, P. (2012). *Bezpieczeństwo cyberprzestrzeni państwa*. Ekonomiczne Problemy Usług, 88.

441. Sienkiewicz, P., Świeboda, H. (2009). *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej*. W: M. Madej, M. Terlikowski (Red.), *Bezpieczeństwo Teleinformatyczne Państwa*. Warszawa.
442. Skarżyński, R. (2009). *Czy istnieje porządek międzynarodowy? Jak starożytne i średniowieczne wzorce myślowe określają terminologię współczesnej nauki o stosunkach międzynarodowych*. W: E. Kuźelewska, K. Stefanowicz (Red.), *Wybrane problemy globalnej i regionalnej polityki międzynarodowej*. Toruń.
443. Smith, B. (2018). *Russian intelligence services and special forces*. Briefing paper, CBP 8430.
444. Smoleń, M. (2004). *Historia Rosji*. W: L. Suchanek (Red.), *Rosjoznawstwo. Wprowadzenie do studiów nad Rosją*. Kraków.
445. Soler, U., Makuch, A., Chałubińska-Jentkiewicz, K. (2023). *Disinformation in Polish Society in 2021 – Trends, Topics, Channels of Transmission*. *Polish Political Science Yearbook*, 52(1).
446. Soloch, P., Pietrzak, P. (2016). *Szczyt NATO w Warszawie: uwarunkowania, rezultaty, wnioski dla Polski*. Bezpieczeństwo Narodowe, 2016/I-IV.
447. Sproule, J. M. (2001). *Authorship and Origins of the Seven Propaganda Devices: A Research Note*. *Rhetoric and Public Affairs*, 4(1).
448. Stawarz, P. (2022). *Polityka wschodnia Unii Europejskiej*. W: K. A. Wojtaszczyk, I. N. Novikova (Red.), *Polska i Rosja w zmieniającej się Europie*. Warszawa.
449. Stępniewski, T. (2020). *Résumé*. W: T. Stępniewski (Red.), *Rosja wobec państw Europy Środkowej i Wschodniej: zagrożenia pozamilitarne*. Lublin.
450. Stolarczyk, M. (2013). *Kontrowersje wokół koncepcji i praktyki polityki wschodniej Polski na przełomie pierwszej i drugiej dekady XXI wieku*. W: K. Miroszewski, M. Stolarczyk (Red.), *Śląsk - Polska - Europa - świat: pamięci Profesora Jana Przewłockiego*. Katowice.
451. Stolarczyk, M. (2013). *Rosja w polityce zagranicznej Polski w okresie pozimnowojennym (aspekty polityczne)*. *Studia Politicae Universitatis Silesiensis*, 11.
452. Sunstein, C. R. (2016). *Fifty shades of manipulation*. *Journal of Marketing Behavior*, 213.
453. Szafrński, R. (1996). *Cyberwar: A Theory of Information Warfare: Preparing for 2020*. W: A. D. Campen, D. H. Deart, R. T. Coodden (Red.), *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Fairfax.
454. Szewczyk, T., Pyznar, M. (2010). *Ochrona infrastruktury krytycznej a zagrożenia asymetryczne*. *Przegląd Bezpieczeństwa Wewnętrznego*, 2/10.

455. Szymanek, J. (2017). *Legislatywa i egzekutywa w prezydenckich i półprezydenckich systemach rządów*. Przegląd Sejmowy, 1(138).
456. Tadeusiewicz, R. (2010). *Zagrożenia w cyberprzestrzeni*. Nauka, 4.
457. Tandoc Jr., E. C., Lim, Z. W., Ling, R. (2018). *Defining "Fake News" A typology of scholarly definitions*. Digital Journalism, 6(2).
458. Tenerowicz, R. (2015). *Nowy liberalizm*. W: R. Zięba, S. Bieleń, J. Zając (Red.), *Teorie i podejścia badawcze w nauce o stosunkach międzynarodowych*. Warszawa.
459. Thomas, T. L. (1998). *Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations*. The Journal of Slavic Military Studies, 11(1).
460. Tymanowski, J. (2022). *Federacja Rosyjska w polityce zewnętrznej Unii Europejskiej*. W: K. A. Wojtaszczyk, I. N. Novikova (Red.), *Polska i Rosja w zmieniającej się Europie*. Warszawa.
461. Udalov, V. (1995). *National Interests and Conflict Reduction*. W: I. W. Zartman, V. A. Kremenyuk (Red.), *Cooperative Security. Reducing Third World Wars*. New York.
462. von Vorys, K. (1957). *The Concept of National Interest*. W: V. van Dyke (Red.), *Some Approaches and Concepts Used in the Teaching of International Politics*. Iowa City.
463. Warchoń, A. (2023). *Rola cyberprzestrzeni w wojnie Rosji z Ukrainą*. Nowa Polityka Wschodnia, 4(39).
464. Wasilewski, J. (2013). *Zarys definicyjny cyberprzestrzeni*. Przegląd bezpieczeństwa wewnętrznego, 9(19).
465. Weremiuk, S. (2014). *Specyfika stosunków polsko-radzieckich w latach 1944-1991*. Przegląd Bezpieczeństwa Wewnętrznego, 11(14).
466. Wierzbicki, A. (2015). *Russkij mir jako projekt restauracyjny imperium*. W: S. Bieleń, A. Skrzypek (Red.), *Rosja. Rozważania imperiologiczne*. Warszawa.
467. Wojciechowski, S. (2014). *Biała księga bezpieczeństwa narodowego RP a problemy i wyzwania w zakresie WPBiO Unii Europejskiej*. W: S. Wojciechowski, A. Potyrała (Red.), *Bezpieczeństwo Polski. Współczesne wyzwania*. Warszawa.
468. Wojciechowski, S. (2019). *Teoretyczne i praktyczne aspekty bezpieczeństwa Polski. 1.1. Wprowadzenie*. W: A. Wejkszner, S. Wojciechowski (Red.), *Współczesne bezpieczeństwo Polski. Międzynarodowy wymiar instytucjonalny*. Warszawa.
469. Wojnowski, M. (2017). *Koncepcja wojny sieciowej Aleksandra Dugina jako narzędzie realizacji celów geopolitycznych Federacji Rosyjskiej*. Przegląd Bezpieczeństwa Wewnętrznego, 9.

470. Wojnowski, M. (2019). *Wybory prezydenckie jako narzędzie destabilizacji państw w teorii i praktyce rosyjskich operacji informacyjno-psychologicznych w XX i XXI w.* Przegląd Bezpieczeństwa Wewnętrznego, 21.
471. Wołos, M. (2015). *Polska widziana z rosyjskiej oddali.* Kultura Współczesna: teoria, interpretacje, krytyka, 2015(1).
472. Wójtowicz, T. (2014). *Od doktryny wojny ludowej do doktryny wojny informacyjnej. Rola nowych technologii w transformacji Chińskiej Armii Ludowo-Wyzwoleńczej.* Kultura i Polityka, 16.
473. Wrzosek, M. (2021). *Rosyjska dominacja informacyjna w sferze militarnej.* W: M. Banasik (Red.), *Informacja czynnikiem warunkującym bezpieczeństwo. Kontekst rosyjski.* Warszawa.
474. Wrzosek, M. (2024). *Rosyjska dezinformacja w konflikcie zbrojnym w Ukrainie.* Bezpieczeństwo Narodowe, 44.
475. Wrzosek, M., Markiewicz, Sz., Modrzejewski, Z. (2018). *Dominacja informacyjna w wojnie hybrydowej.* W: M. Wrzosek, Sz. Markiewicz, Z. Modrzejewski (Red.), *Informacyjny wymiar wojny hybrydowej.* Warszawa.
476. Wrzosek, M., Markiewicz, Sz., Modrzejewski, Z. (Red.). (2019). *Informacyjny wymiar wojny hybrydowej.* Warszawa.
477. Young, O. R., Yand, J., Zagorski, A. (2022). *The "New" Arctic as a Zone of Peaceful Competition.* Polar Perspectives, 11.
478. Zając, J. (2005). *Środki i metody polityki zagranicznej państwa.* W: R. Zięba (Red.), *Wstęp do teorii polityki zagranicznej państwa.* Toruń.
479. Zając, J. (2015). *Teorie ról międzynarodowych.* W: R. Zięba, S. Bieleń, J. Zając (Red.), *Teorie i podejścia badawcze w nauce o stosunkach międzynarodowych.* Warszawa.
480. Zięba, R. (2001). *Wpływ tendencji globalizacyjnych na bezpieczeństwo narodowe.* Rocznik Nauk Politycznych, 3.
481. Zięba, R. (2005). *Cele polityki zagranicznej państwa.* W: R. Zięba (Red.), *Wstęp do teorii polityki zagranicznej państwa.* Toruń.
482. Zięba, R. (2005). *Uwarunkowania polityki zagranicznej państwa.* W: R. Zięba (Red.), *Wstęp do teorii polityki zagranicznej państwa.* Toruń.
483. Zięba, R. (2011). *Uwarunkowania polityki zagranicznej polski na początku drugiej dekady XXI wieku.* Stosunki międzynarodowe – International Relations, 1-2 (T.43).
484. Zięba, R. (2011). *Współczesne stosunki polsko-rosyjskie: uwarunkowania, problemy, implikacje.* Przegląd Politologiczny, 3.

485. Zięba, R. (2012). *O tożsamości nauk o bezpieczeństwie*. Zeszyty Naukowe Akademii Obrony Narodowej, 1 (86).
486. Zięba, R. (2018). *Główne problemy w stosunkach polsko-rosyjskich*. Stosunki Międzynarodowe – International Relations, 3(T. 54).
487. Ziółkowski, J. (2016). *Zarządzanie syndromem oblężenia w demokracji liberalnej*. Studia Politologiczne, 41.
488. Zyblikiewicz, L., Czajowski, M., Bajor, P. (Red.). (2010). *Polityka zagraniczna Federacji Rosyjskiej. Wybrane aspekty z Polską, Ukrainą i Białorusią*. Kraków.
489. Żebrowski, A. (2013). *Bezpieczeństwo informacyjne Polski a walka informacyjna*. Roczniki Kolegium Analiz Ekonomicznych, 29.
490. Żebrowski, A. (2017). *Determinanty walki informacyjnej*. W: H. Batorowska (Red.), *Walka informacyjna: uwarunkowania, incydenty, wyzwania*. Kraków.
491. Żebrowski, A. (2018). *Agentura wpływu uczestnikiem walki informacyjnej*. Studia nad Autorytaryzmem i Totalitaryzmem, 1(40).
492. Żebrowski, A., Żmigrodzka, M. (2012). *Media uczestnikami walki informacyjnej*. Doctrina. Studia społeczno-polityczne, 9.

Artykuły prasowe

493. BBC. *Anonymous: How hackers are trying to undermine Putin.*
<https://www.bbc.com/news/technology-60784526>
494. Biznes Alert. *To nie pierwsza przerwa dostaw ropy z Rosji do Polski.*
<https://biznesalert.pl/rosja-polska-ropa-przyjazn-bialorus-energetyka/>
495. BuzzFeedNews. *Documents Show How Russia's Troll Army Hit America.*
<https://www.buzzfeednews.com/article/maxseddon/documents-show-how-russias-troll-army-hit-america>
496. CNBC. *Hacktivist group Anonymous is using six top techniques to 'embarrass' Russia.*
<https://www.cnbc.com/2022/07/28/how-is-anonymous-attacking-russia-the-top-six-ways-ranked-.html>
497. CNN. *US troops to deploy to Eastern Europe amid Ukraine crisis.*
<https://edition.cnn.com/2022/02/02/politics/us-troops-europe-russia/index.html>
498. CyberDefence24. *Cyberatak na Polską Policję. Znamy szczegóły.*
<https://cyberdefence24.pl/armia-i-sluzby/cyberatak-na-polska-policje-znamy-szczegoly>
499. CyberDefence24. *Cyberatak na Senat. Między innymi z terenu Rosji [AKTUALIZACJA].*
<https://cyberdefence24.pl/cyberbezpieczenstwo/cyberatak-na-senat-marszalek-potwierdza>
500. CyberDefence24. *Dezinformacją w polski atom.* <https://cyberdefence24.pl/polityka-i-prawo/dezinformacja-w-polski-atom>
501. CyberDefence24. *NATO: Artykuł 5 działa również w wypadku cyberataków.*
<https://cyberdefence24.pl/polityka-i-prawo/nato-artykul-5-dziala-rowniez-w-wypadku-cyberatakow>
502. CyberDefence24. *Oficerowie GRU z aktem oskarżenia. Świat poznał sprawców „największych cyberataków w historii”.* <https://cyberdefence24.pl/polityka-i-prawo/oficerowie-gru-z-aktem-oskarzenia-swiat-poznal-sprawcow-najwiekszych-cyberatakow-w-historii>
503. CyberDefence24. *RT i Sputnik oficjalnie zablokowane w UE. Za wdrożenie sankcji odpowiedzialne kraje członkowskie.* <https://cyberdefence24.pl/polityka-i-prawo/rt-i-sputnik-oficjalnie-zablokowane-w-ue-za-wdrozenie-sankcji-odpowiedzialne-kraje-czlonkowskie>

504. CyberDefence24. *Strategia rosyjskich botów w sieci – uderzyć w NATO i Polskę.*
<https://cyberdefence24.pl/polityka-i-prawo/strategia-rosyjskich-botow-w-sieciuderzyc-w-nato-i-polske>
505. CyberDefence24. *Włamanie do Europejskiej Agencji Leków mniej poważne niż zakładano.*
<https://cyberdefence24.pl/polityka-i-prawo/wlamanie-do-europejskiej-agencji-lekow-mniej-powazne-niz-zakladano>
506. CyberDefence24.pl. *Amerykanie "idą" na wojnę informacyjną.*
<https://www.cyberdefence24.pl/amerykanie-ida-na-wojne-informacyjna>
507. CyberDefence24.pl. *Chiny zwycięzcą wojny informacyjnej z USA?*
<https://www.cyberdefence24.pl/chiny-zwyciezca-wojny-informacyjnej-z-usa>
508. Cyberdefence24.pl. *Zachód produkuje broń biologiczną w Gruzji? Dezinformacyjne macki Kremla dosięgają Kaukazu.*
<https://cyberdefence24.pl/bezpieczenstwo-informacyjne/zachod-produkuje-bron-biologiczna-w-gruzji-dezinformacyjne-macki-kremla-dosiegaja-kaukazu>
509. Defence24. *Bliski Wschód wobec wojny na Ukrainie: rosyjska propaganda i biznes.*
<https://defence24.pl/geopolityka/bliski-wschod-wobec-wojny-na-ukrainie-rosyjska-propaganda-i-biznes>
510. Defence24. *Budżet MON na 2023 r. uchwalony.*
<https://defence24.pl/polityka-obronna/budzet-mon-na-2023-r-uchwalony>
511. Defence24. *Wtorek z Defence24.pl: Jak służby monitorują kanały komunikacyjne; Były szef ABW ujawnił cyberatak na MON; Rosyjskie wojny o wpływy; Szczyt NATO w Warszawie coraz bliżej; Rosyjski bombowiec na granicy izraelskiej.*
<https://defence24.pl/wtorek-z-defence24pl-jak-sluzby-monitoruja-kanaly-komunikacyjne-byly-szef-abw-ujawnil-cyberatak-na-mon-rosyjskie-wojny-o-wplywy-szczyt-nato-w-warszawie-coraz-blizej-rosyjski-bombowiec-na-granicy-izraelskiej>
512. DW. *Der Spiegel: RT – instrument rosyjskiej propagandy.*
<https://www.dw.com/pl/der-spiegel-rt-instrument-rosyjskiej-propagandy/a-56724016>
513. DW. *Putinowskie zagrywki z gazem trafiają w punkt zapalny.*
<https://www.dw.com/pl/putinowskie-zagrywki-z-gazem-trafiaj%C4%85-w-punkt-zapalny/a-60282542>
514. DW. *Russia plans Belarus 'absorption' by 2030 — media reports.*
<https://www.dw.com/en/russia-plans-belarus-absorption-by-2030-media-reports/a-64771429>

515. Dziennik Gazeta Prawna. *W ciągu roku od napaści Rosji Polska przekazała Ukrainie uzbrojenie o wartości ponad 2,2 mld euro.* <https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/8667242,polska-dostawy-broni-dla-ukrainy-o-wartosci-ponad-22-mld-euro.html>
516. Dziennik.pl. *Hakerzy z Rosji, Niemiec i Chin najczęściej atakują Polskę. Oto miejsca, które są na celowniku cyberwłamywaczy.* <https://technologia.dziennik.pl/internet/artykuly/563147,ktore-kraje-najczesciej-przeprowadzaja-cyberataki-na-polske.html>
517. Energetyka24. *Cyberwojna o Baltic Pipe? Ataki rosyjskich służb na Czechy, Polskę i Norwegię [ANALIZA].* <https://energetyka24.com/cyberwojna-o-baltic-pipe-ataki-rosyjskich-sluzb-na-czechy-polske-i-norwegie-analiza>
518. EXPRESS. *Russia launches attack on Poland as hackers declare war on 10 countries, including UK.* <https://www.express.co.uk/news/science/1638740/russia-launches-cyberattack-poland-government-sites-shut-down-killnet-ukraine-war>
519. Forces Net. *Russia vs Britain: How do their militaries stack up?* <https://www.forces.net/news/russia-vs-britain-how-do-militaries-stack>
520. Gazeta Wyborcza. *List Putina do Polaków - pełna wersja.* <https://wyborcza.pl/7,75399,6983945,list-putina-do-polakow-pelna-wersja.html>
521. Gazeta.pl. *Afera mailowa. Dworczyk miał pisać do Klarenbacha ws. caracali. "Przekaz jest taki..."*. <https://wiadomosci.gazeta.pl/wiadomosci/7,114884,29592952,afera-mailowa-dworczyk-mial-pisac-do-klarenbacha-ws-caracali.html>
522. interfax-UKRAINE. *SBU liquidates million-strong bot farm destabilizing situation in Ukraine on order of political force.* <https://interfax.com.ua/news/general/850029.html>
523. Jedyńska Polskie Radio. *Sprawa wraku Tu-154M. Guzy: Rosja chce, by wszyscy o nim zapomnieli.* <https://jedyńska.polskieradio.pl/artykul/2490525,sprawa-wraku-tu154m-guzy-rosja-chce-by-wszyscy-o-nim-zapomnieli>
524. Konkret24. *Falszywe wiadomości o "radioaktywnej chmurze znad Czarnobyla". PAA: "Nie ma żadnego zagrożenia".* <https://konkret24.tvn24.pl/polska/falszywe-wiadomosci-o-radioaktywnej-chmurze-znad-czarnobyla-paa-nie-ma-zadnego-zagrozenia-ra1013183>
525. Logistyka. *Polska stała się portem zastępczym i hubem logistycznym dla Ukrainy.* <https://www.logistyka.net.pl/aktualnosci/item/93456-polska-stala-sie-portem-zastepczym-i-hubem-logistycznym-dla-ukrainy>

526. NBC News. *Facebook, Twitter remove disinformation accounts targeting Ukrainians.*
<https://www.nbcnews.com/tech/internet/facebook-twitter-remove-disinformation-accounts-targeting-ukrainians-rcna17880>
527. Niebezpiecznik. *[AKTUALIZACJA #10] Kolejny groźny globalny atak: ransomware Petya (NotPetya). Ofiary także w Polsce. Dotyczy również zaktualizowanych Windowsów!* <https://niebezpiecznik.pl/post/kolejny-grozny-globalny-atak-tym-razem-ransomware-petya-ofiary-sa-takze-w-polsce/>
528. Niebezpiecznik. *ABW i SKW potwierdza: to Rosjanie zhackowali Dworczyka i resztę polskich polityków.* <https://niebezpiecznik.pl/post/abw-i-skw-rosjanie-unc1151-dworczyk-ghostwriter/>
529. Niebezpiecznik. *Co wiemy o rosyjskich szpiegach w poczcie polskich wojskowych.*
<https://zaufanatrzeciastrona.pl/post/co-wiemy-a-czego-nie-o-rosyjskich-szpiegach-w-poczcie-polskich-wojskowych/>
530. Niebezpiecznik. *Informacje o szczepionce na COVID-19 celem hackerów z Rosji – uważają służby USA, UK.* <https://niebezpiecznik.pl/post/informacje-o-szczepionce-na-covid-19-celem-hackerow-z-rosji-uwazaja-sluzby-usa-uk/>
531. Niebezpiecznik. *Masowe telefony z Rosji na numery polskich żołnierzy.*
<https://niebezpiecznik.pl/post/kto-masowo-dzwonil-do-polskich-zolnierzy-z-rosyjskiego-numeru/>
532. Niebezpiecznik. *MON stworzy “wojsko cybernetyczne” z komponentem informacyjno-psychologicznym (INFOOPS).* <https://niebezpiecznik.pl/post/mon-stworzy-wojsko-cybernetyczne-z-komponentem-informacyjno-psychologicznym-infoops/>
533. Niebezpiecznik. *Niezależna.pl i wiele innych serwisów w Polsce zhackowanych. Rozsiewały plotki o ewakuacji Polaków przez żandarmerię i wojska USA.*
<https://niebezpiecznik.pl/post/niezalezna-pl-i-inne-serwisy-w-polsce-zhackowane-rozsiewaly-plotki-o-ewakuacji-polakow-przez-zandarmerie-i-wojska-usa/>
534. Niebezpiecznik. *Portal Money.pl zhackowany. Włamywacz życzył porażki Ukrainie.*
<https://niebezpiecznik.pl/post/portal-money-pl-zhackowany-przez-sily-prorosyjskie/>
535. Niebezpiecznik. *Przełomowy raport CIA, FBI i NSA: to Rosja wpływała na przebieg wyborów prezydenckich w USA.* <https://niebezpiecznik.pl/post/jak-rosjanie-wplywali-na-przebieg-wyborow-prezydenckich-w-usa/>
536. Niebezpiecznik. *Rosjanie atakują połączenia satelitarne, aby zachować anonimowość w sieci.* <https://niebezpiecznik.pl/post/rosjanie-atakuja-satelity-aby-zachowac-anonimowosc-w-sieci/>

537. Niebezpiecznik. *Rosyjskojęzyczny wirus infekował Polaków plikiem o Katyniu*. <https://zaufanatrzeciastrona.pl/post/rosyjskojeczny-wirus-infekowal-polakow-plikiem-o-katyniu/>
538. Niebezpiecznik. *Skandal w Kaspersky. Ten antywirus pomagał rosyjskim służbom wykraść dane z komputerów na całym świecie*. <https://niebezpiecznik.pl/post/skandal-w-kaspersky-ten-antywirus-pomagal-rosyjskim-sluzbom-wykradac-dane-z-komputerow-na-calym-swiecie/>
539. Niebezpiecznik. *To nie Rosjanie a Białorusini zhackowali polskich polityków*. <https://niebezpiecznik.pl/post/bialorus-stoi-za-atakami-na-polskich-politykow-unc1151/>
540. Niebezpiecznik. *UE nakłada sankcje za cyberataki m.in. na rosyjskiego admirała*. <https://niebezpiecznik.pl/post/ue-naklada-sankcje-za-cyberataki-m-in-na-rosyjskiego-admirala/>
541. Niebezpiecznik. *UE odpowiedziała sankcjami na WannaCry oraz... atak na polską KNF*. <https://niebezpiecznik.pl/post/ue-odpowiedziala-sankcjami-na-wannacry-oraz-atak-na-polska-knf/>
542. Niebezpiecznik. *Ukraina informuje o atakach DDoS na MON i banki*. <https://niebezpiecznik.pl/post/ukraina-informuje-o-atakach-ddos-na-mon-i-banki/>
543. Niebezpiecznik. *Włamywacze opublikowali treść e-maila ze skrzynki ministra Dworczyka*. <https://niebezpiecznik.pl/post/wyciek-e-mail-do-ministra-dworczyka/>
544. Niebezpiecznik. *Zdjęcie dowodu i prawa jazdy ministra Dworczyka wykradzione i opublikowane. Razem z "memem"*. <https://niebezpiecznik.pl/post/skany-dowodu-osobistego-i-prawa-jazdy-dworczyka-wykradzione/>
545. NOIZZ. *F-Secure, firma specjalizująca się w cyberbezpieczeństwie, opublikowała mapę ataków wymierzonych w polski internet. Najwięcej włamań przeprowadzają Rosjanie*. <https://noizz.pl/nauka-i-technologia/rosjanie-przeprowadzaja-14-tys-cyberatakow-na-polske-dziennik/w847mxq>
546. NOIZZ. *Nie tylko "Szpiegowo". W Polsce są inne budynki, za które Rosja nie płaci czynszu*. <https://noizz.pl/spoleczenstwo/nie-tylko-szpiegowo-w-polsce-sa-inne-budynki-za-ktora-rosja-nie-placi-czynszu/b5w8pve>
547. OKO.press. *43 portale nadają codziennie antyukraińską propagandę po polsku [RAPORT Z SIECI]*. <https://oko.press/antyukrainska-propaganda-po-polsku-raport-z-sieci/>
548. OKO.press. *Afera mailowa. Jak Przylębska z Dworczykiem oszczędzali na obywatelach, odraczając rozstrzygnięcia w TK*. <https://oko.press/afery-mailowa-przylebska-dworczyk>

549. OKO.press. *Jednak Rosja! To ona według analityków USA stała za operacją, której częścią było #DworczykLeaks*. <https://oko.press/jednak-rosja-tstala-za-dworczykleaks>
550. Onet Wiadomości. *Afera e-mailowa. Doradca premiera prosi Kurskiego i szefa "Wiadomości" o "ładny atak w TVP" na sędziego*. https://wiadomosci.onet.pl/kraj/afere-mailowa-doradca-premiera-prosil-kurskiego-o-ladny-atak-w-tvp/z12hy7e?utm_source=pl.wikipedia.org_viasg_wiadomosci&utm_medium=referral&utm_campaign=leo_automatic&srcc=undefined&utm_v=2
551. Onet Wiadomości. *Rosyjscy hakerzy odbili się od ściany w polskich ministerstwach*. <https://wiadomosci.onet.pl/kraj/hakerski-atak-gru-apt28-na-polskie-msz-i-mon/yhx4xjn>
552. PAP Polska Agencja Prasowa. *Jak Polska pomaga Ukrainie? Sprzęt wojskowy, który przekazujemy*. <https://www.pap.pl/aktualnosci/news%2C1557048%2Cjak-polska-pomaga-ukrainie-sprzet-wojskowy-ktory-przekazujemy>
553. PAP Polska Agencja Prasowa. *Podkomisja smoleńska wzywa MKL i rosyjską prokuraturę do zwrotu wraku Tu-154M*. <https://www.pap.pl/aktualnosci/news%2C1421216%2Cpodkomisja-smolenska-wzywa-mkl-i-rosyjska-prokuratura-do-zwrotu-wraku-tu>
554. PAP Polska Agencja Prasowa. *Polska przekazała czołgi PT-91 Twardy. Sąd już w Ukrainie*. <https://www.pap.pl/aktualnosci/news%2C1381879%2Cpolska-przekazala-czolgi-pt-91-twardy-sa-juz-w-ukrainie>
555. PAP Polska Agencja Prasowa. *Rosja szykuje masowe cyberataki. Na celowniku też Polska*. <https://www.pap.pl/aktualnosci/news%2C1435328%2Crosja-szykuje-masowe-cyberataki-na-celowniku-tez-polska>
556. Polskie Radio 24. *Atak Rosji na Ukrainę. KPMG: co piąta firma odnotowała wzrost cyberataków od czasu wojny*. <https://polskieradio24.pl/42/259/artykul/3120078,atak-rosji-na-ukraine-kpmg-co-piata-firma-odnotowala-wzrost-cyberatakow-od-czasu-wojny>
557. Polskie Radio 24. *Cyberataki na Polskę. Departament Stanu USA: Rosja używa narzędzia do siania dezinformacji i podziałów*. <https://polskieradio24.pl/5/1223/artykul/2761363,cyberataki-na-polske-departament-stanu-usa-rosja-uzywa-narzedzia-do-siania-dezinformacji-i-podzialow>
558. Radio Free Europe. *Russia's Diplomatic Missions In Central Europe*. <https://www.rferl.org/a/russias-diplomatic-missions-in-central-europe-/31215395.html>
559. Reuters. *Chinese military force to take lead on cyber, space defense*. <https://www.reuters.com/article/us-china-military-idUSKCN0V714B>

560. Reuters. *COVID-19 disinformation backfires as Russian deaths climb, EU says.* <https://www.reuters.com/world/europe/covid-19-disinformation-backfires-russian-deaths-climb-eu-says-2021-10-21/>
561. Reuters. *Germany freezes Nord Stream 2 gas project as Ukraine crisis deepens.* <https://www.reuters.com/business/energy/germanys-scholz-halts-nord-stream-2-certification-2022-02-22/>
562. Reuters. *Russia to spend \$600 billion on defence and security by 2025.* <https://www.reuters.com/business/aerospace-defense/russia-spend-600-bln-defence-security-by-2025-source-2022-09-23/>
563. Reuters. *Russia's Prigozhin admits interfering in U.S. elections.* <https://www.reuters.com/world/us/russias-prigozhin-admits-interfering-us-elections-2022-11-07/>
564. RIA. *Международное агентство "Россия сегодня" создается на базе РИА Новости.* <https://ria.ru/20131209/982905485.html>
565. RMF24. *"Dzień wstydu". Hakerzy z grupy Anonymous atakują Rosję.* https://www.rmfm24.pl/raporty/raport-wojna-z-rosja/news-dzien-wstydu-hakerzy-z-grupy-anonymous-atakuja-rosje,nId,6012474#crp_state=1
566. RMF24. *Putin opłacał ekologów? Przełął fortunę, by blokować Zachód przed wydobywaniem gazu.* <https://www.rmfm24.pl/fakty/swiat/news-putin-oplaczal-ekologow-przeal-fortune-by-blokowac-zachod-pr,nId,5925452>
567. Russia Today. *West lying about WWII – Russia.* <https://www.rt.com/russia/547663-ussr-falsly-compated-nazi-germany/>
568. Rzeczpospolita. *Afera mailowa. Tajne informacje w wiadomościach ze skrzynki Dworczyka? Jest śledztwo.* <https://www.rp.pl/polityka/art38044011-afere-mailowa-tajne-informacje-w-wiadomosciach-ze-skrzynki-dworczyka-jest-sledztwo>
569. Rzeczpospolita. *Afera mailowa: Odebranie Ziobrze kontroli nad prokuraturą i sprawdzenie finansów Solidarnej Polski.* <https://www.rp.pl/polityka/art37341181-afere-mailowa-odebranie-ziobrze-kontroli-nad-prokuratura-i-sprawdzenie-finansow-solidarnej-polski>
570. Rzeczpospolita. *Apel Strasburga do Rosji: Oddajcie Polsce wrak Tu-154M.* <https://www.rp.pl/wydarzenia/art9600151-apel-strasburga-do-rosji-oddajcie-polsce-wrak-tu-154m>
571. Rzeczpospolita. *Atak za ACTA: Rządowe strony zablokowane.* <https://www.rp.pl/kraj/art6300061-atak-za-acta-rzadowe-strony-zablokowane>

572. Rzeczpospolita. *Cyberatak na polskie firmy energetyczne.* <https://energia.rp.pl/energetyka/art4985261-cyberatak-na-polskie-firmy-energetyczne>
573. Rzeczpospolita. *Gowin: Wśród maili ze skrzynki Dworczyka znalazł się mój. Był prawdziwy.* <https://www.rp.pl/polityka/art36905441-gowin-wsrod-maili-ze-skrzynki-dworczyka-znalazl-sie-moj-byl-prawdziwy>
574. Rzeczpospolita. *Hakerzy Putina atakują rząd.* <https://www.rp.pl/polityka/art4814691-hakerzy-putina-atakuja-rzad>
575. Rzeczpospolita. *Hakerzy Putina z GRU bez sukcesów w Polsce.* <https://www.rp.pl/polityka/art1570411-hakerzy-putina-z-gru-bez-sukcesow-w-polsce>
576. Rzeczpospolita. *Historyczna chwila: Unia Europejska przestała kupować gaz ziemny z Rosji.* <https://energia.rp.pl/gaz/art37474281-historyczna-chwila-unia-europejska-przestala-kupowac-gaz-ziemny-z-rosji>
577. Rzeczpospolita. *Ilu żołnierzy NATO przebywa obecnie w Polsce?* <https://www.rp.pl/wojsko/art35749601-ilu-zolnierzy-nato-przebywa-obecnie-w-polsce>
578. Rzeczpospolita. *Kontrowersyjny wpis o wycieku z Nord Stream zniknął z konta Sikorskiego.* <https://www.rp.pl/polityka/art37145071-kontrowersyjny-wpis-o-wycieku-z-nord-stream-zniknal-z-konta-sikorskiego>
579. Rzeczpospolita. *Kto płaci najtaniej za rosyjski gaz? Niespodzianka.* <https://energia.rp.pl/gaz/art19020691-kto-placi-najtaniej-za-rosyjski-gaz-niespodzianka>
580. Rzeczpospolita. *Nasilają się ataki hakerskie na Polskę.* <https://www.rp.pl/biznes/art18454601-nasilaja-sie-ataki-hakerskie-na-polske>
581. Rzeczpospolita. *Norton Cybercrime Report 2012: Polacy na celowniku hakerów.* <https://www.rp.pl/media/art5923571-norton-cybercrime-report-2012-polacy-na-celowniku-hakerow>
582. Rzeczpospolita. *Polska otworzyła hub energetycznej pomocy dla Ukrainy.* <https://energia.rp.pl/elektroenergetyka/art37853981-polska-otworzyla-hub-energetycznej-pomocy-dla-ukrainy>
583. Rzeczpospolita. *Polska remontowym hubem dla ukraińskiego uzbrojenia. Firmy pracują dyskretnie.* <https://www.rp.pl/biznes/art37872631-polska-remontowym-hubem-dla-ukraińskiego-uzbrojenia-firmy-pracuja-dyskretnie>
584. Rzeczpospolita. *Prigożyn przyznaje: Rosja ingerowała w wybory w USA. I będzie ingerować.* <https://www.rp.pl/konflikty-zbrojne/art37367861-prigozyn-przyznaje-rosja-ingerowala-w-wybory-w-usa-i-bedzie-ingerowac>

585. Rzeczpospolita. *Telewizja Rossija 1, Polsko-rosyjski rozbiór Ukrainy*. <https://www.rp.pl/Konflikt-na-Ukrainie/181009974-Telewizja-Rossija-1-Polsko-rosyjski-rozbior-Ukrainy.html>
586. Rzeczpospolita. *Zmasowane cyberataki Rosji, Białorusi i Chin na polską armię*. <https://www.rp.pl/gospodarka/art36801221-zmasowane-cyberataki-rosji-bialorusi-i-chin-na-polska-armie>
587. Security Week. *Russian APT Gamaredon Changes Tactics in Attacks Targeting Ukraine*. <https://www.securityweek.com/russian-apt-gamaredon-changes-tactics-attacks-targeting-ukraine/>
588. Sputnik News International. *A new page in Russian-Polish relations after a dark epilogue*. <https://sputnikglobe.com/20100412/158544992.html>
589. Sputnik News International. *Defense or Delusion? The Hidden Motives Behind NATO's East European Buildup*. <https://sputnikglobe.com/20160517/nato-eastern-europe-buildup-political-show-1039748414.html>
590. Sputnik News International. *EU Cuts Military Aid to Ukraine as Arms Dry Up, Kiev on Verge of Losing Conflict, Expert Says*. <https://sputnikglobe.com/20220818/eu-cuts-military-aid-to-ukraine-as-arms-dry-up-kiev-on-verge-of-losing-conflict-expert-says-1099739940.html>
591. Sputnik News International. *EU Policy in Ukraine Could Result in Mass Exodus to Europe*. <https://sputnikglobe.com/20150128/1017467778.html>
592. Sputnik News International. *EU Polish Presidential Advisor Calls US 'Simpletons', Blasts Gov't for Spending Billions on Old US Arms*. <https://sputnikglobe.com/20191221/polish-presidential-advisor-calls-us-simpletons-blasts-govt-for-spending-billions-on-old-us-arms-1077706457.html>
593. Sputnik News International. *Experts reject criticism of Russian probe into Kaczynski crash*. <https://sputnikglobe.com/20110121/162240457.html>
594. Sputnik News International. *LIVE UPDATES: Kiev Ready to Blow Up Krivorozhskaya Thermal Power Plant to Blame Russian Forces – MoD*. <https://sputnikglobe.com/20220627/live-updates-ukrainian-forces-fire-20-shells-overnight-at-village-in-dpr-donetsk-says-1096686158.html>
595. Sputnik News International. *LIVE UPDATES: Ukrainian Nationalists Blow Up Bridge to Town of Schastye Near Lugansk*. <https://sputnikglobe.com/20220531/live-updates-two-people-killed-and-24-wounded-in-lpr-by-ukraines-shelling-over-past-day-1095888448.html>

596. Sputnik News International. *NATO Forces in Eastern Europe May Lead to Endless War, Hostilities – Expert*. <https://sputnikglobe.com/20140828/NATO-Forces-in-Eastern-Europe-May-Lead-to-Endless-War-192413930.html>
597. Sputnik News International. *NATO Suspends All Practical Cooperation with Russia – Statement*. <https://sputnikglobe.com/20140402/NATO-Suspends-All-Practical-Coooperation-with-Russia---Statement-188973288.html>
598. Sputnik News International. *NATO Unveils New Headquarters Inspired by the Nazi SS Lightning Bolts?* <https://sputnikglobe.com/20160627/nato-nazi-ss-brussels-hitler-1042050232.html>
599. Sputnik News International. *No Need for OSCE Monitoring of Entire Russian-Ukrainian Border: Moscow*. <https://sputnikglobe.com/20141202/1015394575.html>
600. Sputnik News International. *Poland Prepares for 'Hybrid War' Through Shady Diplomacy, Arms Buildup*. <https://sputnikglobe.com/20150311/1019352561.html>
601. Sputnik News International. *Polish Bikers Resolve to Ensure Safe Passage for Russia's Night Wolves*. <https://sputnikglobe.com/20150420/1021125256.html>
602. Sputnik News International. *Preferential Treatment of Ukrainian Refugees in EU Stirs Anger Amid Claims of 'Institutional Racism'*. <https://sputnikglobe.com/20221104/preferential-treatment-of-ukrainian-refugees-in-eu-stirs-anger-amid-claims-of-institutional-racism-1103777096.html>
603. Sputnik News International. *Radoslaw Sikorski Is Testing the Limits of Lies*. <https://sputnikglobe.com/20141023/Radoslaw-Sikorski-Is-Testing-the-Limits-of-Lies-194478671.html>
604. Sputnik News International. *Russian Embassy in Berlin Brushes Off Polish Envoy's Claim Nord Stream 2 Will Fund Russian Army*. <https://sputnikglobe.com/20210327/russian-embassy-in-berlin-brushes-off-polish-envoys-claim-nord-stream-2-will-fund-russian-army-1082466992.html>
605. Sputnik News International. *Russian Gas More Profitable Than US LNG, Ex-Austrian Envoy Says as Denmark Hampers Nord Stream 2*. <https://sputnikglobe.com/20191026/russian-gas-nord-stream-2-project-1077157248.html>
606. Sputnik News International. *Shocking Facts of Poland's Kaczynski Plane Crash Revealed*. <https://sputnikglobe.com/20150407/1020580333.html>
607. Sputnik News International. *Three in Four Poles Know Soviet Troops Liberated Auschwitz, New Poll Shows*. <https://sputnikglobe.com/20200221/auschwitz-most-poles-know-well-soviet-army-liberated-nazis-biggest-death-camp-1078365690.html>

608. Sputnik News International. *Ukraine's Membership in NATO is Impossible – German Media*. <https://sputnikglobe.com/20150424/1021324562.html>
609. Sputnik News International. *US-EU 'Transatlantic Renaissance' Plan Falling Apart at Seams*. <https://sputnikglobe.com/20150402/1020387992.html>
610. Sputnik News International. *WWII History Falsification Among Europe's Most Pressing Political Issues - Russian Envoy*. <https://sputnikglobe.com/20200129/wwii-history-falsification-among-europes-most-pressing-political-issues---russian-envoy-1078175428.html>
611. Sputnik News Polska. *„Wagony cennych leków”: MO Rosji o pomocy wyzwolonej Polsce*. <https://pl.sputniknews.com/20210507/mo-rosji-o-pomocy-wyzwolonej-polsce-sputnik-14233563.html>
612. Sputnik News Polska. *17 września po białorusku*. <https://pl.sputniknews.com/20210916/17-wrzesnia-po-bialorusku-16100435.html>
613. Sputnik News Polska. *MO Rosji: Armia Czerwona oddawała Polsce swój chleb*. <https://pl.sputniknews.com/20210509/mo-rosji-armia-czerwona-zsrr-polska-zywnosc-sputnik-14237380.html>
614. Sputnik News Polska. *Operacja Barbarossa. Co piąty czołg podczas hitlerowskiego ataku na ZSRR był produkcji czeskiej*. <https://pl.sputniknews.com/20210622/operacja-barbarossa-niemcy-czolgi-przemysl-zbrojeniowy-czechoslowacja-sputnik-14395140.html>
615. Sputnik News Polska. *Putin podpisał ustawę o zakazie zrównywania roli ZSRR i Niemiec w II wojnie światowej*. <https://pl.sputniknews.com/20210701/putin-podpisal-ustawe-o-zakazie-zrownywania-roli-zsrr-i-niemiec-w-ii-wojnie-swiatowej-15352456.html>
616. Sputnik News Polska. *Rosja odtajniła dokumenty z wiosny 1945 roku. Nie wszystkim w Polsce to się podoba*. <https://pl.sputniknews.com/20210513/rosja-odtajnila-dokumenty-z-wiosny-1945-roku-nie-wszystkim-w-polsce-to-sie-podoba-Sputnik-14268911.html>
617. TASS. *EU ignoring Poland's, Lithuania's cruelty to migrants — Russian diplomat*. <https://tass.com/world/1365325>
618. TASS. *Former Polish Foreign Minister Sikorski thanks US for damaging Nord Stream*. <https://tass.com/world/1514367>
619. TASS. *Kremlin aide certain Poland will "snatch" Ukraine's western regions if given half a Chance*. <https://tass.com/world/1452849>
620. TASS. *Medvedev advises Warsaw to never forget multibillion-dollar Soviet aid*. <https://tass.com/politics/1529445>

621. TASS. *Medvedev blasts Poland's 'talentless politicians puppeteered by US' who fuel Russophobia*. <https://tass.com/politics/1425035>
622. TASS. *Orlen signs oil supply contract with Rosneft*. <https://tass.com/economy/1266603>
623. TASS. *Poland sends to Ukraine over 200 T-72 tanks, several dozen infantry carriers — radio*. <https://tass.com/defense/1445261>
624. TASS. *Poland's lower house votes to brand Russia 'state sponsor of terrorism'*. <https://tass.com/world/1550711>
625. TASS. *Poland's president signs law on establishing Polish-Lithuanian-Ukrainian military brigade*. <https://tass.com/world/792931>
626. TASS. *Polish ex-president blames Kaczynski brothers for Tu-154M plane near Smolensk*. <https://tass.com/world/868868>
627. TASS. *Polish leadership begins work on scenarios of dismembering Ukraine — Russian intelligence*. <https://tass.com/world/1473919>
628. TASS. *Russia's 2021 Parliamentary Elections*. <https://tass.com/russias-2021-parliamentary-elections>
629. TASS. *Russia's national defense budget to total \$154 bln through 2022*. <https://tass.com/defense/1080646>
630. TASS. *Russian diplomat says Poland has undermined bilateral ties for years*. <https://tass.com/politics/1102165>
631. TASS. *Ukraine nationalism threat to peace in Europe — Polish veteran*. <https://tass.com/world/783246>
632. TASS. *Vandalism against memorials to Soviet warriors on the rise abroad, says diplomat*. <https://tass.com/world/1292073>
633. TASS. *Washington, Warsaw work jointly to gather info on blast in east Poland — White House*. <https://tass.com/world/1537277>
634. TASS. *West uses migrants against Belarus in case of Russia-Ukraine conflict — Lukashenko*. <https://tass.com/world/1367773>
635. The Guardian. *Anonymous: the hacker collective that has declared cyberwar on Russia*. <https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia>
636. The Guardian. *German government intranet under 'ongoing attack'*. <https://www.theguardian.com/world/2018/mar/01/german-government-intranet-under-ongoing-attack>

637. The Guardian. *Russia 'secretly working with environmentalists to oppose fracking'*.
<https://www.theguardian.com/environment/2014/jun/19/russia-secretly-working-with-environmentalists-to-oppose-fracking>
638. The Guardian. *'State sponsored' Russian hacker group linked to cyber attacks on neighbours*.
<https://www.theguardian.com/technology/2014/oct/29/russian-hacker-group-cyber-attacks-apt28>
639. The Guardian. *US joins UK in blaming Russia for NotPetya cyber-attack*.
<https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine>
640. The Kyiv Independent. *Leaked document reveals alleged Kremlin plan to take over Belarus by 2030*. <https://kyivindependent.com/investigations/leaked-document-reveals-alleged-kremlin-plan-to-take-over-belarus-by-2030>
641. The New York Times. *Churchill's definition of Russia still rings true*.
<https://www.nytimes.com/2008/08/01/world/europe/01iht-letter.1.14939466.html>
642. The Register. *Leaked IT contractor files detail Kremlin's stockpile of cyber-weapons*. https://www.theregister.com/2023/03/31/vulkan_files_russia/
643. TVN WARSZAWA. *Nie tylko Szpiegowo. "Rosyjskich wysp" jest w Warszawie więcej*.
<https://tvn24.pl/tvnwarszawa/najnowsze/warszawa-lista-nieruchomosci-zajmowanych-przez-rosje-zalegly-czynsz-wynosi-juz-ponad-24-miliony-zlotych-5675616>
644. TVN24. *Dworczyk: złożyłem rezygnację*. <https://tvn24.pl/polska/michal-dworczyk-podal-sie-dymisji-odchodzi-z-funkcji-szefa-kancelarii-prezesa-rady-ministrow-6140126>
645. TVN24. *Ilu żołnierzy NATO jest w Polsce i krajach sąsiednich*. <https://tvn24.pl/swiat/ilu-zolnierzy-nato-jest-w-polsce-i-na-wschodniej-flance-infografika-5639659>
646. TVN24. *Kto w Europie płaci najwięcej za rosyjski gaz? Polska w czołówce*.
<https://tvn24.pl/biznes/najnowsze/kto-w-europie-placi-najwiecej-za-rosyjski-gaz-polska-w-czolowce-ra380494-4437218>
647. TVN24. *Microsoft says discovers hacking targeting democratic institutions in Europe*.
<https://tvn24.pl/tvn24-news-in-english/democratic-institutions-in-europe-attacked-by-hackers-says-microsoft-ra911507-2297074>
648. TVN24. *Prezydencki minister: Wrak jest w Rosji i będzie w Rosji. Nikt z nas tego wraku nie odzyska*. <https://tvn24.pl/polska/katastrofa-smolenska-prezydencki-minister-andrzej-dera-wrak-jest-w-rosji-i-bedzie-w-rosji-nikt-z-nas-tego-wraku-nie-odzyska-6118183>

649. TVN24. *Rzecznik Kremla: wzmocnienie wojskowe NATO w Polsce zmusza nas do podjęcia niezbędnych środków*. <https://tvn24.pl/swiat/pieskow-wojska-nato-w-polsce-zagrozeniem-dla-rosji-4615591>
650. TVP INFO. *Rosyjski ośrodek nad Zegrzem przejęty. Są zdjęcia ze środka*. <https://www.tvp.info/64310764/osrodek-nad-zegrzem-w-skubiance-rosjanie-zostawili-go-w-oplakany-m-stanie-przejmuja-lasy-panstwowe>
651. Wirtualne Media. *Jacek Sasin potwierdza ujawnione maile ze skrzynki Dworczyka. Ambasador Niemiec wezwany z powodu tekstu w „Fakcie”*. <https://www.wirtualnemedial.pl/artykul/jacek-sasin-maile-dworczyka-mateusz-morawiecki>
652. Wprost. *Kaczyński wydał oświadczenie po cyberatakach. „Przeprowadzone z terenu Federacji Rosyjskiej”*. <https://www.wprost.pl/polityka/10458686/cyberataki-na-polskich-politykow-oswiadczenie-jaroslaw-kaczynskiego.html>
653. Wprost. *Rosjanie szpiegowali Sztab Generalny Wojska Polskiego*. <https://www.wprost.pl/496099/rosjanie-szpiegowali-sztab-generalny-wojska-polskiego.html>
654. Wyborcza.biz. *Ile zapłaciliśmy za gazowy monopol Gazpromu?* <https://wyborcza.biz/biznes/51,179190,14853545.html#S.galeria-K.C-B.1-L.1.duzy>
655. Zaufana Trzecia Strona. *Ataki rosyjskich cyberszpiegów na polskie instytucje rządowe*. <https://zaufanatrzeciastrona.pl/post/ataki-rosyjskich-cyberszpiegow-na-polskie-instytucje-rzadowe/>
656. Zaufana Trzecia Strona. *Podobno to Rosjanie stali za zeszłorocznym atakiem na Giełdę Papierów Wartościowych*. <https://zaufanatrzeciastrona.pl/post/podobno-to-rosjanie-stali-za-zeszlorocznym-atakiem-na-gielde-papierow-wartosciowych/>
657. Zaufana Trzecia Strona. *Wyrafinowany backdoor UEFI obecny także w polskich sieciach*. <https://zaufanatrzeciastrona.pl/post/wyrafinowany-backdoor-uefi-obecny-takze-w-polskich-sieciach/>

Źródła internetowe

658. Aleshka, A., *Sputnik Polska. Propaganda Narratives and Cases*. <https://east-center.org/wp-content/uploads/2020/09/Sputnik-Polska-Propaganda.pdf>
659. ARAKIS Enterprise NASK. *Arakis - Innowacyjny system wczesnego ostrzegania o cyberzagrożeniach IT i SCADA*. <https://www.arakis.pl/>
660. Baltic Pipe Project. O projekcie. <https://www.baltic-pipe.eu/pl/o-projekcie/>
661. Bańko, M., *Sowiecki czy radziecki? Słownik Języka Polskiego PWN*. <https://sjp.pwn.pl/poradnia/haslo/sowiecki-czy-radziecki;3265.html>
662. Benedyczak J. (2018). *Założenia i perspektywy polityki Rosji wobec Gruzji*. Biuletyn Polskiego Instytutu Spraw Międzynarodowych, 117(1690) <https://pism.pl/upload/images/artykuly/legacy/files/24742.pdf>
663. Biuletyn Informacji Publicznej. *Śłużba Kontrwywiadu Wojskowego. Certyfikacja wyrobów przeznaczonych do ochrony informacji niejawnych*. <https://bip.skw.gov.pl/skw/bezpieczenstwo-teleinfo/certyfikacja-wyrobow-pr/5110,Certyfikacja-wyrobow-przeznaczonych-do-ochrony-informacji-niejawnych.html>
664. Biuro Bezpieczeństwa Narodowego. *"Spodziewaliśmy się decyzji o przesunięciu programu w czasie, a nie całkowitej jego likwidacji."*. <https://www.bbn.gov.pl/pl/wydarzenia/1882,quotSpodziewalismy-sie-decyzji-o-przesunieciu-programu-w-czasie-a-nie-calkowitej.html>
665. Biuro Bezpieczeństwa Narodowego. (MINI)Słownik BBN. *Propozycje nowych terminów z dziedziny bezpieczeństwa: propaganda*. <https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html>
666. Borden, A., *What is Information Warfare?* <https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/borden.pdf>
667. Britannica Dictionary. *Information*. <https://www.britannica.com/dictionary/information>
668. Burska-Ratajczyk, B., *Postsowiecki i poradziecki. Uniwersytet Łódzki. Poradnia językowa*. <https://poradnia-jezykowa.uni.lodz.pl/faq/postsowiecki-i-poradziecki/>
669. Cambridge Dictionary. *Computerization*. <https://dictionary.cambridge.org/dictionary/english/computerization>
670. Cambridge Dictionary. *Cyberattack*. <https://dictionary.cambridge.org/dictionary/english/cyberattack>

671. Cambridge Dictionary. *Digitalize*. <https://dictionary.cambridge.org/dictionary/english/digitalize?q=digitalization>
672. Cambridge Dictionary. *Disinformation*. <https://dictionary.cambridge.org/dictionary/english/disinformation>
673. Cambridge Dictionary. *Information*. <https://dictionary.cambridge.org/dictionary/english/information>
674. Cambridge Dictionary. *Manipulation*. <https://dictionary.cambridge.org/us/dictionary/english/manipulation>
675. Central Intelligence Agency. *The World Factbook. Russia. Economy*. <https://www.cia.gov/the-world-factbook/countries/russia/#economy>
676. Central Intelligence Agency. *The World Factbook. Russia. Geography*. <https://www.cia.gov/the-world-factbook/countries/russia/#geography>
677. Central Intelligence Agency. *The World Factbook. Russia. Government*. <https://www.cia.gov/the-world-factbook/countries/russia/#government>
678. Central Intelligence Agency. *The World Factbook. Russia. Military and Security*. <https://www.cia.gov/the-world-factbook/countries/russia/#military-and-security>
679. Central Intelligence Agency. *The World Factbook. Russia. People and Society*. <https://www.cia.gov/the-world-factbook/countries/russia/#people-and-society>
680. Centralne Biuro Zwalczenia Cyberprzestępczości. *Zadania Centralnego Biura Zwalczenia Cyberprzestępczości*. <https://cbzc.policja.gov.pl/bzc/o-cbzc/podstawowe-zadania/5,Zadania-Centralnego-Biura-Zwalczenia-Cyberprzestepczosci.html>
681. Centrum Polsko-Rosyjskiego Dialogu i Porozumienia. *Projekty, badania opinii publicznej*. http://cprdip.pl/projekty,badania_opinii_publicznej.html
682. CERT Polska. *O nas*. <https://cert.pl/o-nas/>
683. CERT Polska. *Publikacje CERT Polska*. <https://cert.pl/publikacje/>
684. CERT Polska. *Rekomendacje w związku ze zwiększonym zagrożeniem w cyberprzestrzeni wywołanym sytuacją na Ukrainie*. <https://cert.pl/posts/2022/02/rekomendacje-cyberprzestrzen-ukraina/>
685. CERT.PL NASK. *O nas*. <https://cert.pl/o-nas/>
686. CIDOB Barcelona Centre for International Affairs. *CIDOB International Yearbook 2010. Country profile, Russian Federation*. <https://www.cidob.org/sites/default/files/2025-01/ANUARIO%202010%20ANGLES.pdf>
687. Council on Foreign Relations. *Polish Cyber Defenses and the Russia-Ukraine War*. <https://www.cfr.org/blog/polish-cyber-defenses-and-russia-ukraine-war>

688. CYBER.MIL.PL. *O nas*. <https://www.cyber.mil.pl/o-nas/>
689. CYBER.MIL.PL. *Służba Kontrwywiadu Wojskowego*. <https://www.cyber.mil.pl/articles/o-nas-f/2018-11-20m-suzba-kontrwywiadu-wojskowego/>
690. CYBER.MIL.PL. *Wojska Obrony Cyberprzestrzeni*. <https://www.cyber.mil.pl/wojska-obrony-cyberprzestrzeni/>
691. Czaputowicz, J. (2014). *Mapa współczesnego realizmu: realizm klasyczny, neorealizm, realizm neoklasyczny*. <https://ptsm.edu.pl/wp-content/uploads/publikacje/teoria-realizmu-w-nauce-o-stosunkach-miedzynarodowych/J.Czaputowicz.pdf>
692. Czerep, J., Legucka, A. (2019). *Wzrost zaangażowania Rosji w Afryce*. Biuletyn Polskiego Instytutu Spraw Międzynarodowych, 162(1910). https://www.pism.pl/publikacje/Wzrost_zaangazowania_Rosji_w_Afryce_
693. Darczewska, J. (2014). *Anatomia rosyjskiej wojny informacyjnej Operacja Krymska – studium przypadku*. Punkt widzenia, 42. https://www.osw.waw.pl/sites/default/files/anatomia_rosyjskiej_wojny_informacyjnej.pdf
694. Darczewska, J. (2015). *Diabeł tkwi w szczegółach. Wojna informacyjna w świetle doktryny wojennej Rosji*. Punkt widzenia, 50. https://www.osw.waw.pl/sites/default/files/pw_50_pl_diabel_tkwi_net.pdf
695. Darczewska, J. (2016). *Rosyjskie Siły zbrojne na froncie walki informacyjnej. Dokumenty strategiczne*. Prace OSW, 57. https://www.osw.waw.pl/sites/default/files/prace_57_pl_sily_zbrojne_net.pdf
696. Darczewska, J. (2019). *Między jawną dezinformacją a niejawną praktyką. Gry rosyjskich służb*. Punkt widzenia, 73. https://www.osw.waw.pl/sites/default/files/PW_73_PL_Miedzy-jawna-dezinformacja_net.pdf
697. Darczewska, J., Żochowski, P. (2017). *Środki aktywne. Rosyjski towar eksportowy*. Punkt Widzenia, 64.
698. Demagog. *Jaki jest udział sektora energetycznego w eksporcie i PKB Rosji?* <https://demagog.org.pl/wypowiedzi/jaki-jest-udzial-sektora-energetycznego-w-eksporcie-i-pkb-rosji/>
699. Domańska, M., Menkiszak, M., Rogoża, J., Wiśniewska, I. (2021). *Rosja u progu 2021 roku. Sytuacja polityczna, społeczna i gospodarcza*. Komentarze OSW, 371. https://www.osw.waw.pl/sites/default/files/komentarze_371_0.pdf
700. DQL. *2022 Digital Quality of Life Index*. <https://surfshark.com/dql2022?country=PL>
701. DQL. *2022 Digital Quality of Life Index*. <https://surfshark.com/dql2022>

702. Dyner A. M. (2017). *Nowa Koncepcja rosyjskiej polityki zagranicznej*. Biuletyn Polskiego Instytutu Spraw Międzynarodowych, 1(1443) <https://pism.pl/upload/images/artykuly/legacy/files/22686.pdf>
703. Dyner A. M. (2020). *II wojna światowa w polityce zagranicznej Rosji*. Biuletyn Polskiego Instytutu Spraw Międzynarodowych, 12(1942). <https://www.pism.pl/upload/images/artykuly/e5d8a54c-6ead-4f12-a875-3dc94c043bc7//1580203445419.pdf>
704. Dyner A. M. (2021). *Zaktualizowane kierunki polityki zagranicznej Rosji*. Komentarz PISM, 88/2021 <https://pism.pl/webroot/upload/files/Komentarz%20PISM%20nr%2088-2021.pdf>
705. Dyner A. M. (2022). *Działania hybrydowe Rosji przeciw państwom NATO i UE*. Biuletyn Polskiego Instytutu Spraw Międzynarodowych, 183(2602). [https://www.pism.pl/webroot/upload/files/Biuletyn/Biuletyn%20PISM%20nr%20183%20\(2602\)%2025%20listopada%202022%20r.pdf](https://www.pism.pl/webroot/upload/files/Biuletyn/Biuletyn%20PISM%20nr%20183%20(2602)%2025%20listopada%202022%20r.pdf)
706. Encyclopedia Britannica. *Cyberspace*. <https://www.britannica.com/topic/cyberspace>
707. Encyklopedia PWN. *Cyberprzestrzeń*. <https://sjp.pwn.pl/sjp/cyberprzestrzen;2553915>
708. Encyklopedia PWN. *Cyfryzacja*. <https://encyklopedia.pwn.pl/haslo/cyfryzacja;4007905.html>
709. Encyklopedia PWN. *Informacja*. <https://encyklopedia.pwn.pl/haslo/informacja;3914686.html>
710. Encyklopedia PWN. *Komputeryzacja*. <https://encyklopedia.pwn.pl/haslo/komputeryzacja;3924656.html>
711. Encyklopedia PWN. *Propaganda*. <https://encyklopedia.pwn.pl/haslo/propaganda;3962718.html>
712. Energy Information Administration. *What countries are the top producers and consumers of oil?* <https://www.eia.gov/tools/faqs/faq.php?id=709&t=6>
713. European Commission. Eurostat. *Population and population change statistics*. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Population_and_population_change_statistics
714. European Commission. *In focus: Reducing the EU's dependence on imported fossil fuels*. https://ec.europa.eu/info/news/focus-reducing-eus-dependence-imported-fossil-fuels-2022-apr-20_en
715. European Commission. *The Digital Economy and Society Index (DESI)*. <https://digital-strategy.ec.europa.eu/en/policies/desi>

716. European Council, Council of the European Union. *EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU*. <https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rt-russia-today-and-sputnik-s-broadcasting-in-the-eu/>
717. Gaz System. *Terminal LNG*. <https://www.gaz-system.pl/pl/terminal-lng/terminal-lng.html>
718. Global Firepower. *2023 Poland Military Strength*. https://www.globalfirepower.com/country-military-strength-detail.php?country_id=poland
719. GlobalSecurity.org. *Poland Army Equipment*. <https://www.globalsecurity.org/military/world/europe/pl-army-equipment.htm>
720. Główny Urząd Statystyczny. *Podstawowe dane*. <https://stat.gov.pl/podstawowe-dane/>
721. Główny Urząd Statystyczny. *Spółeczeństwo Informacyjne w Polsce w 2019 roku*. <https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2019-roku,2,9.html>
722. gov.pl. *Disinformation against Poland in 2020 – special services' view*. <https://www.gov.pl/web/sluzby-specjalne/disinformation-against-poland-in-2020--special-services-view>
723. gov.pl. *Kampania szpiegowska wiązana z rosyjskimi służbami specjalnymi*. <https://www.gov.pl/web/baza-wiedzy/kampania-szpiegowska-wiazana-z-rosyjskimi-sluzbami>
724. gov.pl. *Komisja ds. badania wpływów rosyjskich i białoruskich powołana*. <https://www.gov.pl/web/premier/komisja-ds-badania-wplywow-rosyjskich-i-bialoruskich-powolana>
725. gov.pl. *Komisja ds. badania wpływów rosyjskich i białoruskich powołana*. <https://www.gov.pl/web/premier/komisja-ds-badania-wplywow-rosyjskich-i-bialoruskich-powolana>
726. gov.pl. *Krajobraz (cyber)zagrożeń 2021. Raport Europejskiej Agencji ds. Cyberbezpieczeństwa*. <https://www.gov.pl/web/baza-wiedzy/krajobraz-cyberzagrozen-2021---raport-europejskiej-agencji-ds-cyberbezpieczenstwa-enisa>
727. gov.pl. *Krajowy system cyberbezpieczeństwa*. <https://www.gov.pl/web/cyfrizacja/krajowy-system-cyberbezpieczenstwa>
728. gov.pl. *O służbach specjalnych*. <https://www.gov.pl/web/sluzby-specjalne/o-sluzbach-specjalnych3>

729. gov.pl. *Polska na celowniku dezinformacji*. <https://www.gov.pl/web/sluzby-specjalne/polska-na-celowniku-dezinformacji>
730. gov.pl. *Program Zintegrowanej Informatyzacji Państwa*. <https://www.gov.pl/web/cyfryzacja/program-zintegrowanej-informatyzacji-panstwa>
731. gov.pl. *Przedłużenie obowiązywania stopni alarmowych BRAVO oraz CHARLIE-CRP – do 30 listopada 2022r*. <https://www.gov.pl/web/rcb/przedluzenie-obowiazywania-stopni-alarmowych-bravo-oraz-charlie-crp--do-30-listopada-2022r>
732. gov.pl. *Przedłużenie obowiązywania stopni alarmowych do 28 lutego 2023r*. <https://www.gov.pl/web/rcb/przedluzenie-obowiazywania-stopni-alarmowych-do-28-lutego-2023r>
733. gov.pl. *Przedłużenie stopni alarmowych BRAVO oraz CHARLIE-CRP - do 28 lutego 2023*. <https://www.gov.pl/web/cea/przedluzenie-stopni-alarmowych-bravo-oraz-charlie-crp3>
734. gov.pl. *Raport Zespołu ds. Dezinformacji Komisji ds. badania wpływów rosyjskich i białoruskich*. <https://www.gov.pl/web/sprawiedliwosc/raport-zespołu-ds-dezinformacji-komisji-ds-badania-wplywow-rosyjskich-i-bialoruskich>
735. gov.pl. *Russian cyberattacks*. <https://www.gov.pl/web/special-services/russian-cyberattacks>
736. gov.pl. *Stopień alarmowy ALFA-CRP na terenie całego kraju*. <https://www.gov.pl/web/rcb/stopien-alarmowy-alfa-crp-na-terenie-calego-kraju>
737. gov.pl. *Stopień alarmowy ALFA-CRP na terenie całej Polski*. <https://www.gov.pl/web/cyfryzacja/stopien-alarmowy-alfa-crp-na-terenie-calej-polski>
738. gov.pl. *Stopień alarmowy BRAVO-CRP*. <https://www.gov.pl/web/mswia/stopien-alarmowy-bravo-crp>
739. gov.pl. *Trzeci stopień alarmowy CRP na terenie całego kraju*. <https://www.gov.pl/web/rcb/trzeci-stopien-alarmowy-crp-na-terenie-calego-kraju>
740. gov.pl. *Uderzenie dezinformacyjne*. <https://www.gov.pl/web/sluzby-specjalne/uderzenie-dezinformacyjne>
741. gov.pl. *UWAGA – wprowadzono 3 stopień alarmowy CHARLIE-CRP*. <https://www.gov.pl/web/baza-wiedzy/uwaga--wprowadzono-3-stopien-alarmowy-charlie-crp>
742. gov.pl. *W trosce o cyfrowe bezpieczeństwo Polski*. <https://www.gov.pl/web/cppc/w-trosce-o-cyfrowe-bezpieczenstwo-polski>
743. gov.pl. *Wojska Obrony Cyberprzestrzeni*. <https://www.gov.pl/web/obrona-narodowa/wojska-obrony-cyberprzestrzeni>

744. gov.pl. *Współpraca międzynarodowa*. <https://www.gov.pl/web/cyfryzacja/wspolpraca-miedzynarodowa1>
745. gov.pl. *Сайт для громадян України*. <https://www.gov.pl/web/ua>
746. GOV.UK. *Armed Forces announce launch of Cyber Regiment in major modernisation*. <https://www.gov.uk/government/news/armed-forces-announce-launch-of-first-cyber-regiment-in-major-modernisation>
747. Gu, Q., Liu, P., *Denial of Service Attacks*. <https://s2.ist.psu.edu/paper/ddos-chap-gu-june-07.pdf>
748. INFOSEC. *APT28: Cybercrime or State-sponsored Hacking?* <https://resources.infosecinstitute.com/topic/apt28-cybercrime-or-state-sponsored-hacking/>
749. Instytut Pamięci Narodowej. *Katyń 1940. Przyznanie się Rosji*. <https://katyn.ipn.gov.pl/kat/histori/walka-o-prawde/pryznanie-sie-rosji>
750. International Energy Agency. *Russia*. <https://www.iea.org/countries/russia>
751. International Monetary Fund. *World Economic Outlook Database. 2010-2022*. <https://www.imf.org/en/Publications/WEO>
752. International Monetary Fund. *World Economic Outlook Database. April 2022 Edition*. <https://www.imf.org/en/Publications/WEO/weo-database/2022/April>
753. Jakóbowski, J. (2022). *Chiński dylemat. Rosyjska inwazja na Ukrainę a sytuacja strategiczna Chin*. Komentarze Ośrodka Studiów Wschodnich, 435. https://www.osw.waw.pl/sites/default/files/Komentarz_OSW_435.pdf
754. Kaca, E. (2022). *Debata o Partnerstwie Wschodnim w kontekście inwazji Rosji na Ukrainę*. Biuletyn Polskiego Instytutu Spraw Międzynarodowych”, 181(2600). [https://www.pism.pl/webroot/upload/files/Biuletyn/Biuletyn%20PISM%20nr%20181%20\(2600\)%2024%20listopada%202022%20r.pdf](https://www.pism.pl/webroot/upload/files/Biuletyn/Biuletyn%20PISM%20nr%20181%20(2600)%2024%20listopada%202022%20r.pdf)
755. Kancelaria Prezesa Rady Ministrów. *#PomagamUkrainie Szukasz ratunku przed wojną? Chcesz wesprzeć uchodźców? Tu znajdziesz pomoc lub jej udzieliś*. <https://pomagamukrainie.gov.pl/>
756. Kancelaria Prezesa Rady Ministrów. *Polska hubem humanitarnym dla Ukrainy*. <https://www.gov.pl/web/premier/polska-hubem-humanitarnym-dla-ukrainy>
757. Kłosińska, K., *Sowiecki a radziecki*. <https://sjp.pwn.pl/poradnia/haslo/Sowiecki-a-radziecki;18706.html>
758. Kostecki, W. (2014). *Poziomy analizy polityki zagranicznej*. <https://ptsm.edu.pl/wp-content/uploads/publikacje/poziomy-analizy-stosunkow-miedzynarodowych/Kostecki.pdf>

759. KPMG. *Barometr cyberbezpieczeństwa*. <https://kpmg.com/pl/pl/home/insights/2022/05/barometr-cyberbezpieczenstwa-ochrona-cyfrowej-tozsamosci.html>
760. Kugiel P. (2022). *Słabnące partnerstwo Indii i Rosji - niespodziewany efekt wojny na Ukrainie*. Biuletyn Polskiego Instytutu Spraw Międzynarodowych, 174(2593). [https://www.pism.pl/webroot/upload/files/Biuletyn/Biuletyn%20PISM%20nr%20174%20\(2593\)%208%20listopada%202022%20r.pdf](https://www.pism.pl/webroot/upload/files/Biuletyn/Biuletyn%20PISM%20nr%20174%20(2593)%208%20listopada%202022%20r.pdf)
761. Kvachkov, V., *Спецназ России*. http://militera.lib.ru/science/kvachkov_vv/index.html
762. Legucka A., Przychodniak M. (2020). *Dezinformacja Chin i Rosji w trakcie pandemii COVID-19*. Biuletyn Polskiego Instytutu Spraw Międzynarodowych, nr 86(2018) <https://pism.pl/upload/images/artykuly/acecc09f-a097-43cf-b933-9a0e562345a3//1587464655532.pdf>
763. Legucka, A. (2019). *Walka z rosyjską dezinformacją w Unii Europejskiej*. Biuletyn Polskiego Instytutu Spraw Międzynarodowych, 111(1859). <https://pism.pl/upload/images/artykuly/0414d618-2799-421d-8510-b1130a66303e/1570904090174.pdf>
764. Legucka, A. (2022). *Bilans i perspektywy polityki Rosji wobec USA po roku prezydentury Joe Bidena*. Biuletyn Polskiego Instytutu Spraw Międzynarodowych, 23(2442). [https://www.pism.pl/webroot/upload/files/Biuletyn/Biuletyn%20PISM%20nr%2023%20\(2442\)%208%20lutego%202022%20r.pdf](https://www.pism.pl/webroot/upload/files/Biuletyn/Biuletyn%20PISM%20nr%2023%20(2442)%208%20lutego%202022%20r.pdf)
765. Microsoft. *Microsoft Digital Defense Report 2022. Illuminating the threat landscape and empowering a digital defense*. <https://go.microsoft.com/fwlink/?linkid=2213817&clid=0x409&culture=en-us&country=us>
766. Microsoft. *Microsoft Digital Defense Report OCTOBER 2021*. <https://info.microsoft.com/ww-landing-Microsoft-Digital-Defense-Report-Gate.html>
767. Microsoft. *New steps to protect Europe from continued cyber threats*. <https://blogs.microsoft.com/eupolicy/2019/02/20/accountguard-expands-to-europe/>
768. Ministerstwo Cyfryzacji, Instytut Łączności, Collegium Medicum UJ. *Przewodnik po 5G 2019*. <https://www.gov.pl/web/5g/przewodnik-po-5g>
769. Ministerstwo Cyfryzacji. Biuletyn Informacji Publicznej. *Program Zintegrowanej Informatyzacji Państwa - wrzesień 2016 r.* <https://mc.bip.gov.pl/programy-realizowane-w-mc/program-zintegrowanej-informatyzacji-panstwa-wrzesien-2016-r.html>
770. Ministerstwo Obrony Narodowej. *Siły sojusznicze w Polsce*. <https://www.gov.pl/web/obrona-narodowa/sily-sojusznicze-w-polsce>

771. Ministerstwo Obrony Narodowej. *W Polsce będą serwisowane czołgi Leopard z Ukrainy*. <https://www.gov.pl/web/obrona-narodowa/w-polsce-beda-serwisowane-czolgi-leopard-z-ukrainy>
772. Ministerstwo Obrony Narodowej. *Wojska Obrony Cyberprzestrzeni rozpoczynają działalność*. <https://www.gov.pl/web/obrona-narodowa/wojska-obrony-cyberprzestrzeni-rozpoczynaja-dzialalnosc>
773. Ministerstwo Obrony Narodowej. *Wojsko Polskie silne jak nigdy*. <https://www.gov.pl/web/obrona-narodowa/wojsko-polskie-silne-jak-nigdy>
774. Ministerstwo Spraw Wewnętrznych i Administracji. *Biuletyn Informacji Publicznej. Projekt rozporządzenia Rady Ministrów z dnia .. 2011 r. w sprawie Planu Informatyzacji Państwa na lata 2011-2015 (skierowany do uzgodnień międzyresortowych, z 21-dniowym terminem na zgłaszanie uwag)*. <https://archiwumbip.mswia.gov.pl/bip/projekty-aktow-prawnyc/2011/19948,Projekt-rozporzadzenia-Rady-Ministrow-z-dnia-2011-r-w-sprawie-Planu-Informatyzac.html>
775. Ministerstwo Spraw Wewnętrznych i Administracji. *Informacja dla uchodźców z Ukrainy*. <https://www.gov.pl/web/mswia/informacja-dla-uchodzcow-z-ukrainy>
776. Ministerstwo Spraw Zagranicznych. *Informator Ekonomiczny. Gospodarka*. <https://www.gov.pl/web/rosja/informator-ekonomiczny>
777. Ministerstwo Spraw Zagranicznych. *Informator Ekonomiczny. Informacje ogólne*. <https://www.gov.pl/web/rosja/informator-ekonomiczny>
778. Ministerstwo Spraw Zagranicznych. *Internetowa Baza Traktatowa*. <https://traktaty.msz.gov.pl/umowa-4>
779. Ministerstwo Spraw Zagranicznych. *Internetowa Baza Traktatowa*. <https://traktaty.msz.gov.pl/umowa-1>
780. Ministerstwo Spraw Zagranicznych. *Partnerstwo Wschodnie*. <https://www.gov.pl/web/dyplomacja/partnerstwo-wschodnie>
781. Ministerstwo Spraw Zagranicznych. *Polityka wschodnia*. <https://www.gov.pl/web/dyplomacja/polityka-wschodnia>
782. Ministerstwo Spraw Zagranicznych. *Polska w Rosji. Placówki*. <https://www.gov.pl/web/rosja/placowki>
783. *Ministre des Armées. Le commandement de la cyberdéfense (COMCYBER)*. <https://www.defense.gouv.fr/ema/commandement-cyberdefense-comcyber>

784. Nakayama, B. (2020). *American Influence on Russian Information Warfare*. E-International Relations. <https://www.e-ir.info/2020/09/24/american-influence-on-russian-information-warfare/>
785. NASK Cyber POLICY. *Dyrektywa NIS, czyli pierwsze europejskie prawo w zakresie cyberbezpieczeństwa*. <https://cyberpolicy.nask.pl/dyrektywa-nis-czyli-pierwsze-europejskie-prawo-w-zakresie-cyberbezpieczenstwa/>
786. NASK Cyber POLICY. *Sojusz Północnoatlantycki – ewolucja w podejściu do cyberobrony*. <https://cyberpolicy.nask.pl/nato-cyberobrona-zagrozenia-hybrydowe/>
787. NASK. *System wczesnego ostrzegania o cyberzagrożeniach (ARAKIS)*. <https://www.nask.pl/pl/dzialalnosc/nauka-i-biznes/projekty-badawcze/2075,System-wczesnego-ostrzegania-o-cyberzagrozeniach-ARAKIS.html>
788. NATO Review. *Rozszerzenie NATO i Rosja: mity i rzeczywistość*. <https://www.nato.int/docu/review/pl/articles/2014/07/01/rozszerzenie-nato-i-rosja-mity-i-rzeczywistosc/index.html>
789. NATO. *History*. <https://mncne.nato.int/about-us/history>
790. NewsGuard. *Russia-Ukraine Disinformation Tracking Center: 273 Websites Spreading War Disinformation And The Top Myths They Publish*. <https://www.newsguardtech.com/special-reports/russian-disinformation-tracking-center/>
791. Oficjalna strona internetowa Ambasady Federacji Rosyjskiej w Polsce. https://poland.mid.ru/web/polska_pl/
792. Oficjalna strona internetowa Ambasady Federacji Rosyjskiej w Polsce: *Rosja-Polska. Współpraca handlowo-gospodarcza*. https://poland.mid.ru/pl/rossiya_polsha/rossijsko_polskie_otnosheniya_i_voprosy_mezhdunarodnoj_bezopasnosti/torgovo_ekonomicheskoe_sotrudnichestvo/
793. Oficjalna strona internetowa Ambasady Federacji Rosyjskiej w Polsce: *Rosja-Polska. Dialog polityczny*. https://poland.mid.ru/pl/rossiya_polsha/rossijsko_polskie_otnosheniya_i_voprosy_mezhdunarodnoj_bezopasnosti/politicheskij_dialog/
794. Oficjalna strona internetowa Rosyjskiego Ośrodka Nauki i Kultury - Rosyjski Dom w Warszawie. <https://www.ronik.org.pl/>
795. Ośrodek Studiów Wschodnich. *Dywersja na gazociągach Nord Stream 1 i Nord Stream 2*. <https://www.osw.waw.pl/pl/publikacje/analizy/2022-09-29/dywersona-na-gazociagach-nord-stream-1-i-nord-stream-2>

796. Ośrodek Studiów Wschodnich. *Gruzja: napięcia wewnętrzne i nowy kryzys w stosunkach z Rosją*. <https://www.osw.waw.pl/pl/publikacje/analizy/2019-06-26/gruzja-napiecia-wewnetrzne-i-nowy-kryzys-w-stosunkach-z-rosja>
797. Ośrodek Studiów Wschodnich. *Koncepcja polityki zagranicznej Federacji Rosyjskiej*. <https://www.osw.waw.pl/pl/publikacje/analizy/2013-02-20/koncepcja-polityki-zagranicznej-federacji-rosyjskiej>
798. Ośrodek Studiów Wschodnich. *Konsekwencje aneksji Krymu*. <https://www.osw.waw.pl/pl/publikacje/analizy/2014-03-19/konsekwencje-aneksji-krymu>
799. Ośrodek Studiów Wschodnich. *Propaganda masowego rażenia. Rosyjska telewizja w obliczu wojny*. <https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2022-05-06/propaganda-masowego-razenia-rosyjska-telewizja-w-obliczu-wojny>
800. Ośrodek Studiów Wschodnich. *Putin: Ukraińcy to Rosjanie, Ukraina to „anty-Rosja”*. <https://www.osw.waw.pl/pl/publikacje/analizy/2021-07-13/putin-ukraincy-to-rosjanie-ukraina-to-anty-rosja>
801. Ośrodek Studiów Wschodnich. *Rosja wobec szczytu NATO w Warszawie*. <https://www.osw.waw.pl/pl/publikacje/analizy/2016-07-13/rosja-wobec-szczytu-nato-w-warszawie>
802. Ośrodek Studiów Wschodnich. *Rosja: wybory bez wyboru*. <https://www.osw.waw.pl/pl/publikacje/analizy/2021-09-20/rosja-wybory-bez-wyboru>
803. Ośrodek Studiów Wschodnich. *Rosyjski szantaż wobec Zachodu*. <https://www.osw.waw.pl/pl/publikacje/analizy/2021-12-20/rosyjski-szantaż-wobec-zachodu>
804. Ośrodek Studiów Wschodnich. *Wróg z Zachodu. Nowa rosyjska strategia bezpieczeństwa*. <https://www.osw.waw.pl/pl/publikacje/analizy/2021-07-08/wrog-z-zachodu-nowa-rosyjska-strategia-bezpieczenstwa>
805. Piotrowski M. A. (2017). *Amerykańskie oceny dotyczące ingerencji Rosji w przebieg wyborów prezydenckich w USA*. Biuletyn Polskiego Instytutu Spraw Międzynarodowych, nr 8(1450) <https://pism.pl/upload/images/artykuly/legacy/files/22768.pdf>
806. Platforma Przemysłu Przyszłości. *Pierwszy operator uruchomił w Polsce 100 komercyjnych nadajników 5G*. <https://przemyslprzyszlosci.gov.pl/pierwszy-operator-uruchomil-w-polsce-100-komercyjnych-nadajnikow-5g/>
807. Pogorzelski, P. (2021). *Zagrożenia rosyjską dezinformacją w Polsce i formy przeciwdziałania*. <https://www.kew.org.pl/wp-content/uploads/2021/05/Piotr-Pogorzelski-Zagrozenie-rosyjska-dezinformacja-w-Polsce-i-formy-przeciwdzialania-1.pdf>

808. POLITIFACT. *Fact-checking fake news reveals how hard it is to kill pervasive 'nasty weed' online*. <https://www.politifact.com/article/2017/jan/27/fact-checking-fake-news-reveals-how-hard-it-kill-p/>
809. Polski Instytut Spraw Międzynarodowych. *Konflikt na Ukrainie ma kluczowy wpływ na relacje polsko-rosyjskie*. https://pism.pl/konferencje/Konflikt_na_Ukrainie_ma_kluczowy_wp_yw_na_relacje_polsko_rosyjskie
810. Przedstawicielstwo Komisji Europejskiej w Polsce. *Russia Today i Sputnik wyłączone w UE*. https://poland.representation.ec.europa.eu/news/russia-today-i-sputnik-wylaczone-w-ue-2022-03-02_pl
811. Rada Europejska, Rada Unii Europejskiej. *Cyberataki: UE nakłada pierwsze w historii sankcje*. <https://www.consilium.europa.eu/pl/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/>
812. Rada Europejska, Rada Unii Europejskiej. *Partnerstwo Wschodnie*. <https://www.consilium.europa.eu/pl/policies/eastern-partnership/>
813. Rada Europejska, Rada Unii Europejskiej. *Rada Europejska, 23–24 czerwca 2022*. <https://www.consilium.europa.eu/pl/meetings/european-council/2022/06/23-24/>
814. Rada Europejska, Rada Unii Europejskiej. *Reakcja UE wobec rosyjskiej inwazji na Ukrainę*. <https://www.consilium.europa.eu/pl/policies/eu-response-ukraine-invasion/>
815. Radio Sputnik. <https://radiosputnik.ria.ru/>
816. Rand. *Reining in COVID-19 Disinformation from China, Russia, and Elsewhere*. <https://www.rand.org/blog/2021/11/reining-in-covid-19-disinformation-from-china-russia.html>
817. RIA Nowosti. <https://ria.ru/>
818. Rodkiewicz, W. (2017). *Bliskowschodnia polityka Rosji regionalne ambicje, globalne cele*. Prace Ośrodka Studiów Wschodnich, 71. https://www.osw.waw.pl/sites/default/files/prace_71_bliskowschodnia_polityka_rosji_net_0.pdf
819. Rodkiewicz, W. (2020). *Wbrew Ameryce. Polityka Rosji wobec Iranu*. Komentarze OSW, 319. https://www.osw.waw.pl/sites/default/files/komentarze_319_0.pdf
820. Russia.Post. *Russia's changing ethnic landscape: Three takeaways from the 2021 census*. https://russiapost.info/society/ethnic_landscape
821. Rządowe Centrum Bezpieczeństwa. *Systemy infrastruktury krytycznej*. <https://www.gov.pl/web/rcb/systemy-infrastruktury-krytycznej>
822. Serwis Programu Polska Cyfrowa. *Dowiedz się więcej o programie*. <https://www.polskacyfrowa.gov.pl/strony/o-programie/>

823. Sharp, R. (2017). *An Introduction to Malware*. <https://backend.orbit.dtu.dk/ws/portalfiles/portal/139067614/malware.pdf>
824. Sienkiewicz, P., *Część III – Techniczne uwarunkowania rozwoju społeczeństwa informacyjnego. Wizje i modele wojny informacyjnej*. <https://winntbg.bg.agh.edu.pl/skrypty2/0095/373-378.pdf>
825. SimilarWeb. *tass.com*. <https://www.similarweb.com/website/tass.com/#overview>
826. SJP.pl. *Manipulacja*. <https://sjp.pl/manipulacja>
827. Słownik Języka Polskiego PWN. *Informatyzacja*. <https://sjp.pwn.pl/szukaj/informatyzacja.html>
828. Słownik Języka Polskiego PWN. *Komputeryzacja*. <https://encyklopedia.pwn.pl/haslo/komputeryzacja;3924656.html>
829. Służba Kontrwywiadu Wojskowego. *Zadania*. <https://www.skw.gov.pl/zadania.html>
830. Sputnik Images. <https://sputnikmediabank.com/>
831. Sputnik News International. *About Us*. <https://sputniknews.com/docs/index.html>
832. Sputnik News International. <https://sputnikglobe.com/>
833. Sputnik News International. <https://sputniknews.com/>
834. Sputnik News International. *Search*. <https://sputniknews.com/search/?query=Poland>
835. Sputnik News International. *Search*. <https://sputniknews.com/search/?query=>
836. Sputnik News International. *Tag Poland*. https://sputnikglobe.com/geo_Poland/
837. Sputnik News Polska. <https://pl.sputniknews.com/>
838. Sputnik.Polls. https://sputniknews.com/sputnik_polls_2016/
839. Statista. *Military spending in Russia from 1993 to 2021*. <https://www.statista.com/statistics/1203160/military-expenditure-russia/>
840. Straż Graniczna. *Granice RP*. <https://www.strazgraniczna.pl/pl/granica/granice-rp/1910,Granice-RP.html>
841. TASS. *About TASS*. <https://tass.com/today>
842. TASS. *Poland*. <https://tass.com/tag/poland>
843. TASS. *Search*. <https://tass.com/search?searchStr=Poland&sort=date>
844. TASS. *TASS history*. <https://tass.com/history>
845. TASS. <https://tass.com>
846. The Kiel Institute for the World Economy. *Ukraine Support Tracker*. <https://www.ifw-kiel.de/topics/war-against-ukraine/ukraine-support-tracker/?cookieLevel=not-set>
847. The United States Department of Justice. *Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election*. <https://>

- www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election
848. Trading Economics. *Crude oil*. <https://tradingeconomics.com/commodity/crude-oil>
 849. Trading Economics. *Natural gas*. <https://tradingeconomics.com/commodity/natural-gas>
 850. TREND. *Operation Pawn Storm: The Red in SEDNIT*. https://www.trendmicro.com/en_us/research/14/j/operation-pawn-storm-the-red-in-sednit.html
 851. Twitter, Użytkownik Nathaniel Gleicher, Data opublikowania: 28.02.2022 7:17 AM. <https://twitter.com/ngleicher/status/1498180571809280001?s=20&t=PEa6XUCoS C7L6WlyAtwomQ>
 852. U.S. Cyber Command. *Our history*. <https://www.cybercom.mil/About/History/>
 853. U.S. Department of State. *On Russia's Acquisition of UAVs from Iran*. <https://www.state.gov/on-russias-acquisition-of-uavs-from-iran/>
 854. U.S. Department of State. *U.S. Security Cooperation with Ukraine*. <https://www.state.gov/u-s-security-cooperation-with-ukraine/>
 855. U.S. Department of the Treasury. *Ukraine-/Russia-related Sanctions*. <https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/ukraine-russia-related-sanctions>
 856. UN E-Government Knowledgebase. (2003). *Poland*. <https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/135-Poland/dataYear/2003>
 857. UN E-Government Knowledgebase. (2010). *Poland*. <https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/135-Poland/dataYear/2010>,
 858. UN E-Government Knowledgebase. (2012). *Poland*. <https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/135-Poland/dataYear/2012>
 859. United States Census Bureau. *U.S. and World Population Clock*. <https://www.census.gov/popclock/>
 860. van de Velde, J. (2017). *The Dangers of Forceful Countermeasures as a Response to Cyber Election Interference*. https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3719850_code2431285.pdf?abstractid=3043828&mirid=1
 861. Warsaw Institute. *How Long Russian Oil and Gas Reserves Are Enough to Last?* <https://warsawinstitute.org/long-russian-oil-gas-reserves-enough-last/>
 862. Warsaw Institute. *Rosyjska dezinformacja i jej wpływ na sektor energetyczny w krajach V4*. <https://warsawinstitute.org/pl/rosyjska-dezinformacja-i-jej-wplyw-na-sektor-energetyczny-w-krajach-v4/>
 863. Wojsko Polskie. *Zadania – DKWOC*. <https://www.wojsko-polskie.pl/woc/zadania/>

864. World Atlas. *Maps of Russia*. <https://www.worldatlas.com/maps/russia>
865. World Bank. *Open Data. Poland*. <https://data.worldbank.org/country/poland>
866. World Bank. *Open Data. Russian Federation*. <https://data.worldbank.org/country/russian-federation>
867. World Population Review. *Natural Gas by Country 2022*. <https://worldpopulationreview.com/country-rankings/natural-gas-by-country>
868. YouTube. *Jak napaść na państwo (całość) Jurij Bezmienow*. <https://www.youtube.com/watch?v=lWIpfvGrNak>
869. ZDNET. *Microsoft reveals new APT28 cyber-attacks against European political entities*. <https://www.zdnet.com/article/microsoft-reveals-new-apt28-cyber-attacks-against-european-political-entities/>
870. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. *FAQ*. <https://csirt.gov.pl/cer/faq/22,FAQ-NAJCZESCIEJ-ZADAWANE-PYTANIA.html>
871. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. *O nas*. <https://csirt.gov.pl/>
872. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV. *System ARAKIS-GOV*. <https://csirt.gov.pl/cer/system-arakis-gov/310,System-ARAKIS-GOV.html>
873. Znojek, B. (2022). *Kierunki współpracy Rosji z partnerami w Ameryce Łacińskiej*. Biuletyn Polskiego Instytutu Spraw Międzynarodowych, 83(2502). <https://pism.pl/publikacje/kierunki-wspolpracy-rosji-z-partnerami-w-ameryce-lacinskiej>

Tytuły artykułów poddanych badaniom na portalu Sputnik News International

1. *'Not a Sensible Solution': Bundestag Head Warns Against Sabotaging Nord Stream 2*
2. *'Russian Threat' May Cause US to Deploy Patriot Missiles To Lithuania*
3. *15 fatalities as floods swamp Poland and Germany*
4. *2018 Review: Europe Yearns for a Sense of Direction*
5. *A new page in Russian-Polish relations after a dark epilogue*
6. *African Swine Fever Confirmed in Poland*
7. *All Eurozone Candidates Fail to Fulfill Entry Criteria - EU Commission*
8. *Analyst: German Prediction of EU Disintegration Not So Far-Fetched*
9. *Ankara Calls on NATO to Set Unified Approach to Protection of Member States*
10. *Austrian Chancellor Says EU's Policy of Migrant Distribution Among Member States Failed*
11. *Bad Morale: Europeans Grow Weary of Brussels' Policies*
12. *Belarusian Opposition Figure Awarded Freedom Prize by the EU Will 'Sell Belarus Out', Analyst Says*
13. *Belarusian Opposition Figure Tikhanovskaya to Visit Warsaw on 9 September, NGO Says*
14. *Belarus's Lukashenko sends letter to Russia's Medvedev on oil deal*
15. *Berlin Should Pay \$900 Bln in WWII Reparations to Warsaw – Polish MP*
16. *Better a Good Quarrel? 'Peaceful' Norway Seeks NATO Buildup in the North*
17. *Big EU Division to Blame for France-Italy Migrant Boat Row – Analyst*
18. *Brexit Diaries: London Cabbie Holds Backseat Ballot*
19. *Bulgarian Gov't Approves EU-Gazprom Antitrust Dispute Settlement Deal*
20. *Canadian Frigate Joins NATO Anti-Submarine Warfare Drills in North Sea*
21. *Canadians Advised to Avoid Travel to Belarus Amid 'Risk of Armed Conflict With Ukraine'*
22. *Celluloid Magic: Honoring the Academy Awards Ceremony*
23. *Defense Minister Says Slovakia May Soon Host NATO Command Center*
24. *Defense or Delusion? The Hidden Motives Behind NATO's East European Buildup*
25. *Estonia to Propose EU-Wide Ban on Schengen Visas for Russians*
26. *Estonia, US Sign Agreement on Defense Cooperation - Estonian Defense Ministry*
27. *EU Commission Threatens Poland With Lawsuit Over Warsaw's Legal Reforms*
28. *EU Cuts Military Aid to Ukraine as Arms Dry Up, Kiev on Verge of Losing Conflict, Expert Says*

29. *EU Envoys Can Return to Minsk – Belarus*
30. *EU Imposes Border Check Crackdown in the Face of Increased Terror Threat*
31. *EU Lawmaker From Poland Deletes Tweet Thanking US for Damaging Nord Stream Pipeline*
32. *EU Leaders Supported Brexit to Remove Obstacle to Creating EU Army*
33. *EU Over 50% Dependent on Energy Imports in 2015 - Eurostat*
34. *EU Parliament Head Accuses Poland of 'Putinization', What Does He Mean?*
35. *EU Policy in Ukraine Could Result in Mass Exodus to Europe*
36. *EU Steps Up Legal Action Against Poland Over Supreme Court Reform*
37. *EU to give Poland billion euros for strong GDP growth — report*
38. *EU, Russia, Ukraine Brace for Big Changes in Poland Following Elections*
39. *Euro 2012 Will Be Short for Russia - Soldado*
40. *Europe Tearing Itself Apart Over Migrant Crisis*
41. *Europe Will Face 'Catastrophe' if Russia Cuts Off Gas Supplies*
42. *European Parliament Finally Wakes Up to Toxic TTIP Stitch-Up*
43. *European Trade Unions Demand End to Social Dumping of Millions of Workers*
44. *European Union Leaders Agree 'Brexit' Deal*
45. *EU's Ties With Russia Have Hit Rock Bottom, Dialogue Needed, German Foreign Minister Maas Says*
46. *Ex-CIA Agent Calls on Washington to 'Honestly Assess' How US Has Contributed to Russia Tensions*
47. *EXCLUSIVE: 'My Only Purpose Is to Save Europe' – Salvini to Sputnik*
48. *Ex-EU Council Chief Tusk Decries Nord Stream 2 Completion As 'Unforgivable Mistake' of German Egoism*
49. *Experts reject criticism of Russian probe into Kaczynski crash*
50. *Expulsion of Russian Diplomats Shows Lack of 'Western States' Sovereignty'*
51. *Ex-UK Leader Blair Went 'Beyond Facts' Advocating for Iraq War - Chilcot*
52. *Ex-UK Military Chief: Boost Defense Budget to Protect 'Homeland' From Russia*
53. *Facing Discrimination, Polish Minority in Lithuania Boycotts Schools*
54. *Far-Right Activists Hold Torch-Lit March in Memory of Nationalist Leader in Kiev*
55. *Fed Governor Pushes Political-Left Agenda as Excuse for Failed Monetary Course*
56. *Fifty-three hours to Côte d'Azur in first Moscow-Nice train*
57. *Finland Not Ready for Serious Talk With Russia on Europe Security – Minister*

58. *Foreign Singers to Perform Soviet WW2 Songs at Final of 'Road to Yalta' Festival on 1 May*
59. *Former US General Predicts War With China Likely Within 15 Years*
60. *French Medical Volunteer in Ukraine Opens Up About Azov Regiment's 'War Crimes'*
61. *Fur Industry Shrugs Off Gucci Going Animal-Free as Sales Are 'Strong and Robust'*
62. *Further Russian report on Kaczynski plane crash remains to be revealed*
63. *Gazprom Neft considers buying Poland's Lotos*
64. *Gazprom Signs Corrective Gas Price Contract with PGNiG*
65. *Gazprom, EU Energy Chief Agree to Continue Dialogue in Antitrust Probe*
66. *George Soros Named Charity News Outlet's 'Philanthropist of the Year'*
67. *German Officer to Sputnik: Drone Strikes Out of Ramstein Airbase Violate Int Law*
68. *Germany, Poland Need EU Assistance to Overcome Migrant Border Crisis, Seehofer Says*
69. *Germany's Spy Program Revealed as Much Bigger Than Anyone Thought*
70. *Goliath Entering Octagon: 'Iranian Hulk' Announces Debut MMA Fight (PHOTOS)*
71. *Gov't Shutdown Continues; US Only Removes Equipment Not Troops From Syria*
72. *Gradual Lifting of Anti-Russia Sanctions Unrealistic - Polish Ambassador*
73. *GT: Unwise, Irresponsible for Biden to Take Personal Grievances Toward Putin to National Level*
74. *'Have No Illusions': US Missile Defense System is 'Directed Against Russia'*
75. *Helping Hand: Poland Creates Vodka-Pouring Robot*
76. *Hiddink caught out Russian Football Union with exit news*
77. *'History & Geopolitics' Suggest Russia May Reclaim Its Role as EU's Key Gas Supplier*
78. *Hollande: Discussion of NATO Summit Decisions With Russia 'Important'*
79. *Hungary to Host Conference on History of Computer Science*
80. *Indian Air Force Says Shalom To Israel's Largest Air Exercise*
81. *Indians & Africans Fleeing Ukraine Accuse Ukrainian Border Security of Violence, Racism – Videos*
82. *INF Treaty US Abrogation: Chance of New Arms Race is Very Likely - Scholar*
83. *Inquiry Into Iraq Invasion Designed to Avoid Legal Claims Against UK*
84. *Is Polish Teacher in 'Dead Refugees' Scandal Just the Tip of the Iceberg?*
85. *Isinbayeva Puts Victory Over Height in France*
86. *Italy: Rich Regions Want to Secede?*
87. *Just Defense, Right? NATO Chief Wants More Troops in Eastern Europe*

88. *Katyn claims new victims as Polish president's plane crashes*
89. *Kiev and Minsk: the other side of diversification*
90. *Kiev Expects Moscow to Offer Market Gas Price*
91. *Kiev's Hopes for Western Help in E Ukraine Conflict 'a Road to Nowhere'*
92. *Kiev's Move to Label Journalists as a Threat is 'Absurd, Counterproductive'*
93. *Kurdish Groups Engaged in Transporting Migrants to Europe, Russian Security Council Says*
94. *Lavrov: NATO's Incessant Expansion Undermines Stability in Europe*
95. *Lavrov: NATO's Activity Near Russian Borders Remains Major Destabilizing Factor*
96. *Lavrov: Policy of NATO-Centrism Doesn't Help Build Trust Between Russia, Bloc*
97. *Light at the End of the Pipeline: Why Brexit is Good for Nord Stream 2*
98. *LIVE UPDATES: Biden Says Doesn't Agree With Zelensky That Russians Committed 'Genocide'*
99. *LIVE UPDATES: Kiev Ready to Blow Up Krivorozhskaya Thermal Power Plant to Blame Russian Forces - MoD*
100. *LIVE UPDATES: Most of Mercenaries Surrounded on 'Azovstal' Are From European Countries - MoD*
101. *LIVE UPDATES: Ukrainian Nationalists Blow Up Bridge to Town of Schastye Near Lugansk*
102. *LIVE UPDATES: US Won't Provide Ukraine With Weapons That Can Attack Russia - Envoy to UN*
103. *LIVE UPDATES: Zelensky Ready for Dialogue With Putin – Deputy Head of Ukrainian Presidential Office*
104. *Lockheed Martin Wins \$76Mln to Streamline Aegis Missile System Production*
105. *Macron Threatens Sanctions Against EU States That Turn Migrants Away*
106. *Macron's Dream of European Army Unviable Without Single State - French Officers*
107. *Main news of August 6*
108. *Main news of February 2*
109. *Majority Around the World Say US Torture Methods 'Not Justified' - Poll*
110. *Meet Canada's Parliament Candidate Who Had No Idea About Auschwitz*
111. *Member States Slam EU Asylum Proposals Amid Ongoing Migration Chaos*
112. *Merkel Calls for NATO-Russia Council Meeting to Ease Tensions*
113. *'Migrating Here Is No Human Right' - Swedish MEP Slams UN Pact*
114. *Minsk Platform for Peace Talks Important, More Efficient Than Geneva*

115. *Missile Defense Systems Worldwide*
116. *Moscow to Discuss Changes in US Missile Defense Plans*
117. *Moscow Warns Russia-NATO Ties Will Become More Complicated if US Moves Troops From Germany to Poland*
118. *Moscow-Washington Tensions to Further Escalate If US Quits Open Skies Treaty*
119. *Most Powerful Nuclear Research Reactor to Be Built in Russia by 2022 – Rosatom*
120. *Municipal Officials Rally in Poland Against Soaring Energy Costs - Photos, Video*
121. *Mystery About Polish Nazi Gold Train Intensifies After Recent Test*
122. *Nationalists Call to 'Free Poland from Jews' at Auschwitz March - Reports*
123. *NATO Baltic Air Policing Mission Prepares for Handover*
124. *NATO Chief Jens Stoltenberg Unveils Biggest Build-Up Since Cold War*
125. *NATO Devises Ways to Tackle "Increasing Threat" From Russian Submarines*
126. *NATO Expands Along Russia's Borders, Has Gall to Call Moscow the Aggressor*
127. *NATO Forces in Eastern Europe May Lead to Endless War, Hostilities - Expert*
128. *NATO Has No Plans to Increase Baltics, Poland Troop Numbers - NATO Chief*
129. *NATO Head Expected to Meet Ukraine's President on Sidelines of Munich Conference*
130. *NATO Military Activity Near Russia Is Response to Moscow's Actions*
131. *NATO Ministers to Review Cyber Defense in Brussels*
132. *NATO optimistic over European missile shield*
133. *NATO Presence Beside Russia's Borders Contributes to Rising Tensions*
134. *NATO Secretary General Says Alliance Seeks Constructive Relationship With Russia*
135. *NATO Slams Putin Visit to Abkhazia While Goading Russia in Eastern Europe*
136. *NATO States Should Focus on Troops' Combat Readiness, Not GDP-Linked Costs – AfD*
137. *NATO Suspends All Practical Cooperation with Russia - Statement*
138. *NATO to Deploy Battalions in Poland and Baltic States in 2017 - Stoltenberg*
139. *NATO Unleashed Reckless Militarism at Warsaw Alliance Summit*
140. *NATO Unveils New Headquarters Inspired by the Nazi SS Lightning Bolts?*
141. *Netherlands, Poland to Create News Agency to Counter 'Russian Propaganda'*
142. *New Coach Must Keep Liberal Discipline - Izmailov*
143. *New Mysterious Monolith Made of Unusual Material Discovered in San Francisco - Photos*
144. *New Polish President: Putin Can Walk All Over Me, but He Won't Wake Me Up*
145. *Next NATO Summit Due July 8-9, 2016 in Poland – Secretary General*

146. *No changes in Russian-Polish relations after Kaczynski plane crash reports - Polish speaker*
147. *'No Constructive Dialogue': Two Issues NATO Refused to Discuss With Russia*
148. *No Easy Ride for Britain as EU States Want Brussels to Offer a Tough Brexit Deal*
149. *No Need for OSCE Monitoring of Entire Russian-Ukrainian Border: Moscow*
150. *No Pants Subway Ride: People Strip Down to Participate in Pantless Flash Mob*
151. *No violations at Russia's parliamentary elections - observers*
152. *Nord Stream 2 Cannot Be Halted Without Berlin's Consent, EU Commission Says*
153. *Normal Diplomatic Discussions With NATO Impossible in Light of Bloc's Moves, Russia Says*
154. *Norwegian Fishing Industry Hardest-Hit by Anti-Russia Sanctions*
155. *Number of NATO Troops Near Russian Borders Tripled Since 2012 - Defense Minister*
156. *Obama Calls Protection of Eastern Europe 'Sacrosanct' Obligation of US*
157. *Obama Provides US Intelligence With Greater Access to Intercepted Communications*
158. *OPINION: Poland Uses Russia as Bogeyman Before European Parliament Election*
159. *OSCE to Monitor Nagorno-Karabakh Ceasefire*
160. *Over 11,200 Migrants Tried to Cross Into Germany From Belarus Via Poland in 2021*
161. *'Patron Saint of the Balkans': Viktor Orban Sends Barbed Wire to Macedonia*
162. *Paying For Gas Via Russia-Proposed Mechanism is Violation of Sanctions, EU Official Says*
163. *Pentagon Awards Contract to Accelerate Missile Defense Deployment in Poland*
164. *Poland Abortion Protest: 'We Come for Common Goal, to Fight for Our Choice'*
165. *Poland and Israel: Hot Debate Over the Holocaust*
166. *Poland celebrates 600 years since the Battle of Grunwald*
167. *Poland Could Send Four F-16 Jets to Patrol Syrian Airspace*
168. *Poland Expects Contract to Buy Eight Patriot Missile Systems by Year-End - MoD*
169. *Poland Increases Its Long-Range Striking Capabilities With New US Missiles*
170. *Poland Looking Forward to Ukraine's EU Membership*
171. *Poland May Join UK in Expelling Russian Diplomats Over Skripal Case - Reports*
172. *Poland Missile Strike Highlights High Stakes in Ukraine*
173. *Poland Prepares for 'Hybrid War' Through Shady Diplomacy, Arms Buildup*
174. *Poland Puts No Pressure on London Over Brexit Process Pace*
175. *Poland Requests European Commission Investigate Possible Gas Price Manipulation*
176. *Poland says no warrant for Chechen separatist Zakayev, but will detain him (Update 2)*

177. *Poland Seized \$6 Million Worth of Smuggled Goods on Russia's Border in 2016*
178. *Poland to Create Missile Defense System Based on US Patriot System in 10 Years*
179. *Poland to Demand \$1.3 Trillion From Germany in Reparations for WWII Damage: Ruling Party*
180. *Poland to honor Russian gas deal only on condition of 10 pct discount*
181. *Poland to Lose \$700 Million Due to Decrease in Exports to Russia Until Year End - Agency*
182. *Poland votes in close presidential runoff*
183. *Poland Weighs Up Contesting Tusk's EU Council Presidency Due to Vote Procedure*
184. *Poland Willing to Have Best Possible Relations With US – Polish President Duda*
185. *Poland, Hungary Expect EU Budget Proposals From Germany, Polish Government Says*
186. *Poland, Hungary Warned of EU Sanctions Over Migrant Transfers*
187. *Poland's S&P Lowered Credit Rating Shows Propaganda Effects – Tusk*
188. *Poland's Interior Minister Opposes UN Migration Deal*
189. *Poland's Supreme Court Upholds Refusal to Extradite Film Director Polanski to US*
190. *Polarized European Election Shows National Politics 'Different in Each Country'*
191. *Poles Stuck in Russia After Warsaw's Introduction of Border Restrictions*
192. *Poles to vote at presidential polls in Russian consulate general (Update 2)*
193. *Policy Differences Threaten 'Split Between Europe and Washington' - Prof*
194. *Polish Air Force chief was in cockpit of crashed presidential plane*
195. *Polish Bikers Resolve to Ensure Safe Passage for Russia's Night Wolves*
196. *Polish Defense Minister Discusses 'Fort Trump' at Pentagon*
197. *Polish envoy to intl. aviation body says defense minister pressured him*
198. *Polish EP Member Plans Crimea Visit, Calls for More Trade With Russia*
199. *Polish Foreign Ministry Summons Israeli Ambassador Over Criticism of Students' Safety*
200. *Polish Journalist's Work Permit Withdrawal 'Symmetrical Measure' - Ministry*
201. *Polish Officer Accused of Spying for Russia Sentenced to Six Years in Jail*
202. *Polish Parliament's Group Demands Explanation on Deletion of Tu-154 Crash Report*
203. *Polish PM to Call for Confidence Vote in Gov't Ahead of EU Leaders' Summit*
204. *Polish Politician Says NATO Should Arm Kiev With Advanced Lethal Weaponry*
205. *Polish Politician: Refugees 'Should Be Sent to Fight for Their Countries'*
206. *Polish Premier 'Frustrated' by French, EU Support for Nord Stream 2*
207. *Polish premier vows support for Belarusian opposition*
208. *Polish President Duda Says Parliament Scraps Plan to Limit Media Access*

209. *Polish President Says He Would Never Allow Poles to be 'Vilified' Over Holocaust*
210. *Polish President Says Trump May Come for State Visit in July*
211. *Polish President Slams Hooliganism at Euro 2012*
212. *Polish Presidential Advisor Calls US 'Simpletons', Blasts Gov't for Spending Billions on Old US Arms*
213. *Polish Senator Leaves Party Over Remarks About Putin in Interview With Sputnik*
214. *Polish Special Forces Claimed to Be Secretly Deployed to Donbass*
215. *Polish Special Services to Be Blamed for Concealing 2010 Plane Crash Data*
216. *Political Academy Awards, Fake News and 'Election Meddling': Highlights From Putin-Trump G20 Meet*
217. *'Political Gesture': Slovakia to Replace Russia's MiGs with US F-16s*
218. *Political Past, Muslim Migration – Roots of European Antisemitism EXPLAINED*
219. *Pompeo Accuses Russia of Having 'Grand Designs of Dominating Europe'*
220. *Poroshenko to Present Strategic Defense Bulletin at NATO Warsaw Summit*
221. *Possible Boycott of 2018 World Cup Over Skripal Case Nonsensical - Belgian FM*
222. *Powering The New Europe: Coventry Becomes Latest Location For Battery Gigafactory*
223. *Preferential Treatment of Ukrainian Refugees in EU Stirs Anger Amid Claims of 'Institutional Racism'*
224. *President Komorowski Believes in Victory in 2nd Round of Poland's Elections*
225. *Putin 'Only Real Statesman Left in Anti-ISIL War – Rest are Chamberlains'*
226. *Putin Recalls How Ukraine Cut Off Gas Supplies to EU in 2008 Over Price Row*
227. *Radoslaw Sikorski Is Testing the Limits of Lies*
228. *Redeployment of US Nukes to Poland Would Be Direct Violation of Russia-NATO Agreement, Lavrov Warns*
229. *Reforms Hotly Debated in French Election Amid Massive Economic Challenges*
230. *Report From Calais Where I'm Attacked by Migrants, Police Stand by*
231. *Revolt Against Centrists, Leftists in EU Will Lead to Right-Wing Rise – Scholar*
232. *Robot Teams Compete to Handle Future Disasters*
233. *Romania plans to replace obsolete Soviet fighters with U.S. F-16s*
234. *Russia Beats Egypt in FIVB Men's Volleyball Championship*
235. *Russia Has Eradicated Euro 2012 Touts – Official*
236. *Russia has nothing to hide about Katyn tragedy - Putin*
237. *Russia is Perceived as the Country Stopping the West From Achieving Hegemony Across the World*

238. *Russia to be Ukraine's Sole Gas Provider – Minister*
239. *Russia to Carry Out Observation Flight Over Poland Under Open Skies Treaty*
240. *Russia to Play Italy, France in Summer Warm-up Games*
241. *Russia Vows to Ensure Security if NATO Reinforcement in E Europe Continues*
242. *Russia Will Not Be Dragged Into a 'New Arms Race Imposed by US, NATO'*
243. *Russia Will Respond to NATO's Missile Defense Buildup in Europe – General*
244. *Russia, US to Continue Talks on INF Treaty: Pentagon*
245. *Russia's Global Image More Negative than Positive – Poll*
246. *Russia-Bashing Swedish Ex-Premier Becomes Aide to Russian Tycoon*
247. *Russia-Belarus Zapad-2017 Drills Purely Defensive - Deputy Defense Minister*
248. *Russian Cold Snap Kills 215*
249. *Russian Detained in Poland Over Launching Drone Over Gov't Buildings*
250. *Russian Embassy in Berlin Brushes Off Polish Envoy's Claim Nord Stream 2 Will Fund Russian Army*
251. *Russian Foreign Ministry Spokeswoman Zakharova Holds Weekly Press Briefing*
252. *Russian Gas More Profitable Than US LNG, Ex-Austrian Envoy Says as Denmark Hampers Nord Stream 2*
253. *Russian Gas Supplies to Austria Down by 15 Percent: Reports*
254. *Russian General Staff Chief, NATO Head Talk Via Phone for 1st Time Since Freeze*
255. *Russian Journalist Files Lawsuit Over Revoked Polish Residence Permit*
256. *Russian Press - Behind the Headlines, September 5*
257. *Russian Press at a Glance, Wednesday, June 15, 2011*
258. *Russian Rossotrudnichestvo Rejects EU Parliament Accusations of Propaganda*
259. *Russian State Duma to Respond to Polish Soviet Monuments' Demolition Bill*
260. *Russian, EU diplomats to discuss European security in Veliky Novgorod*
261. *Russian, Polish presidents to assess Smolensk air disaster probe*
262. *Russia's Izmailov: I Expected More From the Poles*
263. *Saakashvili Deprived of Ukrainian Citizenship Arrives in Poland*
264. *Saakashvili Says Ukraine in a Shambles, Faces Becoming 'Failed State'*
265. *Scoot Over, NATO! EU Army Plan to Press Ahead*
266. *Scott Ritter Gives Updates on Gonzalo Lira, War in Ukraine, and More*
267. *Shirokov Supports Spalletti for Russia Coach*
268. *Shocking Facts of Poland's Kaczynski Plane Crash Revealed*
269. *Shortsighted Choice: European MP Slams Brussels Over Anti-Russian Sanctions*

270. *Show Me the Money! Why US 2% NATO Spending Requirement Makes No Sense for Europe*
271. *Situation at Belarusian-Polish Border After Migrants Made Attempts to Storm It*
272. *Six Months of Fratricide War in Donbas*
273. *Slovak Authorities Level Cemetery Containing Graves of Russian WWI Soldiers With Bulldozer*
274. *Slovakia Promises Brussels Shakedown as It Heads EU Presidency*
275. *Smoke From the 'Burning' Eurozone Scares Away Poland's Central Bank*
276. *Spain Draws 0-0 Against Sweden at Euro 2020*
277. *Spain Uninterested in Building More LNG Terminals - Enagas*
278. *Speculation Over Roger Federer's Tennis Future Escalates After Swiss Star Drops Retirement Hint*
279. *Stop 'Bailing Out Rest of Europe': German MEP Slams Berlin Reportedly Pumping €19 Bln Into EU Budget*
280. *Stop Soros Act: Hungarian Gov't Submits Stricter Bill on NGOs to Parliament*
281. *Stratfor: Ukraine Coup Plotted by US Over Russian Stance on Syria*
282. *Suicide Rate Rises Among Young US Veterans - Study*
283. *Sweden Resisting EU's Attempts to Put All Eggs Into 'Euro Basket'*
284. *Teachers From 30 Countries Complete Online Course on Digital Learning, Russian Culture*
285. *Ten German Refugees, Asylum Seekers Test Positive for Coronavirus – UNHCR*
286. *Tens of Thousands of Nationalists March in Polish Capital on Independence Day*
287. *'The Blood of Polish Jews Cries From the Ground' - Israeli Minister*
288. *'The Fish Rots From the Head?' Not Only Brussels Responsible for EU Crisis*
289. *The War on Fossil Fuels, FTX, and Virtue Signaling at the World Cup*
290. *Think Brexit Was Bad? Wait Till Europe Gets a Load of Poland*
291. *This Week in Pictures (November 11-17)*
292. *Thousands Gather in Kiev to Mark 70 Years of Controversial Insurgent Army*
293. *Three in Four Poles Know Soviet Troops Liberated Auschwitz, New Poll Shows*
294. *Top Polish politician heads to Moscow parade to cement ties*
295. *Trump Retweets Germany-Bashing Posts as US Envoy Threatens Troop Pullout*
296. *Trump Won't Commemorate 80th WWII Anniversary in Poland*
297. *Trump: US to Put Tariffs on \$325bln of Chinese Goods if Washington Doesn't Agree a Deal With Beijing*

298. *Turkey Signs First Agreement on Delivery of Drones to NATO Country, Poland*
299. *U.S. Invites Russian Cooperation on Missile Defense*
300. *U.S. missile defense in Europe 'real threat' to Russia - General Staff*
301. *U.S. Wants Poland to Extradite Fugitive Filmmaker Roman Polanski*
302. *UEFA bans smoking at Euro 2012*
303. *UK Court Hears Case of Stolen Nuclear Submarine Documents – Reports*
304. *UK to Deploy Tanks, Drones to Eastern Europe to 'Boost NATO Presence'*
305. *UKIP MEP Welcomes Bannon's Right-Wing Initiative 'to Stand Up to Soros'*
306. *Ukraine and Poland Talk Teamwork on Military Helicopter Production*
307. *Ukraine wants to restore gas exports to Poland - paper*
308. *Ukraine, Poland to Develop New Generation Patrol Plane*
309. *Ukraine's Membership in NATO is Impossible – German Media*
310. *Uncertain World: Russia and the United States: A Precarious Balance*
311. *United States of Europe' Would Become a 'German Dictate' – Czech Politician*
312. *URGENT: Volcanic eruption in Iceland might delay Kaczynski's funeral*
313. *US Analyst Explains How NATO Countries Can 'Neutralise' Russian Exclave of Kaliningrad*
314. *US Army Testing of Soviet T-55 Tank Ended in Horrific Accident, Declassified Report Reveals*
315. *US Embassy to Suspend Issuing Non-Immigrant Visas in Russia Starting From Aug 23*
316. *US Flexes Muscles, Plans to Quadruple Military Budget in Europe in 2017*
317. *US Instructs Polish Forces on Patriot Anti-Missile Operation - Pentagon*
318. *US LNG Imports 'Not a Game Changer' for Poland – Specialist*
319. *US Military Coup for Euro Meltdown?*
320. *US Missiles' Deployment to Romania, Poland Banned Under INF Treaty - Moscow*
321. *US Mission to NATO Releases Cartoon About 'Deadly Russian INF-Violating Missile' ... Gets Missile Wrong*
322. *US Paratroopers Arrive in Ukraine as Fighting Intensifies in Donbass*
323. *US' Patriot Missile Systems to Be Obsolete by the Time They Arrive in Poland*
324. *US Reaction to Donald Cook Fiasco Should Be: 'What Were We Doing There?'*
325. *US Reopens Restocks With Tanks Cold War-Era Storage in Netherlands*
326. *US Reportedly Mulling Sending Bradley Fighting Vehicles to Ukraine in Future Aid Package*
327. *US Senate Bill Aims to Freeze Russian Gold Reserves*

328. *US to Announce Evacuation of Its Embassy in Kiev on Saturday, Report Claims*
329. *US to Start Training 780 Ukrainian National Guard Soldiers Shortly – Biden*
330. *US Torture Tactics Go Global: Is Gitmo Just The Tip Of The Iceberg?*
331. *US Upgrades Patriot Air Defense System Radar*
332. *US-EU 'Transatlantic Renaissance' Plan Falling Apart at Seams*
333. *Van Rijsselberge Surfs to Olympic Sailing Gold*
334. *Volgograd Ready to Welcome International Football Fans at 2018 World Cup*
335. *Warsaw Brushes Off EU Commission's 'Unjustified' Threats on Accepting Refugees*
336. *Warsaw Could Ask Germany for \$1Trln in WWII Reparations - Polish Committee Chief*
337. *Warsaw Expects New Afghan Migrant Flow at Border Organized by Minsk in Next Months*
338. *Warsaw to Abolish Criminal Penalty for Saying Poland Aided in Holocaust*
339. *Warsaw, Brussels Close to Resolving Dispute Over Court Reform*
340. *West Playing 'Double Game' by Calling on Delhi to Stop Trade With Russia, Indian FM Agrees With MP*
341. *Western Ukraine Sees Housing Boom as East Burns*
342. *What Does Poland's Cabinet Reshuffle Actually Mean?*
343. *What the Russian papers say*
344. *What to Expect From the First Official Phone Call Between Putin and Trump*
345. *What's Behind German Intelligence Chief's Warning of 'Greater Russian Threat'*
346. *White House Stops Calling Ukraine Invasion 'Imminent,' Says Putin's Decision Remains Unknown*
347. *Who Called For United States to Withdraw From NATO?*
348. *Why NATO Rejects Legitimacy of Moscow's 'Security Zone'*
349. *Why Poland Says It Wants Crimea Back in Ukraine (But Actually Doesn't)*
350. *Why Russian Football Fans Became Focus of Western Media Attention*
351. *Why Russia's Iskander Missiles Are 'Guarantors of Power Balance in Europe'*
352. *Why Truman Doctrine Has Lost Its Appeal For Isolationist President Trump*
353. *Wild Boars Paralyze Airport in Polish Capital*
354. *Wind of (Demographic) Change: Europe's Muslim Population Set to Triple by 2050*
355. *World's tallest Jesus statue finally assembled in Poland*
356. *WWII History Falsification Among Europe's Most Pressing Political Issues - Russian Envoy*
357. *'Your Average British Neo-Nazi Is Slightly Psychotic & Cowardly' – Watchdog Rep.*

358. *Zelensky's Presence at NATO Summit Hinges on Situation in Ukraine, Ability to Leave Country: Report*

Tytuły artykułów poddanych badaniom na witrynie agencji informacyjnej TASS

1. *Actions of Polish border guards can lead to conflict — Belarusian state border committee*
2. *Ambassador: Poland's decision to deny entry to Russian bikers will not go unnoticed*
3. *Cargo of bulletproof vests allegedly for Ukrainian army detained on Polish-German border*
4. *Communist propaganda ban not aiming to dismantle Soviet WWII memorials, vows Polish envoy*
5. *Diplomat vows levelheaded explanation as to who is guilty for Poland missile crash*
6. *EU ignoring Poland's, Lithuania's cruelty to migrants — Russian diplomat*
7. *EU states discussed \$62 price cap for Russian oil — Bloomberg*
8. *Europe, Russia want gas market out of sanction discussion — PM*
9. *Expulsion of Russian ambassador in Warsaw possible — Polish Foreign Ministry*
10. *Foreign Ministry: Polish minister's remarks re US testify to his political realism*
11. *Former Polish Foreign Minister Sikorski thanks US for damaging Nord Stream*
12. *German chancellor to attend events dedicated to anniversary of WWII outbreak*
13. *Influx of migrants arriving in Germany via Belarus, Poland eases somewhat — DPA*
14. *Kremlin aide certain Poland will "snatch" Ukraine's western regions if given half a chance*
15. *Kremlin dismisses Polish defense minister's accusations against Russia*
16. *Lithuanian shipping companies eye Russian-German ferry line bypassing Poland*
17. *Medvedev advises Warsaw to never forget multibillion-dollar Soviet aid*
18. *Medvedev blasts Poland's 'talentless politicians puppeteered by US' who fuel Russophobia*
19. *Migrants tossing stun grenades at Polish soldiers at border — Polish defense ministry*
20. *Minsk believes establishing US military base in Poland not to ensure regional stability*
21. *Minsk proposes holding border talks with Warsaw to solve critical issues*
22. *Missile incident in Poland was provocation against Minsk, Moscow — Lukashenko*
23. *Monument to Red Army soldiers in south of Poland being dismantled*
24. *Moscow ready to work with Poland's new leadership on condition of mutual respect*
25. *Moscow urges Poland to stop fanning hate*
26. *NATO ambassadors to hold emergency meeting over incident in Poland — Reuters*
27. *NATO says Ukrainian S-300 missile fell in Poland, but blames Russia*
28. *No unity in EU over sanctions, some states protest — Poland PM*

29. *Number of coronavirus cases in Poland surpasses 32,000*
30. *Number of migrants on Belarusian-Polish border is growing, says official*
31. *Official at Auschwitz museum describes Polish minister's remark as 'political debate'*
32. *Orlen signs oil supply contract with Rosneft*
33. *PGNiG sees halt of gas supplies by Gazprom as a breach of contract*
34. *Poland and Germany trying to elaborate responses to possible risks of Nord Stream 2 — PM*
35. *Poland demands that Russia increase motor transportation quotas threefold — ministry*
36. *Poland denies Russian journalist chance to study materials of court case against him*
37. *Poland dismisses reports mercenaries fighting in Ukraine*
38. *Poland does not let Russian defense minister's jet into its airspace*
39. *Poland doesn't explain stripping Russian journalist of residence permit — foreign ministry*
40. *Poland expects discount for Gazprom supplies this year*
41. *Poland foreign ministry informed in time on Night Wolves' ride — Russia's embassy*
42. *Poland has no recording of Putin's talks with Tusk on dividing Ukraine*
43. *Poland sends to Ukraine over 200 T-72 tanks, several dozen infantry carriers — radio*
44. *Poland suspends reverse-flow pumping of gas to Ukraine*
45. *Poland's attitude to Russia close to madness — Kremlin spokesman*
46. *Poland's decision to fine Gazprom politically motivated, says Russian Foreign Ministry*
47. *Poland's Duda hopes 'all doubts resolved' with Russia on World War II history*
48. *Poland's lower house votes to brand Russia 'state sponsor of terrorism'*
49. *Poland's president signs law on establishing Polish-Lithuanian-Ukrainian military brigade*
50. *Poland's top brass accuses Minsk, Moscow of fomenting migration crisis on Polish border*
51. *Poles horrified at Ukraine's glorification of Nazi quisling, says community leader*
52. *Polish authorities in Warsaw occupy Russian diplomatic real estate — Russian ambassador*
53. *Polish consulate staffer in Irkutsk declared persona non grata*
54. *Polish ex-president blames Kaczynski brothers for Tu-154M plane near Smolensk*
55. *Polish leadership begins work on scenarios of dismembering Ukraine — Russian intelligence*
56. *Polish politician says sanctions against Russia should affect president Putin*

57. *Polish president attending Victory Day celebrations in Moscow 'hard to imagine' — envoy*
58. *Polish top diplomat does not rule out further expansion of US military presence*
59. *Preliminary info contests Russian origin of missile that fell in Poland — Biden*
60. *Presidential elections in Poland - manifestation of populism surge in Europe — diplomat*
61. *Press review: Why Bolton got the boot and has a date been set for the Normandy Quartet*
62. *Putin expects relations with Poland's new head to be based on mutual respect of interests*
63. *Rights of migrants at Belarus border with Poland are not respected - UN spokesperson*
64. *Russia expels Polish diplomats in tit-for-tat move — Foreign Ministry*
65. *Russia keeping close eye on Belarusian-Polish border strife, says Kremlin spokesman*
66. *Russia urges Poland to meet its commitments on WWII memorials*
67. *Russia waits for Poland's new proposals on Tu-154M memorial*
68. *Russia, Belarus to clean Druzhba pipeline without assistance from Poland*
69. *Russian ambassador to Poland handed diplomatic note over missile incident*
70. *Russian diplomat says Poland has undermined bilateral ties for years*
71. *Russian embassy to look into seizure of recreation center by Polish authorities — envoy*
72. *Russian Foreign Ministry slams Poland's duplicity in migrant crisis*
73. *Russian Foreign Ministry waits for Poland's response to protest against vandalism*
74. *Russian gas transit to Poland suspended from January 19 — operator*
75. *Russian lawmaker calls Poland's suggestion to step up pressure on Russia "shortsighted"*
76. *Russian pilot intercepted by Polish jet was uninformed of temporary closed zone — official*
77. *Russian, Lithuanian, Polish rescuers to drill elimination of oil spill*
78. *Russian, Polish deputy foreign ministers to meet on July 12*
79. *Statements by Polish Deputy PM may aggravate tensions in Europe, Kremlin says*
80. *Transit of migrants is organized by EU mafia — Lukashenko*
81. *Two Polish soldiers hurt by migrants trying to cross into Poland from Belarus*
82. *UK Foreign Office looking into reports of alleged Russian missiles in Poland*
83. *Ukraine nationalism threat to peace in Europe — Polish veteran*
84. *Ukrainian and Polish presidents meet to discuss anti-Russian sanctions*
85. *US experts to join Poland's inquiry of Tuesday's missile explosion*
86. *Vandalism against memorials to Soviet warriors on the rise abroad, says diplomat*
87. *WADA presidential election to take place on November 7, 2019 in Poland*
88. *Warsaw statements on Aeroflot's involvement in migration crisis are not true — Lavrov*

89. *Washington, Warsaw work jointly to gather info on blast in east Poland — White House*
90. *Washington's INF Treaty pullout to make life more dangerous for Europeans — Russian MP*
91. *West uses migrants against Belarus in case of Russia-Ukraine conflict — Lukashenko*