

**Uniwersytet Śląski w Katowicach
Wydział Prawa i Administracji**

Robert Łasa

**Prawnomiędzynarodowa ochrona infrastruktury
krytycznej podczas konfliktu zbrojnego**

**rozprawa doktorska
przygotowana pod kierunkiem naukowym
dr hab. Joanny Nowakowskiej-Małuseckiej, prof. UŚ**

Katowice 2026

Spis treści

Wykaz skrótów	4
Wstęp	7
1 Znaczeniowe uwarunkowanie kategorii „infrastruktura krytyczna”	16
1.1 Wprowadzenie	16
1.2 Leksykalne uwarunkowanie wyrażenia „infrastruktura krytyczna”	17
1.3 Termin „infrastruktura krytyczna” jako termin języka prawnego	20
1.4 Termin „infrastruktura krytyczna” jako termin języka prawniczego	41
1.4.1 Ustalenie znaczenia pojęcia infrastruktura krytyczna w pracach organizacji międzynarodowych	41
1.4.2 Doktrynalne ustalenie znaczenia pojęcia infrastruktury krytycznej	47
1.4.3 Orzecnicze ustalenie znaczenia pojęcia infrastruktury krytycznej	50
1.5 Podsumowanie	51
2 Infrastruktura krytyczna w międzynarodowym prawie humanitarnym	54
2.1 Wprowadzenie	54
2.2 Ewolucja norm prawnych chroniących infrastrukturę krytyczną w międzynarodowym prawie humanitarnym	55
2.2.1 Rekonstrukcja standardu ochrony infrastruktury krytycznej w prawie haskim i prawie genewskim	55
2.2.1.1 Prawo genewskie	55
2.2.1.2 Prawo haskie	59
2.2.1.3 Kodeks Liebera	63
2.2.2 Standard ochrony infrastruktury krytycznej w międzynarodowym prawie humanitarnym po 1977 roku	66
2.2.2.1 Cel wojskowy	67
2.2.2.2 Dobra o charakterze cywilnym	72
2.2.2.3 Dobra niezbędne do przeżycia ludności cywilnej	73
2.2.2.4 Obiekty zawierające niebezpieczne siły	73
2.2.2.5 Środowisko naturalne	74
2.3 Współczesne wyzwania a ochrona infrastruktury krytycznej w międzynarodowym prawie humanitarnym	76
2.3.1 Rozwój nowych technologii a ochrona infrastruktury krytycznej	77
2.3.1.1 Dobra niematerialne	79
2.3.1.2 Zagrożenia cybernetyczne	80
2.3.2 Zmienny charakter konfliktu zbrojnego	84
2.4 Podsumowanie	87

3	Multicentryczny charakter standardu ochrony infrastruktury krytycznej	89
3.1	Wprowadzenie	89
3.2	Ochrona infrastruktury krytycznej a zagrożenia hybrydowe	89
3.2.1	Geneza pojęcia wojny hybrydowej	90
3.2.2	Działania organizacji międzynarodowych podejmowane przeciwko zagrożeniom hybrydowym.....	95
3.3	Ochrona infrastruktury krytycznej a zagrożenia terrorystyczne.....	107
3.3.1	Geneza pojęcia terroryzmu	107
3.3.2	Działania organizacji międzynarodowych podejmowane przeciwko zagrożeniom terrorystycznym.....	113
3.4	Podsumowanie.....	120
4	Obowiązki stron konfliktu zbrojnego w zakresie ochrony infrastruktury krytycznej	123
4.1	Wprowadzenie	123
4.2	Ochrona infrastruktury krytycznej przez pryzmat fundamentalnych zasad MPH .	123
4.3	Środki ostrożności podczas ataku na infrastrukturę krytyczną	130
4.3.1	Wybór i weryfikacja celu.....	131
4.3.2	Ocena skutków ataku.....	132
4.3.3	Kontrola nad atakiem.....	133
4.3.4	Ostrzeżenie przed atakiem.....	134
4.3.5	Lokalizacja celów wojskowych.....	135
4.4	Środki walki wykorzystywane do ataków na infrastrukturę krytyczną.....	135
4.4.1	Zakaz powodowania nadmiernego i zbędnego cierpienia.....	136
4.4.2	Przegląd uzbrojenia	138
4.4.3	Broń masowego rażenia.....	140
4.4.3.1	Broń biologiczna	140
4.4.3.2	Broń chemiczna	143
4.4.3.3	Broń jądrowa	146
4.4.4	Broń zapalająca.....	158
4.4.5	Amunicja kasetowa.....	160
4.5	Podsumowanie.....	161
5	Skutki niezapewnienia ochrony infrastrukturze krytycznej podczas konfliktu zbrojnego	163
5.1	Wprowadzenie	163
5.2	Skutki ataku na obiekty infrastruktury krytycznej chronione przez międzynarodowe prawo humanitarne	164

5.2.1	Skutki ataku na obiekty medyczne i pomoc humanitarną	164
5.2.2	Skutki ataku na dobra niezbędne do przetrwania ludności cywilnej	169
5.2.3	Skutki ataku na obiekty zawierające niebezpieczne siły	175
5.2.4	Skutki ataku na środowisko naturalne	179
5.3	Odpowiedzialność za atak na infrastrukturę krytyczną	181
5.3.1	Odpowiedzialność państwa	184
5.3.2	Odpowiedzialność jednostki	188
5.4	Podsumowanie	198
Zakończenie		200
Bibliografia		207
Spis tabel		236

Wykaz skrótów

ARPANET	Advanced Research Projects Agency Network (Sieć Agencji Zaawansowanych Projektów Badawczych)
ARSIWA	Articles on Responsibility of States for Internationally Wrongful Acts (Artykuły o odpowiedzialności państw za akty międzynarodowo bezprawne z 2001 roku)
BZZW	Berlińskie Zasady dotyczące Zasobów Wodnych z 2004 r.
CBRJ	Środki chemiczne, biologiczne, radioaktywne i jądrowe
CERT-EU	Computer Emergency Response Team for the EU Institutions (Zespół Reagowania na Incydenty Komputerowe Instytucji Unijnych)
CSIRT	Computer Security Incident Response Team (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego)
CTC	Counter-Terrorism Committee (Komitet ds. Zwalczania Terroryzmu)
CTED	Counter-Terrorism Committee Executive Directorate (Dyrekcja Wykonawcza ds. Zwalczania Terroryzmu)
Euratom	Europejska Wspólnota Energii Atomowej
GOVSATCOM	Governmental Satellite Communications (Rządowa Łączność Satelitarna)
ICAO	International Civil Aviation Organization (Organizacji Międzynarodowego Lotnictwa Cywilnego)
KE	Komisja Europejska
KG	Konwencje genewskie o ochronie ofiar wojny z 1949 r.
KNZ	Karta Narodów Zjednoczonych z 1945 r.
KPM	Komisja Prawa Międzynarodowego
Konwencja CCW	Konwencja o zakazie lub ograniczeniu pewnych broni konwencjonalnych, które mogą być uznawane za powodujące nadmierne cierpienia lub niepotrzebne skutki z 1980 r.
MAEA	Międzynarodowej Agencji Energii Atomowej
MKCK	Międzynarodowy Komitet Czerwonego Krzyża
MPH	międzynarodowe prawo humanitarne
MPPGSiK	Międzynarodowy pakt praw gospodarczych, społecznych i kulturalnych z 1966 r.

MTF	multilateral trading facility (wielostronna platforma obrotu)
MTK	Międzynarodowy Trybunał Karny
MTKJ	Międzynarodowy Trybunał Karny dla byłej Jugosławii
MTKR	Międzynarodowy Trybunał Karny dla Rwandy
MTS	Międzynarodowy Trybunał Sprawiedliwości
NATO	North Atlantic Treaty Organization (Organizacja Traktatu Północnoatlantyckiego)
NPOIK	Narodowy Program Ochrony Infrastruktury Krytycznej
NPT	Treaty on the Non-Proliferation of Nuclear Weapons (Układ o nierozprzestrzaniu broni jądrowej z 1968 r.)
OBWE	Organizacja Bezpieczeństwa i Współpracy w Europie
OECD	Organisation for Economic Co-operation and Development (Organizacja Współpracy Gospodarczej i Rozwoju)
ONZ	Organizacja Narodów Zjednoczonych
OTF	organised trading facilities (zorganizowana platforma obrotu)
PD I	Protokół dodatkowy do Konwencji Genewskich z 1949 r. dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych z 1977 r.
PD II	Protokół dodatkowy do Konwencji Genewskich z 1949 r. dotyczący ochrony ofiar konfliktów zbrojnych niemających charakteru międzynarodowego z 1977 r.
PE	Parlament Europejski
Rada	Rada Unii Europejskiej
RB ONZ	Rada Bezpieczeństwa Organizacji Narodów Zjednoczonych
RCB	Rządowe Centrum Bezpieczeństwa
RE	Rada Europy
RSF	Rapid Support Forces (Siły Szybkiego Wsparcia)
SAF	Sudanese Armed Forces (Sudańskie Siły Zbrojne)
SCSL	Special Court for Sierra Leone (Sąd Specjalny dla Sierra Leone)
SIPRI	Stockholm International Peace Research Institute
SJP PWN	Słownik Języka Polskiego Wydawnictwa Naukowego PWN
SSA	Surveillance system for attacks on health care (System monitorowania ataków na służbę zdrowia)

STSM	Stały Trybunał Sprawiedliwości Międzynarodowej
TSUE	Trybunał Sprawiedliwości Unii Europejskiej
UE	Unia Europejska
UNOSOM I	United Nations Operation in Somalia I (Operacja Narodów Zjednoczonych w Somalii I)
UNOSOM II	United Nations Operation in Somalia I (Operacja Narodów Zjednoczonych w Somalii II)
UNRWA	United Nations Relief and Works Agency for Palestine Refugees in the Near East (Agencja Narodów Zjednoczonych ds. Pomocy Uchodźcom Palestyńskim na Bliskim Wschodzie)
WE	Wspólnota Europejska
WHO	World Health Organization (Światowa Organizacja Zdrowia)
WSJP PAN	Wielki Słownik Języka Polskiego Polskiej Akademii Nauk
ZO ONZ	Zgromadzenie Ogólne Organizacji Narodów Zjednoczonych

Wstęp

Uzasadnienie tematu rozprawy

Poczucie bezpieczeństwa należy do podstawowych potrzeb każdego człowieka. Jest ono rozumiane jako „bodziec stwarzający warunki konieczne dla właściwego funkcjonowania organizmu ludzkiego, utrzymywania równowagi psychicznej i zdolności umysłowych”¹. Jest więc dobrostanem bezpośrednio odnoszącym się do człowieka². Jednak bezpieczeństwo to także proces w rozumieniu działalności określonych podmiotów (najczęściej właściwych organów państwowych) zmierzający do „zapewnienia możliwości przetrwania, rozwoju i swobody realizacji własnych interesów w konkretnych warunkach, poprzez wykorzystywanie okoliczności sprzyjających (szans), podejmowanie wyzwań, redukowanie ryzyka oraz przeciwdziałanie (zapobieganie i przeciwstawianie się) wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów”³. Taka definicja wpisuje się w koncepcję bezpieczeństwa państwa, a więc – w rozumieniu G. Jelinka – trwałego związku ludzi stale zamieszkujących określone terytorium, podlegających władzy zwierzchniej⁴. Bezpieczeństwo państwa może być rozumiane na dwa sposoby⁵. W pierwszym ujęciu – negatywnym – oznacza wolność od zagrożeń zewnętrznych (najczęściej w kontekście militarnym), wpływających na istnienie państwa. Natomiast drugie ujęcie – pozytywne – wykracza poza ramy egzystencjonalne państwa i rozszerza pojęcie bezpieczeństwa między innymi o ekologię czy rozwój gospodarczy.

Problematyka bezpieczeństwa państwa skupia się na trzech filarach: politycznym, militarnym oraz gospodarczym⁶. Każdy z tych filarów wzajemnie na siebie oddziałuje

¹ T. Pszczołowski, *Mała encyklopedia prakseologii i teorii organizacji*, Zakład Prakseologii Instytutu Filozofii i Socjologii PAN, Wrocław–Warszawa–Kraków–Gdańsk 1978, s. 172.

² A. Tyczkowska-Kowerczyk, *Zadania podejmowane na rzecz bezpieczeństwa publicznego wśród społeczności lokalnej jako przejaw działalności administracji publicznej*, „Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy”, 2020, nr 36 (3), s. 70.

³ S. Koziej, *Między piekłem a rajem. Szare bezpieczeństwo na progu XXI wieku*, Wydawnictwo Adam Marszałek, Toruń 2006, s. 7.

⁴ M. Żmigrodzki (red.), *Encyklopedia politologii. Tom 1 Teoria polityki*, Wydawnictwo Zakamycze, 1999, s. 218. Państwo jako instytucja zwierzchnia spełnia trzy podstawowe funkcje: adaptacyjną (dostosowanie działalności organów państwa do zmieniającej się rzeczywistości), regulacyjną (określenie zasad działania państwa, w szczególności tworzenie wewnętrznego ładu i porządku) oraz innowacyjną (wskazywanie i wprowadzanie zmian w działalności państwa). Spełnienie przez państwo tych trzech funkcji wpływa na jego prawidłowe funkcjonowanie i bezpieczeństwo, zob. K. Sidorkiewicz, *Współczesne ujęcie funkcji państwa*, „Studia Elbląskie”, 2010, nr 11, s. 221.

⁵ M. Szuniewicz, *Ochrona bezpieczeństwa państwa jako przesłanka ograniczenia praw i wolności jednostki w świetle Europejskiej Konwencji Praw Człowieka*, Wydawnictwo C.H. Beck, Warszawa 2016, s. 10-11.

⁶ J. Płaczek, *Filary bezpieczeństwa narodowego. Zarys teorii*, Wydawnictwo Lotniczej Akademii Wojskowej, Dąblin 2022, s. 10.

i w zależności od tego, czy państwo znajduje się w stanie pokoju czy konfliktu zbrojnego, prym będzie wiódł inny filar⁷. Jednak co pozostaje wspólne dla każdego z tych filarów to pewne zadania zmierzające do bezpieczeństwa państwa, jak zapewnienie ochrony infrastruktury krytycznej⁸. Polska Strategia Bezpieczeństwa Narodowego z 2020 roku przewiduje, że ochrona infrastruktury krytycznej stanowi jeden z elementów zwiększenia odporności i zdolności obronnych państwa⁹. Dlaczego ochrona infrastruktury krytycznej pełni aż tak ważną rolę w bezpieczeństwie narodowym? Ponieważ właściwe funkcjonowanie jej obiektów jest kluczowe dla zapewnienia bezpieczeństwa ludności tego państwa, między innymi poprzez dostęp do żywności, wody pitnej czy opieki medycznej, ale także może przysłużyć się rozwojowi poziomu życia, na przykład poprzez systemy teleinformatyczne czy transportowe¹⁰.

Rola jaką infrastruktura krytyczna pełni w systemach bezpieczeństwa narodowego i międzynarodowego, oddziałując nie tylko na państwa, ale przede wszystkim na ludność uwidacznia jej newralgiczny charakter. Niestety jej „wrażliwość” często jest przyczyną ataków na nią nakierowanych. W czasie pokoju infrastruktura krytyczna jest najczęściej zagrożona atakami w cyberprzestrzeni, czego przykładem mogą być ataki na polską infrastrukturę wodną w latach 2024-2025, przeprowadzone przez hakerów powiązanych z Federacją Rosyjską¹¹.

Jednak szczególne zagrożenia wiążą się z atakami na infrastrukturę krytyczną podczas konfliktu zbrojnego. Spowodowane jest to tym, że obiekty infrastruktury krytycznej zapewniają podstawowe potrzeby ludności cywilnej (dostęp do żywności, wody pitnej, ciepła, energii elektrycznej czy opieki medycznej), które ze względu na działania zbrojne są i tak już mocno ograniczone. Dlatego międzynarodowe prawo humanitarne (MPH) jako gałąź prawa międzynarodowego reguluje prawa i obowiązki stron międzynarodowego i niemiędzynarodowego konfliktu zbrojnego (ale także okupacji wojennej i walk

⁷ W stanie pokoju prym wiodzie filar gospodarczy, natomiast w przypadku konfliktu zbrojnego podstawą bezpieczeństwa państwa są filary militarny i polityczny, zob. J. Płaczek, *Filary bezpieczeństwa...*, s. 10.

⁸ A. Lasota-Jądrzak, *Bezpieczeństwo infrastruktury krytycznej państwa*, „Rocznik Bezpieczeństwa Morskiego”, 2013, Rok VII, s. 173.

⁹ Polska, *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2020, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf (dostęp: 18.05.2026), s. 16. W lipcu 2025 roku przyjęto nową Strategię Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej jednak dokument nie został upubliczniony, zob. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, <https://www.gov.pl/web/premier/strategia-bezpieczenstwa-narodowego-rzeczypospolitej-polskiej> (dostęp: 18.05.2026).

¹⁰ B. Kosowski, *Infrastruktura krytyczna w systemie bezpieczeństwa narodowego*, „Safety & Fire Technology”, 2019, vol. 54, iss. 2, s. 133.

¹¹ *When Red Lines Cross Blue Lines: Cyber Attacks on Poland's Water Infrastructure – Part I*, <https://lieber.westpoint.edu/when-red-lines-cross-blue-lines-cyber-attacks-polands-water-infrastructure-part-i/> (dostęp: 18.05.2026).

narodowowyzwoleńczych), a jego celem jest zapewnienie ochrony ofiarom konfliktu zbrojnego, w szczególności ludności cywilnej. Bezpieczeństwo ludności cywilnej bezpośrednio wymaga prawidłowego funkcjonowania infrastruktury krytycznej, jednak ochrona jej obiektów w MPH jest ograniczona. Jest to spowodowane między innymi brakiem odpowiedniego zdefiniowania infrastruktury krytycznej w tym dziale prawa międzynarodowego. Zamiast tego, MPH wprowadza sektorową ochronę obiektów, które potencjalnie mogą zostać zakwalifikowane do infrastruktury krytycznej, jak obiekty medyczne, dobra niezbędne dla przetrwania ludności cywilnej obejmujące między innymi magazyny z żywnością czy wodą pitną, ale także obiekty zawierające „niebezpieczne siły”, czyli tany, groble oraz elektrownie atomowe. Zastosowanie rozproszonej ochrony obiektów infrastruktury krytycznej przekłada się na jej ograniczoną efektywność, a co za tym idzie, przyczynia się do zwiększonych negatywnych skutków ataków na te obiekty. Przykładem braku skutecznej ochrony są izraelskie ataki na system ochrony zdrowia w Strefie Gazy, gdzie od 7 października 2023 roku do 11 czerwca 2025 roku odnotowano ponad 700 ataków, które skutkowały śmiercią ponad 900 osób i zniszczeniem ponad 30 szpitali¹². Szpitale oraz inne obiekty medyczne znajdujące się w Libanie są również celami ataku podczas konfliktu w 2026 roku pomiędzy Stanami Zjednoczonymi, Izraelem a Iranem i jego sojusznikami, takimi jak Hezbollah. Tylko przez pierwsze trzy tygodnie konfliktu w Libanie zginęło ponad 1000 osób, a ponad 50 obiektów medycznych zostało zniszczonych¹³.

Obowiązujące normy MPH tylko w nieznacznym stopniu przewidują ochronę obiektów infrastruktury krytycznej. Jak pokazują praktyka państw, w krajowych systemach prawnych do infrastruktury krytycznej zalicza się szereg urządzeń i systemów, które odgrywają kluczową rolę w zapewnieniu bezpieczeństwa tak państwa, jak i jego obywateli¹⁴. Natomiast MPH, w zakresie infrastruktury krytycznej, wprowadza ochronę ograniczoną jedynie do obiektów medycznych, dóbr niezbędnych dla przetrwania ludności cywilnej, obiektów zawierających niebezpieczne siły oraz środowiska naturalnego.

¹² *UN experts appalled by relentless Israeli attacks on Gaza's healthcare system*, <https://www.ohchr.org/en/press-releases/2025/08/un-experts-appalled-relentless-israeli-attacks-gazas-healthcare-system> (dostęp: 18.05.2026).

¹³ *War in the Middle East: Iran nuclear facility hit as equivalent of 'one classroom of children' killed, wounded daily in Lebanon*, <https://news.un.org/en/story/2026/03/1167175> (dostęp: 18.05.2026).

¹⁴ W ramach krajowych systemów prawnych do infrastruktury krytycznej zalicza się między innymi sektory transportu, energetyczny, telekomunikacji czy dostępu do żywności i wody pitnej, zob. C. Gallais and E. Filiol, *Critical Infrastructure: Where Do We Stand Today? A Comprehensive and Comparative Study of the Definitions of a Critical Infrastructure*, „Journal of Information Warfare”, 2017, vol. 16, no. 1, s. 69-70 oraz 80-82.

Cel rozprawy, problem badawczy i hipotezy badawcze

Celem pracy jest rekonstrukcji definicji infrastruktury krytycznej z norm międzynarodowego prawa humanitarnego, ale także ustalenie współczesnego sposobu jego rozumienia, po to by możliwym było opracowanie – tak ważnego obecnie – standardu ochrony infrastruktury krytycznej w MPH.

Na ile jednak zrekonstruowana definicja infrastruktury krytycznej powinna uwzględniać model przedmiotowo-podmiotowy, zgodnie z którym infrastruktura krytyczna służy ochronie państwa jako instytucji, ale pośrednio wpływa również na ochronę jego obywateli, a na ile, jak w MPH, jedynie model podmiotowy – ukierunkowany wyłącznie na ludność cywilną? Innymi słowy, czy kategoria infrastruktury krytycznej, dająca się zrekonstruować z MPH, jest zakresowo wystarczająca by współcześnie chronić ową infrastrukturę, uwzględniając dynamicznie zmieniające się współczesne wyzwania? Rozwikłanie tej, jakże ważkiej naukowo i doniosłej praktycznie, kwestii uczyniono **głównym problemem badawczym** niniejszej rozprawy. U podstaw tego legły dwa argumenty. Po pierwsze, sam fakt braku definicji analizowanego pojęcia nie stanowi takiego czy innego niedoszacowania normatywnego w tym zakresie, ale nade wszystko jego brak uniemożliwia wyznaczenie skutecznego systemu ochrony infrastruktury krytycznej. Po drugie, obowiązujące normy MPH muszą zostać skonfrontowane z wybranymi wyzwaniami współczesności.

Rozwikłanie tak ujętego problemu badawczego wsparte zostanie konfirmacją lub falsyfikacją następujących **hipotez badawczych**:

1. Na ile, w związku z brakiem definicji pojęcia infrastruktury krytycznej w MPH, jego regulacje prawne zapewniają jedynie minimalny standard ochrony obiektów potencjalnie zaliczanych do infrastruktury krytycznej, a na ile rekonstrukcja tego standardu wymaga wyjścia poza normy MPH?
2. Czy pojęcie infrastruktury krytycznej nie powinno być współcześnie rozumiane jako całość powiązanych ze sobą funkcjonalnie systemów zapewniających bezpieczeństwo państwa i jego obywateli? Innymi słowy, czy z racji funkcji infrastruktury krytycznej nie powinna być ona rozpatrywana nie tylko i wyłącznie jako system i obiekty zapewniające bezpieczeństwo ludności cywilnej, ale przede wszystkim zapewniające bezpieczeństwo państwa jako instytucji? Czy w związku z tym pojęcie infrastruktury krytycznej nie powinno stanowić konglomeratu – ujmując rozumienie infrastruktury

krytycznej jako całości powiązanych ze sobą funkcjonalnie systemów zapewniających bezpieczeństwo państwa i jego obywateli?

3. Analizując współczesną dynamicznie zmieniającą się sytuację geopolityczną, jakie systemy, potencjalnie uznawane za infrastrukturę krytyczną, są przedmiotem ochrony w MPH? Czy jest tak, że podczas ataku na infrastrukturę krytyczną, atak ten pozbawia ochrony MPH? Na ile zatem współcześnie - *de lege lata* - potrzeba skutecznej ochrony infrastruktury krytycznej i na ile zrekonstruowany standard tej ochrony jest w stanie podołać współczesnym wyzwaniom, tak różnym od tych, kiedy tworzone były normy, dość anachronicznego już, MPH?

Struktura rozprawy oraz metody badawcze

Tematyka niniejszej rozprawy obejmuje prawnomiędzynarodową ochronę infrastruktury krytycznej podczas konfliktu zbrojnego. Badania podejmują problem istotny z punktu widzenia dzisiejszego pola walki i idących za tym regulacji prawnych, ale także obejmują normy spoza MPH, w tym regulacje unijne czy przepisy krajowe. Tak określona tematyka rozprawy określa jej strukturę składającą się z pięciu rozdziałów.

Rozdział pierwszy, zatytułowany „Znaczeniowe uwarunkowanie kategorii „infrastruktura krytyczna””, stanowi trzyczęściową analizę pojęcia infrastruktury krytycznej. W pierwszej części, odwołując się do słowników języka polskiego oraz języka angielskiego, ustalono leksykalne uwarunkowania pojęcia infrastruktury krytycznej. W drugiej części analizie poddano pojęcie infrastruktury krytycznej jako terminu języka prawnego. W zakresie prawa międzynarodowego badaniami objęto wyłącznie regulacje unijne, ponieważ tylko Unia Europejska (UE) w wymiarze międzynarodowym zdefiniowała pojęcie infrastruktury krytycznej oraz opracowała szeroki system jej ochrony. Na drugą część składają się również badania pojęcia infrastruktury krytycznej w aktach normatywnych Stanów Zjednoczonych, Federacji Rosyjskiej oraz Chińskiej Republiki Ludowej. Jako kryterium wyboru tych państw zastosowano ich zróżnicowane podejście do definiowania infrastruktury krytycznej, ale także dostosowanie jej ochrony do współczesnych wyzwań. Co więcej, każde z tych państw, jako potęga militarna ma wpływ na międzynarodowy pokój i bezpieczeństwo. W ramach drugiej części analizie poddano również pojęcie infrastruktury krytycznej w polskim systemie prawnym. Chociaż Polska, jako państwo członkowskie UE, musi dostosować swoje przepisy do regulacji unijnych, to ze względu na fakt bycia państwem flankowym Organizacji Paktu Północnoatlantyckiego posiada szeroko unormowaną ochronę infrastruktury krytycznej.

W trzeciej części przeanalizowano pojęcie infrastruktury krytycznej w rozumieniu języka prawniczego, dlatego odwołano się do prac organizacji międzynarodowych, doktryny oraz orzecznictwa sądowego. Szczególną uwagę poświęcono Organizacji Narodów Zjednoczonych (ONZ), Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE), Organizacji Paktu Północnoatlantyckiego (NATO) oraz Organizacji Współpracy Gospodarczej i Rozwoju (OECD). Każda z tych organizacji wpisuje się w inny filar bezpieczeństwa narodowego i międzynarodowego. ONZ oraz OBWE stanowią filar polityczny, a ich prace w zakresie infrastruktury krytycznej obejmują przede wszystkim zagrożenia terrorystyczne. NATO jako organizacja wojskowa jest przedstawicielem filaru militarnego, tym samym jej prace nad infrastrukturą krytyczną dotyczą zagrożeń wynikających z konfliktów zbrojnych. Ostatnia organizacja, OECD, to filar gospodarczy, a jej prace skupiają się na wpływie infrastruktury krytycznej na rozwój gospodarczy państw i ich obywateli.

Drugi rozdział, zatytułowany „Infrastruktura krytyczna w międzynarodowym prawie humanitarnym”, stanowi próbę ustalenia standardu ochrony infrastruktury krytycznej w MPH. Rozdział został podzielony na trzy części. W pierwszej z nich zrekonstruowany zostanie standard ochrony infrastruktury krytycznej w prawie genewskim i haskim. Celem rekonstrukcji jest nie tylko odnalezienie źródeł ochrony poszczególnych obiektów podczas konfliktu zbrojnego we współczesnym MPH, ale także analiza postanowień Konwencji genewskich z 1949 roku¹⁵, które stanowią trzon MPH. W drugiej części analizie poddane zostaną postanowienia Protokołów dodatkowych I i II z 1977 roku (PD I i PD II)¹⁶, które obecnie stanowią podstawę dla ustalenia standardu ochrony infrastruktury krytycznej podczas konfliktu zbrojnego. W szczególności przeanalizowany zostanie obowiązek rozróżnienia między celami wojskowymi a dobrami o charakterze cywilnym. Co więcej, analizą objęta będzie rozproszona ochrona poszczególnych obiektów w MPH, a więc obiektów niezbędnych dla przeżycia ludności cywilnej, zawierających niebezpieczne siły, a także obiektów przemysłowych w kontekście ich zagrożenia dla środowiska naturalnego. W ostatniej, trzeciej części obecnie obowiązujący standard ochrony infrastruktury krytycznej, a więc ten po 1977 roku, zostanie poddany analizie w kontekście potencjalnego ryzyka utraty tej ochrony. Jej zakresem objęte zostaną zagrożenia wynikające ze stosowania nowych technologii, w tym działań militarnych

¹⁵ *Konwencja o polepszaniu losu rannych i chorych w armiach czynnych, Konwencja o polepszaniu losu rannych, chorych i rozbitków sił zbrojnych na morzu, Konwencja o traktowaniu jeńców wojennych, Konwencja o ochronie osób cywilnych podczas wojny*, Genewa, 12.08.1949, Dz. U. z 1956 r., nr 56, poz. 175.

¹⁶ *Protokoły dodatkowe do Konwencji genewskich z 12 sierpnia 1949 r., dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych (Protokół I) oraz dotyczący ochrony ofiar niemiędzynarodowych konfliktów zbrojnych (Protokół II)*, Genewa, 8.06.1977, Dz. U. z 1992 r., nr 41, poz. 175.

podejmowanych w cyberprzestrzeni, ale także zagrożenia wynikające ze zmiennego charakteru konfliktu zbrojnego i wynikającej z tego osłabionej ochrony infrastruktury krytycznej.

W trzecim rozdziale, zatytułowanym „Multicentryczny charakter standardu ochrony infrastruktury krytycznej”, wskazane będą standardy ochrony infrastruktury krytycznej wypracowane w toku działalności organizacji międzynarodowych, nieodnoszące się do sytuacji konfliktu zbrojnego. W pierwszej kolejności mowa będzie o ochronie infrastruktury krytycznej przed zagrożeniami hybrydowymi. W tym celu uwzględnione zostaną prace podejmowane na forum UE oraz NATO, ponieważ te organizacje na co dzień podejmują walkę między innymi z rosyjskimi działaniami hybrydowymi. Następnie znajdą się odniesienia do ochrony infrastruktury krytycznej przed zagrożeniami terrorystycznymi. Za podstawę ustalenia tego standardu ochrony posłużą prace organizacji międzynarodowych tak ogólnosiwiatowych (ONZ), jak i regionalnych (Rada Europy). Zrekonstruowanie ochrony infrastruktury krytycznej w razie zagrożeń hybrydowych i terrorystycznych pozwoli na wyprowadzenie dobrych praktyk, które następnie mogą znaleźć swoje zastosowanie podczas konfliktu zbrojnego.

Czwarty rozdział, o tytule „Obowiązki stron konfliktu zbrojnego w zakresie ochrony infrastruktury krytycznej” stanowi powrót do postanowień MPH. W pierwszej części ustalone zostaną normy wynikające z podstawowych zasad MPH, które warunkują działania podejmowane wobec infrastruktury krytycznej podczas konfliktu zbrojnego. Zasady jako szkielet MPH, posiadające status norm zwyczajowych są podstawowymi wyznacznikiem legalności potencjalnej działalności stron konfliktu zbrojnego. W drugiej części określony zostanie katalog środków ostrożności mający zastosowanie przez strony konfliktu w celu wyeliminowania lub co najmniej ograniczenia negatywnych skutków ataku na infrastrukturę krytyczną. W ostatniej, trzeciej części wskazane zostaną środki walki wykorzystywane do atakowania obiektów infrastruktury krytycznej. Szczególnie uwzględniono zagrożenia płynące z użycia broni masowego rażenia, które wpływają na bezpieczeństwo infrastruktury krytycznej na kilku płaszczyznach.

Ostatni, piąty rozdział zatytułowany „Skutki niezapewnienia ochrony infrastrukturze krytycznej podczas konfliktu zbrojnego” zawiera rozważania dotyczące skutków braku tytułowej ochrony. Pierwsza część odnosi się do skutków ataku, który ma rzeczywisty wpływ na ludność cywilną oraz środowisko naturalne. W drugą część ustalone zostały przesłanki odpowiedzialności za ataki wymierzone w infrastrukturę krytyczną podczas konfliktu zbrojnego. W pierwszej kolejności wskazano na możliwość przypisania winy państwu za

działanie niezgodne z prawem międzynarodowym jakim jest atak na infrastrukturę krytyczną. Dodatkowo ustalono możliwość przypisania odpowiedzialności karnej jednostce, która dopuściła się ataku na infrastrukturę krytyczną kwalifikowanego jako zbrodnie wojenna w oparciu o Rzymski Statut Międzynarodowego Trybunału Karnego z 1998 roku (Statut MTK)¹⁷.

Podstawową metodą wykorzystaną w badaniach była metoda dogmatyczna, która posłużyła do analizy tekstów prawnych, przy szczególnym uwzględnieniu norm prawa międzynarodowego. Wykładni poddane zostały także akty prawa krajowego. Podjęte działania umożliwiły zestawienie ze sobą różnych sposobów zarówno definiowania, jak i ochrony infrastruktury krytycznej, w tym znalezienie podobieństw umożliwiających stworzenie uniwersalnego modelu ochrony, który mógłby mieć zastosowanie podczas konfliktu zbrojnego. Oprócz aktów prawa krajowego i międzynarodowego ważnym elementem badania była analiza orzecznictwa sądów krajowych i trybunałów międzynarodowych. W tym celu metoda dogmatyczna posłużyła do wskazania, w jaki sposób orzecznictwo radzi sobie ze zdefiniowaniem pojęcia infrastruktury krytycznej.

Jak wykazano powyżej, badaniom poddane zostały przepisy prawa krajowego kilku państw. W tym celu zastosowano również metodę komparatystyczną. Jej wykorzystanie pozwoliło poddać krytycznej analizie normy prawa materialnego, w szczególności ustalając jak w każdym z tych państw kształtuje się ochrona infrastruktury krytycznej, z uwzględnieniem nowoczesnych zagadnień, takich jak chińska informatyczna infrastruktura krytyczna.

Uzupełnieniem powyższych była metoda teoretyczna, konieczna przede wszystkim z perspektywy zbadania wagi fundamentalnych zasad międzynarodowego prawa humanitarne, jak zasada rozróżniania, proporcjonalności oraz konieczności wojskowej, w kontekście obierania infrastruktury krytycznej za cel podczas konfliktu zbrojnego. W tym celu konieczne było zbadanie stanowiska doktryny oraz efektów prac prowadzonych na forach organizacji międzynarodowych. W głównej mierze odnosi się to do Międzynarodowego Komitetu Czerwonego Krzyża (MKCK), który przez ostatnie lata aktywnie uczestniczył w dyskusji nad rozszerzeniem ochrony infrastruktury krytycznej podczas konfliktu zbrojnego, wydając w tym celu opracowania ze wskazówkami dotyczącymi tej problematyki. Ponadto szczególną uwagę należy zwrócić na prace ONZ, której głównym celem jest utrzymanie międzynarodowego pokoju i bezpieczeństwa. Niemniej ważne są osiągnięcia w tym zakresie

¹⁷ *Rzymski Statut Międzynarodowego Trybunału Karnego*, Rzym, 17.07.1998, Dz. U. z 2003 r., nr 78, poz. 708.

regionalnych organizacji międzynarodowych. Warto wspomnieć o regulacjach chroniących infrastrukturę krytyczną, które przyjęto w UE czy Radzie Europy.

Genezy ochrony obiektów infrastruktury krytycznej w MPH należy doszukiwać się już w pierwszych kodyfikacjach prawa genewskiego i prawa haskiego, jak na przykład w Konwencji o polepszeniu losy rannych w armiach w polu z 1864 roku¹⁸ czy Regulaminach haskich z 1899 i 1907 roku¹⁹. W związku z tym konieczne było zastosowanie metody historycznej, która posłużyła nie tylko do odtworzenia standardów ochrony obiektów potencjalnie zaliczanych do infrastruktury krytycznej, ale również do analizy konkretnych konfliktów zbrojnych mających wpływ na późniejsze regulacje w tym zakresie, jak wojna włosko-austriacki (bitwa pod Solferino), czy wojna secesyjna.

¹⁸ *Konwencja o polepszeniu losu rannych w armiach w polu*, Genewa, 22.08.1864, w: P. K. Marszałek, *Międzynarodowe prawo humanitarne konfliktów zbrojnych. Dokumenty*, Wydawnictwo C.H. Beck, Warszawa 2019, s. 299-300.

¹⁹ *Konwencja o poszanowaniu praw i zwyczajów wojny na lądzie i załącznik do niej: Regulamin dotyczący praw i zwyczajów wojny na lądzie*, Haga, 29.07.1899, w: P. K. Marszałek, *Międzynarodowe prawo humanitarne ...*, s. 21-30.

1 Znaczeniowe uwarunkowanie kategorii „infrastruktura krytyczna”

1.1 Wprowadzenie

W związku z tym, że problematyką niniejszej rozprawy jest prawnomiędzynarodowa ochrona infrastruktury krytycznej podczas konfliktu zbrojnego, w pierwszej kolejności należy podjąć próbę odpowiedzi na pytanie co jest przedmiotem ochrony oraz wskazać powody, dla których ta ochrona jest zapewniana. W tym celu konieczne jest zdefiniowanie pojęcia infrastruktury krytycznej oraz określenie jej zakresu – aspektu przedmiotowego i aspektu podmiotowego.

Ustalenie znaczenia pojęcia infrastruktury krytycznej wymaga przeprowadzenia trzyczęściowej analizy tego pojęcia. Pierwsza część odnosi się do leksykalnych uwarunkowań wyrażenia „infrastruktura krytyczna” odwołując się zarówno do słowników języka polskiego, jak i słowników języka angielskiego.

Druga część to analiza terminu „infrastruktura krytyczna” jako terminu języka prawnego. W tej części analizie poddano definicje legalne pojęcia infrastruktury krytycznej pochodzące z aktów normatywnych UE oraz wybranych państw – Stanów Zjednoczonych, Federacji Rosyjskiej, Chińskiej Republiki Ludowej oraz Rzeczypospolitej Polskiej. Prawo UE jest jedyną międzynarodową regulacją, która zdefiniowała pojęcie „infrastruktura krytyczna” oraz stworzyła system bezpieczeństwa tej infrastruktury. Natomiast kryterium wyboru krajowych regulacji jest odmienne kształtowanie definicji infrastruktury krytycznej oraz poziom zapewnienia jej bezpieczeństwa, uwzględniając współczesne cyber-zagrożenia. Ponadto USA, Rosja oraz Chiny są światowymi potęgami militarnymi²⁰, które odgrywają istotną rolę w zapewnieniu międzynarodowego pokoju i bezpieczeństwa. Natomiast Polska jako państwo flankowe NATO jest szczególnie narażona na ataki hybrydowe ze strony Rosji i Białorusi, w tym ataki wymierzone w infrastrukturę krytyczną²¹.

Trzecia część stanowi analizę terminu „infrastruktura krytyczna” jako terminu języka prawniczego. W tym celu przedstawiono pojęcie infrastruktury krytycznej w znaczeniu prezentowanym przez organizacje międzynarodowe – ONZ, OBWE, NATO oraz OECD.

²⁰ 2026 Military Strength Ranking, <https://www.globalfirepower.com/countries-listing.php> (dostęp: 12.05.2026).

²¹ Kolejne ataki na infrastrukturę krytyczną w Polsce, <https://cyberdefence24.pl/cyberbezpieczenstwo/kolejne-ataki-na-infrastrukture-krytyczna-w-polsce> (dostęp: 22.06.2024).

Tak ONZ, jak i OBWE w swoich pracach nad infrastrukturą krytyczną skupiają się przede wszystkim na zagrożeniach wynikających z zagrożeń terrorystycznych. NATO jako sojusz wojskowy analizuje zagrożenia militarne dla infrastruktury krytycznej, w tym wynikające z toczących się obecnie konfliktów zbrojnych. Prace OECD w zakresie infrastruktury krytycznej są poświęcone jej wpływom na rozwój gospodarczy i społeczny państw i ich obywateli. Ponadto przeanalizowano rozumienie pojęcia „infrastruktura krytyczna” w doktrynie oraz orzecznictwie, zarówno polskich sądów, jak i trybunałów międzynarodowych – Trybunału Sprawiedliwości Unii Europejskiej (TSUE) oraz MTKJ. TSUE w swoim orzecznictwie posługuje się terminem „infrastruktura krytyczna”, jednak w innym kontekście niż bezpieczeństwo państwa. Natomiast MTKJ odnosi się do standardów ochrony poszczególnych sektorów, które potencjalnie mogą zostać zaliczone do systemów infrastruktury krytycznej.

1.2 Leksykalne uwarunkowanie wyrażenia „infrastruktura krytyczna”

Słowniki języka polskiego nie definiują wyrażenia „infrastruktura krytyczna”, na próżno również szukać definicji tego pojęcia w słownikach języka angielskiego. Zamiast tego, pojęcia „infrastruktura” oraz „krytyczna” należy poddać osobnej analizie i dopiero na tej podstawie możliwe będzie stworzenie leksykalnego uwarunkowania wyrażenia „infrastruktura krytyczna”.

Pojęcie infrastruktury wywodzi się z języka łacińskiego, a konkretnie z połączenia dwóch słów – *infra* oraz *structura*²². Choć w języku polskim nie pojawia się pojęcie „infra” (łac. pod, poniżej), to na uwagę zasługuje pojęcie „struktury”. Wielki Słownik Języka Polskiego Polskiej Akademii Nauk (WSJP PAN) jako jedną z definicji pojęcia „struktury” podaje „układ i wzajemne relacje elementów składowych jakiejś całości”, a także „twór zbudowany w określony sposób z powiązanych ze sobą elementów”²³. Podobnie pojęcie „struktury” zostało zdefiniowane w Słowniku Języka Polskiego Wydawnictwa Naukowego PWN (SJP PWN). W SJP PWN strukturę rozumie się jako „całość zbudowaną w pewien sposób z poszczególnych elementów”²⁴. Odwołując się do języka angielskiego należy zauważyć, że pojęcie *structure* posiada zdecydowanie więcej znaczeń niż w języku polskim. Oxford Advanced Learner's Dictionary jako *structure* wskazuje „the way in which the parts of something are connected

²² łac. *infra* – „pod, poniżej”, łac. *structura* – „budowa, struktura”, zob. *infrastruktura*, https://wsjp.pl/haslo/do_druku/42645/infrastruktura (dostęp: 5.06.2024).

²³ *Struktura*, https://wsjp.pl/haslo/do_druku/15988/struktura (dostęp: 5.06.2024).

²⁴ *Struktura*, <https://sjp.pwn.pl/szukaj/struktura.html> (dostęp: 5.06.2024).

together, arranged or organized; a particular arrangement of parts”, „*a thing that is made of several parts, especially a building a stone/brick/wooden structure*”, „*the state of being well organized or planned with all the parts linked together; a careful plan*”²⁵. Cambridge Dictionary natomiast definiuje *structure* jako „*the way in which the parts of a system are arranged or organized, or the system itself*”, „*an object such as a building, that has been built or arranged in a particular way*”²⁶. Co więcej, w języku angielskim pojęcie *structure* jest również czasownikiem, przez co może być również rozumiane jako „*to plan, organize, or arrange the parts of something*”²⁷. Przedstawione definicje pozwalają wywnioskować, że za pojęciem „struktury” kryje się jedna większa całość, w ramach której należy wyróżnić wiele pomniejszych elementów. Dopiero połączenie mniejszych elementów w jedną całość przynosi oczekiwane skutki.

Pojęcie „infrastruktury” w WSJP PAN jest rozumiane jako „urządzenia i instytucje umożliwiające sprawne działanie gospodarce i społeczeństwu”²⁸. Dodatkowo podkreślono jej użyteczny charakter, wskazując na ewentualne wykorzystanie pojęcia „infrastruktura”, np. infrastruktura drogowa, infrastruktura kolejowa, infrastruktura informatyczna²⁹. W SJP PWN oprócz pojęcia „infrastruktury”, które zdefiniowano jako „urządzenia i instytucje usługowe niezbędne do należytego funkcjonowania społeczeństwa i produkcyjnych działów gospodarki”, pojawiają się również pojęcia „infrastruktura ekonomiczna” oraz „infrastruktura społeczna”³⁰. Infrastruktura ekonomiczna to „infrastruktura obejmująca usługi w zakresie transportu, komunikacji, energetyki itp.”, a infrastruktura społeczna jest definiowana jako „infrastruktura obejmująca usługi w dziedzinie prawa, oświaty, służby zdrowia itp.”³¹. W języku angielskim pojęcie „infrastruktury” jest definiowane bardzo podobnie do znaczenia przyjętego w języku polskim. Zgodnie z Oxford Advanced Learner's Dictionary „*infrastructure*” to „*the basic systems and services that are necessary for a country or an organization to run smoothly, for example buildings, transport and water and power supplies*”³². Natomiast Cambridge Dictionary ten sam termin określa jako „*the basic systems and services, such as transport and power supplies, that a country or organization uses in order*

²⁵ *Structure*, https://www.oxfordlearnersdictionaries.com/definition/english/structure_1?q=structure (dostęp: 5.06.2024).

²⁶ *Structure*, <https://dictionary.cambridge.org/dictionary/english/structure> (dostęp: 5.06.2024).

²⁷ *Tamże*.

²⁸ *Infrastruktura*, https://wsjp.pl/haslo/do_druku/42645/infrastruktura (dostęp: 5.06.2024)

²⁹ *Tamże*.

³⁰ *Infrastruktura*, <https://sjp.pwn.pl/szukaj/infrastruktura.html> (dostęp: 5.06.2024).

³¹ *Tamże*.

³² *Infrastructure*, <https://www.oxfordlearnersdictionaries.com/definition/english/infrastructure?q=infrastructure> (dostęp: 5.06.2024).

to work effectively” oraz „the basic structure of an organization or system which is necessary for its operation, esp. public water, energy, and systems for communication and transport”³³. Powyższe definicje uwidaczniają zakres zarówno przedmiotowy, jak i podmiotowy infrastruktury. Przede wszystkim infrastruktura jest zbiorem niezależnie działających od siebie systemów, urządzeń i instytucji, np. systemy energetyczne, systemy transportowe, wodociągi (aspekt podmiotowy). Jednak w połączeniu ze sobą te systemy, urządzenia czy instytucje tworzą nie tylko strukturę niezbędną dla działania państwa, ale również strukturę do bezpiecznego i sprawnego życia jego obywateli (aspekt podmiotowy).

Z kolei pojęcie „krytyczny” wywodzi się z języka greckiego – *kritikós*, co oznacza osądzający. Również w słownikach języka polskiego pojęcie to definiuje się między innymi jako „surowo lub negatywnie oceniający kogoś lub coś”³⁴. Idąc za WSJP PAN, krytyczny to także „taki, który wyraża krytykę - ocenę wskazującą, że coś nie ma wartości, nie jest prawdziwe lub jest niewłaściwe w danej sytuacji” czy „związany z umiejętnością dokonywania krytyki - działania polegającego na tym, że postrzega się jakąś rzecz lub zjawisko z wykorzystaniem różnorodnych kryteriów, aby następnie ocenić je jako całość lub ze wskazaniem na poszczególne elementy”³⁵. Z powyższego wynika, że w języku polskim „krytyczny” odnosi się tylko i wyłącznie do sposobu wyrażania swojej opinii lub podejmowania oceny pewnych zachowań. Analiza przywołanych definicji jasno wskazuje, że „krytyczny” w jego potocznym znaczeniu nie odnosi się do określenia czegoś ważnego czy niezbędnego.

Pojęcie „krytyczny” odmiennie jednak kształtuje się w języku angielskim. Oczywiście tak samo jak w języku polskim jest rozumiane jako „expressing disapproval - saying what you think is bad about somebody/something”³⁶ czy „giving or relating to opinions or judgments on books, plays, films, etc.”³⁷, jednak Cambridge Dictionary jako *critical* rozumie także „of the greatest importance” oraz „extremely important to the progress or success of something”³⁸. Zgodnie z przywołanymi definicjami pojęcie „krytyczny” odnosi się głównie do wyrażania swojej opinii, opisywania sytuacji lub zachowań. W mniejszym stopniu, i tylko w języku angielskim, pojęcie „krytyczny” definiuje również ważność czy istotność danego zjawiska.

³³ *Infrastructure*, <https://dictionary.cambridge.org/dictionary/english/infrastructure> (dostęp: 5.06.2024).

³⁴ *Krytyczny*, <https://sjp.pwn.pl/szukaj/krytyczny.html> (dostęp: 5.06.2024).

³⁵ *Krytyczny*, https://wsjp.pl/haslo/do_druku/36941/krytyczny (dostęp: 5.06.2024).

³⁶ *Critical*, <https://www.oxfordlearnersdictionaries.com/definition/english/critical?q=critical> (dostęp: 5.06.2024).

³⁷ *Critical*, <https://dictionary.cambridge.org/dictionary/english/critical> (dostęp: 5.06.2024).

³⁸ *Tamże*.

Podsumowując powyższe należy przyjąć, że infrastruktura krytyczna stanowi zbiór systemów, urządzeń oraz instytucji, które zapewniają państwu, jak i jego obywatelom możliwość sprawnego funkcjonowania, ale także roztaczają nad nimi szeroko rozumiany parasol bezpieczeństwa. Rozumie się przez to zarówno bezpieczeństwo na podstawowym poziomie jak dostęp do żywności, wody pitnej, ale również dostęp do nowoczesnych usług, jak usługi komunikacyjne czy usługi informatyczne.

Na potrzeby niniejszej rozprawy przyjmuje się, że „infrastruktura krytyczna” odnosi się do wszystkich systemów państwowych oraz powiązanych z nią systemów sektora prywatnego, które ze względu na swoją ważność służą zapewnieniu bezpieczeństwa państwa i jego obywateli.

1.3 Termin „infrastruktura krytyczna” jako termin języka prawnego

W wymiarze prawa międzynarodowego kluczowym momentem dla zdefiniowania pojęcia infrastruktury krytycznej było przyjęcie na forum UE Dyrektywy Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dyrektywa 2008/114/WE)³⁹. Impulsem do uchwalenia aktu prawnego mającego na celu uregulowanie ochrony infrastruktury krytycznej w granicach UE był wystosowany 20 października 2004 r. przez Komisję Europejską (KE) komunikat do Rady UE (Rada) i Parlamentu Europejskiego (PE) pt. „Ochrona infrastruktury strategicznej w walce z terroryzmem”⁴⁰. Celem Komunikatu było przygotowanie przez KE zarysu działań ochrony infrastruktury strategicznej (w oficjalnym tłumaczeniu na język polski występuje pojęcie infrastruktury strategicznej, które jest tożsame z pojęciem infrastruktury krytycznej) oraz wskazanie dodatkowych środków, które mogłyby wspomóc istniejące już środki w ochronie infrastruktury strategicznej⁴¹. W Komunikacie KE zdefiniowała infrastrukturę krytyczną jako zakłady fizyczne i urządzenia technologii informacyjnych, sieci, usługi i aktywa, których zakłócenie pracy lub zniszczenie miałyby poważny wpływ na zdrowie, bezpieczeństwo lub dobrobyt ekonomiczny obywateli lub na skuteczność funkcjonowania rządów w państwach członkowskich⁴². Na podstawie Komunikatu

³⁹ Dyrektywa Rady 2008/114/WE w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, 8.12.2008, Dz. Urz. UE L 345/75 z 23.12.2008.

⁴⁰ *Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism*, 20.10.2004, COM/2004/0702 final, <https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52004DC0702> (dostęp: 5.06.2024).

⁴¹ *Tamże*, s. 3.

⁴² *Tamże*, s. 3-4.

infrastruktura krytyczna obejmuje swym zakresem szereg systemów wpływających na bezpieczeństwo państwa oraz jego obywateli. Poniższa tabela prezentuje przykładowe elementy poszczególnych systemów infrastruktury strategicznej.

Tabela 1. Systemy infrastruktury strategicznej

System	Przykład
Instalacje i sieci energetyczne	Produkcja energii elektrycznej, ropy naftowej i gazu, magazyny i rafinerie, system transmisji i dystrybucji
Technologie komunikacyjne i informacyjne	Telekomunikacja, radio i telewizja, oprogramowanie, sprzęt i sieci komputerowe, w tym Internet
Finanse	Bankowość, papiery wartościowe i inwestycje
Opieka zdrowotna	Szpitala, zakłady opieki zdrowotnej i punkty krwiodawstwa, laboratoria i farmaceutyki, poszukiwania i ratownictwo, pogotowie ratunkowe
Żywność	Bezpieczeństwo, środki produkcji, dystrybucja hurtowa i przemysł spożywczy
Woda	Tamy, zbiorniki, oczyszczalnie i sieci wodociągowe
Transport	Lotniska, porty, urządzenia intermodalne, sieci kolejowe i tranzytu masowego, systemy kontroli ruchu
Produkcja, składowanie i transport niebezpiecznych towarów	Materiały chemiczne, biologiczne, radiologiczne i nuklearne
Rząd	Usługi podstawowe, urządzenia, sieci informacyjne, aktywa i kluczowe krajowe lokalizacje i pomniki

Źródło: Opracowanie własne na podstawie: *Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism*, 20.10.2004, COM/2004/0702 final, <https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52004DC0702> (dostęp: 5.06.2024), s. 4.

Jak wskazuje KE powyższe elementy stanowią jedynie przykład tego co wchodzi w zakres infrastruktury krytycznej, a szczegółowy i pełny wykaz elementów infrastruktury krytycznej powinien zostać opracowany zarówno na szczeblu unijnym, jak i w prawie wewnętrznym każdego z państw członkowskich UE⁴³. O tym jaki system powinien zostać zaliczony do infrastruktury krytycznej decyduje jego identyfikacja, poprzez zastosowanie trzech kryteriów:

1. zakres - utratę elementu strategicznej infrastruktury ocenia się na podstawie wielkości obszaru geograficznego, który mógłby zostać dotknięty jego utratą lub niedostępnością – międzynarodowy, krajowy, prowincjonalny/terytorialny lub lokalny;

⁴³ *Tamże*, s. 4.

2. waga - stopień wpływu lub utraty można ocenić jako: żaden, minimalny, umiarkowany lub poważny. Do kryteriów, które można wykorzystać do oceny potencjalnej wagi, należą:
 - a. wpływ społeczny (wielkość dotkniętej populacji, utrata życia, choroba, poważne uszkodzenie ciała, ewakuacja),
 - b. wpływ gospodarczy (oddziaływanie na PKB, znaczenie strat gospodarczych i/lub pogorszenie produktów lub usług),
 - c. wpływ ekologiczny (wpływ na społeczeństwo i środowisko),
 - d. współzależność (z innymi elementami infrastruktury strategicznej),
 - e. wpływ polityczny (zaufanie w umiejętności rządu);
3. skutki czasowe - to kryterium określa, w jakim momencie utrata elementu mogłaby mieć poważny wpływ społeczny, gospodarczy, ekologiczny lub polityczny⁴⁴.

Na podstawie definicji przedstawionej przez KE oraz biorąc pod uwagę kryteria identyfikujące systemy jako infrastrukturę strategiczną należy uznać, że poszczególne systemy, potencjalnie zaliczane do infrastruktury strategicznej, są obecnie obsługiwane nie tylko przez państwo, ale również mogą być obsługiwane przez sektor prywatny. Szczególnie widoczne jest to w systemach komunikacyjnych i informatycznych, czy finansowych. W Polsce, w 2022 roku prawie cztery tysiące przedsiębiorców świadczyło usługi telekomunikacyjne, a większość z nich prowadziła działalność gospodarczą jednoosobowo⁴⁵. W przypadku usług finansowych na rynku funkcjonowało prawie 600 podmiotów świadczących usługi bankowe, w tym 30 banków komercyjnych⁴⁶. Dopuszczenie do zarządzania systemami infrastruktury strategicznej podmiotów prywatnych nie zwalania podmiotów publicznych z odpowiedzialności za zapewnienie im bezpieczeństwa. Wręcz przeciwnie, podmioty publiczne powinny być w pełni zaangażowane w zapewnienie bezpieczeństwa systemom zarządzanym przez podmioty prywatne⁴⁷. Przede wszystkim wynika to ze skutków jakie niesie ze sobą zniszczenie lub uszkodzenie infrastruktury strategicznej, np. brak komunikacji pomiędzy kluczowymi organami administracji rządowej czy brak dostępu do żywności lub wody pitnej dla obywateli. Co więcej, organy administracji publicznej, w szczególności

⁴⁴ *Tamże*, s. 5.

⁴⁵ Urząd Komunikacji Elektronicznej, *Raport o stanie rynku telekomunikacyjnego w 2022 roku*, Warszawa 2023, <https://bip.uke.gov.pl/raporty/raport-o-stanie-rynku-telekomunikacyjnego-za-2022-rok,78.html> (dostęp: 5.06.2024), s. 10.

⁴⁶ Komisja Nadzoru Finansowego, *Informacja na temat sytuacji sektora bankowego w 2022 roku*, Warszawa 2023, https://www.knf.gov.pl/?articleId=85173&p_id=18 (dostęp: 5.06.2024), s. 5.

⁴⁷ UE, *Communication from the Commission...*, s. 4.

te związane z zapewnieniem bezpieczeństwa, jak policja czy straż pożarna, mają szersze uprawnienia w zakresie zapobiegania atakom na infrastrukturę krytyczną bądź zapobiegania negatywnym skutkom takich ataków⁴⁸.

Cztery lata po wydaniu Komunikatu KE została przyjęta Dyrektywa 2008/114/WE, która jako pierwszy akt normatywny o randze międzynarodowej, zdefiniowała pojęcie infrastruktury krytycznej i nakreśliła ramy jej ochrony⁴⁹. Widoczne są tu wpływy wydanego w 2004 roku Komunikatu KE. Przede wszystkim podobieństwo widać w definicji infrastruktury krytycznej, gdyż Dyrektywa 2008/114/WE definiuje ją jako składnik, system lub część infrastruktury zlokalizowane na terytorium państw członkowskich UE, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz których zakłócenie lub zniszczenie miałyby istotny wpływ na dane państwo członkowskie w wyniku utraty tych funkcji (art. 2 lit. a Dyrektywy). Jednak w odróżnieniu od Komunikatu KE, Dyrektywa 2008/114/WE wprowadziła też pojęcie europejskiej infrastruktury krytycznej, która zdefiniowano jako infrastrukturę krytyczną zlokalizowaną na terytorium państw członkowskich, której zakłócenie lub zniszczenie miałyby istotny wpływ na co najmniej dwa państwa członkowskie (art. 2 lit. b Dyrektywy). To, czy wpływ jest istotny, ocenia się w odniesieniu do kryteriów przekrojowych. Obejmuje to skutki wynikające z międzysektorowych współzależności z innymi rodzajami infrastruktury. Istotną różnicą pomiędzy infrastrukturą krytyczną zdefiniowaną w Komunikacie KE a definicją europejskiej infrastruktury krytycznej z Dyrektywy 2008/114/WE jest ilość systemów zaliczanych do infrastruktury krytycznej. Pojęcie europejskiej infrastruktury krytycznej skupia się przede wszystkim na dwóch sektorach – energetyce oraz transporcie⁵⁰. Oczywiście, to w gestii państw członkowskich leży rozpoznanie poszczególnych sektorów potencjalnie zaliczanych do infrastruktury krytycznej, natomiast w Dyrektywie 2008/114/WE to właśnie tylko te dwa sektory zostały wskazane jako europejska infrastruktura krytyczna. Dyrektywa 2008/114/WE wprowadziła czteroetapową procedurę identyfikującą potencjalne sektory europejskiej infrastruktury krytycznej:

⁴⁸ Szczegółowe standardy ochrony infrastruktury krytycznej zostaną przedstawione w rozdziale III niniejszej rozprawy.

⁴⁹ R. Maciejewski, *Ochrona infrastruktury krytycznej – narracje prawne i politologiczne*, FNCE Sp. z o.o., Poznań 2019, s. 197.

⁵⁰ *Załącznik I do Dyrektywa Rady 2008/114/WE w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony*, 8.12.2008, Dz. Urz. UE L 345/75 z 23.12.2008.

1. etap I - każde państwo członkowskie stosuje kryteria sektorowe w celu dokonania pierwszej selekcji infrastruktury krytycznej w danym sektorze;
2. etap II - każde państwo członkowskie stosuje definicje infrastruktury krytycznej zgodnie z art. 2 lit. a) Dyrektywy w odniesieniu do potencjalnej europejskiej infrastruktury krytycznej rozpoznanej w etapie 1;
3. etap III - każde państwo członkowskie stosuje transgraniczny element definicji europejskiej infrastruktury krytycznej zgodnie z art. 2 lit. b) Dyrektywy w odniesieniu do potencjalnej europejskiej infrastruktury krytycznej, która przeszła dwa pierwsze etapy tej procedury. Potencjalna europejska infrastruktura krytyczna, która jest zgodna z tą definicją, przechodzi następny etap tej procedury. W przypadku infrastruktury świadczącej niezbędne usługi bierze się pod uwagę to, czy dostępne są alternatywy, a także czas trwania zakłócenia/naprawy;
4. etap IV - każde państwo członkowskie stosuje kryteria przekrojowe w odniesieniu do pozostałej potencjalnej europejskiej infrastruktury krytycznej. Kryteria przekrojowe uwzględniają: rozmiar strat oraz – w przypadku infrastruktury świadczącej niezbędne usługi – to, czy dostępne są alternatywy, a także czas trwania zakłócenia/naprawy. Potencjalna europejska infrastruktura krytyczna, która nie spełnia kryteriów przekrojowych nie będzie uważana za europejską infrastrukturę krytyczną⁵¹.

Z uwagi na to, że europejska infrastruktura krytyczna oddziałuje na co najmniej dwa państwa członkowskie, w przypadku identyfikacji jednego z powyższych sektorów jako europejskiej infrastruktury krytycznej, państwo członkowskie, które dokonało tej identyfikacji powinno poinformować inne zainteresowane państwa członkowskie o tej identyfikacji. Istotną rolę w identyfikacji europejskiej infrastruktury krytycznej pełniła KE. Na podstawie art. 3 Dyrektywy 2008/114/WE mogła ona pomóc państwom członkowskim, na ich wniosek, w rozpoznaniu potencjalnej europejskiej infrastruktury krytycznej. Ponadto KE mogła zwrócić uwagę odpowiednich państw członkowskich na istnienie potencjalnej infrastruktury krytycznej, wobec której można uznać, że spełnia ona kryteria wymagane do wyznaczenia jej jako europejskiej infrastruktury krytycznej. Tak samo jak w Komunikacie KE, w art. 3 ust.

⁵¹ Załącznik III do Dyrektywa Rady 2008/114/WE w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, 8.12.2008, Dz. Urz. UE L 345/75 z 23.12.2008.

2 Dyrektywa 2008/114/WE wprowadziła kryteria umożliwiające identyfikację potencjalnej europejskiej infrastruktury krytycznej – kryteria przekrojowe. Zalicza się do nich:

1. kryterium ofiar w ludziach - oceniane w odniesieniu do ewentualnej liczby ofiar śmiertelnych lub liczby rannych;
2. kryterium skutków ekonomicznych - oceniane w odniesieniu do wielkości strat ekonomicznych lub pogorszenia towarów lub usług, w tym potencjalnych skutków ekologicznych;
3. kryterium skutków społecznych - oceniane w odniesieniu do wpływu na zaufanie opinii publicznej, cierpień fizycznych i zakłócenia codziennego życia, w tym utraty podstawowych usług.

Powyższe kryteria obejmują swym zakresem jedynie wycinek z kryteriów zaproponowanych w Komunikacie KE. Jednak skupiają się na bezpieczeństwie nie samego państwa a jego obywateli, szczególnie widać to w zakresie kryterium ewentualnej liczby ofiar czy cierpienia fizycznego. W Dyrektywa 2008/114/WE nie określono progów dla poszczególnych kryteriów. To KE wraz z państwami członkowskimi powinna ustalić przybliżone progi, które mają być stosowane do identyfikacji europejskiej infrastruktury krytycznej (informacje na temat są niejawne, zob. art. 3 ust. 2 Dyrektywy 2008/114/WE).

Dostrzegając ograniczony charakter ochrony wynikającej z Dyrektywy 2008/114/WE, obejmujący tylko dwa sektory infrastruktury krytycznej – energetykę i transport, na forum UE Parlament i Rada uchwaliły Dyrektywę 2022/2557 z dnia 14 grudnia 2022 roku w sprawie odporności podmiotów krytycznych i uchylającą dyrektywę Rady 2008/114/WE (Dyrektywa 2022/2557)⁵². Przyjęty akt stanowi odpowiedź UE na zwiększone zagrożenie bezpieczeństwa infrastruktury krytycznej, obejmującej już nie tylko energetykę i transport, ale też inne sektory.

W przeciwieństwie do Dyrektywy 2008/114/WE w Dyrektywie 2022/2557 nie wprowadzono pojęcia europejskiej infrastruktury krytycznej. Zamiast tego, obok pojęcia infrastruktury krytycznej, za którą rozumie się składnik, obiekt, sprzęt, sieć lub system lub część składnika, obiektu, sprzętu, sieci lub systemu, niezbędne do świadczenia usługi kluczowej (art. 2 pkt 4 Dyrektywy), wprowadzono dwa pojęcia – podmiotu krytycznego i usługi kluczowej. Za podmiot krytyczny uznano podmiot publiczny lub prywatny zidentyfikowany przez państwo członkowskie zgodnie z art. 6 Dyrektywy jako należący do jednej z kategorii

⁵² Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE, 14.12.2022, Dz. Urz. UE L 333/164 z 27.12.2022.

wymienionych w trzeciej kolumnie tabeli w załączniku (art. 2 pkt 1 Dyrektywy). Natomiast jako usługę kluczową rozumie się usługę, która ma decydujące znaczenie dla utrzymania niezbędnych funkcji społecznych, niezbędnej działalności gospodarczej, zdrowia i bezpieczeństwa publicznego lub środowiska (art. 2 pkt 5 Dyrektywy). Dla prawidłowej identyfikacji podmiotów krytycznych oraz usług kluczowych do Dyrektywy załączono zestawienie sektorów, podsektorów oraz kategorii podmiotów, które są objęte uregulowaniami Dyrektywy, co zaprezentowano w poniższej tabeli:

Tabela 2. Sektory, podsektory i kategorie podmiotów dla Dyrektywy 2022/2557

Sektor	Podsektor	Kategoria podmiotów
Energia*	Energia elektryczna	Przedsiębiorstwa energetyczne
	System ciepłowniczy i chłodniczy	Operatorzy systemów ciepłowniczych lub systemów chłodniczych
	Ropa naftowa	Operatorzy ropociągów
	Gaz	Przedsiębiorstwa dostarczające gaz
	Wodór	Operatorzy produkcji, magazynowania i przesyłu wodoru
Transport*	Transport lotniczy	Przewoźnicy lotniczy
	Transport kolejowy	Przedsiębiorstwa kolejowe
	Transport wodny	Armatorzy śródlądowego, morskiego i przybrzeżnego wodnego transportu pasażerów i towarów
	Transport drogowy	Organy administracji drogowej odpowiedzialne za zarządzanie ruchem drogowym
	Transport publiczny	Podmioty świadczące usługi publiczne w zakresie transportu pasażerskiego
Bankowość	—	Instytucje kredytowe

Sektor	Podsektor	Kategoria podmiotów
Infrastruktura rynków finansowych	–	Operatorzy systemów obrotu MTF ⁵³ lub OTF ⁵⁴
Zdrowie*	–	Podmiot świadczący opiekę zdrowotną na terenie państwa członkowskiego
Woda pitna	–	Dostawcy i dystrybutorzy wody przeznaczonej do spożycia przez ludzi
Ścieki	–	Przedsiębiorstwa zbierające, odprowadzające lub oczyszczające ścieki komunalne, ścieki bytowe i ścieki przemysłowe
Infrastruktura cyfrowa*	–	Dostawcy usług chmurowych
Administracja publiczna	–	Podmioty administracji publicznej w ramach instytucji rządowych na szczeblu centralnym zdefiniowane przez państwa członkowskie zgodnie z prawem krajowym
Przestrzeń kosmiczna	–	Operatorzy infrastruktury naziemnej będącej własnością państw członkowskich lub podmiotów prywatnych i przez nie zarządzanej i obsługiwanej, którzy wspierają świadczenie usług kosmicznych
Produkcja, przetwarzanie i dystrybucja żywności	–	Przedsiębiorstwa spożywcze zajmujące się wyłącznie logistyką i dystrybucją hurtową oraz produkcją przemysłową i przetwórstwem przemysłowym na dużą skalę

⁵³ Wielostronna platforma obrotu definiowana jako system wielostronny prowadzony przez firmę inwestycyjną lub operatora rynku, który kojarzy wiele deklaracji gotowości zakupu i sprzedaży instrumentów finansowych przez osoby trzecie – w systemie i zgodnie ze swoimi zasadami niemającymi charakteru uznaniowego – w sposób skutkujący zawarciem kontraktu, zob. art. 4 pkt 22 *Dyrektywy Parlamentu Europejskiego i Rady 2014/65/UE w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE*, 15.05.2014, Dz. Urz. UE L 173/349 z 12.6.2014.

⁵⁴ Zorganizowana platforma obrotu definiowana jako system wielostronny niebędący rynkiem regulowanym ani MTF, w ramach którego umożliwia się interakcję wielu deklaracji gotowości zakupu i sprzedaży obligacji, strukturyzowanych produktów finansowych, uprawnień do emisji lub instrumentów pochodnych, składanych przez osoby trzecie w sposób skutkujący zawarciem kontraktu, zob. art. 4 pkt 22 *Dyrektywy 2014/65/UE*.

* Dla wskazanych sektorów Dyrektywa 2022/2557 przewiduje większą ilość kategorii podmiotów, jednak dla celu poglądowego wskazano jeden przykład takiego podmiotu.

Źródło: Opracowanie własne na podstawie załącznika do Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE, 14.12.2022, Dz. Urz. UE L 333/164 z 27.12.2022.

Państwa członkowskie, opierając się na sektorach i podsektorach wskazanych w załączniku do Dyrektywy 2022/2557, w terminie do 17 lipca 2026 roku są zobowiązane zidentyfikować podmioty krytyczne występujące w danym państwie. Dodatkowo, przy identyfikacji podmiotów krytycznych, państwa członkowskie powinny kierować się trzema warunkami określonymi w art. 6 pkt 2 Dyrektywy 2022/2557. Po pierwsze, za podmiot krytyczny należy uznać podmiot, który świadczy co najmniej jedną usługę kluczową. Po drugie, podmiot prowadzi działalność na terytorium tego państwa członkowskiego i jego infrastruktura krytyczna znajduje się na terytorium tego państwa członkowskiego. Po trzecie, zakłócenie działalności podmiotu krytycznego miałoby istotne skutki zakłócające dla świadczenia przez podmiot co najmniej jednej usługi kluczowej lub dla świadczenia innych usług kluczowych w sektorach określonych w załączniku, które zależą od tej usługi kluczowej lub tych usług kluczowych. Ponadto podmioty zidentyfikowane przez państwo jako podmioty krytyczne powinny zostać o tym fakcie poinformowane w terminie jednego miesiąca od identyfikacji.

Przyjęcie Dyrektywy 2022/2557 stanowiło krok w zapewnieniu skuteczniejszej ochrony infrastruktury krytycznej w ramach UE. Przede wszystkim rozszerzono katalog o dziewięć nowych sektorów objętych tą ochroną (Dyrektywa 2008/114/WE regulowała ochronę tylko dwóch sektorów). Co więcej, w 2023 roku KE przyjęła Rozporządzenie delegowane 2023/2450 uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2557 przez ustanowienie wykazu usług kluczowych⁵⁵, w którym wskazała szeroki zakres usług kluczowych. Co istotne, katalog ma charakter otwarty, a państwa członkowskie UE przy identyfikacji podmiotów kluczowych nie powinny się ograniczać tylko do usług tam wskazanych.

Pomimo, że pojęcie infrastruktury krytycznej jest używane już od ponad dwudziestu lat, jak do tej pory tylko UE zdecydowała się na jego zdefiniowanie, jednocześnie wprowadzając

⁵⁵ Rozporządzenie delegowane Komisji (UE) 2023/2450 uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2557 przez ustanowienie wykazu usług kluczowych, 25.07.2023, Dz. Urz. UE L 2023/2450 z 30.10.2023.

skuteczne standardy ochrony infrastruktury krytycznej, wpływające na bezpieczeństwo państwa członkowskich.

W porównaniu do regulacji międzynarodowych, to prawo wewnętrzne poszczególnych państwa charakteryzuje się zdefiniowaniem infrastruktury krytycznej. W polskim systemie prawnym pojęcie infrastruktury krytycznej zostało zdefiniowane w Ustawie o zarządzaniu kryzysowym z 2007 roku (Ustawa o zarządzaniu kryzysowym)⁵⁶. Zgodnie ze słowniczkiem z art. 3 Ustawy za infrastrukturę krytyczną uważa się 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. Ustawa określiła również 11 systemów, które należy zaliczyć do infrastruktury krytycznej. Oprócz tego, słowniczek zawiera definicję ochrony infrastruktury krytycznej, za którą uważa się 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, a także szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie (zob. art. 3 Ustawy o zarządzaniu kryzysowym).

Prawidłowa ochrona infrastruktury krytycznej wymaga od instytucji oraz organów państwowych współpracy na różnych płaszczyznach działalności administracji publicznej. Jako podstawowe działanie należy wyróżnić przygotowanie przez Rządowe Centrum Bezpieczeństwa we współpracy z ministrami i kierownikami urzędów centralnych właściwych w sprawach bezpieczeństwa Narodowego Programu Ochrony Infrastruktury Krytycznej. Głównym celem dokumentu jest stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej (zob. art. 5b Ustawy o zarządzaniu kryzysowym), jednak sam program zawiera w sobie pośrednie cele, które są określane osobno każdego roku. W 2023 roku jako cele pośrednie wyznaczono: zdobycie określonego poziomu świadomości, wiedzy i kompetencji wszystkich uczestników Programu w zakresie znaczenia infrastruktury krytycznej dla sprawnego funkcjonowania państwa oraz sposobów i metod jej ochrony, wprowadzenie metodyki oceny ryzyka uwzględniającej pełny wachlarz zagrożeń, w tym metodyki postępowania z zagrożeniami o bardzo małym prawdopodobieństwie i katastrofalnych skutkach, wprowadzenie skoordynowanego i opartego na ocenie ryzyka

⁵⁶ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz. U. z 2007 r., nr 89, poz. 590.

podejścia do realizacji zadań z zakresu ochrony infrastruktury krytycznej, budowa partnerstwa między uczestnikami procesu ochrony infrastruktury krytycznej oraz wprowadzenie mechanizmów wymiany i ochrony informacji przekazywanych między uczestnikami procesu ochrony infrastruktury krytycznej⁵⁷.

Kluczowym etapem w zapewnianiu ochrony infrastruktury krytycznej jest dokładne wyznaczenie obiektów, urządzeń i systemów wchodzących w zakres infrastruktury krytycznej. Dzieje się to wieloetapowo, za pomocą metody, którą można przyrównać do działania sitka. Kryteria co wchodzi w zakres infrastruktury krytycznej ustaliło RCB wraz z ministrami i kierownikami urzędów centralnych, przy wsparciu przedsiębiorców prywatnych. Przede wszystkim należy wyróżnić dwa podstawowe kryteria: systemowe oraz przekrojowe⁵⁸. Pierwsze z nich określa ilościowo lub podmiotowo funkcje obiektu, urządzenia, instalacji lub usługi, których spełnienie może spowodować zaliczenie do infrastruktury krytycznej⁵⁹. Natomiast kryterium przekrojowe określa parametry odnoszące się do skutków zniszczenia bądź zaprzestania funkcjonowania obiektu, urządzenia, instalacji lub usługi, jak: ofiary w ludziach, skutki finansowe, czas odbudowy czy efekt międzynarodowy⁶⁰. Sama identyfikacja infrastruktury krytycznej odbywa się w trzech etapach:

Tabela 3. Etapy identyfikacji infrastruktury krytycznej

Etap	Czynności
Etap 1.	Zastosowanie kryteriów systemowych, celem dokonania pierwszej selekcji obiektów, instalacji, urządzeń lub usług, które potencjalnie mogłyby zostać uznane za infrastrukturę krytyczną w danym systemie.
Etap 2.	Przyrównanie definicji infrastruktury krytycznej z art. 3 pkt 2 Ustawy o zarządzaniu kryzysowym do danego obiektu, celem sprawdzenia, czy obiekt, urządzenie, instalacja lub usługa pełni kluczową rolę dla bezpieczeństwa państwa i jego obywateli oraz czy służy zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców.

⁵⁷ RCB, *Narodowy Program Ochrony Infrastruktury Krytycznej*, Warszawa 2023, s. 8.

⁵⁸ *Tamże*, s. 13.

⁵⁹ *Tamże*.

⁶⁰ *Tamże*.

Etap	Czynności
Etap 3.	Zastosowanie kryteriów przekrojowych do obiektów, urządzeń oraz systemów wyodrębnionych w etapach 1. i 2., celem oceny potencjalnych skutków zniszczenia lub zaprzestania funkcjonowania potencjalnej infrastruktury krytycznej.

Zródło: Opracowanie własne na podstawie: Rządowe Centrum Bezpieczeństwa, *Narodowy Program Ochrony Infrastruktury Krytycznej*, Warszawa 2023, s. 13-14.

Ze względu na kluczowe znaczenie dla bezpieczeństwa państwa, szczegółowe kryteria są publikowane jako niejawnny załącznik do NPOIK.

Obiekty, urządzenia czy systemy zidentyfikowane na podstawie procedury identyfikacji infrastruktury krytycznej są zaliczane do jednego z jedenastu sektorów wymienionych w art. 3 pkt 2 lit. a-k Ustawy o zarządzaniu kryzysowym. Do pierwszego sektora zalicza się system zaopatrzenia w energię i paliwa. Jest to jeden z kluczowych elementów prawidłowego działania państwa, gdzie zasób surowców energetycznych (np. ropa naftowa, gaz ziemny, węgiel kamienny) stanowi podstawę zabezpieczenia energetycznego państwa⁶¹. Wszystkie urządzenia techniczne oraz pozatechniczne elementy ich funkcjonowania, służące zapewnieniu bezpieczeństwa energetycznego są definiowane jako infrastruktura energetyczna⁶². System infrastruktury energetycznej jest tworzony przez urządzenia, które służą najpierw do pozyskania energii pierwotnej, a następnie jej przetwarzania, transportu i magazynowania⁶³. W związku ze złożonością oraz istotnością sektora energetycznego państwo powinno podjąć niezbędne kroki w celu zapewnienia jego bezpieczeństwa. Przez bezpieczeństwo energetyczne rozumie się stan gospodarki umożliwiający pokrycie bieżącego i perspektywicznego zapotrzebowania odbiorców na paliwa i energię w sposób technicznie i ekonomicznie uzasadniony, przy zachowaniu wymagań ochrony środowiska (art. 3 pkt 16 Ustawy z dnia 10 kwietnia 1997 r. Prawo energetyczne, dalej: Prawo energetyczne)⁶⁴. Ponadto Prawo energetyczne zdefiniowało pojęcie zagrożeń bezpieczeństwa dostaw energii elektrycznej, przez które rozumie się stan systemu elektroenergetycznego lub jego części, uniemożliwiający zapewnienie bezpieczeństwa pracy sieci elektroenergetycznej lub równoważenie dostaw energii elektrycznej z zapotrzebowaniem na tę energię (art. 3 pkt 16d Prawo energetyczne).

⁶¹ M. Molendowska, M. Ostrowska, P. Górski, *Infrastruktura krytyczna jako element bezpieczeństwa – wymiar europejski i krajowy*, Wydawnictwo Adam Marszałek, Toruń 2021, s.87.

⁶² J. Adamkiewicz, *Militarny kontekst bezpieczeństwa infrastruktury energetycznej*, w: P. Kwiatkiewicz, R. Szerbowski, K. Stańczyk, R. Sobków (red.), *Energetyka w kręgu bezpieczeństwa i techniki*, FNCE Sp. z o.o., Poznań 2019, s. 153.

⁶³ *Tamże*.

⁶⁴ Ustawa z dnia 10 kwietnia 1997 r. Prawo energetyczne, Dz. U. z 1997 r., nr 54, poz. 348.

Analizując przepisy o bezpieczeństwie energetycznym oraz biorąc pod uwagę jego zagrożenia należy stwierdzić, że bezpieczeństwo energetyczne stanowi szeroki zakres obowiązków państwa, gdzie oprócz posiadania zasobów energetycznych, konieczne jest zapewnienie bezpieczeństwa tym zasobom. Dzieje się to przez prowadzenie efektywnej infrastruktury energetycznej, jak utrzymanie w dobrym stanie technicznym urządzeń tej infrastruktury czy zapewnienie bezpieczeństwa fizycznego tym urządzeniom (np. ochrona fizyczna, ochrona kontrwywiadowcza). Podjęcie odpowiednich kroków zabezpieczających infrastrukturę energetyczną pozwala uniknąć zróżnicowanych zagrożeń. Przykładowo sektor energetyczny może być narażony na działania przyrody (np. awaria elektrowni jądrowej Fukushima Dai-Ichi w 2011 r.⁶⁵), błędy techniczne lub błąd człowieka (np. awaria elektrowni jądrowej w Czarnobylu⁶⁶), ale również akty terroryzmu lub działania militarne, również z wykorzystaniem zdolności cybernetycznych (np. rosyjski cyberatak na ukraińską sieć energetyczną w 2015 r.⁶⁷).

Drugim sektorem wymienionym w Ustawie o zarządzaniu kryzysowym jest system łączności. Zgodnie z definicją przedstawioną przez J. Milewskiego systemem łączności jest przekazywanie informacji, poprzez pocztę oraz telekomunikację, jak również radiofonie i telewizję⁶⁸. Jako telekomunikację należy rozumieć nadawanie, odbiór lub transmisję informacji, niezależnie od ich rodzaju, za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną⁶⁹. System łączności w idealny sposób przedstawia zależności rządzące infrastrukturą krytyczną, tj. relacje państwo-obywatel. Odpowiada za prawidłową komunikację pomiędzy państwem oraz obywatelem, pomiędzy strukturami państwowymi, ale również pomiędzy samymi obywatelami⁷⁰.

Trzeci sektor stanowi system sieci teleinformatycznych. Zgodnie z definicją wynikającą z art. 2 pkt 3 Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną⁷¹ przez systemy teleinformatyczne rozumie się zespół współpracujących ze sobą urządzeń

⁶⁵ Co wydarzyło się w elektrowni jądrowej Fukushima Dai-Ichi w Japonii 10 lat temu?, <https://www.gov.pl/web/polski-atom/co-wydarzylo-sie-w-elektrowni-jadrowej-fukushima-dai-ichi-w-japonii-10-lat-temu> (dostęp: 21.06.2024).

⁶⁶ *Assessments of the Radiation Effects from the Chornobyl Nuclear Reactor Accident*, <https://www.unscear.org/unscear/en/areas-of-work/chernobyl.html> (dostęp: 21.06.2024).

⁶⁷ Electricity Information Sharing and Analysis Center, *Analysis of the Cyber Attack on the Ukrainian Power Grid* Defense Use Case, Washington DC 2016, <https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf> (dostęp: 21.06.2024), s. IV.

⁶⁸ J. Milewski, *Identyfikacja infrastruktury krytycznej i jej zagrożeń*, „Zeszyty Naukowe AON” 2016, nr 4, s. 105.

⁶⁹ *Tamże*.

⁷⁰ *Tamże*.

⁷¹ Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz. U. z 2002 r., nr 144, poz. 1204.

informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego. Z kolei zgodnie z art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne⁷² siecią telekomunikacyjną są systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju. Prawidłowe działanie systemów teleinformatycznych jest możliwe dopiero, gdy wszystkie urządzenia zostaną połączone za pomocą sieci telekomunikacyjnej. Ich głównym zadaniem jest przekazywanie informacji, jednocześnie wysyłając i odbierając dane⁷³. W ramach wykonywania swoich zadań, organy administracji publicznej korzystają z systemów teleinformatycznych dedykowanych przetwarzaniu i gromadzeniu różnorodnych danych oraz z wydzielonych fizycznie lub logicznie, będących własnością organów administracji publicznej lub też dzierżawionych od operatorów sieci telekomunikacyjnych⁷⁴. Po raz kolejny pokazuje to jak usługi prywatne łączą się z usługami publicznymi, tym samym opierając się na wspólnej zależności.

Czwartym sektorem jest system finansowy. RCB pod pojęciem systemu finansowego rozumie ogół norm prawnych oraz zespół instytucji finansowych, których zadaniem jest gromadzenie, dzielenie i wydatkowanie zasobów pieniężnych państwa. Sprawnie funkcjonujący system finansowy ma decydujące znaczenie dla prawidłowego funkcjonowania państwa i społeczeństwa⁷⁵. W ramach systemu finansowego wyróżnia się cztery segmenty:

1. budżetowy - ogół norm prawnych oraz struktur organizacyjnych regulujących funkcjonowanie budżetu państwa i jednostek samorządu terytorialnego. Z budżetu państwa finansowane są wszystkie działania mające na celu wypełnienie ustawowych obowiązków państwa wobec obywatela;
2. bankowy - ogół norm prawnych regulujących zasady prowadzenia działalności bankowej, tworzenia i organizacji banków, oddziałów i przedstawicielstw banków

⁷² Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, Dz. U. z 2004 r., nr 171, poz. 1800.

⁷³ RCB, *Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik 1. Charakterystyka systemów infrastruktury krytycznej*, Warszawa 2013, s. 36.

⁷⁴ *Tamże*.

⁷⁵ *Tamże*, s. 37.

zagranicznych, a także oddziałów instytucji kredytowych oraz norm ostrożnościowych ustalanych przez Komisję Nadzoru Finansowego;

3. ubezpieczeniowy - reguluje tworzenie, podział i organizację rynku ubezpieczeniowego. Ubezpieczenia dzielą się na dwie kategorie - ubezpieczenia społeczne (mają na celu prewencyjną i ubezpieczeniową ochronę zdrowia, zdolności do wykonywania pracy oraz życia ludności, są przymusowe i powszechne) oraz ubezpieczenia na życie, osobowe i majątkowe (ten rodzaj działalności ubezpieczeniowej wykonują zakłady ubezpieczeń w oparciu o zezwolenia organu nadzoru. Zakład ubezpieczeń może wykonywać działalność ubezpieczeniową wyłącznie w formie spółki akcyjnej albo towarzystwa ubezpieczeń wzajemnych);
4. kapitałowy - dokonywany jest obrót średnio i długoterminowych instrumentów finansowych (np. akcje i obligacje). Obrót dokonuje się głównie na Giełdzie Papierów Wartościowych, która jest spółką akcyjną powołaną przez Skarb Państwa⁷⁶.

Następnym sektorem jest system zaopatrzenia w żywność. Jest to dziedzina gospodarki, na którą składa się wytworzenie środków produkcyjnych (np.: nawozy, pasze) i usług dla rolnictwa, produkcja i pozyskiwanie surowców żywnościowych (w rolnictwie, rybactwie, leśnictwie, łowiectwie), skup surowców żywnościowych, ich przechowywanie i transport, przetwórstwo surowców żywnościowych, obrót towarowy produktami żywnościowymi (magazynowanie i przechowywanie żywności, handel hurtowy i detaliczny, eksport i import) oraz system bezpieczeństwa żywności obejmujący wszystkie składowe łańcucha zaopatrzenia w żywność⁷⁷. Na bezpieczeństwo żywnościowe składa się szereg czynników, do których należy zaliczyć przede wszystkim dostęp do pożywienia ubogiej ludności, łańcuchy żywnościowe czy dystrybucja żywności⁷⁸. Organizacja Narodów Zjednoczonych ds. Wyżywienia i Rolnictwa definiuje bezpieczeństwo żywnościowe jako sytuację, w której wszyscy ludzie przez cały czas mają fizyczny, społeczny i ekonomiczny dostęp do wystraczającej, bezpiecznej i odżywczej żywności, zaspokajającej ich potrzeby żywieniowe i preferencje dla prowadzenia aktywnego i zdrowego życia⁷⁹. W związku z funkcją jaką pełni bezpieczeństwo żywnościowe, jest ono przedmiotem regulacji zarówno na poziomie krajowym, jak i poziomie międzynarodowym⁸⁰.

⁷⁶ *Tamże*, s. 37-40.

⁷⁷ *Tamże*, s. 42.

⁷⁸ *Tamże*.

⁷⁹ Organizacja Narodów Zjednoczonych ds. Wyżywienia i Rolnictwa, *Food Security. Policy Brief*, June 2006, Issue 2, https://www.fao.org/fileadmin/templates/faoitaly/documents/pdf/pdf_Food_Security_Cocept_Note.pdf (dostęp: 21.06.2024), s. 1.

⁸⁰ Zob. art. 11 ust. 2 lit. a-b *Międzynarodowego Paktu Praw Gospodarczych, Społecznych i Kulturalnych*, Nowy Jorku, 19.12.1966, Dz. U. z 1977, nr 38, poz. 169.

System zaopatrzenia w żywność jest jedną z podstawowych gałęzi gospodarki państwowej, przyczynia się do rozwoju ekonomicznego państwa, ale przede wszystkim zaspokaja podstawowe potrzeby obywateli⁸¹. Zgodnie z raportem Międzynarodowego Programu Żywnościowego za 2023 rok, prawie 300 milionów osób w 59 krajach cierpiało z powodu wysokiego poziomu głodu⁸². Jako jeden z głównych czynników wystąpienia głodu wskazuje się konflikty zbrojne. Ten problem widoczny jest na przykład w Sudanie czy Strefie Gazy⁸³. W związku z toczącym się od kwietnia 2023 roku konflikcie w Sudanie ponad 20 milionów osób stało w obliczu braku dostępu do żywności. Toczyący się od października 2023 roku konflikt pomiędzy Izraelem a Hamasem doprowadził do zagrożenia dla bezpieczeństwa żywnościowego obejmującego aż 2 miliony ludności Strefy Gazy. Powyższe sytuacje pokazują jak wrażliwy jest system zaopatrywania w żywność na sytuację konfliktu zbrojnego, tym samym wskazując krytyczny charakter tego systemu.

Do szóstego sektora zalicza się system zaopatrzenia w wodę. RCB definiuje ten sektor jako powiązane ze sobą przedsiębiorstwa i urządzenia pobierające, uszlachetniające, dostarczające i oczyszczające wodę dla ludności i przemysłu⁸⁴. Do głównego zadania systemu zaopatrzenia w wodę należy dostarczanie tego surowca w odpowiedniej ilości i jakości (zgodnie ze szczegółowymi przepisami) określonym odbiorcom, w szczególności obywatelom⁸⁵. Tak samo jak system zaopatrywania w żywność, systemy dostarczania wody są narażone na ataki, zarówno podczas konfliktu zbrojnego, jak również cyberataki poza konfliktem zbrojnym. W maju 2020 roku Iran przeprowadził cyberatak wymierzony w izraelski system wodociągowy, który został skutecznie zablokowany⁸⁶.

System ochrony zdrowia jest kolejnym sektorem zaliczanym do infrastruktury krytycznej na podstawie Ustawy o zarządzaniu kryzysowym. Pod pojęciem systemu ochrony zdrowia należy rozumieć zespół osób i instytucji mający za zadanie zapewnić opiekę zdrowotną ludności, a jego sprawne funkcjonowanie (wraz z systemem ratowniczym) jest gwarantem praw obywatela zapisanych w Konstytucji RP⁸⁷. Światowa Organizacja Zdrowia (WHO) definiuje system ochrony zdrowia jako formalne usługi zdrowia, do których zalicza się świadczenie

⁸¹ RCB, *Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik 1* ..., s. 42.

⁸² Światowy Program Żywnościowy, *Global Report on Food Crises (GRFC) 2024*, <https://www.fslnplatform.org/report/global-report-food-crises-2024/> (dostęp: 21.06.2024), s. 5.

⁸³ *Tamże*, s. 6.

⁸⁴ RCB, *Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik 1* ..., s. 58.

⁸⁵ M. Molendowska, M. Ostrowska, P. Górski, *Infrastruktura krytyczna* ..., s.131.

⁸⁶ *Izrael: odparto poważny cyberatak na system wodociągów*, <https://cyberdefence24.pl/polityka-i-prawo/izrael-odparto-powazny-cyberatak-na-system-wodociagow> (dostęp: 21.06.2024).

⁸⁷ RCB, *Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik 1* ..., s. 60.

profesjonalnej pomocy medycznej, działania z zakresu tzw. medycyny tradycyjnej, stosowanie leków (zarówno tych przepisanych przez lekarzy, jak i kupowanych „bez recepty”)⁸⁸. Dodatkowo, do systemu ochrony zdrowia zalicza się pozostałe czynności, które służą poprawie zdrowia, np. edukację zdrowotną⁸⁹. Głównym celem systemu ochrony zdrowia jest poprawa i ciągły rozwój zdrowia ludzkości, ale także ochrona przed nadmiernymi kosztami zabiegów i środków medycznych⁹⁰. Polski system ochrony zdrowia swoim zakresem obejmuje pięć podmiotów, którymi są: świadczeniobiorcy (pacjenci), instytucja ubezpieczenia zdrowotnego pełniąca funkcję płatnika (Narodowy Fundusz Zdrowia), świadczeniodawcy (podmioty wykonujące działalność leczniczą, zgodnie z art. 4 i 5 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej⁹¹), organy kontroli i nadzoru (np. Państwowa Inspekcja Sanitarna czy Rzecznik Praw Pacjenta) oraz Ministerstwo Zdrowia (organ wyznaczający kierunki polityki zdrowotnej kraju oraz posiadający uprawnienia kontrolne, a także działający przy nim konsultanci krajowi w poszczególnych specjalnościach medycznych)⁹².

Jak ważny jest sprawny i skuteczny system ochrony zdrowia pokazała pandemia COVID-19. Na podstawie danych WHO pandemia, która oficjalnie została ogłoszona w 2020 roku, swój szczyt osiągnęła w grudniu 2022 roku z potwierdzonymi 44 milionami osób zarażonych na całym świecie⁹³. W jej trakcie obiekty medyczne wielokrotnie stanowiły cel cyberataków, co miało przynieść podwójny efekt – zastraszenie ludności (motywowane politycznie) oraz chęć wzbogacenia się poprzez otrzymanie okupu za odblokowanie dostępu do sieci komputerowej szpital⁹⁴. Przykładem zastraszania ludności, powiązanim z rozpowszechnianiem dezinformacji w zakresie szkodliwości szczepionek przeciwko COVID-19, jest cyberatak z początku grudnia 2022 roku wymierzony w Europejską Agencję Leków, za który odpowiedzialny był najprawdopodobniej rosyjski wywiad cywilny⁹⁵. Chęcią zysku wykazały się natomiast osoby odpowiedzialne za cyberatak na szpital w Brnie z 13 marca

⁸⁸ WHO, *The World Health Report 2000. Health systems: Improving Performance*, Geneva 2000, s. 5.

⁸⁹ *Tamże*.

⁹⁰ *Tamże*, s. 8.

⁹¹ Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej, Dz. U. z 2011 r., nr 112, poz. 654.

⁹² RCB, *Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik I...*, s. 60

⁹³ *Number of COVID-19 cases reported to WHO*, <https://data.who.int/dashboards/covid19/cases> (dostęp: 21.06.2024).

⁹⁴ R. Łasa, *Cyberbezpieczeństwo służby zdrowia podczas pandemii COVID-19. Aspekty prawa międzynarodowego*, w: M. Halushchenko, Ł. D. Bartosik, M. Urbańczyk (red.), *Pandemia COVID-19. Aspekty polityczne, społeczne, ekonomiczne i prawne*, Wydawnictwo Naukowe ArchaeGraph Diana Łukomiak, Poznań 2022, s. 30.

⁹⁵ Por. *Cyberattack on the European Medicines Agency*, <https://www.ema.europa.eu/en/news/cyberattack-european-medicines-agency> (dostęp: 21.06.2024) oraz *Rosyjscy i chińscy hakerzy stali za atakami na Europejską Agencję Leków*, <https://www.cyberdefence24.pl/rosyjscy-i-chinscy-hakerzy-stali-za-atakami-na-europejska-agencje-lekow> (dostęp: 21.06.2024).

2020 roku, o czym świadczyć ma sposób w jakim go dokonano⁹⁶. Analiza udokumentowanych cyberataków podczas pandemii COVID-19, których celem był sektor służby zdrowia prowadzi do wniosków, że głównymi sprawcami byli pospolici przestępcy, niepowiązani politycznie z żadnym z państw, cechujący się często minimalnym doświadczeniem w działaniach hakerskich⁹⁷.

System transportowy jest uznawany za kolejny sektor infrastruktury krytycznej. Definiowany jest jako przemieszczanie ludzi, ładunków (przedmiot transportu) w przestrzeni przy wykorzystaniu odpowiednich środków transportu. Przemieszczanie dóbr, ludzi i usług stanowi jedną z podstawowych cech charakterystycznych dla współczesnej gospodarki i społeczeństwa, dlatego sprawnie funkcjonujący system transportowy stanowi jeden z filarów nowoczesnego państwa⁹⁸. Transport dzieli się na dwie kategorie. Pierwszą z nich jest transport pasażerski (komunikacja), natomiast druga kategoria to transport towarów (ładunków)⁹⁹. Ponadto transport może zostać podzielony z uwagi na jego rodzaj i drogę przewozową. Taki podział obejmuje: transport kolejowy, samochodowy, lotniczy, żeglugę śródlądową oraz żeglugę morską¹⁰⁰.

Następnym sektorem w ramach infrastruktury krytycznej jest system ratownictwa. Pod pojęciem systemu ratownictwa należy rozumieć ogół środków i przedsięwzięć organizacyjnych podejmowanych w celu ratowania zdrowia i życia, mienia i środowiska, znajdującym się w niebezpieczeństwie oraz przewidywania, rozpoznawania i likwidacji skutków zdarzeń. Razem z systemem ochrony zdrowia stanowi podstawę realizacji konstytucyjnych praw obywateli do ochrony ich życia i zdrowia¹⁰¹. Istotą ratownictwa jest jego powszechność, co oznacza, że ratownictwo jest prowadzone na każdym szczeblu administracji państwa oraz w każdym czasie – pokoju, wojny lub katastrofy¹⁰². W rozumieniu podmiotowym do ratownictwa zalicza się wszystkie służby, których głównym zadaniem jest niesienie pomocy

⁹⁶ Niezidentyfikowane osoby zaszyfrowały dane na serwerach szpitala, a przywrócenie prawidłowego działania systemu zajęło kilka tygodni, zob. *Brno University Hospital ransomware attack (2020)*, [https://cyberlaw.ccdcoe.org/wiki/Brno_University_Hospital_ransomware_attack_\(2020\)](https://cyberlaw.ccdcoe.org/wiki/Brno_University_Hospital_ransomware_attack_(2020)) (dostęp: 21.06.2024).

⁹⁷ Por. O. A. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, J. Spiegel, *The Law of Cyber-Attack*, „California Law Review”, 2012, vol. 100, no. 4, s. 833-835 oraz H. S. Lallie, L. A. Shepherd, J. R. C. Nurse, A. Erola, G. Epiphaniou, C. Maple, X. Bellekens, *Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic*, „Computers & Security”, 2021, vol. 105, no. 1, s. 12-13.

⁹⁸ RCB, *Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik 1...*, s. 62.

⁹⁹ *Tamże*.

¹⁰⁰ M. Molendowska, M. Ostrowska, P. Górski, *Infrastruktura krytyczna ...*, s.153.

¹⁰¹ *Tamże*, s. 164.

¹⁰² *Tamże*.

ludziom w sytuacjach zagrożenia życia i zdrowia, np. ratownictwo medyczne czy straż pożarna¹⁰³.

System zapewniający ciągłość działania administracji publicznej jest kolejnym sektorem infrastruktury krytycznej. Administrację publiczną definiuje się jako prawo władcze wykonywania zadań przypisywanych przez porządek prawny państwu i jego organom lub innym podmiotom wykonującym funkcje władcze¹⁰⁴. W ramach polskiego systemu prawnego wyróżnia się dwie główne gałęzie administracji publicznej – administrację rządową (np. Prezes Rady Ministrów wraz z pozostałymi ministrami, szefowie służb porządkowych i służb specjalnych – Komendant Główny Policji, Szef Agencji Bezpieczeństwa Wewnętrznego) oraz administrację samorządową (np. wójt, rada gminy)¹⁰⁵. Do głównych funkcji administracji publicznej należy zaliczyć funkcję porządkowo-reglamentacyjną (ochrona porządku publicznego i bezpieczeństwa zbiorowego), funkcję świadczenia usług publicznych lub ich świadczenia za pośrednictwem instytucji świadczących, należących do sektora publicznego oraz funkcję regulatora rozwoju gospodarczego (np. wydawanie zezwoleń, nakładanie ceł)¹⁰⁶.

Ostatnim sektorem wchodzącym w skład infrastruktury krytycznej jest system produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych. Ani przemysł chemiczny, ani przemysł jądrowy (promieniotwórczy) nie zostały zdefiniowane w polskim ustawodawstwie. Co więcej obecnie na terenie Polski nie istnieje żaden obiekt jądrowy wykorzystywany do produkcji energii elektrycznej, ani żaden obiekt funkcjonalnie powiązany z produkcją energii elektrycznej z wykorzystaniem technologii jądrowej¹⁰⁷. Odmienne kształtuje się sytuacja z przemysłem chemicznym. Produkcja chemiczna stanowi jeden z kluczowych sektorów gospodarki państwowej¹⁰⁸. Do tej gałęzi przemysłu zalicza się między innymi produkcję wyrobów farmaceutycznych, chemii gospodarczej czy nawozów sztucznych. Od momentu rozpoczęcia pełnoskalowej inwazji rosyjskiej na Ukrainę, ataki na obiekty przemysłowe stały się częścią „wojny hybrydowej” prowadzonej wobec Państw Zachodu przez Rosję. Przykładem jest rozbicie w 2024 roku, na terytorium Polski grupy sabotażystów,

¹⁰³ *Tamże*.

¹⁰⁴ RCB, *Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik 1 ...*, s. 70.

¹⁰⁵ *Tamże*.

¹⁰⁶ M. Molendowska, M. Ostrowska, P. Górski, *Infrastruktura krytyczna ...*, s.175-176.

¹⁰⁷ RCB, *Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik 1 ...*, s. 76.

¹⁰⁸ M. Molendowska, M. Ostrowska, P. Górski, *Infrastruktura krytyczna ...*, s.185.

działających na zlecenie rosyjskiego wywiadu, której celem było zniszczenie między innymi fabryki farb pod Wrocławiem¹⁰⁹.

Pojęcie infrastruktury krytycznej w prawie amerykańskim pojawiło się po raz pierwszy w 1996 roku wraz z zatwierdzeniem zarządzenia wykonawczego nr 13010 dot. ochrony infrastruktury krytycznej (ang. *Executive Order EO 13010 Critical Infrastructure Protection*, zarządzenie wykonawcze nr 13010)¹¹⁰. Zgodnie z postanowieniami tego zarządzenia za infrastrukturę krytyczną uznano obiekty i systemy, których niesprawność lub zniszczenie miałyby wyniszczający wpływ na obronę lub bezpieczeństwo gospodarcze Stanów Zjednoczonych. W tym zakresie wskazywano siedem kluczowych sektorów, tj.: telekomunikację, systemy elektroenergetyczne, magazynowanie i transport gazu oraz ropy, bankowość i finanse, system zaopatrzenia w wodę, służby ratownicze (m.in. ratownictwo medyczne, policja, straż pożarna) oraz ciągłość rządów (administracja publiczna). Jako główne zagrożenia dla powyższych systemów wskazano ataki fizyczne oraz cybernetyczne.

Przełomowym rokiem dla ochrony infrastruktury krytycznej w USA był 2001 rok, kiedy w życie weszła Ustawa o ochronie infrastruktury krytycznej (ang. *Critical Infrastructures Protection Act of 2001*), która zredefiniowała pojęcie infrastruktury krytycznej w amerykańskim systemie prawnym¹¹¹. Od tego momentu za infrastrukturę krytyczną uważa się systemy i aktywa, zarówno fizyczne, jak i wirtualne, tak istotne dla Stanów Zjednoczonych, że niesprawność lub zniszczenie takich systemów i aktywów miałoby osłabiający wpływ na bezpieczeństwo narodowe, bezpieczeństwo gospodarcze, zdrowie publiczne (zob. lit. e Ustawy o ochronie infrastruktury krytycznej). Na mocy Ustawy powołano Narodowe Centrum Symulacji i Analizy Infrastruktury (ang. *National Infrastructure Simulation and Analysis Center*), którego zadaniem jest wspieranie działań związanych z przeciwdziałaniem terroryzmowi, oceną zagrożeń i ograniczaniem ryzyka ataku na infrastrukturę krytyczną.

W Rosji nie wprowadzono do użycia terminu „infrastruktura krytyczna”¹¹². Natomiast stosuje się dwa pojęcia - obiekty o krytycznym znaczeniu oraz potencjalnie niebezpieczne

¹⁰⁹ *We Wrocławiu szykował sabotaż na zlecenie rosyjskich służb. Trafił w ręce ABW*, <https://infosecurity24.pl/sluzby-specjalne/agencja-bezpieczenstwa-wewnetrznego/we-wroclawiu-szykowal-sabotaz-na-zlecenie-rosyjskich-sluzb-trafil-w-rece-abw> (dostęp: 21.06.2024).

¹¹⁰ USA, *Executive Order EO 13010 Critical Infrastructure Protection*, 15.07.1996, <https://irp.fas.org/offdocs/eo13010.htm> (dostęp: 5.06.2024).

¹¹¹ *Tamże*.

¹¹² R. Łasa, *Międzynarodowe prawo humanitarne – bufor bezpieczeństwa pomiędzy infrastrukturą krytyczną a cyberatakiem*, w: M. Banasik, A. Rogozińska (red.), *Teoria i praktyka bezpieczeństwa międzynarodowego: kontekst rosyjski*, Wydawnictwo Difin S.A., Warszawa 2021, s. 271.

obiekty¹¹³. Pierwszy z nich odnosi się do obiektów, których „uszkodzenie lub zniszczenie doprowadziłoby do utraty kontroli nad tymi obiektami przez państwo oraz wpłynęłoby na bezpieczeństwo ludności”¹¹⁴. Natomiast potencjalnie niebezpieczne obiekty są „obiettami, w granicach których znajdują się budynki lub budowle o dużym stopniu odpowiedzialności lub takie, w których w jednym czasie może przebywać więcej niż pięć tysięcy osób”¹¹⁵.

W prawie rosyjskim zdecydowano się na pewnego rodzaju dualizm, który umożliwiłby objęcie ochroną tych obiektów, które w danym momencie spełniałyby określone przesłanki, na przykład obiekt, w którym w jednym czasie może przebywać ponad pięć tysięcy osób. W rosyjskim podejściu można zauważyć odejście od sztywnego wyznaczania ustawami co konkretnie wchodzi w zakres infrastruktury krytycznej, tak jak ma to miejsce w państwach zachodnich, które wyznaczają określone sektory wchodzące w skład infrastruktury krytycznej, np. sektor energetyczny¹¹⁶.

Najnowszymi regulacjami prawnymi dotyczącymi infrastruktury krytycznej mogą poszczycić się Chiny. W lipcu 2021 roku Rada Państwa opublikowała Rozporządzenie o ochronie infrastruktury krytycznej informatycznej (ang. *Security Protection Regulations on the Critical Information Infrastructure*)¹¹⁷. Zaznaczyć należy, że sama definicja infrastruktury krytycznej informatycznej w chińskim systemie prawnym istnieje już od 2017 roku, pomimo tego dopiero w 2021 roku uchwalono akt prawny regulujący kwestie jej ochrony.

Za infrastrukturę krytyczną informatyczną uważa się infrastrukturę z ważnych branż i sektorów, w tym komunikacji publicznej i usług informacyjnych, energetyki, transportu, systemu zaopatrzenia w wodę, finansów, usług publicznych i e-administracji, a także innych branż i sektorów, które mogą stanowić poważne zagrożenie dla bezpieczeństwa narodowego, środków do życia ludzi i interesu publicznego, jeśli ich dane zostaną uszkodzone, zniszczone lub dojdzie do ich wycieku¹¹⁸.

Pomimo tego, że chińskie przepisy prawne dotyczące ochrony infrastruktury krytycznej w kontekście zagrożeń płynących z cyberprzestrzeni są jednymi z najnowszych tego typu

¹¹³ C. Pursiainen, *Russia's Critical Infrastructure Policy: What do we Know About it?*, „European Journal for Security Research”, 2021, vol. 6, s. 25.

¹¹⁴ *Tamże*.

¹¹⁵ *Tamże*.

¹¹⁶ *Tamże*, s. 34.

¹¹⁷ *China Issues New Regulations to Protect the Critical Information Infrastructure*, <https://www.lw.com/thoughtLeadership/China-Issues-New-Regulations-to-Protect-the-Critical-Information-Infrastructure> (dostęp: 18.12.2022).

¹¹⁸ *China Issues Its First Network Security Law*, <https://www.lw.com/thoughtLeadership/LW-china-issues-first-network-security-law> (dostęp: 18.12.2022).

regulacji na świecie, to należy zauważyć, że większość państw pełniących kluczowe role w bezpieczeństwie międzynarodowym, np. Stany Zjednoczone, posiada takie regulacje już od kilkunastu lat.

1.4 Termin „infrastruktura krytyczna” jako termin języka prawniczego

W związku z dość ubogim zasobem definicyjnym infrastruktury krytycznej mającym swe oparcie w obowiązującym prawie, zarówno tym krajowym, jak i międzynarodowym, pojęcie infrastruktury krytycznej jest obecnie definiowane głównie na gruncie języka prawniczego. W szczególności dużą rolę odgrywają tutaj organizacje międzynarodowe oraz doktryna. W mniejszym stopniu problematyka infrastruktury krytycznej jest poruszana w orzecznictwie sądów, gdzie zdecydowany prym wiodą sądy krajowe.

1.4.1 Ustalenie znaczenia pojęcia infrastruktura krytyczna w pracach organizacji międzynarodowych

Problematyka bezpieczeństwa infrastruktury krytycznej jest szeroko dyskutowana na forum organizacji międzynarodowych, głównie ze względu na rolę jaką odgrywa w krajowym oraz międzynarodowym systemie bezpieczeństwa. Jak wykazano wcześniej infrastruktura krytyczna wpływa na bezpieczeństwo nie tylko państwa na terytorium którego się znajduje, ale również może wpływać na bezpieczeństwo państw sąsiadujących. Szczególnie widać to na przykładzie państw członkowskich UE, gdzie tworzy się europejską infrastrukturę krytyczną. Jednak ze względu na swój charakter infrastruktura krytyczna pozostaje w centrum uwagi większości organizacji międzynarodowych, ponieważ współcześnie ma istotny wpływ na bezpieczeństwo obywateli oraz zdolności militarne państw. Dlatego też problematyką zidentyfikowania oraz ochrony infrastruktury krytycznej zajmują się takie organizacje międzynarodowe jak ONZ, NATO, OBWE czy OECD.

Wyzwaniem dla współczesnego świata, a także dla ochrony infrastruktury krytycznej są zagrożenia terrorystyczne. Ta problematyka zagrożeń terrorystycznych nabrała szczególnego znaczenia po 11 września 2001 roku, kiedy terroryści z Al-Kaidy dopuścili się ataków na Nowy Jork, Waszyngton oraz Pensylwanię¹¹⁹. Rada Bezpieczeństwa ONZ (RB ONZ) zdecydowanie potępiła ataki terrorystyczne wymierzone w USA, jednocześnie wzywając wszystkie państwa do walki z terroryzmem, który zagraża międzynarodowemu pokojowi i bezpieczeństwu¹²⁰.

¹¹⁹ RB ONZ, *Resolution 1368 (2001)*, 12.09.2001, S/RES/1368 (2001).

¹²⁰ RB ONZ, *Resolution 1373 (2001)*, 28.09.2001, S/RES/1373 (2001).

Państwa powinny w szczególności skupić się na walce z finansowaniem terroryzmu, w tym kryminalizować wszelkie zachowania mające na celu zbieranie i przekazywanie funduszy organizacjom terrorystycznym¹²¹. Celem usprawnienia walki z międzynarodowym terroryzmem oraz koordynacji działań wymienionych w rezolucji RB ONZ nr 1373, Rada postanowiła powołać do życia Komitet (ang. *Counter-Terrorism Committee* – CTC). W 2004 roku doszło do rozbudowy CTC, powołując tym samym organ plenarny, w skład którego wchodzi wszyscy członkowie RB ONZ, biuro składające się z przewodniczącego oraz wiceprzewodniczącego oraz organ wspierający biuro – Dyрекcję Wykonawczą ds. Zwalczania Terroryzmu (CTED)¹²². Szczególna rola przypadła Dyrektorowi Wykonawczemu stojącemu na czele CTED¹²³. Do jego zadań należy między innymi nadzór nad wykonaniem decyzji CTC czy raportowanie o postępach w zwalczaniu terroryzmu przez poszczególne państwa¹²⁴. W 2017 roku RB ONZ przyjęła rezolucję nr 2341, zgodnie z którą wezwano do dalszej współpracy w zwalczaniu międzynarodowego terroryzmu¹²⁵. W rozumieniu rezolucji istotnym aspektem walki z terroryzmem powinno być wzmacnianie bezpieczeństwa infrastruktury krytycznej. Jak słusznie zauważyła RB ONZ państwa same decydują co powinno zaliczać się do ich infrastruktury krytycznej, jednak przy obecnym rozwoju technologicznym rośnie współzależność infrastruktury krytycznej między państwami, co widać między innymi w sektorze komunikacyjnym czy sektorze energetycznym¹²⁶. Zdaniem RB ONZ zapewnienie skutecznej ochrony infrastruktury krytycznej wpływa bezpośrednio nie tylko na bezpieczeństwo narodowe i publiczne, ale również na dobrobyt i dobrostan (ang. *well-being and welfare*) ludności danego państwa¹²⁷. Niespełna miesiąc po przyjęciu przez RB ONZ rezolucji nr 2341, CTED podjęło próbę zdefiniowania pojęcia infrastruktury krytycznej¹²⁸. Wskazując na kompilację różnych definicji infrastruktury krytycznej, zarówno wywodzących się z doktryny, jak i praktyki, CTED wymieniło potencjalne sektory, które można zaliczyć do infrastruktury krytycznej, na przykład komunikację, ratownictwo, energetykę, finanse, tamy,

¹²¹ *Tamże*, s.2.

¹²² RB ONZ, *Resolution 1535 (2004)*, 26.03.2004, S/RES/1535 (2004).

¹²³ *Letter from the Chairman of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Security Council*, 19.02.2004, S/2004/124.

¹²⁴ *Tamże*, s. 7.

¹²⁵ RB ONZ, *Resolution 2341 (2017)*, 13.02.2017, S/RES/2341 (2017).

¹²⁶ *Tamże*, s. 2.

¹²⁷ *Tamże*.

¹²⁸ CTC, *Physical protection of critical infrastructure against terrorist attacks, Counter-Terrorism Committee Executive Directorate Trends Report*, March 2017, <https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted-trends-report-march-2017-final.pdf> (dostęp: 5.06.2024), s. 2-3.

żywność, zdrowie, usługi publiczne, przemysł czy transport¹²⁹. CTED zwróciło również uwagę na dwa kluczowe problemy pojawiające się w zakresie definiowania i bezpieczeństwa infrastruktury krytycznej. Po pierwsze, zdecydowana większość infrastruktury krytycznej pozostaje w sektorze prywatnym (szacunkowo 80% infrastruktury krytycznej państw zachodnich znajduje się w sektorze prywatnym)¹³⁰. Brak odpowiedniego nadzoru ze strony państw nad infrastrukturą krytyczną może wpływać na zapewnienie jej skutecznej ochrony, dlatego konieczna jest współpraca na linii sektor publiczny – sektor prywatny. CTED jako potencjalny sposób nawiązania współpracy na płaszczyźnie ochrony infrastruktury krytycznej wskazuje partnerstwo publiczno-prywatne¹³¹. Po drugie, należy ustalić znaczenie pojęcia „krytyczny”¹³². W związku z rozwojem technologicznym coraz częściej „krytyczny” staje się pojęciem płynnym, którego znaczenie cały czas ewoluuje. Dodatkowo państwa spotykają się z trudnościami w zakresie ustalenia priorytetów pomiędzy poszczególnymi „krytycznymi” sektorami. Nierzadko osoby odpowiedzialne za zidentyfikowanie infrastruktury krytycznej nie chcą podjąć decyzji o wykreśleniu danego sektora z listy infrastruktury krytycznej obawiając się negatywnych konsekwencji. Jednocześnie decydują się na marnowanie zasobów, na przykład pieniężnych, które mogłyby przyczynić się do poprawy ochrony infrastruktury krytycznej¹³³. Zdaniem CTED, biorąc pod uwagę opisane problemy, państwa tworząc ramy identyfikacji oraz ochrony infrastruktury krytycznej powinny brać pod uwagę relacje pomiędzy sektorem publicznym i sektorem prywatnym oraz znaczenie określonego sektora¹³⁴.

Infrastruktura krytyczna jako system zapewniający bezpieczeństwo zarówno państwu, jak i jego obywatelom, odgrywa istotną rolę również podczas konfliktu zbrojnego. Od momentu rozpoczęcia konfliktu zbrojnego o pełnym międzynarodowym charakterze pomiędzy Rosją a Ukrainą w lutym 2022 roku infrastruktura krytyczna wielokrotnie była celem ataków tak ze strony rosyjskiej¹³⁵, jak i ukraińskiej¹³⁶. Na początku rosyjskiej inwazji na Ukrainę doszło do zniszczenia w regionie chersońskim tamy na Kanale Północnokrymskim¹³⁷. Atak pozbawił

¹²⁹ *Tamże*, s. 2.

¹³⁰ *Tamże*.

¹³¹ *Tamże*.

¹³² *Tamże*, s. 2.

¹³³ *Tamże*.

¹³⁴ *Tamże*, s. 2-3.

¹³⁵ B. Pacek, P. Pacek, *Russia's devastating impact on critical infrastructure during the hybrid war in Ukraine*, „Bezpieczeństwo. Teoria i Praktyka”, 2023, nr 2 (LI), s. 13.

¹³⁶ *Ukrainian Drone Attack Sets Major Russian Oil Refinery on Fire*, <https://www.bloomberg.com/news/articles/2024-05-01/ukrainian-drone-attack-sets-major-russian-oil-refinery-on-fire> (dostęp: 5.06.2024).

¹³⁷ B. Pacek, P. Pacek, *Russia's devastating...*, s. 18.

dostępu do świeżej wody wiele ukraińskich miast, na przykład Mariupol, tym samym powodując poważny kryzys humanitarny.

O tym jak ważna jest infrastruktura krytyczna podczas konfliktu zbrojnego świadczy również stanowisko Stałego Przedstawicielstwa Hiszpanii przy ONZ, przedstawione w piśmie do Sekretarza Generalnego ONZ¹³⁸. Określono w nim ochronę cywilnej infrastruktury krytycznej, jako jeden z trzech głównych obowiązków strony w konflikcie zbrojnym¹³⁹. Dodatkowo wskazano, że sektory takie jak służba zdrowia oraz edukacja stanowią podstawę cywilnej infrastruktury krytycznej¹⁴⁰.

Problematyką zapewnienia bezpieczeństwa infrastrukturze krytycznej zajmują się również organizacje międzynarodowe regionalne. We wspieranie ochrony infrastruktury krytycznej przed zagrożeniami terrorystycznym angażuje się OBWE¹⁴¹. Infrastruktura krytyczna jest niezbędna dla rozwoju nowoczesnych społeczeństw i wpływa bezpośrednio na poprawę jakości życia ludności¹⁴². W ramach działalności OBWE skupia się przede wszystkim na rozwoju bezpieczeństwa sektora energetycznego¹⁴³. Sama Organizacja nie wprowadziła wprawdzie własnej definicji pojęcia infrastruktury krytycznej, ale powołuje się na definicje pochodzące z aktów prawa krajowego wybranych państw (np. Stanów Zjednoczonych, Niemiec) i wskazuje punkty styczne każdej definicji, co pozwala na zidentyfikowanie tejże infrastruktury¹⁴⁴. Podkreśla się, że infrastruktura krytyczna przyczynia się przede wszystkim do bezpieczeństwa publicznego oraz dobrostanu gospodarczego i społecznego. Jest systemem połączonych ze sobą sektorów, które teoretycznie są od siebie niezależne, jednak awaria jednego z nich może mieć wpływ na prawidłową działalność pozostałych, np. awaria systemu energetycznego. Dlatego zadaniem państwa, jako głównego podmiotu chroniącego infrastrukturę krytyczną, jest zapewnienie równowagi w jej funkcjonowaniu, przede wszystkim w zakresie sektora energetycznego¹⁴⁵. Ponadto OBWE wskazała następujące sektory, które należy zaliczyć do infrastruktury krytycznej: energia (elektryczność, ropa, gazy naturalne),

¹³⁸ *Letter from the Permanent Representative of Spain to the United Nations addressed to the Secretary-General*, 1.04.2019, A/73/822-S/2019/285, s. 4.

¹³⁹ Do pozostałych dwóch zalicza się zapewnienie sukcesu misji wojskowej oraz ochronę własnych sił zbrojnych, zob. R. Łasa, *Międzynarodowe prawo humanitarne – bufor bezpieczeństwa...*, s. 272.

¹⁴⁰ *Letter from the Permanent Representative of Spain...*, s. 2-3.

¹⁴¹ OBWE, *Decision No. 6/07 Protecting Critical Energy Infrastructure from Terrorist Attack*, 30.11.2007, MC.DEC/6/07.

¹⁴² OBWE, *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace*, Vienna 2013, <https://cdn.osce.org/sites/default/files/f/documents/4/b/103500.pdf> (dostęp: 5.06.2024), s. 16.

¹⁴³ OBWE, *Decision No. 6/07...*, s. 2.

¹⁴⁴ OBWE, *Good Practices Guide...* (dostęp: 5.06.2024), s. 16.

¹⁴⁵ *Tamże*, s. 19.

technologie informacyjne i komunikacyjne (telekomunikacja, Internet, systemy nadawcze), ruch drogowy i transport (lotnictwo, logistyka, transport kolejowy), opieka zdrowotna (lekarstwa, szczepionki, laboratoria), zaopatrzenie w wodę (tamy, przechowywanie i dystrybucja wody), finanse i ubezpieczenia (banki, giełdy, usługi finansowe, firmy ubezpieczeniowe), rządy i administracja (rząd, parlament, instytucje prawne, system ratownictwa), żywność (handel żywnością, rolnictwo), media i kultura (radio, prasa, zabytki)¹⁴⁶.

Z uwagi na to, że infrastruktura krytyczna odgrywa kluczową rolę w obronności państwa, co przenosi się między innymi na jego siłę militarną, nad jej pojęciem podjęto również dyskusję na forum NATO¹⁴⁷, także wzorując się na definicjach krajowych¹⁴⁸. Pod pojęciem infrastruktury krytycznej rozumie się obiekty i usługi, które mają kluczowe znaczenie dla podstawowych czynności danego społeczeństwa lub te, bez których funkcjonowanie danego społeczeństwa byłoby znacznie utrudnione¹⁴⁹. W głównej mierze te obiekty i usługi będą obejmowały sektor transportu (lądowy, powietrzny, morski), sektor energetyczny, sektor rządowy (ze szczególnym uwzględnieniem sił porządkowych, wojska oraz systemu ratownictwa), sektor technologiczny i komunikacyjny, sektor żywnościowy, służbę zdrowia oraz instytucje finansowe¹⁵⁰. Jak wskazuje M. Jopling, coraz częściej w ramach pojęcia infrastruktury krytycznej wyodrębnia się również cyber-infrastrukturę krytyczną¹⁵¹. W związku z intensywnym rozwojem nowoczesnych technologii zakres ochrony cyber-infrastruktury krytycznej niejednokrotnie przewyższa zakres ochrony „klasycznej” infrastruktury krytycznej.

Od pewnego czasu na forum NATO podejmuje się dyskusje nad ochroną podmorskiej infrastruktury krytycznej¹⁵². W porównaniu do pojęcia infrastruktury krytycznej w klasycznym rozumieniu, pojęcie podmorskiej infrastruktury krytycznej jest trudniejsze w zdefiniowaniu ze względu na brak woli politycznej państw członkowskich NATO¹⁵³. Jednak biorąc pod uwagę wypracowane dotychczas definicje infrastruktury krytycznej, dodając do tego aspekt obiektów

¹⁴⁶ *Tamże*, s. 18.

¹⁴⁷ S. Jaśkiewicz-Kamińska, *Prawo do bezpiecznej infrastruktury krytycznej*, Instytut Wydawniczy EuroPrawo, Warszawa 2016, s. 32.

¹⁴⁸ M. Jopling, *The Protection of Critical Infrastructures. Special Report*, NATO Parliamentary Assembly, 24.08.2007, 162 CDS 07, https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/270/270907/270907jopling_en.pdf (dostęp: 5.06.2024), s. 2-3.

¹⁴⁹ *Tamże*, s. 2.

¹⁵⁰ *Tamże*, s. 3.

¹⁵¹ *Tamże*, s. 2.

¹⁵² S. Monaghan, O. Svendsen, M. Darrah, E. Arnold, *NATO's Role in Protecting Critical Undersea Infrastructure*, Center for Strategic and International Studies, December 2023, s. 1.

¹⁵³ *Tamże*, s. 5.

i usług morskich, można stwierdzić, że podmorską infrastrukturą krytyczną są wszystkie sektory kluczowe dla zapewnienia podstawowych czynności społecznych, takich jak handel, dostawy żywności i energii, bezpieczeństwo i obronność, komunikacja, transport, turystyka i zarządzanie środowiskiem¹⁵⁴. Jaki sektor konkretnie będzie należał do podmorskiej infrastruktury krytycznej, decyduje przede wszystkim wewnętrzna polityka każdego państwa. Dla jednego z państw kluczowym sektorem będzie połów ryb, dla innego ochrona podmorskiej infrastruktury energetycznej¹⁵⁵. Potrzeba zdefiniowania, a następnie skuteczna ochrona podwodnej infrastruktury krytycznej wynika z rosyjskich zagrożeń hybrydowych, czego przykładem jest uszkodzenie obu rurociągów Nord Stream w 2022 roku¹⁵⁶.

Poza zagrożeniami militarnymi oraz terrorystycznymi, infrastruktura krytyczna odgrywa również istotną rolę w rozwoju gospodarczym oraz społecznym państwa. Na forum OECD podjęto próby zdefiniowania infrastruktury krytycznej oraz wyznaczenia ram jej skutecznej ochrony, w celu rozwoju gospodarczego i społecznego państw członkowskich¹⁵⁷. Tak jak przy wcześniej opisanych organizacjach międzynarodowych, OECD również korzysta z krajowych definicji infrastruktury krytycznej. Jak słusznie zauważono, pojęcie infrastruktury krytycznej składa się z dwóch niezależnych wyrazów – „krytyczny” oraz „infrastruktura”¹⁵⁸. Pojęcie infrastruktury jest szeroko rozumiane i swoim zakresem obejmuje zarówno infrastrukturę fizyczną, jak i aktywa niematerialne, w tym sieć (*ang. web*)¹⁵⁹. Pojęcie „krytyczna” wskazuje na infrastrukturę niezbędną dla wsparcia dobrobytu gospodarczego i społecznego, bezpieczeństwa publicznego i funkcjonowania kluczowych obowiązków rządowych¹⁶⁰. W przypadku OECD wymieniono również przykładowe sektory, które potencjalnie mogą zostać zaliczone do infrastruktury krytycznej. Mogą nimi być sektory energetyczny, telekomunikacji, finansowy, służby zdrowia, żywności i zaopatrzenia w wodę, transportowy, rządowy, chemiczny, ratownictwa, przemysłu zbrojeniowego oraz inne sektory, na przykład sektor badawczy¹⁶¹.

¹⁵⁴ *Tamże*.

¹⁵⁵ *Tamże*.

¹⁵⁶ *Tamże*, s. 1-2.

¹⁵⁷ OECD, *Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security*, Investment Division, Directorate for Financial and Enterprise Affairs Organisation for Economic Co-operation and Development, May 2008, s. 2.

¹⁵⁸ *Tamże*, s. 3.

¹⁵⁹ *Tamże*.

¹⁶⁰ *Tamże*.

¹⁶¹ *Tamże*, s. 5.

Prawidłowe zdefiniowanie, a następnie zabezpieczenie infrastruktury krytycznej pozytywnie wpływa na rozwój dobrobytu państwa i jego obywateli¹⁶². Wielokrotnie dochodziło do uszkodzeń lub zniszczeń infrastruktury krytycznej, co miało bezpośrednie przełożenie na społeczeństwo. Oprócz wyżej wspomnianych zagrożeń terrorystycznych oraz militarnych, dużym niebezpieczeństwem dla infrastruktury krytycznej są również zagrożenia naturalne, jak powodzie czy trzęsienia ziemi¹⁶³. Za przykład posłużyć może trzęsienie ziemi w 2011 roku w Japonii, kiedy doszło do uszkodzenia elektrowni atomowej Fukushima, co skutkowało obniżeniem krajowej produkcji energii elektrycznej aż o 50%¹⁶⁴. Rok później, w stanach Nowy Jork oraz New Jersey doszło do potężnego huraganu Sandy, który wywołał powódź, pozbawiając prawie 6 milionów ludzi środków transportu¹⁶⁵. Takie sytuacje obrazują jak ważne jest konkretne zdefiniowanie infrastruktury krytycznej, żeby następnie zapewnić jej niezbędną ochronę, co znajdzie swoje bezpośrednie przełożenie na bezpieczeństwo ludności, ale także przyniesie jej dobrobyt społeczny i gospodarczy.

1.4.2 Doktrynalne ustalenie znaczenia pojęcia infrastruktury krytycznej

Problematyka infrastruktury krytycznej jest szeroko poruszana nie tylko w dyskursie prawniczym, ale ze względu na swój uniwersalny charakter również w innych naukach, szczególnie w naukach o bezpieczeństwie¹⁶⁶. Analiza definicji zaproponowanych zarówno przez prawników, jak i badaczy związanych z innymi naukami w dalszym ciągu nie pozwala wypracować jednolitej definicji infrastruktury krytycznej. Przede wszystkim wynika to z roli jaką infrastruktura krytyczna pełni w bezpieczeństwie danego państwa. To państwo powinno zdefiniować czym konkretnie jest w jego systemie prawnym infrastruktura krytyczna, co się do niej zalicza i jakie podejmuje się kroki celem jej skutecznej ochrony. Oczywiście, przedstawiciele doktryny mogą, a nawet powinni wyodrębnić wspólny trzon pojęcia infrastruktury krytycznej, który stanowiłby podstawę dla jej dalszego definiowania, tak w ustawodawstwie krajowym, jak i w aktach prawa międzynarodowego.

¹⁶² *Making of critical infrastructure resilience a policy priority*, https://www.oecd-ilibrary.org/sites/02f0e5a0-en/1/2/1/index.html?itemId=/content/publication/02f0e5a0-en&_csp_=eb11192b2c569d5c3d1424677826106a&itemIGO=oecd&itemContentType=book (dostęp: 5.06.2024).

¹⁶³ *Tamże*.

¹⁶⁴ *Tamże*.

¹⁶⁵ *Tamże*.

¹⁶⁶ M. Cieślarczyk, *Problematyka bezpieczeństwa infrastruktury krytycznej postrzegana z różnych perspektyw badawczych*, w: A. Trybulska (red.), *Ochrona infrastruktury krytycznej*, Wydawnictwo Wyższej Szkoły Policji, Szczytno 2010, s. 19-28.

Analizując definicje infrastruktury krytycznej zaproponowane przez przedstawicieli nauki, na pierwszy plan wysuwa się ich przedmiotowy charakter określający to co wchodzi w zakres tej infrastruktury – obiekty, systemy, konkretne sektory¹⁶⁷. Natomiast w większości definicji charakter podmiotowy infrastruktury krytycznej został ograniczony, wskazując tylko, że infrastruktura krytyczna służy państwu i jego obywatelom.

Z uwagi na to, że pojęcie infrastruktury krytycznej jest stosunkowo nowym pojęciem¹⁶⁸, w badaniach naukowych pojawiają się kolejne, nowe jej definicje. W 2010 roku M. Bennett oraz V. Gupta zaproponowali ujęcie infrastruktury krytycznej jako podstawowych usług niezbędnych do przeżycia każdemu człowiekowi¹⁶⁹. Uznali oni, że istnieje sześć sposobów na utratę życia przez człowieka oraz trzy podstawowe potrzeby człowieka, które jeśli są zapewnione chronią przed utratą życia – schronienie (chroni przed ciepłem i zimnem), zaopatrzenie (chroni przed głodem i pragnieniem), bezpieczeństwo (chroni przed chorobami i urazami). Przez schronienie rozumie się nie tylko sam budynek, ale również zbiór usług, zapewniający jego prawidłowe funkcjonowanie, jak elektryczność czy sieć wodociągów. Najszerszym pojęciem jest bezpieczeństwo, pod którym kryją się zarówno działalność służb porządkowych, na przykład policji czy wojska, ale także cały sektor ratownictwa i służby zdrowia, w tym szpitale. Istota infrastruktury krytycznej skupia się na aspekcie podmiotowym, a więc w centrum jest ochrona ludności¹⁷⁰. Prawidłowo funkcjonująca infrastruktura krytyczna pozytywnie wpływa na zabezpieczenie tych trzech podstawowych potrzeb człowieka.

Inne pojęcie infrastruktury krytycznej, zaprezentowane przez Z. Trejnisę, dzieli ją na infrastrukturę techniczną oraz infrastrukturę społeczną¹⁷¹. Infrastruktura techniczna oraz społeczna, zdaniem autora, zaliczają się do infrastruktury materialnej. Oprócz tego możliwe jest również wyodrębnienie infrastruktury niematerialnej¹⁷². W jej zakres wchodzi na przykład: wykształcenie społeczeństwa, tradycja, kultura czy poczucie odpowiedzialności. Jest to koncepcja zdecydowanie odbiegająca od standardów infrastruktury krytycznej jako połączonych systemów i obiektów służących zapewnianiu bezpieczeństwa państwa i jego obywateli, ale ukazuje nieostrość pojęcia infrastruktury krytycznej. Pojęcie infrastruktury

¹⁶⁷ M. Molendowska, M. Ostrowska, P. Górski, *Infrastruktura krytyczna ...*, s. 76-77.

¹⁶⁸ *Tamże*, s. 76.

¹⁶⁹ M. Bennett, V. Gupta, *Dealing in Security understanding vital services and how they keep you safe*, http://resiliencemaps.org/files/Dealing_in_Security.July2010.en.pdf (dostęp: 5.06.2024).

¹⁷⁰ *Tamże*.

¹⁷¹ Z. Trejnis, *Infrastruktura Krytyczna – Koncepcje i Zarys*, w: A. Trybulska (red.), *Ochrona infrastruktury krytycznej*, Wydawnictwo Wyższej Szkoły Policji, Szczytno 2010, s. 67.

¹⁷² *Tamże*, s. 67.

technicznej powinno być rozumiane jako „systemy urządzeń i instytucji niezbędnych do należytego funkcjonowania gospodarki, a więc uzbrojenie techniczne terenu w zakresie: komunikacji, transportu, łączności, energetyki, telekomunikacji, zaopatrzenia w wodę itp.”¹⁷³. Dodatkowo autor zwrócił uwagę na cechy charakterystyczne infrastruktury krytycznej, do których należy zaliczyć między innymi długi okres eksploatacji czy nakłady inwestycyjne na rozwój infrastruktury technicznej, które nie przynoszą bezpośrednio zysku¹⁷⁴. Natomiast pojęcie infrastruktury społecznej jest rozumiane jako „celowo rozmieszczana sieć urządzeń, której elementami są odpowiednio zaprojektowane obiekty, stanowiące warunki elastycznego wykonywania funkcji w zaspokajaniu potrzeb społecznych stosując nowoczesne zdobycze postępu naukowo-technicznego, wdrażanego przez odpowiednio wykwalifikowane kadry, działające w określonym systemie organizacyjno-prawnym”¹⁷⁵. W tym ujęciu infrastruktura społeczna składa się z dwóch podsystemów, które mają znaczenie podstawowe w celu spełnienia jego funkcji oraz znaczenie pomocnicze w stosunku do działalności podstawowej¹⁷⁶. Infrastruktura społeczna o znaczeniu podstawowym składa się z obiektów służących wykonywaniu działalności podstawowej (jak szpital) z obiektami ściśle związanymi z tą działalnością, niezbędnymi do prawidłowego działania obiektu głównego (jak sala operacyjna, wyposażenie zapewniające działalność podstawową czy system organizacyjno-prawny normujący zasady działania i zaspokajania określonych potrzeb społecznych)¹⁷⁷. Natomiast podsystemy pomocnicze, to pozostałe wyposażenie, np. meble biurowe, urządzenia grzewcze oraz kadra pomocnicza gospodarcza i administracyjna¹⁷⁸. Według Z. Trejnisa infrastrukturę społeczną cechują między innymi długi okres użytkowania obiektów infrastruktury, publiczny charakter działania urządzeń infrastruktury czy duże znaczenie czynnika ludzkiego w celu prawidłowego działania urządzeń infrastruktury¹⁷⁹.

W związku z intensywnym rozwojem nowoczesnych technologii, pojawiają się również pojęcia infrastruktury krytycznej mocno nawiązujące do cyberprzestrzeni. Jednym z takim przykładów jest pojęcie infrastruktury krytycznej zaprezentowane przez C. M. Newbilla¹⁸⁰. Zgodnie z nim niemożliwe jest przyjęcie stałego znaczenia infrastruktury krytycznej.

¹⁷³ *Tamże*, s. 67-68.

¹⁷⁴ *Tamże*, s. 68.

¹⁷⁵ *Tamże*.

¹⁷⁶ *Tamże*.

¹⁷⁷ *Tamże*.

¹⁷⁸ *Tamże*.

¹⁷⁹ *Tamże*.

¹⁸⁰ C. M. Newbill, *Defining Critical Infrastructure for a Global Application*, „Global Legal Studies” 2019, vol. 26, no. 2, s. 778-779.

Jako główny powód wskazuje się przywołany wcześniej rozwój nowoczesnych technologii, który w istotny sposób wpływa na funkcjonowanie zarówno państw, jak i jego obywateli. Ponadto rozwój technologii sprawił, że większość systemów zaliczanych do infrastruktury krytycznej jest ściśle ze sobą powiązana i często niemożliwe jest ich poprawne działanie kiedy dojdzie do uszkodzenia jednego z systemów¹⁸¹. Jak podkreśla O. Gross, komputery oraz technologie informacyjno-komunikacyjne stanowią obecnie system nerwowy nowoczesnego społeczeństwa¹⁸². Wymusza to rozszerzenie definicji infrastruktury krytycznej o kwestie związane z cyberbezpieczeństwem oraz uszczegółowienie samego pojęcia infrastruktury krytycznej o komponenty teleinformatyczne.

1.4.3 Orzecnicze ustalenie znaczenia pojęcia infrastruktury krytycznej

Pojęcie infrastruktury krytycznej w orzecznictwie sądów i trybunałów, tak krajowych jak i międzynarodowych, pojawia się rzadko. Na gruncie prawa międzynarodowego tylko UE zdefiniowała pojęcie infrastruktury krytycznej i dlatego właśnie w orzecznictwie TSUE znajdują się odwołania do pojęcia infrastruktury krytycznej. Są to jednak sporadyczne przypadki, do których zaliczyć należy przede wszystkim opinię Rzecznika Generalnego TSUE z 11 stycznia 2024 roku¹⁸³. Przedmiotem spornej decyzji i zaskarżonego wyroku była problematyka wyszukania produktów i przedstawienia jego wyników na stronie internetowej Google. W odpowiedzi na wyszukiwanie produktu wyszukiwarka lub porównywarka produktów wyświetla jako wyniki różne strony internetowe, na których można kupić poszukiwany produkt. Mogły to być strony internetowe sprzedawców lub platform sprzedażowych, takich jak eBay lub Amazon¹⁸⁴.

W samej opinii Rzecznik Generalny TSUE nie zdefiniował infrastruktury krytycznej, zamiast tego wskazał, że TSUE podjął próby zdefiniowania pojęcia „*essential facility*” (w polskiej wersji językowej orzeczenia użyto pojęcia infrastruktury krytycznej)¹⁸⁵. Aby określić czy dana usługa lub obiekt mogą zostać zaliczone do tzw. *essential facility* TSUE wprowadziło konieczność weryfikacji poprzez tzw. Kryteria Bronnera:

¹⁸¹ *Tamże*.

¹⁸² O. Gross, *Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-incidents*, „Cornell International Law Journal”, 2015, vol. 48, nr 3, s. 481.

¹⁸³ TSUE, *Opinia Rzecznika Generalnego – Google LLC, Alphabet, Inc., C-48/22 P*, 11.01.2024, ECLI:EU:C:2024:14.

¹⁸⁴ *Tamże*, par. 10.

¹⁸⁵ *Tamże*, par. 58.

1. odmowa usługi wyeliminuje wszelką konkurencję na rynku ze strony osoby żądającej tej usługi,
2. odmowa nie jest obiektywnie uzasadniona,
3. usługa sama w sobie była niezbędna do prowadzenia działalności gospodarczej i niemożliwe byłoby zastosowanie rzeczywistego lub potencjalnego substytut tej usługi¹⁸⁶.

Pojęcie *essential facility*, w rozumieniu wyroku C-7/97 oraz opinii Rzecznika Generalnego TSUE C-48/22 P, jako infrastruktury krytycznej zostało ograniczone tylko i wyłącznie do elementów niezbędnych do prawidłowego funkcjonowania działalności gospodarczej.

Analiza orzecznictwa międzynarodowych trybunałów karnych wskazuje, że w ich pracach niejednokrotnie zajmowano się problematyką ochrony sektorów, które potencjalnie mogą zostać zaliczone do infrastruktury krytycznej. Szczególną uwagę należy zwrócić na orzecznictwo MTKJ. Między innymi w orzeczeniu w sprawie przeciwko dowódcy Sił Zbrojnych Republiki Serbskiej – Stanislavovi Galiciowi, Trybunał określił warunki, które muszą zostać spełnione przed atakiem na obiekty szpitalne¹⁸⁷. Jednak w żadnym z orzeczeń MTKJ nie przywołał pojęcia infrastruktury krytycznej. Może to wynikać z okresu kiedy MTKJ działał, czyli przełomu lat 90. i wczesnych lat 2000. Wtedy pojęcie infrastruktury krytycznej dopiero się tworzyło i nie było szeroko używane.

W polskim orzecznictwie pojęcie infrastruktury krytycznej często pojawia się w wyrokach sądów administracyjnych¹⁸⁸. Jednak żaden z wyroków nie definiuje tego pojęcia.

1.5 Podsumowanie

Na podstawie powyższych rozważań należy stwierdzić, że pojęcie infrastruktury krytycznej jest pojęciem nieostrym. Wątpliwym wydaje się ustalenie jednej wspólnej definicji infrastruktury krytycznej dla społeczności międzynarodowej, ze względu na rolę jaką infrastruktura krytyczna odgrywa w zapewnieniu bezpieczeństwa państwa. Każde państwo z osobna, w celu skutecznej ochrony infrastruktury krytycznej, może decydować jakie sektory

¹⁸⁶ TSUE, *Wyrok w sprawie Oscar Bronner GmbH & Co. KG*, C-7/97, 26.12.1998, ECLI:EU:C:1998:569, par. 37 in.

¹⁸⁷ MTKJ, *Prosecutor v. S. Galić*, Judgment on Appeal, 30.11.2006, IT-98-29, par. 340–346.

¹⁸⁸ Por. wyrok Wojewódzkiego Sądu Administracyjnego we Wrocławiu, 2.02.2023, II SA/Wr 283/22, postanowienie Wojewódzkiego Sądu Administracyjnego w Gliwicach, 7.06.2023, III SAB/Gl 99/23, wyrok Wojewódzkiego Sądu Administracyjnego w Poznaniu, 21.09.2023, I SA/Po 440/23.

będą uważane za taką infrastrukturę. Oczywiście możliwe jest wskazanie pewnych podstawowych sektorów, które bez wątpienia należą do infrastruktury krytycznej, co znajduje odzwierciedlenie w wyżej analizowanych definicjach, na przykład sektor energetyczny, sektor służby zdrowia.

Proces identyfikacji infrastruktury krytycznej jest zdecydowanie procesem zawiłym, ale szczególnie ważnym nie tylko dla państwa samego w sobie, ale przede wszystkim dla jego obywateli. W trakcie procesu identyfikacji państwa muszą sprostać określonym wyzwaniom, które doprowadzą do ustalenia znaczenia infrastruktury krytycznej. Przede wszystkim sektor publiczny i sektor prywatny muszą ustalić metodologię, którą będą wspólnie wykorzystywać do identyfikacji infrastruktury krytycznej¹⁸⁹. Drugim wyzwaniem jest rozróżnienie infrastruktury, która wpływa na bezpieczeństwo ogólnokrajowe, a która przyczynia się do bezpieczeństwa regionalnego¹⁹⁰. Kolejnym wyzwaniem jest zapewnienie bezpieczeństwa przetwarzanym informacjom o infrastrukturze krytycznej oraz wszystkim innym informacjom, które pojawią się w trakcie procesu identyfikacji infrastruktury krytycznej, a mogą mieć wpływ na bezpieczeństwo wewnętrzne i zewnętrzne państwa¹⁹¹. Ostatnim wyzwaniem przy identyfikacji infrastruktury krytycznej jest rozszerzanie jej pojęcia o nowe sektory, które nie wpływają bezpośrednio na bezpieczeństwo państwa. Należy tu wskazać sektor edukacji oraz kultury. F. Lazrak wskazał, że dziedzictwo kulturowe z racji swojego znaczenia historycznego, ale także charakteru „mienia społecznego” stanowi duszę danego miejsca, tym samym powinno zostać zakwalifikowane jako infrastruktura krytyczna¹⁹². Z perspektywy skutecznej ochrony infrastruktury krytycznej, rozszerzenie jej pojęcia o sektory takie jak edukacja czy kultura wydaje się jednak niebezpieczne. Włączenie w zakres infrastruktury krytycznej szkół, uniwersytetów czy dóbr kulturalnych, które bez wątpienia odgrywają istotną rolę w kształtowaniu się państwa, obywateli czy narodu, może doprowadzić do osłabienia ochrony tej infrastruktury z powodu nadmiaru obiektów, które nie wypełniają przesłanki „krytyczności”.

Należy również pamiętać, że nie jest możliwe stworzenie jednej, „stałej” definicji infrastruktury krytycznej nawet dla jednego państwa, ponieważ infrastruktura krytyczna jest zjawiskiem płynnym. To, że dany sektor w dniu dzisiejszym jest sektorem niezbędnym dla

¹⁸⁹ M. Jopling, *The Protection...*, s. 2.

¹⁹⁰ *Tamże*.

¹⁹¹ *Tamże*.

¹⁹² F. Lazrak, P. Nijkamp, P. Rietveld, J. Rouwendal, *Cultural heritage and creative cities: an economic evaluation perspective*, Serie Research Memoranda 0036, VU University Amsterdam, 2009, s. 2.

poprawnego i skutecznego działania państwa nie oznacza, że ten sam sektor będzie niezbędny dla państwa za pięć czy dziesięć lat.

Brak definicji infrastruktury krytycznej w międzynarodowym prawie humanitarnym wymusza zrekonstruowanie definicji infrastruktury krytycznej na podstawie tego jak MPH nazywa i jak chroni poszczególne obiekty służące bezpieczeństwu ludności cywilnej. Z racji funkcji infrastruktury krytycznej, nie można jej rozpatrywać tylko i wyłącznie jako systemów i obiektów zapewniających bezpieczeństwo ludności cywilnej, ale przede wszystkim zapewnienia bezpieczeństwa państwa jako instytucji. W momencie zapewnienia bezpieczeństwa instytucji państwowych, państwo jest w stanie sprawnie chronić ludność cywilną podczas konfliktu zbrojnego, tym samym spełnione są funkcje ochronne MPH. Jednak samo MPH nie przyznaje ochrony instytucjom państwowym, przez co brakuje elementu przedmiotowego w potencjalnej definicji infrastruktury krytycznej.

Biorąc powyższe ustalenia pod uwagę, na potrzeby niniejszej rozprawy, należy przyjąć, że infrastruktura krytyczna jest to struktura połączonych ze sobą urządzeń, obiektów oraz systemów (w tym dóbr o charakterze niematerialnym), które wpływają na bezpieczeństwo państwa oraz ludności, oddziałując na trzy główne kategorie – schronienie, zaopatrzenie oraz bezpieczeństwo. Każda z powyższych kategorii obejmuje swoim zakresem poszczególne sektory, które mogą zostać potencjalnie uznane za infrastrukturę krytyczną.

2 Infrastruktura krytyczna w międzynarodowym prawie humanitarnym

2.1 Wprowadzenie

Infrastruktura krytyczna jako struktura połączonych ze sobą urządzeń i obiektów o szczególnym znaczeniu dla zapewnienia bezpieczeństwa państwa i ludności pełni istotną rolę w trakcie konfliktu zbrojnego. Jednak jako zjawisko stosunkowo nowe, a przede wszystkim niezdefiniowane na gruncie MPH, infrastruktura krytyczna *per se* nie podlega ochronie wynikającej z przepisów prawa humanitarnego. W związku z brakiem wprost wyrażonej ochrony infrastruktury krytycznej konieczne jest stworzenie standardu jej ochrony podczas konfliktu zbrojnego na podstawie rekonstrukcji norm współczesnego MPH w zakresie ochrony obiektów, które mogą zostać zaliczone do infrastruktury krytycznej.

W tym celu zaprezentowano dwuczęściową analizę standardów ochrony zapewnianej przez MPH. Pierwsza część stanowi rekonstrukcję standardu ochrony infrastruktury krytycznej od połowy XIX wieku aż do drugiej połowy XX wieku. Dodatkowo rozważania na temat prawa haskiego i prawa genewskiego zostały rozszerzone o praktyczne aspekty stosowania praw i zwyczajów wojny na przykładzie wojny secesyjnej oraz Kodeksu Liebera. Druga część to analiza regulacji MPH wprowadzonych protokołami dodatkowymi z 1977 roku. W szczególności skupiono się na zasadzie rozróżniania, a co za tymi idzie na analizie problematyki infrastruktury krytycznej jako potencjalnego celu wojskowego lub dobra o charakterze cywilnym.

Analiza standardów ochrony infrastruktury krytycznej została wsparta rozważaniami na temat współczesnych zagrożeń w ochronie infrastruktury krytycznej podczas konfliktu zbrojnego. W tym celu poddano analizie wykorzystywanie nowoczesnych technologii, zarówno w kontekście możliwości ochrony tej infrastruktury, ale również w kontekście możliwości przeprowadzenia ataku na infrastrukturę krytyczną. Ponadto przedstawiono problematykę zmiennego charakteru konfliktu zbrojnego, co potencjalnie wpływa na stopień zapewnianej ochrony infrastrukturze krytycznej.

2.2 Ewolucja norm prawnych chroniących infrastrukturę krytyczną w międzynarodowym prawie humanitarnym

Rozwój nowoczesnych technologii jest wpisany w prowadzenie konfliktów zbrojnych. W związku z tym MPH, aby zapewnić skuteczną ochronę ofiarom wojny, cały czas ewoluowało, dostosowując swoje normy do wymagań ówczesnych standardów i technik pola walki. Początkowe regulacje MPH ograniczały się tylko do pojedynczych postanowień, lecz z czasem przybrały bardziej rozbudowanych i szczegółowy charakter.

2.2.1 Rekonstrukcja standardu ochrony infrastruktury krytycznej w prawie haskim i prawie genewskim

Międzynarodowe prawo humanitarne kodyfikowane od schyłku XIX wieku do połowy XX wieku, cechował dualizm. Odróżniano dwa odrębne działy prawa konfliktów zbrojnych – prawo genewskie oraz prawo haskie. Prawo genewskie w głównej mierze dotyczyło ochrony ofiar wojny, natomiast prawo haskie ograniczało środki i metody walki. Pomimo, że oba działy regulowały odrębne kwestie, to w obu przypadkach można odnaleźć podstawy ochrony obiektów, które potencjalnie mogłyby zostać zaliczone do infrastruktury krytycznej.

2.2.1.1 Prawo genewskie

Podwaliny współczesnego MPH są następstwem krwawej bitwy pod Solferino, stoczonej 24 kwietnia 1859 r. pomiędzy wojskami francusko-piemonckimi a austriackimi¹⁹³. W trwającej niespełna piętnaście godzin potyczce udział wzięło ponad 300 tysięcy żołnierzy z czego 6 tysięcy zginęło, a około 40 tysięcy zostało poważnie rannych¹⁹⁴. Kwestią rozstrzygającą o brutalności tej bitwy był brak odpowiedniego zaplecza medycznego, zarówno po stronie francusko-piemonckiej, jak i austriackiej. Wojska francuskie dysponowały tylko trzema lekarzami oraz sześcioma pomocnikami, a główny szpital był oddalony o kilka kilometrów od pola walki¹⁹⁵. Brak odpowiedniej infrastruktury medycznej musiał zostać zastąpiony prowizorycznymi „szpitalami”, które były tworzone w okolicznych domostwach oraz kościołach¹⁹⁶. Wszystkiemu przyglądał się szwajcarski przedsiębiorca H. Dunant, który

¹⁹³ *Dunant's original humanitarian vision. Dunant and the Battle of Solferino*, <https://www.elac.ox.ac.uk/programmes-projects/solferino-21/dunants-original-humanitarian-vision/> (dostęp: 17.10.2024).

¹⁹⁴ F. Bugnion, *Birth of an idea: the founding of the International Committee of the Red Cross and of the International Red Cross and Red Crescent Movement: from Solferino to the original Geneva Convention (1859-1864)*, „International Review of the Red Cross”, 2012, vol. 94, no. 888, s. 1301.

¹⁹⁵ *Tamże*.

¹⁹⁶ *Tamże*.

tęgo samego dnia, w sprawach biznesowych, przybył do miejscowości Castiglione della Pieve¹⁹⁷. Widząc ogrom zniszczeń i cierpienia jakie przyniosła bitwa H. Dunant postanowił pomóc rannym i potrzebującym. Jego praca polegała na opatrywaniu rannych, spisywaniu ostatnich słów żołnierzy, ale również dzięki swoim kontaktom biznesowym na zbiórce funduszy na pomoc humanitarną¹⁹⁸. Negatywne doświadczenia H. Dunanta poskutkowały opracowaniem konwencji, która pozwoliłaby sformułować międzynarodową zasadę, o nienaruszalnym charakterze, stanowiącą podstawę do utworzenia stowarzyszeń zajmujących się pomocą rannym w różnych europejskich krajach¹⁹⁹.

Odpowiedzią na propozycję H. Dunanta było zawiązanie 17 lutego 1863 roku Stałego Międzynarodowego Komitetu Pomocy Rannym Żołnierzom (ang. *Permanent International Committee for the Relief of Wounded Soldiers*)²⁰⁰. Celem działalności Komitetu²⁰¹ było wprowadzenie neutralności służb medycznych podczas konfliktu zbrojnego, uregulowanie ich szczególnej ochrony oraz opracowanie rozpoznawalnego znaku tych służb. Ponadto H. Dunant dążył do sformowania stowarzyszeń pomocy rannym w każdym europejskim kraju. 29 października 1863 roku doszło do podpisania Rezolucji Międzynarodowej Konferencji w Genewie, której celem było utworzenie sieci krajowych komitetów pomocy rannym, wspierających wojskowe służby medyczne²⁰². W Rezolucji określono podstawowe zasady działania krajowych komitetów. Ich obowiązkiem miało być wspomaganie wojskowych służb medycznych w czasie wojny wszelkimi dostępnymi środkami (zob. art. 1 Rezolucji Międzynarodowej Konferencji w Genewie z 1863 roku). W ramach tej pomocy wyszczególniono zorganizowanie ochotniczego personelu, ale także możliwość wysłania tego personelu, po uzyskaniu zgody dowództwa, na pole bitwy ze specjalnym oznakowaniem – białą opaską z czerwonym krzyżem (zob. art. 5, 6 i 7 Rezolucji Międzynarodowej Konferencji

¹⁹⁷ H. Dunant, *A Memory of Solferino*, International Committee of the Red Cross, Geneva, English version American Red Cross (1939, 1959), s. 8-9.

¹⁹⁸ F. Bugnion, *Birth of an idea...*, s. 1303.

¹⁹⁹ „On certain special occasions, as, for example, when princes of the military art belonging to different nationalities meet at Cologne or Chilons, would it not be desirable that they should take advantage of this sort of congress to formulate some international principle, sanctioned by a Convention inviolate in character, which, once agreed upon and ratified, might constitute the basis for societies for the relief of the wounded in the different European countries?”, zob. H. Dunant, *A Memory...*, s. 126.

²⁰⁰ F. Bugnion, *Birth of an idea...*, s. 1311.

²⁰¹ Obecna nazwa „Międzynarodowy Komitet Czerwonego Krzyża” została przyjęta na posiedzeniu Komitetu Genewskiego 20 października 1875 roku, zob. F. Bugnion, *Birth of an idea...*, s. 1309. Współcześnie MKCK działa w oparciu o Statutu Międzynarodowego Komitetu Czerwonego Krzyża przyjęty 21 grudnia 2017 roku jako stowarzyszenie utworzone na podstawie art. 60 i następnych szwajcarskiego kodeksu cywilnego, zob. *Statutes of the International Committee of the Red Cross*, 21.12.2017, <https://www.icrc.org/en/document/statutes-international-committee-red-cross-0> (dostęp: 27.10.2024).

²⁰² Rezolucja Międzynarodowej Konferencji w Genewie, Genewa, 29.10.1863, w: P. K. Marszałek, *Międzynarodowe prawo humanitarne...*, s. 297-298.

w Genewie z 1863 roku). Również w czasie pokoju krajowe komitety powinny prowadzić swoją działalność, która zapewni ich skuteczność w działaniu podczas konfliktu zbrojnego. Do głównych zadań komitetów w trakcie pokoju należy organizowanie pomocy materialnej oraz prowadzenie szkoleń ochotniczego personelu medycznego (zob. art. 4 Rezolucji Międzynarodowej Konferencji w Genewie z 1863 roku). Rezolucja zawiera również zbiór rekomendacji, usprawniających ochronę służby i infrastruktury medycznej. Korpus medyczny wszystkich armii (a przynajmniej tej samej armii) powinien korzystać z jednolitego znaku rozpoznawczego. Tak samo karetki pogotowia oraz szpitale powinny we wszystkich krajach być oznakowane jednolitą flagą. Z punktu widzenia skutecznej ochrony obiektów oraz personelu medycznego bardzo ważne jest wprowadzenie zasady neutralności karetek pogotowia, szpitali oraz oficjalnego personelu medycznego, jak również ochotniczego personelu medycznego (zob. rekomendacje w Rezolucji Międzynarodowej Konferencji w Genewie z 1863 roku). Przyjęcie Rezolucji stanowiło podstawę dla stworzenia Międzynarodowego Ruchu Czerwonego Krzyża i Czerwonego Półksiężyca²⁰³. Uchwalenie Rezolucja z 1863 roku stanowi jeden z fundamentów pozytywnych zmian na polu walki. Chociaż nie ograniczono liczby konfliktów zbrojnych to wprowadzone zmiany doprowadziły do poprawy warunków rannych żołnierzy²⁰⁴.

Dostrzegając szansę na dalszy rozwój ochrony personelu medycznego Komitet Genewski postanowił zorganizować konferencję międzynarodową z zamiarem przyjęcia aktu prawnego zobowiązującego państwa-strony do ochrony wojskowego personelu medycznego²⁰⁵. Konferencja odbyła się pomiędzy 8 a 22 sierpnia 1864 roku, a udział w niej wzięło szesnaście państw. Konferencja z 1864 roku była pierwszym takim wydarzeniem o skali międzynarodowej, w ramach której przyjęto umowę międzynarodową, żeby ustalić regulację prawną mającą oddziaływać na przyszłe konflikty²⁰⁶. Jej efektem było uchwalenie 22 sierpnia 1864 roku Konwencji o polepszeniu losu rannych w armiach w polu (Konwencja genewska z 1864 roku). W Konwencji określono katalog obiektów oraz osób, które w trakcie działań wojennych są chronione i uznawane za bezstronne. Zalicza się do nich: ambulanse wraz z personelem, szpitale wojskowe wraz z personelem, w tym personelem kwatermistrza, służby medyczne, administracyjne, transportowe oraz kapelanów (zob. art. 1 i 2 Konwencji genewskiej z 1864 roku). Istotną cechą tych obiektów i personelu było korzystanie z odróżniającego znaku.

²⁰³ F. Bugnion, *Birth of an idea...*, s. 1320.

²⁰⁴ P. Boissier, *History of the International Committee of the Red Cross, From Solferino to Tsushima*, Henry Dunant Institute, Geneva 1985, s. 80.

²⁰⁵ F. Bugnion, *Birth of an idea...*, s. 1323.

²⁰⁶ *Tamże*, s. 1324.

Obiekty posługiwały się jednolitą flagą opatrzoną czerwonym krzyżem na białym tle, natomiast personel medyczny posługiwał się opaską opatrzoną takim samym znakiem. Również ludność cywilna zaangażowana w pomoc rannym była chroniona przed atakami. Dodatkowo dom, w którym udzielono schronienia i opieki rannemu kombatantowi był obiektem chronionym, a jego mieszkańcy byli zwolnieni z kontrybucji wojennych (zob. art. 5 Konwencji genewskiej z 1864 roku).

Chociaż Konwencja genewska z 1864 roku podlegała wielokrotnym zmianom, a ostatecznie wygasła w 1949 roku²⁰⁷, była pierwszą umową międzynarodową, która w tak szeroki sposób uregulowała ochronę obiektów i personelu medycznego podczas konfliktu zbrojnego. Postanowienia Konwencji dotyczyły zarówno aspektu podmiotowego, jak i przedmiotowego potencjalnej infrastruktury krytycznej. W aspekcie przedmiotowym Konwencja objęła swym zakresem obiekty, jak ambulanse czy szpitale. Natomiast w aspekcie przedmiotowym postanowienia Konwencji odnosiły się nie tylko do personelu medycznego, ale także cywilów angażujących się w pomoc rannym. Ponadto Konwencja oraz prace konferencji dyplomatycznej dały podstawy do powstania jednej z najważniejszych zasad międzynarodowego prawa humanitarnego, czyli zasady humanitaryzmu.

Wygaśnięcie Konwencji genewskiej z 1864 roku zostało poprzedzone opracowaniem czterech konwencji genewskich, gdzie pierwsze trzy dotyczące: polepszenia losu rannych i chorych (I Konwencja genewska z 1949 roku), polepszenia losu rannych, chorych i rozbitków sił zbrojnych na morzu (II Konwencja genewska z 1949 roku), traktowania jeńców wojennych (III Konwencja genewska z 1949 roku) stanowiły powtórzenie między innymi Konwencji genewskiej o polepszeniu losu chorych i rannych w armiach czynnych z 1929 roku²⁰⁸ oraz Konwencji dotyczącej traktowania jeńców wojennych z 1929 roku²⁰⁹. Całkowicie nowo opracowanym aktem prawnym była Konwencja genewska dotycząca ochrony ludności cywilnej (IV Konwencja genewska z 1949 roku). Tak samo jak Konwencja genewska z 1864 roku, KG z 1949 roku wprowadziły ochronę tylko sektora medycznego, z uwzględnieniem jego przedmiotowo-podmiotowego charakteru (postanowienia KG chronią zarówno obiekty medyczne, jak i personel medyczny)²¹⁰. Dla prawidłowego zabezpieczenia

²⁰⁷ *Konwencja o polepszeniu losu rannych w armiach w polu*, Genewa, 22.08.1864, w: P. K. Marszałek, *Międzynarodowe prawo humanitarne*..., s. 299.

²⁰⁸ *Konwencja Genewska o polepszeniu losu chorych i rannych w armjach czynnych*, Genewa, 27.07.1929, Dz. U. z 1932 r., nr 103, poz. 864.

²⁰⁹ *Konwencja dotycząca traktowania jeńców wojennych*, Genewa, 27.07.1929, Dz. U. z 1932 r., nr 103, poz. 866.

²¹⁰ J. Pictet, *The Medical Profession and International Humanitarian Law*, „International Review of the Red Cross”, 1985, vol. 25, no. 247, s. 198-199.

dostępu do opieki medycznej podczas konfliktu zbrojnego strony KG, w czasie pokoju oraz po rozpoczęciu działań zbrojnych, mogą tworzyć strefy i miejscowości sanitarne (art. 23 I KG, art. 14 IV KG). Są to specjalnie wyznaczone obszary pozostające pod ochronę MPH, stworzone dla leczenia osób poszkodowanych działaniami zbrojnymi²¹¹. W aspekcie podmiotowym sektora medycznego postanowienia KG przewidują przede wszystkim ochronę personelu medycznego (art. 24, 25 KG I, art. 36 KG II), jednak art. 20 KG IV wprowadza również ochronę personelu administracyjnego szpitali cywilnych.

Analiza norm prawa genewskiego pozwala wywnioskować, że konwencje genewskie wprowadziły minimalne standardy ochrony jednego konkretnego sektora infrastruktury krytycznej, mianowicie sektora opieki zdrowia. Ochrona opiera się na aspekcie przedmiotowo-podmiotowym infrastruktury krytycznej, a więc obejmuje nie tylko samo bezpieczeństwo obiektów medycznych (aspekt przedmiotowy), ale także bezpieczeństwo personelu medycznego (aspekt podmiotowy).

2.2.1.2 Prawo haskie

Koniec XIX wieku przyniósł kolejny moment przełomowy w stosunkach międzynarodowych w postaci Konferencji Pokojowej, która odbyła się pomiędzy 18 maja a 29 lipca 1899 roku w Hadze²¹². Z propozycją zorganizowania konferencji, której prace miały skupić się na kwestii rozbrojenia oraz arbitrażu, wystąpił rosyjski car Mikołaj II²¹³. Konieczność prawnego uregulowania środków i metod walki podyktowana była rozwojem nowych technologii militarnych²¹⁴. Dodatkowo pod koniec XIX wieku państwa coraz częściej podejmowały współpracę militarną, jednak przełom stulecia cechował się krwawymi konfliktami.

²¹¹ Przykładem strefy sanitarnej był obszar wokół szpitala w Osijek, utworzony na mocy porozumienia pomiędzy Chorwacją a Socjalistyczną Federacyjną Republiką Jugosławii. Ze strefy ochronnej mogli skorzystać ranni kombataneci, kobiety w ciąży, matki dzieci poniżej siódmego roku życia, dzieci poniżej 15. roku życia oraz osoby powyżej 65. roku życia, zob. art. 1, 2 ust. 1 i 4 ust. 1 *Agreement Relating to the Establishment of a Protected Zone around the Hospital of Osijek, between the Federal Republic of Yugoslavia and Croatia*, Pècs, 27.12.1991, https://theirwords.org/media/transfer/doc/sc_yu_croatia_serbia_1991_05-a9cc261d359aa66dc002e823921202f6.pdf (dostęp: 15.05.2026).

²¹² *1899 First Hague Peace Conference*, <https://www.vredespaleis.nl/peace-palace/history/125-years-since-the-first-hague-peace-conference/1899-first-hague-peace-conference/?lang=en> (dostęp: 27.10.2024).

²¹³ S. Barcroft, *The Hague Peace Conference of 1899*, „Irish Studies in International Affairs”, 1989, vol. 3, no. 1, s. 55.

²¹⁴ *Tamże*.

W 1898 roku doszło do wybuchu wojny pomiędzy Stanami Zjednoczonymi a Królestwem Hiszpanii²¹⁵. Jako oficjalną przyczynę wybuchu konfliktu wskazuje się zatonięcie amerykańskiego pancernika USS Maine w porcie w Hawanie (Kuba ówczesnie znajdowała się pod panowaniem hiszpańskim). Konflikt toczył się na dwóch frontach. Amerykańskie siły zbrojne walczyły z siłami hiszpańskimi głównie na Karaibach (zwłaszcza na Kubie), jednak walki odbywały się również na Filipinach²¹⁶. Istotną rolę podczas wojny odegrała marynarka wojenna. Amerykanie dysponowali kilkunastoma nowoczesnymi okrętami wojennymi, co pozwoliło im uzyskać zdecydowaną przewagę nad słabszą hiszpańską marynarką wojenną²¹⁷.

Do kolejnego konfliktu zbrojnego przełomu XIX i XX wieku doszło pomiędzy 1899 a 1901 rokiem na terytorium północno-wschodnich Chin²¹⁸. Tak zwane powstanie bokserów było zbrojnym zrywem ludności chińskiej wymierzonym przeciwko cudzoziemcom. Swoją nazwę zawdzięcza stowarzyszeniu „Pięść w imię sprawiedliwości i pokoju” (Bokserzy), które skupiało osoby trenujące sztuki walki. Przyczyną wybuchu powstania było nadmierne eksploatowanie Chin przez europejskie mocarstwa, co nabrało dynamizmu po zawarciu Traktatu nankińskiego z 1842 roku²¹⁹. Wiązało się to również z chrystianizacją Chin. Europejscy misjonarze nawracali ludność tubylczą na chrześcijaństwo, natomiast Bokserzy cechowali się podejściem antychrześcijańskim oraz antyklerykalnym. Ich ofiarami stawali się zarówno misjonarze, jak i chińscy konwertyci. Kluczowym momentem powstania bokserów było wysłanie międzynarodowych sił humanitarnych, głównie składających się z brytyjskich, niemieckich, rosyjskich, amerykańskich, francuskich, austriackich, japońskich oraz włoskich sił zbrojnych. Celem ekspedycji było uwolnienie uwięzionych w Pekinie przedstawicieli dyplomatycznych oraz innych obywateli różnych państw²²⁰. Operacja została przeprowadzona z wykorzystaniem oddziałów marynarki wojennej oraz licznych sił lądowych (łącznie zebrano około 19 tysięcy żołnierzy), które miały przywrócić łączność pomiędzy Pekinem a portem w Tianjin (Taku)²²¹. Do zakończenia operacji doszło 14 sierpnia 1900 roku, kiedy

²¹⁵ [Existence of war - Spain.] By the President of the United States of America: a proclamation Whereas by an act of Congress approved April 25, 1898, it is declared that war exists and that war has existed since the 21st day of April, A. D. 1898, <https://www.loc.gov/resource/rbpe.23901800/?st=text> (dostęp: 27.10.2024).

²¹⁶ A. J. Echevarria, *The Civil War to the Boxer Rebellion*, w: A. J. Echevarria, *Reconsidering the American way of war: US military practice from the revolution to Afghanistan*, Georgetown University Press, Washington D.C. 2014, s. 99.

²¹⁷ *Tamże*, s. 98.

²¹⁸ *Boxer Rebellion*, <https://www.britannica.com/event/Boxer-Rebellion> (dostęp: 27.10.2024).

²¹⁹ *Treaty of Nanjing (Nanking)*, 29.08.1842, <https://china.usc.edu/treaty-nanjing-nanking-1842> (dostęp: 27.10.2024).

²²⁰ A.J. Echevarria, *The Civil War ...*, s. 104.

²²¹ *Tamże*, s. 104-105.

międzynarodowe siły humanitarne zajęły Pekin. Akcja zbrojna z wykorzystaniem międzynarodowych sił ukazała istotę współpracy państw w celu zapewnienia międzynarodowego bezpieczeństwa²²².

Co więcej, dostrzegając potrzebę zacieśnienia współpracy międzynarodowej zdecydowano się zwołać konferencję pokojową, której celem było opracowanie trzech głównych zagadnień: arbitrażu międzynarodowego, rozbrojenia oraz prawa wojny²²³. Dla MPH kluczowym osiągnięciem konferencji było przyjęcie 29 lipca 1899 roku Regulaminu haskiego²²⁴.

W Regulaminie zidentyfikowano strony biorące udział w konflikcie zbrojnym. Na podstawie art. 1 Regulaminu haskiego z 1899 roku prawa i zwyczaje wojenne obowiązują nie tylko regularne armie, ale również milicje i korpusy ochotników, którzy spełniają łącznie cztery warunki:

1. pozostają pod dowództwem osoby odpowiedzialnej za swoich podwładnych,
2. posiadają stały, wyróżniający się znak rozpoznawczy, widoczny z odległości,
3. noszą swoją broń w sposób otwarty i widoczny,
4. prowadzą swoją działalność w zgodzie z prawem i zwyczajami wojny.

Dodatkowo za stronę wojującą, w rozumieniu art. 2 Regulaminu haskiego z 1899 roku, należy uznać ludność terytorium, które nie zostało zajęte i która przy nadejściu nieprzyjaciela spontanicznie chwyciła za broń, żeby stawić opór wojskom przeciwnika, nie mając jednocześnie czasu na zorganizowanie się w oddziały milicji lub korpus ochotniczy.

Postanowienia Regulaminu haskim z 1899 roku w szerokim zakresie odnoszą się do sposobów prowadzenia konfliktu zbrojnego, czyli metod walki. Wprowadzenie takiej regulacji miało przyczynić się do zwiększenia ochrony newralgicznych, a w dzisiejszym rozumieniu krytycznych obiektów. Zgodnie z art. 27 Regulaminu w czasie oblężeń i bombardowań strony powinny podjąć wszelkie niezbędne kroki, żeby w jak największym stopniu ochronić budowle przeznaczone na cele religijne, sztuki, nauki, charytatywne, szpitale i miejsca gromadzenia chorych i rannych. Jednakże wykorzystanie tych obiektów do celów wojskowych wyłączało ich ochronę przed atakiem.

²²² *Tamże*, s. 105.

²²³ G. Best, *Peace Conferences and the Century of Total War: The 1899 Hague Conference and What Came After*, „International Affairs (Royal Institute of International Affairs 1944-)”, 1999, vol. 75, no. 3, s. 625.

Zgodnie z ustaleniami konferencji pokojowej z 1899 roku następne konferencje miały odbywać się co siedem lat, jednak w związku z wojną rosyjsko-japońską druga konferencja pokojowa odbyła się dopiero w 1907 roku²²⁵. W jej obradach, rozpoczętych 15 czerwca 1907 roku uczestniczyły czterdzieści cztery państwa (co znaczenie przewyższało liczbę uczestników pierwszej konferencji)²²⁶. Prace konferencji skupiły się przede wszystkim na dalszym rozwoju zasady humanitaryzmu podczas konfliktu zbrojnego. Owocem obrad było przyjęcie trzynastu konwencji z zakresu międzynarodowego arbitrażu, rozbrojenia oraz prawa wojny²²⁷.

18 października 1907 roku na konferencji przyjęto między innymi Konwencję dotyczącą praw i zwyczajów wojny lądowej wraz z Regulaminem dotyczącym praw i zwyczajów wojny lądowej (IV Konwencja haska, Regulamin haski z 1907 r.)²²⁸. Konwencja wraz z załącznikiem stanowiły powtórzenie regulacji z 1899 roku. Przykładowo art. 27 Regulaminu haskiego z 1907 roku (powtórzenie art. 27 Regulaminu z 1899 roku) stanowi, że szpitale oraz inne miejsca, w których gromadzeni są chorzy i ranni powinny zostać wyłączone spod obłążeń i bombardowań. Ochrona nie obowiązywała w przypadku, gdy obiekty miały służyć celom wojennym. Oprócz zakazu atakowania obiektów medycznych Regulamin nakazywał właściwe oznaczenie szpitali oraz innych obiektów medycznych, poprzez zastosowanie widocznych znaków, które powinny zostać notyfikowane stronie przeciwnej (zob. art. 27 Regulaminu haskiego z 1907 roku).

Innym aktem przyjętym podczas drugiej konferencji pokojowej była Konwencja o bombardowaniu przez morskie siły zbrojne w czasie wojny (IX Konwencja haska)²²⁹. Ochrona rozciągała się również na obiekty religijne, szpitale oraz miejsca zbiórek rannych i chorych, pod warunkiem że nie były one wykorzystywane do celów wojskowych (zob. art. 5 IX Konwencji haskiej). Natomiast w art. 2 Konwencja określiła katalog obiektów będących potencjalnymi celami ataku. Zaliczono do nich zakłady wojskowe lub morskie, składy broni lub sprzętu wojennego, warsztaty i instalacje, mogące być użyte dla potrzeb floty lub armii nieprzyjacielskiej oraz okręty wojenne, znajdujące się w porcie.

²²⁵ S. Barcroft, *The Hague...*, s. 67.

²²⁶ J. Q. Barrett, *The Path from the 1907 Hague Conference to Nuremberg and Forward*, „Studies in Transnational Legal Policy”, 2008, vol. 39, s. 7.

²²⁷ *Tamże*.

²²⁸ *Konwencja dotycząca praw i zwyczajów wojny lądowej, podpisana wraz z odnośnym Regulaminem*, Haga, 18.10.1907, Dz. U. z 1927 r., nr 21, poz. 161.

²²⁹ *Konwencja o bombardowaniu przez morskie siły zbrojne w czasie wojny*, Haga, 18.10.1907, Dz. U. z 1936 r., nr 6 poz. 66.

Chociaż regulacje prawa haskiego odnosiły się bezpośrednio do sposobów prowadzenia działań zbrojnych, a nie do ochrony określonych obiektów czy osób, to na podstawie postanowień Regulaminów haskich z 1899 i 1907 roku możliwe jest wyprowadzenie ograniczonego standardu ochrony obiektów potencjalnie zaliczonych do infrastruktury krytycznej. Standard prawa haskiego przewidywał ochronę dwóch sektorów infrastruktury krytycznej. Po pierwsze, były to szpitale i inne obiekty medyczne zaliczane do sektora zdrowia. Po drugie, były to porty, klasyfikowane jako obiekty sektora transportu morskiego. Jednak ich ochrona była ograniczona do momentu wykorzystania ich do celów wojskowych.

2.2.1.3 Kodeks Liebera

Równocześnie z tworzeniem się załączków prawa genewskiego, na kontynencie amerykańskim doszło do pierwszego konfliktu zbrojnego, w którym zastosowanie znalazły wewnętrzne regulacje praw i zwyczajów wojennych. Konfliktem tym była wojna domowa w Stanach Zjednoczonych z lat 1861-1865 (wojna secesyjna), tocząca się pomiędzy rządem USA (dalej: Północ, Unia) a Skonfederowanymi Stanami Ameryki (dalej: Południe, Konfederacja)²³⁰. Jedną z głównych przyczyn wybuchu wojny secesyjnej była próba zniesienia niewolnictwa przez ówczesnie urzędującego prezydenta Stanów Zjednoczonych Abrahama Lincolna²³¹. Kluczową rolę odgrywały również kwestie ekonomiczne. Pomimo tego, że to Północ była lepiej rozwiniętym oraz zindustrializowanym terytorium USA, to Południe było handlowo związane z Wielką Brytanią oraz Francją²³². Z portów Południa na Stary Kontynent wypływały transporty bawełny, które napędzały europejski przemysł tekstylny. Toczyący się konflikt mógł negatywnie wpłynąć na relacje amerykańskiego rządu z krajami europejskimi.

A. Lincoln stanął przed wyzwaniem nie tylko utrzymania porządku konstytucyjnego w kraju, ale również poszanowania prawa międzynarodowego²³³. Jednym z pomysłów na osłabienie sił Konfederatów była blokada wszystkich ich portów, co skutecznie ograniczyłoby wpływy z handlu bawełną, jednakże niewystarczające siły marynarki wojennej mogłyby przeprowadzić nieefektywną blokadę tych portów. Skutkowałoby to nie tylko oporem ze strony mocarstw europejskich, ale także złamaniem postanowień Deklaracji poszanowania prawa

²³⁰ A. Mindrup, *The Lieber Code: A Historical Analysis of the Context and Drafting of General Orders No. 100*, „The Cardinal Edge”, 2021, vol. 1 (27), s. 4.

²³¹ G. Gunderson, *The Origin of the American Civil War*, „The Journal of Economic History”, 1974, vol. 34, nr 4, s. 915-916.

²³² A. Mindrup, *The Lieber Code...*, s.5.

²³³ Abraham Lincoln objął urząd prezydenta USA na miesiąc przed wybuchem wojny secesyjnej, zob. A. Mindrup, *The Lieber Code...*, s. 4.

morskiego (dalej: Deklaracja paryska z 1856 roku)²³⁴, która wprowadziła przesłanki skutecznej blokady portów morskich. Zgodnie z Deklaracją, aby blokada została uznana za wiążącą musi być skuteczna, a to oznacza, że siły blokujące muszą być na tyle wystarczające i efektywne aby uniemożliwić całkowity dostęp do wybrzeża nieprzyjaciela. Północ obawiała się, że siła jej marynarki wojennej jest niewystarczająca, żeby skutecznie zablokować dostęp do wybrzeża Konfederacji²³⁵. Pomimo tego, w 1861 roku rząd amerykański zdecydowała się zablokować południowe wybrzeże, jednocześnie ogłaszając stosowanie Deklaracji paryskiej z 1856 roku bez formalnego przystąpienia do niej²³⁶.

Istotnym problemem, niepokojącym dowództwo generalne armii unijnej, był sposób prowadzenia walki z Konfederatami. Pod koniec 1862 roku naczelny dowódca armii Unii Henry Halleck powołał komisję mającą na celu przygotowanie regulaminu prowadzenia działań zbrojnych²³⁷. W skład komisji wszedł między innymi Francis Lieber, niemiecki prawnik, który pod naciskiem władz pruskich wyemigrował do USA, a od 1857 roku zajmował stanowisko profesora na Uniwersytecie Columbia w Nowym Jorku²³⁸.

Rezultatem pracy F. Liebera było opracowanie kodeksu regulującego działania zbrojne. Kodeks został przyjęty 24 kwietnia 1863 roku przez prezydenta Stanów Zjednoczonych Rozkazem Generalnym numer 100, pod nazwą Instrukcje dla dowództw Armii Stanów Zjednoczonych w polu (dalej: Kodeks Liebera)²³⁹. Według Kodeksu Liebera działania zbrojne miały opierać się na zasadzie konieczności wojskowej, którą rozumiano jako podejmowanie takich środków, które są niezbędne do zakończenia wojny i są zgodne z prawem i zwyczajami wojennymi (zob. art. 14 Kodeksu Liebera). Pomimo tego, że konieczność wojskowa nie dopuszcza okrucieństwa²⁴⁰, to w art. 15 Kodeksu jako jeden z jej przykładów wymieniono wszelkie zniszczenie mienia oraz blokowanie ruchu na drogach i w kanałach, podróży lub komunikacji, a także uniemożliwienie przez wroga wykorzystywania środków do życia. Doktryna konieczności wojskowej nie uzyskała poparcia wśród Konfederatów. Uważali oni,

²³⁴ W 1856 roku, w następstwie wojny krymskiej, państwa uczestniczące w tym konflikcie, jak Francja, Wielka Brytania, Carstwo Rosyjskie oraz Imperium Osmańskie przyjęły deklarację regulującą między innymi blokadę wybrzeża, zob. *Deklaracja poszanowania prawa morskiego*, Paryż, 16.04.1856, w: P. K. Marszałek, *Międzynarodowe prawo humanitarne...*, s. 51.

²³⁵ A. Mindrup, *The Lieber Code...*, s.5.

²³⁶ *Deklaracja poszanowania prawa morskiego...*, s. 51.

²³⁷ A. Mindrup, *The Lieber Code ...*, s.7.

²³⁸ *Tamże*, s.4.

²³⁹ USA, *Instrukcje dla dowództw Armii Stanów Zjednoczonych w polu zatwierdzone przez prezydenta Stanów Zjednoczonych*, 23.04.1863, w: P. K. Marszałek, *Międzynarodowe prawo humanitarne...*, s. 3-20.

²⁴⁰ Art. 16 Kodeksu Liebera „Konieczność wojskowa nie dopuszcza okrucieństwa – to znaczy zadawania cierpień dla samego cierpienia lub zemsty, ani okaleczenia ani ranienia, chyba, że w czasie walki, ani tortur, by wymusić przyznanie się...”

że postępowanie żołnierzy Unii w zgodzie z koniecznością wojskową doprowadzi do naruszeń przyjętych praw i zwyczajów wojennych, ponieważ każdą zbrodnię będzie można wytłumaczyć koniecznością wojskową i osiągnięciem celu militarnego²⁴¹. Jednak celem regulacji wprowadzonych w Kodeksie Liebera nie było zapewnienie bezkarności żołnierzom, zasłaniających się koniecznością wojskową, a wprowadzenie poszanowania praw i zwyczajów wojennych w oparciu o zasady sprawiedliwości, honoru oraz humanitaryzmu (zob. art. 4 Kodeksu Liebera). Chociaż głównym celem każdego konfliktu zbrojnego jest wygrana, to żołnierze, nawet w oparciu o konieczność wojskową, nie powinni dążyć do tego za wszelką cenę, pomijając tak ważne zasady jak sprawiedliwość, honor oraz humanitaryzm.

Pomimo, że Kodeks Liebera nie zawierał rozdziału poświęconego ochronie infrastruktury krytycznej, to analiza jego postanowień pozwala sformułować standardy ochrony obiektów, zaliczonych dziś do tej infrastruktury. Regulacje Kodeksu wskazują na przedmiotowy charakter infrastruktury krytycznej. Zwycięzca konfliktu był uprawniony do przejęcia całego majątku publicznego oraz przejęcia, na własny użytek lub na pożytek własnego rządu, wszystkich dochodów z nieruchomości strony przeciwnej (zob. art. 31 Kodeksu Liebera). Zgodnie z postanowieniami art. 34 Kodeksu do majątku publicznego nie zaliczano takich obiektów jak kościoły, szpitale oraz inne placówki o charakterze wyłącznie charytatywnym, ustanowione dla celów edukacji lub promowania wiedzy (np. uniwersytety czy muzea). Celem wprowadzonych ograniczeń było, pomimo ewentualnej przegranej, zapewnienie podstawowych usług mogących wpływać na bezpieczeństwo ludności, na przykład dostęp do opieki medycznej. Jednak obiekty te mogły podlegać opodatkowaniu w celu zaspokojenia potrzeb publicznych. Dodatkowo szpitale, biblioteki, dzieła sztuki, zbiory naukowe oraz wszelkie cenne instrumenty (na przykład teleskopy) podlegały fizycznej ochronie i powinny zostać zabezpieczone przed wszelkimi możliwymi zniszczeniami, nawet jeśli podczas oblężenia lub bombardowania znajdują się w miejscach umocnionych (zob. art. 35 Kodeksu Liebera).

Doświadczenia wojny secesyjnej pokazują, że nawet własność prywatna, pod odpowiednimi warunkami, może być rozpatrywana jako infrastruktura krytyczna. W trakcie prowadzonych działań zbrojnych żołnierze Unii wielokrotnie niszczyli zbiory bawełny należące do Konfederatów²⁴². Celem zniszczeń bynajmniej nie było pozbawienie strony

²⁴¹ B.M. Carnahan, *Lincoln, Lieber and the Laws of War: The Origins and Limits of the Principle of Military Necessity*, „The American Journal of International Law”, 1998, vol. 92, nr 2, s 217-218.

²⁴² *Tamże*, s 226.

przeciwniej zapasów bawełny by uniemożliwić im produkcję odzieży wojskowej, a uderzenie w infrastrukturę ekonomiczną Konfederatów. Jak zostało już wspomniane, Stany Skonfederowane posiadały pokaźne pola uprawne bawełny, co stanowiło podstawę rozwoju gospodarczego, między innymi dzięki handlowi z państwami europejskimi. Ataki na składy bawełny wiązały się ze sporami międzynarodowymi, gdyż celem ataków była bawełna prawnie należąca już do Wielkiej Brytanii²⁴³. Po wojnie przed trybunałem arbitrażowym w sprawie pomiędzy Stanami Zjednoczonymi a Wielką Brytanią, amerykańscy przedstawiciele bronili ataków na brytyjskie składy bawełny uznając je za zgodne z zasadą konieczności wojskowej²⁴⁴.

Pomimo, że Kodeks Liebera stanowił zdecydowane *novum* w zakresie regulacji praw i zwyczajów wojny, przede wszystkim wprowadzał jako fundament działalności sił zbrojnych konieczność wojskową, to w ściśle ograniczony sposób uregulował kwestię ochrony obiektów niezbędnych dla zapewnienia bezpieczeństwa ludności cywilnej. Z obiektów medycznych tylko szpitale uzyskały odpowiedni zakres ochrony podczas konfliktu zbrojnego, chociaż w okresie wojny secesyjnej nastąpił rozwój usług medycznych na polu walki²⁴⁵. Autor Kodeksu zdecydował się podzielić obiekty występujące w konflikcie zbrojnym na dwie kategorie: własność publiczną oraz własność prywatną. W zakresie własności publicznej wprowadzono ochronę tylko ograniczonej liczby obiektów, do których zaliczają się między innymi szpitale. W przypadku własności prywatnej nie wprowadzono takiej ochrony, a co więcej powołując się na konieczność wojskową można było dokonać całkowitego zniszczenia własności prywatnej, jak w przypadku brytyjskiej bawełny. Kodeks Liebera, w odróżnieniu od współczesnych norm prawa międzynarodowego, nie przewidywał ochrony infrastruktury ekonomicznej.

2.2.2 Standard ochrony infrastruktury krytycznej w międzynarodowym prawie humanitarnym po 1977 roku

Dychotomiczny podział MPH stracił rację bytu w 1977 roku wraz z przyjęciem dwóch protokołów dodatkowych do KG z 1949 roku (PD I i PD II). Przyjęcie protokołów zwiększyło ochronę obiektów mogących zostać zaliczonych do infrastruktury krytycznej podczas konfliktu zbrojnego, poprzez rozszerzenie katalogu obiektów szczególnie chronionych. Kluczowym było

²⁴³ *Tamże*.

²⁴⁴ *Tamże*.

²⁴⁵ Wojna secesyjna stanowiła szczególny okres w rozwoju medycyny w Stanach Zjednoczonych. W celu zapewnienia odpowiedniej opieki medycznej rannym żołnierzom podjęto szereg czynności usprawniających działania personelu medycznego, w tym pielęgniarzy oraz osób zajmujących się obsługą ambulansów (ówcześnie nie używano terminu „ratowników medycznych”). Zob. D. C. Smith, *Military Medical History: The American Civil War*, „OAH Magazine of History”, 2005, vol. 19, nr 5, s. 17-19.

również zdefiniowanie zasady rozróżniania, która oznacza, że w celu zapewnienia poszanowania i ochrony ludności cywilnej oraz dóbr o charakterze cywilnym, strony konfliktu zbrojnego powinny zawsze odróżniać ludność cywilną od kombatanów oraz dobra o charakterze cywilnym od celów wojskowych, tym samym powinny kierować swoje operacje jedynie przeciwko celom wojskowym (zob. art. 48 PD I). O jej istocie dla MPH świadczy nienaruszalny charakter, niedopuszczający jakichkolwiek odstępstw²⁴⁶.

W opinii doradczej w sprawie legalności groźby lub użycia broni jądrowej z 1996 roku MTS potwierdził, że zasada rozróżniania, obok zasady niepowodowania zbędnego cierpienia, jest jedną z dwóch głównych zasad MPH o charakterze zwyczajowym²⁴⁷. Jednocześnie Trybunał wskazał, że pod żadnym pozorem zasada rozróżniania nie może zostać naruszona. Działanie państwa w sprzeczności z nią stanowią pogwałcenie prawa międzynarodowego²⁴⁸. Naruszenie zasady rozróżniania prowadzi również do odpowiedzialności karnej jednostki. Zgodnie z art. 8 ust. 2 lit. (b) Statutu MTK atak na ludność cywilną, obiekty o charakterze cywilnym lub jakiegokolwiek inny atak wymierzony w ludność cywilną stanowi zbrodnię wojenną. Tym samym, zarówno dowództwo wojskowe, jak i żołnierze wykonujący rozkazy, dopuszczając się naruszenia zasady rozróżniania, popełniają zbrodnię wojenną. Dlatego dokonując ataku na obiekty infrastruktury krytycznej, zarówno dowódcy, jak i żołnierze podejmujący działania zbrojne, powinni określić charakter tych obiektów, rozróżniający czy stanowią one cel wojskowy czy dobro o charakterze cywilnym.

2.2.2.1 Cel wojskowy

Definicja celu wojskowego została wprowadzona w art. 52 ust. 2 PD I, zgodnie z którym za cel wojskowy uznaje się obiekty, które z powodu swej natury, swego rozmieszczenia, swego przeznaczenia lub wykorzystania wnoszą istotny wkład do działalności wojskowej i których całkowite lub częściowe zniszczenie, zajęcie lub zneutralizowanie daje określoną korzyść w danej sytuacji. W przedstawionej definicji uwidaczniają się dwa podstawowe elementy. Po pierwsze, pojawia się opis samego obiektu (natura, lokalizacja, przeznaczenie lub wykorzystanie), a po drugie, opis skutków zniszczenia tego obiektu (korzyść dla strony przeciwnej)²⁴⁹. Tak zdefiniowany cel pozwala, w każdym przypadku indywidualnie,

²⁴⁶ MTKJ, *Prosecutor v. Stanislav Galić*..., par. 191.

²⁴⁷ MTS, *Legality of the threat or use of nuclear weapons*, Advisory Opinion, 8.07.1996, ICJ Reports, 1996, par. 78-79.

²⁴⁸ *Tamże*, par. 79.

²⁴⁹ Y. Sandoz, Ch. Swinarski, B. Zimmermann, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (dalej: Y. Sandoz et al., *Commentary to APs*...), International Committee of the Red Cross, Geneva 1987, s. 635.

rozpatrywać jego wojskowy charakter. Ustalenie katalogu zamkniętego celów wojskowych mogłoby doprowadzić do sytuacji, w której obiekt rzeczywiście wykorzystywany do działalności wojskowej nie znajdowałby się w katalogu, tym samym przeciwnik nie mógłby legalnie przeprowadzić ataku.

Powszechnie przyjętym jest, że definicja celu wojskowego posiada charakter normy zwyczajowej. Oznacza to, że każde państwo jest zobowiązane do jej przestrzegania, tym samym uznając definicję celu wojskowego z art. 52 ust. 2 PD I²⁵⁰. Jak zatem wygląda określanie celów wojskowych w państwach nie będących stroną PD I? Należy zwrócić uwagę na legislację dwóch państw, które obecnie przyjmuje się za jedne z najbardziej rozwiniętych militarnie oraz zdolnych do prowadzenia szeroko zakrojonych działań militarnych – USA oraz Izraela.

Stanowisko Stanów Zjednoczonych odnośnie do definicji celu wojskowego zawartej w art. 52 ust. 2 PD I jest jednoznaczne. Już w 1987 roku doradca prawny Departamentu Stanu oficjalnie oświadczył, że omawiana definicja znajduje potwierdzenie w amerykańskiej praktyce²⁵¹. Dekadę później rząd Stanów Zjednoczonych potwierdził, że uznaje definicję z art. 52 ust. 2 PD I za prawo zwyczajowe, jednocześnie wskazując, że cele wojskowe w amerykańskiej praktyce są szeroko interpretowane i obejmują między innymi obiekty lądowe czy obiekty gospodarcze wspierające działalność militarną²⁵². Stanowisko to znalazło również odzwierciedlenie w ustawodawstwie krajowym Stanów Zjednoczonych, gdyż definicja z art. 52 ust. 2 PD I została powtórzona w § 950p (a) (1) *Military Commissions Act* z 2009 roku²⁵³. Cele wojskowe zaś jako obiekty szerzej zostały określone w podręczniku wojskowym Departamentu Obrony USA z 2015 roku²⁵⁴. Uznano w nim, że cele wojskowe dzielą się na dwie kategorie – sprzęt wojskowy i bazy oraz obiekty zawierające cele wojskowe. Do pierwszej kategorii zalicza się wojskowy sprzęt znajdujący się na lądzie, w powietrzu oraz na morzu (np. pojazdy, statki, broń i amunicja), ale także bazy wojskowe lądowe, lotnicze i na morzu,

²⁵⁰ MTKJ, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia*, The Hague, 8.06.2000, „International Legal Materials”, 2000, vol. 39, nr 5, § 35.

²⁵¹ M. P. Dupuis, J. Q. Heywood, M. Y. F. Sarko, *The Sixth Annual American Red Cross-Washington College of Law Conference on International Humanitarian Law: A Workshop on Customary International Law and the 1977 Protocols Additional to the 1949 Geneva Conventions*, „American University Journal of International Law and Policy”, 1987, vol. 2, nr 2, p. 436.

²⁵² J. M. Henckaerts, L. Doswald-Beck, *Customary International Humanitarian Law Volume I: Rules*, Cambridge, 2005, s. 31.

²⁵³ USA, *Military Commissions Act*, 28.10.2009, <https://www.govinfo.gov/content/pkg/USCODE-2009-title10/html/USCODE-2009-title10-subtitleA-partII-chap47A-subchapVIII-sec950p.htm> (dostęp: 27.10.2024).

²⁵⁴ USA, *Department of Defense Law of War Manual, June 2015 (Updated December 2016)*, <https://www.onlinelibrary.ihl.org/wp-content/uploads/2021/05/USA-Law-of-War-Manual.pdf> (dostęp: 27.10.2024), s. 211-212.

bez rozróżnienia czy służą tylko celom szkoleniowym, dowodzeniu czy mają charakter ofensywny (np. kwatera główna, obiekty wywiadowcze)²⁵⁵. Natomiast do drugiej kategorii zalicza się wszystkie obiekty pośrednio wpływające na działalność militarną, jak miejsca magazynowania sprzętu wojskowego czy obiekty stanowiące zakwaterowanie lub schronienie żołnierzy²⁵⁶. Co więcej, w podręczniku wojskowym wprowadzono tzw. *a two-part test*, które pozwala ocenić czy dany obiekt wpisuje się w definicję obiektu wojskowego. Test wprowadza dwa elementy, którymi powinien wykazywać się obiekt wojskowy. Po pierwsze, obiekt w skuteczny sposób przyczynia się do działań wojennych, a po drugie, zaatakowanie, zdobycie lub zneutralizowanie tego obiektu zapewni w danych okolicznościach zdecydowaną przewagę militarną²⁵⁷. Zaatakowanie obiektu, który spełnia obie przesłanki, a więc przyczynia się do działań wojskowych, a jego zniszczenie przyniesie zdecydowaną przewagę militarną, pozwala siłom zbrojnym na pewność co do militarne go charakteru obiektu, co przekłada się na legalność ataku.

W porównaniu do Stanów Zjednoczonych Izrael nie zdefiniował w ustawodawstwie krajowym czym jest cel wojskowy, jednak zgodnie ze stanowiskiem sił zbrojnych należy go rozumieć zgodnie z treścią art. 52 ust. 2 PD I²⁵⁸. Aby obiekt został zakwalifikowany jako obiekt wojskowy, dla Izraela kluczowe jest aby jego zniszczenie przyniosło skuteczną przewagę militarną²⁵⁹. Istotnym dla oceny czy zachodzi przewaga militarna jest czas kiedy ta decyzja jest podejmowana. Jak zauważono w raporcie po operacji militarnej Izraela w Gazie pomiędzy grudniem 2008 roku a styczniem 2009 roku, decyzja powinna być podejmowana przez dowodzącego w czasie rzeczywistym, na podstawie dostępnych informacji wywiadowczych, a nie być oceniania dopiero po pewnym czasie (w ujęciu historycznym)²⁶⁰. Oznacza to, że dowódca w momencie przeprowadzenia ataku dysponuje wszystkimi niezbędnymi informacjami na temat charakteru obiektu – tego czy rzeczywiście wypełnia przesłanki celu wojskowego, bowiem tylko wtedy możliwe jest prawidłowe podjęcie decyzji o ataku.

Zgodnie z art. 52 ust. 2 PD I elementem charakterystycznym dla celu wojskowego jest jego natura. Każdy cel wojskowy, który ze swej natury przyczynia się do osiągnięcia korzyści

²⁵⁵ *Tamże*.

²⁵⁶ *Tamże*.

²⁵⁷ *Tamże*, s. 212.

²⁵⁸ J. M. Henckaerts, L. Doswald-Beck, *Customary...*, s. 186.

²⁵⁹ Izrael, *Israel's War with Hizbullah. Preserving Humanitarian Principles While Combating Terrorism*, Diplomatic Notes No. 1, Ministry of Foreign Affairs of Israel, April 2007, s. 5.

²⁶⁰ Izrael, *The Operation in Gaza 27 December 2008 – 18 January 2009. Factual and Legal Aspects*, 29.07.2009, <https://www.jewishvirtuallibrary.org/jsourc/Peace/GazaOpReport0709.pdf> (dostęp: 27.10.2024), s. 39.

wojskowej, jest legalnym celem ataku w świetle międzynarodowego prawa humanitarnego. Przez naturę rozumie się wkład, który obiekt wnosi w działalność wojskową²⁶¹. Podstawą w badaniu natury celu wojskowego jest jego rodzaj, czyli czy obiekt jest wykorzystywany przez siły zbrojne, np. magazyny z bronią i amunicją²⁶². Jak wskazuje się w doktrynie, ustalenie, że cel ze swojej natury przyczynia się do osiągnięcia korzyści wojskowej, nie wymaga od atakujących podejmowania dalszych ustaleń, czy istnieją inne przesłanki pozwalające na atak tego celu²⁶³.

Następnym kryterium, które definiuje cel wojskowy jest jego lokalizacja. Na podstawie tego kryterium cel staje się celem wojskowym tylko ze względu na to w jakim miejscu się znajduje²⁶⁴. W podręcznikach wojskowych wskazuje się, że cel wojskowy zajmuje określony teren, który ze względu na jego położenie wnosi istotny wkład w działalność wojskową i musi zostać z tego powodu przejęty lub zniszczony²⁶⁵. Jako przykład celu wojskowego ze względu na rozmieszczenie wskazuje się przyczółki, miejscowości czy konkretne budynki²⁶⁶.

Kryterium przeznaczenia i wykorzystania celu wojskowego należy rozważać jako kryterium o charakterze temporalnym²⁶⁷. Sam termin „przeznaczenie” oznacza, że na dany moment obiekt jeszcze nie stanowi celu wojskowego, ale w przyszłości stanie się takim celem. Natomiast zwrot „wykorzystanie” świadczy o korzystaniu z danego obiektu już w teraźniejszości²⁶⁸. Przykładem celu wojskowego wykorzystywanego w danej chwili może być budynek cywilny, w którym rozmieszczone zostały wrogie oddziały sił zbrojnych lub utworzono na jego terenie magazyn broni i amunicji. Jako przykład celu o przeznaczeniu wojskowym w przyszłości można wskazać lotnisko cywilne lub cywilne porty morskie, które w konflikcie zbrojnym mogą być wykorzystywane przez siły zbrojne, tym samym stając się celami wojskowymi²⁶⁹.

²⁶¹ Y. Sandoz et al., *Commentary to APs...*, s. 636.

²⁶² USA, *Department of Defense...*, s. 213.

²⁶³ P. Grzebyk, *Cele osobowe i rzeczowe w konfliktach zbrojnych w świetle prawa międzynarodowego*, Wydawnictwo Naukowe SCHOLAR, Warszawa 2018, s. 145.

²⁶⁴ Y. Sandoz et al., *Commentary to APs...*, s. 636.

²⁶⁵ Por. USA, *Department of Defense...*, s. 212 oraz Wielka Brytania, *JSP 383 The Joint Service Manual of the Law of Armed Conflict*, Joint Service Publication 383, 2004 Edition, <https://assets.publishing.service.gov.uk/media/5a7952bfe5274a2acd18bda5/JSP3832004Edition.pdf>, (dostęp: 27.10.2024), s. 55.

²⁶⁶ P. Grzebyk, *Cele osobowe...*, s. 147.

²⁶⁷ Y. Sandoz et al., *Commentary to APs...*, s. 636.

²⁶⁸ Wielka Brytania, *JSP 383...*, s. 56.

²⁶⁹ USA, *Department of Defense...*, s. 213.

Ostatnie kryterium – korzyści wojskowej, należy rozumieć jako przewagę, którą siły zbrojne osiągnęły nad swoim przeciwnikiem przez zniszczenie określonego celu wojskowego²⁷⁰. Istotnym czynnikiem jest czas, w którym korzyść wojskowa się pojawia. Powinno to nastąpić od razu, nie może to być korzyść, która zostanie osiągnięta dopiero w przyszłości²⁷¹. Jak stanowi art. 52 ust. 2 PD I korzyść wojskową można osiągnąć poprzez całkowite lub częściowe zniszczenie, zajęcie lub zneutralizowanie celu wojskowego. Co ważne, samo osiągnięcie korzyści militarnej nie zawsze musi wiązać się ze zniszczeniem danego obiektu, ale może również wywierać wpływ psychologiczny na stronę przeciwną, między innymi poprzez osłabienie jej morale²⁷².

Definiując infrastrukturę krytyczną jako strukturę połączonych ze sobą urządzeń, obiektów oraz systemów (w tym dóbr o charakterze niematerialnym), które wpływają na bezpieczeństwo państwa oraz ludności, obejmującą swoim zakresem między innymi sektory energetyki, łączności czy transportu należy uznać, że przy spełnieniu warunków określonych w art. 52 ust. 2 PD I obiekty te mogą zostać zakwalifikowane jako legalne cele ataku podczas konfliktu zbrojnego. Za cel wojskowy, zgodnie z art. 52 ust. 2 PD I, należy uznać sektor łączności, który stanowi podstawę prawidłowego zarządzania działaniami zbrojnymi na polu walki. Łączność wojskowa jest integralną częścią dowodzenia i kontroli nad siłami zbrojnymi w każdej fazie działań zbrojnych, od planowania, przez realizację, aż do oceny skutków tych działań²⁷³. Prawidłowe funkcjonowanie wojskowych systemów łączności wpływa bezpośrednio na skuteczność prowadzonych operacji zbrojnych, dlatego atak na ten system wypełnia przesłanki legalnego celu ataku. Po pierwsze, ze swojej natury system łączności wojskowej przyczynia się do osiągnięcia korzyści militarnej przez stronę przeciwną, ponieważ umożliwia dowodzenie siłami zbrojnymi na polu walki. Po drugie, zniszczenie systemu łączności wojskowej strony przeciwnej przynosi natychmiastową korzyść wojskową stronie atakującej, ponieważ uniemożliwia przeciwnikowi utrzymanie kontroli dowództwa nad siłami zbrojnymi pozostającymi na polu walki.

²⁷⁰ Y. Sandoz et al., *Commentary to APs...*, s. 636.

²⁷¹ *Tamże*.

²⁷² USA, *Department of Defense...*, s. 213.

²⁷³ R. Mustafovski, *Military Communications Doctrine - A Systematic Guide to Command, Control, and Communications in Modern Armed Forces*, LAP LAMBERT Academic Publishing, London/Chisinau 2026, s. 171.

2.2.2.2 Dobra o charakterze cywilnym

W przeciwieństwie do celów wojskowych, dobra o charakterze cywilnym są szczególnie chronione w MPH (zob. art. 52 ust. 1 PD I). Przede wszystkim trzeba zwrócić uwagę na zmianę semantyczną, gdzie w przypadku celu wojskowego, samo użycie zwrotu „cel” oznacza, że siły zbrojne mogą przeprowadzić atak na dany obiekt lub osobę²⁷⁴. Zupełnie inaczej wygląda to w przypadku obiektów cywilnych, odnośnie do których użyto sformułowania „dobra o charakterze cywilnym”. Pozwala to przypuszczać, że dany obiekt nie może być celem ataku, a jak sama nazwa wskazuje jest czymś co powinno pozostawać pod ochroną.

Z racji, że wszystko co nie jest celem wojskowym stanowi dobro o charakterze cywilnym należy przyjąć, że zdecydowana większość obiektów posiada charakter cywilny. Znalazło to swoje potwierdzenie w art. 52 ust. 3 PD I, gdzie określono zasadę domniemania dóbr o charakterze cywilnym, w szczególności jeśli chodzi o normalny użytek takich obiektów jak szkoły czy miejsca kultu religijnego. Znaczna część dóbr o charakterze cywilnym może zostać zaliczona do obiektów szczególnie chronionych.

Co więcej, niektóre obiekty określane jako dobra o charakterze cywilnym spełniają przesłanki infrastruktury krytycznej, mianowicie stanowią strukturę połączonych ze sobą urządzeń, obiektów oraz systemów, które wpływają na bezpieczeństwo państwa oraz ludności. W kontekście dóbr o charakterze cywilnym kluczowym aspektem tych obiektów jako infrastruktury krytycznej jest oddziaływanie na poczucie bezpieczeństwa ludności cywilnej, ale również utrzymywanie dostępu do zaopatrzenia i schronienia podczas konfliktu zbrojnego. Ochrona poszczególnych dóbr o charakterze cywilnym znajduje podwójne uzasadnienie (aspekt pozytywny i negatywny). Do dóbr o charakterze cywilnym zalicza się między innymi dobra niezbędne do przeżycia ludności cywilnej oraz obiekty zawierające niebezpieczne siły. Prawidłowe funkcjonowanie tych obiektów zapewnia dostęp ludności cywilnej do podstawowych usług realizujących jej potrzeby, jak dostęp do żywności, wody pitnej, energii elektrycznej czy ciepła (aspekt pozytywny). Jednak zakłócenie prawidłowego działania tych obiektów, a także obiektów wpływających na bezpieczeństwo środowiska naturalnego może doprowadzić do utraty zdrowia lub życia ludności cywilnej (aspekt negatywny). Dlatego należy przyjąć, że ochrona infrastruktury krytycznej, służącej ludności cywilnej wykracza daleko poza samą ochronę obiektów, a tak naprawdę stanowi zabezpieczenie ludności cywilnej przed

²⁷⁴ Y. Sandoz et al., *Commentary to APs...*, s. 634.

negatywnymi skutkami konfliktu zbrojnego²⁷⁵. Widoczne jest to szczególnie w skutkach ataków na dobra o charakterze cywilnym, które powodują śmierć, niedożywienie i odwodnienie, ale także zakłócają działanie instytucji publicznych, co wymusza dostarczenie pomocy humanitarnej²⁷⁶.

2.2.2.3 Dobra niezbędne do przeżycia ludności cywilnej

W art. 54 PD I i art. 14 PD II wprowadzono kategorię obiektów służących przetrwaniu ludności cywilnej, których żadna ze stron konfliktu bez wyjątku, nie może atakować, niszczyć, zabierać czy czynić nieużytecznymi. Zalicza się do nich obiekty takie jak zapasy żywności, urządzenia i zbiorniki z wodą do picia oraz urządzenia nawadniające. Lista ta ma otwarty charakter²⁷⁷, co z perspektywy współczesnych wyzwań dla ochrony infrastruktury krytycznej jest dobrym rozwiązaniem, gdyż umożliwia dostosowanie szerokiej gamy obiektów i systemów wchodzących w skład infrastruktury krytycznej do postanowień art. 54 PD I i art. 14 PD II²⁷⁸.

Szczególna uwaga powinna zostać poświęcona ochronie zapasów żywności, systemów dostarczających świeżą wodę oraz systemów irygacyjnych. Prawidłowe funkcjonowanie tych systemów jest kluczowe dla działania państwa oraz bezpieczeństwa ludności cywilnej, dlatego systemy dostarczania i filtrowania wody powinny być odpowiednio chronione. Jednak systemy te coraz częściej stają się celami ataków, czego przykładem jest cyberatak z maja 2020 roku, wymierzony w izraelskie wodociągi, który udało się skutecznie udaremnić²⁷⁹. Niektórzy podnoszą, że rozwiązaniem problemu ataku na systemy irygacyjne byłoby utworzenie stref neutralnych wokół źródeł wody, co służyłoby ochronie tych miejsc²⁸⁰.

2.2.2.4 Obiekty zawierające niebezpieczne siły

Innym typem obiektów chronionych na mocy postanowień art. 56 PD I i art. 15 PD II, są budowle i urządzenia zawierające niebezpieczne siły. Za takie budowle i urządzenia uważa się zapory, groble oraz elektrownie atomowe. Wyróżniają się one na tle innych chronionych obiektów tym, że nawet w momencie gdy stanowią cele wojskowe nie mogą być atakowane.

²⁷⁵ Humanity in War, *Global Initiative to Galvanize Political Commitment to International Humanitarian Law. Progress Report*, October 2025, <https://www.upholdhumanityinwar.org/sites/default/files/2025-10/Global%20IHL%20Initiative%20Progress%20Report%20October%202025%20ENGLISH.pdf> (dostęp: 12.05.2026) s. 33.

²⁷⁶ *Tamże*, s. 34.

²⁷⁷ Y. Sandoz et al., *Commentary to APs...*, s. 655.

²⁷⁸ J. Milewski, *Identyfikacja infrastruktury...*, s. 102-103.

²⁷⁹ *Israel: odparto poważny cyberatak...*

²⁸⁰ N. Jorgensen, *The Protection of Freshwater in Armed Conflict*, „Journal of International Law and International Relations”, 2007, vol. 3, nr 2, s. 73.

Wynika to ze skutków jakie wywołałyby takie ataki zarówno wśród ludności cywilnej, jak i w środowisku naturalnym.

Szeroko dyskutowana była kwestia otwartości tego katalogu, szczególnie w perspektywie poszerzenia go o instalacje oraz obiekty zajmujące się produkcją lub przetwarzaniem chemicznych substancji²⁸¹. W doktrynie podnosi się, że obiekty zawierające niebezpieczne siły, a niewymienione w katalogu art. 56 PD I są chronione na podstawie art. 55 PD I, co spowodowane jest potencjalnymi skutkami ataku na te obiekty. Uwolnienie niebezpiecznych sił, jak zanieczyszczeń chemicznych czy czynników chorobotwórczych, które nastąpiłoby po zaatakowaniu między innymi fabryki środków chemicznych, potencjalnie może wyrządzić rozległe, długotrwałe i poważne szkody w środowisku naturalnym²⁸². Właśnie dlatego przyjmuje się, że ochrona fabryk chemicznych i obiektów podobnych została poddana reżimowi art. 55 PD I. Jednak takie podejście stwarza zagrożenie podczas konfliktu zbrojnego o charakterze międzynarodowym, ponieważ w PD II nie uregulowano ochrony środowiska naturalnego. Norma art. 56 PD I została powtórzona w art. 15 PD II, a więc obiekty zawierające niebezpieczne siły są chronione podczas tego konfliktu. Inaczej jest z ochroną środowiska naturalnego, która nie znajduje uregulowania w PD II. Oznacza to, że uznanie obiektów chemicznych i podobnych za nienależące do kategorii obiektów zawierających niebezpieczne siły pozbawia skutecznej ochrony tych obiektów w konflikcie zbrojnym o charakterze międzynarodowym.

2.2.2.5 Środowisko naturalne

Środowisko naturalne od pewnego czasu jest otaczane szczególną ochroną, zarówno na płaszczyźnie krajowej, jak i międzynarodowej. MPH również reguluje jego ochronę. I tak, zgodnie z art. 55 ust. 1 PD I zabronione jest działanie, które mogłoby spowodować rozległe, długotrwałe i poważne szkody w środowisku naturalnym, jednak MPH nie definiuje tych przesłanek, co może przyczyniać się do nadinterpretacji, skutkując tym samym nieproporcjonalnymi atakami na środowisko naturalne²⁸³.

W celu prawidłowej ochrony środowiska naturalnego podczas konfliktu zbrojnego państwa powinny kierować się podstawowymi zasadami MPH²⁸⁴. Jak wynika z zasady rozróżniania, jeżeli środowisko naturalne nie stanowi celu wojskowego, to powinno być

²⁸¹ Y. Sandoz et al., *Commentary to APs...*, s. 666.

²⁸² *Tamże*, s. 668.

²⁸³ P. Grzebyk, *Cele osobowe...*, s. 190-191.

²⁸⁴ MTS, *Legality of the threat...*, par. 62.

traktowane jak obiekt cywilny i w związku z tym nie może być celem ataku. W art. 2 ust. 4 Protokołu w sprawie zakazów lub ograniczeń użycia broni zapalających, załączonego do Konwencji o zakazie lub ograniczeniu użycia pewnych broni konwencjonalnych, które mogą być uważane za powodujące nadmierne cierpienia lub mające niekontrolowane skutki z 1980 roku²⁸⁵ lasy oraz inna roślinność nie mogą być celem ataku przy pomocy broni zapalającej, chyba że środowisko naturalne jest wykorzystywane do ukrycia lub maskowania żołnierzy lub obiektów wojskowych.

Niszczenie środowiska naturalnego, a szczególnie lasów wykorzystywanych przez siły zbrojne jako miejsca ukrycia, stało się powszechną praktyką. Już amerykańscy żołnierze w trakcie wojny w Wietnamie w latach 60. XX wieku palili olbrzymie połacie lasów tropikalnych, żeby zwalczyć komunistycznych partyzantów²⁸⁶. Podobne działania podejmowano również w późniejszych konfliktach, na przykład w Timorze Wschodnim²⁸⁷. Użycie broni zapalającej wobec środowiska naturalnego przyczyniło się do wielu negatywnych skutków, nie tylko wobec samego środowiska, ale pośrednio wpływając na ludność cywilną. Szacuje się, że użycie napalmu przez siły zbrojne Stanów Zjednoczonych w Wietnamie przyczyniło się do znacznej utraty roślin hodowlanych i żywego inwentarza²⁸⁸.

MTS w opinii doradczej w sprawie legalności groźby lub użycia broni jądrowej z 1996 roku słusznie zauważył, że państwa muszą postępować proporcjonalnie w osiągnięciu celów wojskowych, a poszanowanie środowiska naturalnego jest jedną z oznak tej proporcjonalności²⁸⁹. Przy planowaniu ataku strony konfliktu powinny rozważyć czy dany atak nie przyniesie szkód pośrednich, między innymi w postaci zniszczenia środowiska naturalnego, co również mogłoby pośrednio wpływać na bezpieczeństwo ludności cywilnej²⁹⁰. Jako przykład można wskazać atak na fabrykę chemiczną, co spowodowałoby uwolnienie zanieczyszczeń do środowiska naturalnego²⁹¹.

²⁸⁵ *Protokół w sprawie zakazów lub ograniczeń użycia broni zapalających (Protokół III), załączony do Konwencji o zakazie lub ograniczeniu użycia pewnych broni konwencjonalnych, które mogą być uważane za powodujące nadmierne cierpienia lub mające niekontrolowane skutki*, Genewa, 10.10.1980, Dz. U. z 1984 r., nr 23, poz. 104.

²⁸⁶ M. Kaldor, *New and Old War. Organized Violence in a Global Era*, Stanford University Press, Cambridge 2012, 3. wydanie, s. 103.

²⁸⁷ *Tamże*.

²⁸⁸ *Reasons for US failure in defeating the Vietcong*, <https://www.bbc.co.uk/bitesize/guides/z9xcwmn/revision/3> (dostęp: 12.05.2026).

²⁸⁹ MTS, *Legality of the threat...*, par. 30.

²⁹⁰ MKCK, *Guidelines on the Protection of the Natural Environment in Armed Conflict. Rules and Recommendations Relating to the Protection of the Natural Environment Under International Humanitarian Law, with Commentary*, International Committee of the Red Cross, Geneva 2020, s. 53-54.

²⁹¹ *Tamże*, s. 54.

Obecnie prawo międzynarodowe stoi przed dużym wyzwaniem jakim jest ochrona środowiska naturalnego, w szczególności podczas konfliktu zbrojnego. Konieczny jest rozwój instytucji prawa międzynarodowego w tym zakresie. Jednak od pewnego czasu można zauważyć pewne postępy. W 2022 roku Komisja Prawa Międzynarodowego przyjęła projekt zasad chroniących środowisko naturalne podczas konfliktu zbrojnego²⁹². Głównym celem Projektu Zasad jest wzmocnienie ochrony środowiska, w tym podejmowanie środków mających na celu zapobieganie szkodom, ich łagodzenie oraz naprawienie już powstałych szkód (zob. Zasada 2 Projektu Zasad). Przyjęcie tych zasad bez wątpienia pozytywnie wpływa na rozwój ochrony środowiska naturalnego podczas konfliktu zbrojnego, jednak w dalszym ciągu trwa dyskusja nad ich charakterem prawnym²⁹³. Szczególnie widoczne jest to w stanowisku Stanów Zjednoczonych, które podnoszą, że rozwiązania zaproponowane przez KPM nie stanowią kodyfikacji prawa zwyczajowego, a w większości skupiają się na instrumentach *soft law*, co dowodzi braku ich prawnie wiążącego charakteru²⁹⁴.

2.3 Współczesne wyzwania a ochrona infrastruktury krytycznej w międzynarodowym prawie humanitarnym

Od kilku lat zaobserwować można intensywny rozwój nowoczesnych technologii, które są wykorzystywane w podwójny sposób. Część z nich służy doskonaleniu metod i środków walki, które pozwalają efektywniej atakować stronę przeciwną. Jednak nowoczesne technologie przyczyniają się również do ochrony infrastruktury krytycznej. Współczesne zarządzanie bezpieczeństwem infrastruktury krytycznej przechodzi proces „digitalizacji”, a więc zwiększenia jej odporności w cyberprzestrzeni²⁹⁵. Jest to odpowiedź na wzmożone cyberataki wymierzone w obiekty infrastruktury krytycznej, których celem jest zakłócenie prawidłowego działania państwa i oddziaływanie psychologiczne na ludność cywilną²⁹⁶. Dlatego zagrożenia związane z nowoczesnymi technologiami wpływającymi na

²⁹² KPM, *Draft principles on protection of the environment in relation to armed conflicts*, Yearbook of the ILC, 2022, vol. II, Part Two.

²⁹³ *Draft Principles on Protection of the Environment in Armed Conflict*, <https://lieber.westpoint.edu/draft-principles-protection-environment-armed-conflict/?fbclid=IwAR0xvz-MQYuHgZGsBaypc4viHBleCVAN78pKQTokoflDD8us0S8iC1rplWM> (dostęp: 27.10.2024).

²⁹⁴ USA, *Comments of the United States on the International Law Commission's draft principles on the protection of the environment in relation to armed conflicts*, 6.10.2021, https://legal.un.org/ilc/sessions/73/pdfs/english/poe_us.pdf (dostęp: 27.10.2024).

²⁹⁵ S. A. Argyroudis, S. A. Mitoulis, E. Chatzi, J. W. Baker, I. Brilakis, K. Gkoumas, M. Vousdoukas, W. Hynes, S. Carluccio, O. Keou, D. M. Frangopol, I. Linkov, *Digital technologies can enhance climate resilience of critical infrastructure*, „Climate Risk Management”, 2022, vol. 35, s. 6.

²⁹⁶ MKCK, The statement of ICRC President Mirjana Spoljaric, 23.03.2026, <https://www.icrc.org/en/statement/icrc-president-war-on-essential-infrastructure-is-war-on-civilians> (dostęp: 15.05.2026).

bezpieczeństwo infrastruktury krytycznej należy podzielić na dwie kategorie: identyfikację nowoczesnych technologii jako części składowych infrastruktury krytycznej (szczególnie status prawny dóbr niematerialnych w MPH²⁹⁷) oraz cyberataki wymierzone w infrastrukturę krytyczną podczas konfliktu zbrojnego²⁹⁸.

Wyzwaniem dla ochrony infrastruktury krytycznej podczas konfliktu zbrojnego jest również jego zmienny charakter, który wpływa na klasyfikację prawną ochrony infrastruktury krytycznej. Konflikt zbrojny o charakterze niemiędzynarodowym wprowadza ograniczoną ochronę niektórych obiektów mogących zostać zakwalifikowanymi jako infrastruktura krytyczna, na przykład obiektów, które powinny zostać objęte normami chroniącymi środowisko naturalne²⁹⁹. Dopiero kwalifikacja konfliktu zbrojnego jako międzynarodowego wprowadza pełną ochronę MPH³⁰⁰.

2.3.1 Rozwój nowych technologii a ochrona infrastruktury krytycznej

Konflikty zbrojne często było kołem napędowym dla rozwoju nowoczesnych technologii, które z czasem wchodziły do powszechnego użytku. Przykładem takiej technologii jest Internet. Początki rozwoju sieci na wzór dzisiejszego Internetu sięgają już lat 60. XX wieku, kiedy amerykańska armia dążyła do stworzenia nowego sposobu komunikacji pomiędzy placówkami wojskowymi w kraju. Taka infrastruktura miała być odporna na ataki z zewnątrz, zapewniając ciągłą łączność. Zaprojektowaniem tej sieci zajęła się *Advanced Research Projects Agency*, będąca częścią amerykańskiego Departamentu Obrony³⁰¹. Naukowcom udało się opracować program o nazwie *Advanced Research Projects Agency Network* (ARPANET), który był pierwszym przedsięwzięciem przypominającym dzisiejszą sieć komputerową.

Dążenia amerykańskich sił zbrojnych do stworzenia nowego źródła komunikacji pokrywają się czasowo z ówczesną dyskusją na temat nowoczesnych technologii i ich statusu

²⁹⁷ Ch. Johannot-Gradis, *Protecting the past for the future: How does law protect tangible and intangible cultural heritage in armed conflict?*, „International Review of the Red Cross”, 2015, vol. 97, no. 900, s. 1274-1275.

²⁹⁸ L. Gisel, T. Rodenhäuser, K. Dörmann, *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts*, „International Review of the Red Cross”, 2020, vol. 102, no. 913, s. 290.

²⁹⁹ M. M. Kenig-Witkowska, *Protection of the environment in times of non-international armed conflicts – a gap to be filled in*, „Studia Iuridica”, 2018, t. 78, s. 184.

³⁰⁰ Ch. Byron, *Armed Conflicts: International or Non-International?*, „Journal of Conflict and Security Law”, 2001, vol. 6, iss. 1, s. 90.

³⁰¹ ARPANET United States defense program, <https://www.britannica.com/topic/ARPANET> (dostęp: 27.10.2024).

w MPH³⁰². Nowe technologie, obejmujące na przykład instalacje nadawcze, stacje telewizyjne, telefony czy telegrafy zostały uznane przez MKCK jako cele wojskowe³⁰³.

Internet jako środek komunikacji bez wątpienia przynosi olbrzymią korzyść wojskową, ponieważ daje możliwość komunikowania się na odległość, co jest szczególnie potrzebne w trakcie prowadzenia operacji zbrojnych, gdzie dowództwo naczelne znajduje się czasami setki kilometrów od pola walki. Dlatego zniszczenie Internetu jako środka komunikacji również daje dużą korzyść wojskową, ponieważ odcina możliwość komunikowania się strony przeciwnej. Jednak Internet jest również jedną z najpopularniejszych form komunikacji wśród ludności cywilnej. Obecnie większość ludzi korzysta z różnego rodzaju mediów społecznościowych, ale należy pamiętać, że Internet jest wykorzystywany również do osiągnięcia celów gospodarczych przez państwo³⁰⁴.

Wojskowa geneza powstania Internetu i jego obecne, powszechne wykorzystanie przez ludność cywilną pozwala stwierdzić, że Internet podczas konfliktu zbrojnego może stanowić tak cel wojskowy, jak i dobro o charakterze cywilnym. Cyberprzestrzeń jest współcześnie wykorzystywana przez siły zbrojne do prowadzenia działań o charakterze militarnym, ale stanowi także centrum zarządzania nowoczesnymi technologiami wojskowymi, na przykład poprzez kontrolę pojazdów bezzałogowych³⁰⁵. Internet wykorzystany w taki sposób może stanowić legalny cel ataku podczas konfliktu zbrojnego. Jednak Internet powinien być rozpatrywany także w kontekście infrastruktury krytycznej (jako sektor teleinformatyczny), wpływającej na bezpieczeństwo ludności cywilnej. Szczególnie widoczne było to w trakcie pandemii COVID-19, kiedy życie miliarda ludzi zostało całkowicie „przeniesione” do Internetu³⁰⁶. Wszystkie podstawowe usługi, łącznie z dostępem do opieki zdrowotnej zostały przeniesione na platformy internetowe. W takim przypadku Internet przyjmuje formę dobra o charakterze cywilnym, a MPH powinno zapewnić mu skuteczną ochronę. Niestety współczesny standard ochrony MPH nie jest wystarczający dla bezpieczeństwa Internetu, tym

³⁰² M. Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford 2014, s. 191.

³⁰³ *Tamże*.

³⁰⁴ *Tamże*.

³⁰⁵ K. Kowalczevska, *Computer network operations in the light of ius in bello*, „Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje”, 2014, nr 15, s. 140-141.

³⁰⁶ T. E. Hutchins, *Safeguarding civilian internet access during armed conflict: Protecting humanity's most important resource in war*, „The Columbia Science & Technology Law Review”, 2020, vol. XXII, s. 179.

samym właściwym byłoby podjęcie dyskusji nad sformułowaniem nowych norm chroniących Internet jako sektor infrastruktury krytycznej³⁰⁷

2.3.1.1 Dobra niematerialne

Rozwój nowych technologii wprowadził do użytku dobra, które nie mają swojej fizycznej formy, a często przybierają postać tylko konkretnych danych³⁰⁸. Stanowi to poważne wyzwanie interpretacyjne czy MPH znajduje swoje zastosowanie. Jak wskazywano w komentarzach do PD I obiekty to rzeczy materialne (ang. *material thing*), jednak te opracowania zostały wydane w 1987 roku, kiedy rozwój nowych technologii nie był jeszcze na tak zaawansowanym etapie³⁰⁹.

Uznanie dobra niematerialnego jako celu wojskowego budzi więc spór w doktrynie. Można wskazać dwie szkoły rozumienia dóbr niematerialnych jako celów wojskowych. Pierwsza z nich, reprezentowana przez M. M. Schmitta, uznaje, że samo zniszczenie danych nie będzie powodowało ataku na cel wojskowy dopóki nie dojdzie do zmian w świecie fizycznym³¹⁰. Zgodnie z prezentowanym stanowiskiem dobra niematerialne nie mieszczą się w powszechnej definicji obiektu³¹¹. Zamiast tego, aby obiekt infrastruktury informatycznej został zakwalifikowany jako cel wojskowy musi spełnić przesłanki określone w art. 52 ust. 2 PD I, czyli ze swojej natury, lokalizacji, wykorzystania oraz przeznaczenia musi dawać przewagę wojskową. Jako typowy przykład infrastruktury informatycznej, która z natury jest celem wojskowym należy wskazać komputery oraz inne systemy z nimi związane, które zostały stworzone na potrzeby wojska³¹². Przesłanka lokalizacji celu wojskowego również wzbudza kontrowersje, ponieważ wymaga się aby była to fizyczna lokalizacja, mająca odzwierciedlenie w świecie fizycznym, dlatego adresu IP nie można uznać za przesłankę lokalizacyjną³¹³. Wykorzystanie obiektu cywilnego do celów militarnych skutkuje utratą charakteru cywilnego danego obiektu, a sam obiekt może stać się legalnym celem ataku, np. wykorzystanie przez żołnierzy cywilnej sieci komputerów³¹⁴. Oceniając przeznaczenie celu wojskowego, należy

³⁰⁷ *Tamże*, s. 180.

³⁰⁸ A. Kacała-Szwarczyńska, *Cyberatak w świetle międzynarodowego prawa humanitarnego konfliktów zbrojnych*, „Journal of Modern Science”, 2019, tom 2, nr 41, s. 179.

³⁰⁹ Y. Sandoz et al., *Commentary to APs...*, s. 633.

³¹⁰ M. N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge 2017, s. 437.

³¹¹ *Tamże*.

³¹² *Tamże*, s. 438.

³¹³ *Tamże*.

³¹⁴ *Tamże*.

ocenić korzyści wojskowe, który pojawią się dopiero w przyszłości³¹⁵. M. M. Schmitt jako przykład infrastruktury informatycznej, która ze swojego przeznaczenia jest celem wojskowym wskazuje zakup oprogramowania militarnego lub transport satelitów umożliwiających kontakt pomiędzy żołnierzami³¹⁶.

Druga szkoła, reprezentowana między innymi przez K. Maćaka, wskazuje, że dobra niematerialne również można uznać za cele w międzynarodowym prawie humanitarnym³¹⁷. K. Maćak twierdzi, że eksperci tworzący Tallinn Manual 2.0 błędnie przyjęli założenie, zgodnie z którym obiekt powinien być interpretowany na podstawie art. 31 Konwencji wiedeńskiej o prawie traktatów z 1969 roku³¹⁸, w zwykłym tego słowa znaczeniu. Zamiast tego, w przypadku dóbr niematerialnych, można kierować się wykładnią technologiczną oraz teleologiczną, które mają zastosowanie zarówno do prawa traktatowego, jak i prawa zwyczajowego³¹⁹. Nowe technologie charakteryzują się intensywnymi zmianami, co oznacza, że cele w konflikcie zbrojnymi mogą dynamicznie zmieniać swój charakter, tym samym wymaga się dostosowania norm MPH do współczesnych wymagań technologicznych³²⁰. Dlatego dobra niematerialne powinny zostać zaliczone do kategorii obiektów wojskowych. Przykładem może być kod źródłowy, który jest unikalny i przypisywany do danego obiektu, na przykład elektrowni lub szpitala. Ingerencja w kod lub jego zniszczenie może doprowadzić do negatywnych skutków w prawidłowym działaniu obiektu, do którego jest przypisany lub przyczynić się nawet do zniszczenia tego obiektu.

2.3.1.2 Zagrożenia cybernetyczne

Chociaż cyberprzestrzeń już od pewnego czasu jest traktowana jako piąty teatr działań wojennych, to w dalszym ciągu wzbudza kontrowersje oraz trudności w interpretacji obowiązujących norm międzynarodowego prawa humanitarnego w kontekście działań cybernetycznych. Wytlumaczenie pojęcia cyberprzestrzeni znajduje się zarówno w aktach prawnych, jak w opracowaniach naukowych. Artykuł 2 ust. 1b ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej z 2002 roku określa cyberprzestrzeń jako

³¹⁵ Zob. s. 71 niniejszej rozprawy.

³¹⁶ M. N. Schmitt, *Tallinn Manual 2.0...*, s. 438-439.

³¹⁷ K. Maćak, *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law*, „Israel Law Review”, 2015, vol. 48, nr 1, s. 13.

³¹⁸ *Konwencja Wiedeńska o Prawie Traktatów*, Wiedeń, 23.05.1969, Dz. U. z 1990 r., nr 74, poz. 439.

³¹⁹ MTS, *North Sea Continental Shelf (Germany v. Denmark, Germany v. Netherlands)*, Dissenting Opinion of Judge Tanaka, 20.02.1969, ICJ Reports, 1969, s. 182.

³²⁰ K. Maćak, *Military Objectives 2.0...*, s. 30.

przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne (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)³²¹. Natomiast jedna z definicji, pochodząca ze środowiska akademickiego, uznaje cyberprzestrzeń za „sieć łączącą systemy komputerowe obejmujące jednostki centralne i ich oprogramowania, ale także dane, sposoby i środki ich przesyłania. Cyberprzestrzeń obejmuje systemy powiązań internetowych, usługi teleinformatyczne oraz systemy zapewniające prawidłowe funkcjonowanie kraju, tj. systemy transportu, łączności, systemy infrastruktury energetycznej, wodociągowej i gazowej czy ochrony zdrowia”³²². Pomimo pewnych rozbieżności definicyjnych, bez wątpienia można wymienić pewne cechy charakterystyczne cyberprzestrzeni. Są to niezależność od miejsca, odległości, czasu, granic oraz względna anonimowość³²³.

Idąc tym tokiem można stwierdzić, że trudności definicyjne wzbudza również pojęcie „cyberataku”. Z uwagi na fakt, że technik przeprowadzania cyberataków jest wiele (*malware* – programy blokujące dostęp do danych na komputerze, ataki DoS lub DDoS – blokujące dostęp do stron internetowych)³²⁴, a cele takich ataków mogą być rozmaite, trudno jest wypracować jednolitą definicję cyberataku. Zgodnie z definicją podaną przez amerykański *National Institute of Standards and Technology* za cyberatak uważa się atak za pośrednictwem cyberprzestrzeni, którego celem jest dokonanie zakłóceń, wyłączenia, zniszczenia lub złośliwego wykorzystywania sieci komputerowej, zniszczenie integralności danych lub kradzież informacji³²⁵. Zupełnie inną definicję przywołano w opracowaniu specjalistów z zakresu prawa międzynarodowego, działających we współpracy z NATO *Cooperative Cyber Defence Centre of Excellence*, dotyczącym norm prawnych regulujących prowadzenie cyberoperacji³²⁶. Posiłkując się definicją ataku pochodzącą z PD I, za cyberatak uznano cyberoperację, defensywną i ofensywną, która może spowodować obrażenia bądź śmierć ludzi

³²¹ Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, Dz. U. z 2002 r., nr 156, poz. 1301.

³²² P. Tekielska, Ł. Czekaj, *Działanie służb w Unii Europejskiej realizujących zadania na rzecz bezpieczeństwa cybernetycznego*, w: M. Górka (red.) *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Wydawnictwo Difin S.A., Warszawa 2014, s. 163.

³²³ T. Aleksandrowicz, *Świat w sieci. Państwa – społeczeństwa – ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Wydawnictwo Difin S.A., Warszawa 2014, s. 12.

³²⁴ R. Maciejewski, *Problem ochrony infrastruktury...*, s. 33-34.

³²⁵ *Cyber Attack*, https://csrc.nist.gov/glossary/term/cyber_attack (dostęp: 27.10.2024).

³²⁶ M. N. Schmitt, *Tallinn Manual 2.0...*, s. 415.

lub uszkodzenia bądź zniszczenia obiektów (budynki, instalacje, itp.)³²⁷. W rozumieniu MPH za cyberoperację należy uznać wykorzystanie cyberataku jako środka walki, tj. konkretne uzbrojenie (*malware*, DoS) lub metodę walki czyli konkretną taktykę (szerzenie propagandy wojennej, zastraszanie ludności cywilnej).

Jednym z pierwszych konfliktów zbrojnych, podczas którego użyto cyberataku jako środka walki był konflikt w byłej Jugosławii w latach 90. XX wieku. W jego trakcie strona serbska zaatakowała stronę internetową NATO poprzez odmowę publicznego dostępu³²⁸. Istotna z punktu widzenia tego ataku jest kluczowa cecha charakterystyczna cyberataku, a mianowicie anonimowość. Poza tym, że atak wyszedł od strony serbskiej NATO nie posiadało żadnych informacji kto konkretnie odpowiadał za ten atak.

Obecnie cyberataki stanowią systematycznie wykorzystywaną metodę walki. Szczególnie jest to widoczne w konfliktach zbrojnych, w które zaangażowana jest Rosja. Przed podjęciem działań konwencjonalnych wobec Gruzji w 2008 roku Rosjanie przeprowadzili serię cyberataków wymierzonych w gruzińskie strony rządowe, co uniemożliwiło komunikację w zakresie bieżących działań zbrojnych³²⁹. Co jednak istotne, cyberataki nie były przeprowadzone przez regularne siły zbrojne Rosji, a przez prywatne osoby, powiązane ze służbami specjalnymi³³⁰.

Celem rosyjskich cyberataków stała się również ukraińska infrastruktura krytyczna. Należy wskazać co najmniej dwa poważne ataki wymierzone w ukraińską sieć energetyczną, do których doszło w 2015 roku³³¹ i 2016 rok³³². Oba ataki miały miejsce w okresie zimowy, pozbawiając tysiące osób dostępu do ogrzewania. W przeciwieństwie do cyberataków z 2008 roku, za atakami z 2015 i 2016 roku, stali oficerowi Głównego Zarządu Wywiadowczego Federacji Rosyjskiej³³³.

³²⁷ *Tamże*.

³²⁸ *Serbs launch cyberattack on NATO*, <https://fcw.com/1999/04/serbs-launch-cyberattack-on-nato/195288/> (dostęp: 27.10.2024).

³²⁹ P. Shakarian, *The 2008 Russian Cyber Campaign Against Georgia*, „Military Review”, 2011, November-December, s. 63-64.

³³⁰ M. Rzeszuta, *Sieć. Piąty Teatr Działań Wojennych: 2008 – Informatyczna Blokada Gruzji*, „Układ Sił”, 2020, nr 23, s. 53.

³³¹ *Blackout w zachodniej Ukrainie – cyber atak o wymiarze międzynarodowym*, <https://pulaski.pl/komentarz-blackout-w-zachodniej-ukrainie-cyber-atak-o-wymiarze-miedzynarodowym/> (dostęp: 27.10.2024).

³³² *Ukraine's power outage was a cyber attack: Ukrenergo*, <https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA> (dostęp: 27.10.2024).

³³³ USA, *United States District Court Western District of Pennsylvania*, Indictment, 15.10.2020, <https://www.justice.gov/usao-wdpa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware> (dostęp: 27.10.2024).

Sytuacja z 2008 roku została powtórzona w 2022 roku podczas rosyjskiej agresji na Ukrainę. Już w styczniu, czyli miesiąc przed inwazją, Rosjanie rozpoczęli szeroko zakrojoną operację w cyberprzestrzeni, mającą na celu blokowanie stron rządowych oraz służb specjalnych Ukrainy³³⁴. W obecnej fazie konfliktu, w 2026 roku, działalność w cyberprzestrzeni obejmuje przede wszystkim propagandę wojenną, której celem jest terroryzowanie ludności cywilnej³³⁵, a cyberataki wymierzone w infrastrukturę krytyczną są skutecznie odpierane przez ukraińskie służby specjalne³³⁶.

Przytoczone powyżej przykłady pokazują, że obiekty infrastruktury krytycznej pozostają częstym celem cyberataku podczas konfliktu zbrojnego. Stanowi to poważne zagrożenie zarówno dla bezpieczeństwa państwa, jak i ludności cywilnej, ponieważ atak przeprowadzony w cyberprzestrzeni może przez długi czas nie powodować zmian w świecie fizycznym, a tylko zakłócać prawidłowe działanie obiektu. Jednak współczesne MPH nie przewiduje skutecznej ochrony przed działaniami w cyberprzestrzeni. Co więcej, samo prowadzenie operacji w cyberprzestrzeni w dalszym ciągu wzbudza spór w doktrynie. Większość przedstawicieli doktryny wskazuje, że do cyberoperacji zastosowanie znajdują przepisy zarówno *ius ad bellum* oraz *ius in bello*³³⁷. W mniejszości natomiast pozostaje pogląd, że zastosowanie *ius in bello* do działań w cyberprzestrzeni pozwoliłoby na uznanie cyberataku za atak w rozumieniu art. 49 PD I, tym samym dopuszczając do potencjalnej eskalacji konfliktu z udziałem sił konwencjonalnych³³⁸. Dla skutecznej ochrony infrastruktury krytycznej właściwym jest pogląd reprezentowany przez większość doktryny, a więc stosowanie *ius in bello* dla operacji prowadzonych w cyberprzestrzeni. Pozwala to na wprowadzenie minimalnych standardów ochrony obiektów potencjalnie zaliczanych do infrastruktury krytycznej.

³³⁴ Cyberatak na Ukrainę. Nie działają strony ministerstwa obrony i sił zbrojnych, problemy w bankach, <https://cyberdefence24.pl/cyberbezpieczenstwo/trwa-cyberatak-na-ukraine-nie-dzialaja-strony-ministerstwa-obrony-i-sil-zbrojnych-problemy-w-bankach> (dostęp: 27.10.2024).

³³⁵ Wojenna cenzura i propaganda Rosji, <https://www.pism.pl/publikacje/wojenna-cenzura-i-propaganda-rosji> (dostęp: 27.10.2024).

³³⁶ SBU odparła rosyjskie cyberataki na infrastrukturę krytyczną, <https://cyberdefence24.pl/polityka-i-prawo/sbu-odparla-rosyjskie-cyberataki-na-infrastrukture-krytyczna> (dostęp: 27.10.2024).

³³⁷ A. Małecka, *Cyber-operations under international law*, „Colloquium: pedagogika, nauki o polityce i administracji”, 2022, t. 14, nr 3, s. 159.

³³⁸ R. Abrashin, *On Thin Ice: Qualification of Cyber-Attacks on Personal Data under International Humanitarian Law*, „Журнал ВШЭ по международному праву (HSE University Journal of International law)”, 2024, vol. 2, no. 4, s. 50.

2.3.2 Zmienny charakter konfliktu zbrojnego

MPH *expressis verbis* wyróżnia dwa rodzaje konfliktów zbrojnych – międzynarodowy konflikt zbrojny oraz niemiędzynarodowy konflikt zbrojny. Międzynarodowy konflikt zbrojny został określony jako konflikt pomiędzy co najmniej dwoma państwami (wspólny artykuł 2 dla czterech KG z 1949 roku). Artykuł 1 ust. 4 PD I rozszerzył definicję międzynarodowego konfliktu zbrojnego na walki przeciwko rządowi rasistowskiemu oraz przeciwko panowaniu kolonialnemu, w ramach których ludy realizują swoje prawo do samostanowienia. PD I był tworzony w latach 70. XX wieku, a więc w czasach kiedy wiele państw, szczególnie afrykańskich, walczyło przeciwko metropoliom. Starając się zapewnić odpowiednią ochronę walczącym o wolność, zdecydowano się wprowadzić postanowienia o walkach wyzwoleniczych³³⁹. Dodatkowej regulacji poddano również okupację, którą – najprościej – rozumie się jako faktyczne sprawowanie władzy nad terytorium strony przeciwnej.

Jak wskazano powyżej stronami międzynarodowego konfliktu zbrojnego co do zasady są państwa. Konflikty w byłej Jugosławii w latach 90. XX wieku uwiaryściły problem scharakteryzowania konfliktu zbrojnego, w którym stronami były państwo oraz niepaństwowa grupa zbrojna, kontrolowana przez inne państwo³⁴⁰. Aby państwo ponosiło odpowiedzialność za działania kontrolowanej grupy zbrojnej, musi sprawować nad nią całkowitą kontrolę (ang. *overall control*). MTKJ w sprawie przeciwko Duško Tadićowi przedstawił szereg warunków, które muszą zostać spełnione aby państwo sprawowało całkowitą kontrolę nad grupą zbrojną³⁴¹. Przede wszystkim wymaga się, aby państwo brało udział w organizowaniu, planowaniu oraz koordynowaniu podejmowanych przez grupę zbrojną działań militarnych, ale także powinno udzielać im niezbędnego wsparcia w zakresie finansowania działalności, szkolenia członków oraz dostarczania potrzebnego wyposażenia³⁴².

Odmienne stanowisko zaprezentował MTS w sprawie Nikaragui przeciwko Stanom Zjednoczonym jeszcze w 1986 roku³⁴³. W orzeczeniu tym MTS rozpatrzył możliwość przypisania Stanom Zjednoczonym odpowiedzialności za naruszenia prawa międzynarodowego dokonanych przez siły *Contras*. W tym celu Trybunał dokonał analizy w jakim stopniu rząd amerykański sprawował kontrolę nad wspieranymi bojówkami. Zgodnie

³³⁹ Y. Sandoz et al., *Commentary to APs...*, s. 51-52.

³⁴⁰ A. Cassese, *The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia*, „European Journal of International Law”, 2007, vol. 18, nr 4, s. 655.

³⁴¹ MTKJ, *The Prosecutor v. Duško Tadić*, Appeals Chamber Judgment, 15.07.1999 r., IT-94-1, par. 137.

³⁴² *Tamże*.

³⁴³ MTS, *Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. USA)*, Judgment, 27.06.1986, ICJ Reports, 1986, par. 115.

z ustaleniami MTS Stany Zjednoczone nie odpowiadały za powstanie *Contras*, natomiast wspierały to ugrupowanie finansowo, dostarczając uzbrojenie czy szkoląc bojówki³⁴⁴. Aby rozstrzygnąć o potencjalnej odpowiedzialności Stanów Zjednoczonych Trybunał posłużył się tzw. *effective control test*³⁴⁵. Oznacza to, że nawet jeśli pomoc finansowa oraz szkoleniowa Stanów Zjednoczonych okazała się niezbędna do działania *Contras*, to bez skutecznej kontroli nad ich działalnością nie sposób przypisać im odpowiedzialności za czyny popełnione przez bojówki, jak kierowanie lub wymuszanie popełnienia czynów sprzecznych z prawem międzynarodowym³⁴⁶.

Kwestią istotną, pozwalającą określić czy doszło do rozpoczęcia międzynarodowego konfliktu zbrojnego jest ustalenie intensywności walk pomiędzy stronami. W orzecznictwie wskazuje się, że strony konfliktu powinny osiągnąć pewien poziom intensywności walk³⁴⁷. W tym przypadku intensywność walk należy rozumieć jako długotrwałą przemoc, występującą na dużą skalę. Zatem krótkotrwałe potyczki pomiędzy siłami zbrojnymi poszczególnych państw nie będą prowadziły do powstania konfliktu zbrojnego o charakterze międzynarodowym, czego przykładem są walki na granicy pakistańsko-indyjskiej (napięcia na granicy sięgają końca lat 40. XX wieku)³⁴⁸. W trakcie tych starć niejednokrotnie dochodziło do strat zarówno wśród żołnierzy, jak i sprzętu, jednak ze względu na brak intensywności nie można zaklasyfikować tego jako konfliktu zbrojnego o charakterze międzynarodowym.

Niemieждународowy konflikt zbrojny został zdefiniowany jako konflikt pomiędzy siłami zbrojnymi państwa a rozłamowymi siłami zbrojnymi lub innymi zorganizowanymi uzbrojonymi grupami (art. 1 ust. 1 PD II). Uznanie zorganizowanej grupy zbrojnej za stronę międzynarodowego konfliktu zbrojnego wiąże się z wypełnieniem dwóch warunków, tj. grupa musi pozostawać pod odpowiedzialnym dowództwem oraz musi sprawować taką kontrolę nad częścią jej terytorium, że może przeprowadzać ciągłe i spójne operacje wojskowe oraz stosować postanowienia PD II.

Aby w międzynarodowym konflikcie zbrojnym zastosowanie znalazły postanowienia PD II ważne jest określenie odpowiedniego stopnia intensywności oraz zorganizowania stron konfliktu. Celem prawidłowego określenia intensywności działań

³⁴⁴ *Tamże*, par. 108.

³⁴⁵ *Tamże*, par. 115.

³⁴⁶ *Tamże*.

³⁴⁷ MTKJ, *The Prosecutor v. Dusko Tadić*, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2.10.1995 r., IT-94-1, par. 70.

³⁴⁸ *Conflict Between India and Pakistan*, <https://www.cfr.org/global-conflict-tracker/conflict/conflict-between-india-and-pakistan> (dostęp: 27.10.2024).

zbrojnych pod uwagę należy wziąć: liczbę konfrontacji, czas trwania oraz ich intensywność, rodzaj broni i innego sprzętu wojskowego użytych podczas konfrontacji, liczbę i kaliber wystrzelonej amunicji, liczbę osób i rodzaj sił biorących udział w walkach, liczbę ofiar, zakres zniszczeń materialnych, liczbę cywilów uciekających ze strefy walki oraz ewentualne zaangażowanie RB ONZ³⁴⁹. O zorganizowaniu grupy zbrojnej, zgodnie z wymaganiami MPH, świadczy:

1. hierarchia dowodzenia wraz z określonymi zasadami i mechanizmami dyscypliny,
2. posiadanie bazy wojskowej,
3. kontrolowanie określonego terytorium,
4. dostęp do uzbrojenia i innego sprzętu wojskowego,
5. prowadzenie rekrutacji i szkolenia wojskowego,
6. zdolność planowania, koordynowania i prowadzenia operacji wojskowych,
7. zdolność tworzenia strategii wojskowej i stosowania taktyki wojskowej,
8. zdolność podejmowania jednolitych decyzji oraz negocjowania i zawierania umów, takich jak zawieszenie broni czy porozumienia pokojowe³⁵⁰.

Stosowanie powyższych kryteriów pozwala określić czy zastosowanie znajdą normy wynikające z PD II, a więc czy miejsce ma międzynarodowy konflikt zbrojny czy są to jeszcze wewnętrzne napięcia i rozruchy regulowane przez prawo wewnętrzne państwa, z uwzględnieniem ochrony wynikającej z międzynarodowego prawa praw człowieka (art. 1 ust. 2 PD II). Wpływa to bezpośrednio na ochronę ludności cywilnej oraz obiektów szczególnie chronionych, ponieważ z momentem wystąpienia międzynarodowego konfliktu zbrojnego zaczynają obowiązywać normy MPH, a tym samym zwiększa się zakres ochrony obiektów zaliczanych do infrastruktury krytycznej.

Właściwa identyfikacja charakteru (międzynarodowego lub międzynarodowego) konfliktu zbrojnego wpływa na szerszy lub węższy zakres ochrony obiektów infrastruktury krytycznej. Sytuacja konfliktu zbrojnego o charakterze międzynarodowym wprowadza najszerszą ochronę obiektów infrastruktury krytycznej³⁵¹. Na podstawie PD I ochrona obejmuje swym zakresem obiekty niezbędne dla przeżycia ludności cywilnej, obiekty zawierające niebezpieczne siły (elektrownie atomowe, tamy oraz groble), ale także szeroko rozumiane

³⁴⁹ MTKJ, *The Prosecutor v. Haradinaj et al.*, Trial Chamber Judgement, 3.04.2008 r., IT- 04-84-T, par. 49.

³⁵⁰ *Tamże*, par. 60.

³⁵¹ R. Bartels, *Timelines, borderlines and conflicts. The historical evolution of the legal divide between international and non-international armed conflicts*, „International Review of the Red Cross”, 2009, vol. 91, no. 873, s. 67.

środowisko naturalne, a jego normy należy odnosić między innymi do fabryk chemicznych. Odmienne sytuacja infrastruktury krytycznej kształtuje się w przypadku konfliktu zbrojnego o charakterze międzynarodowym, który cechuje się ograniczonym zakresem ochrony³⁵². PD II wprowadza ochronę obiektów niezbędnych dla przeżycia ludności cywilnej i obiektów zawierających niebezpieczne siły. Natomiast w przypadku konfliktu zbrojnego o charakterze międzynarodowym całkowicie została pominięta kwestia ochrony środowiska naturalnego, a co za tym idzie obiektów infrastruktury krytycznej z sektora chemicznego, których uszkodzenie lub zniszczenie doprowadzi nie tylko do dewastacji środowiska naturalnego, ale również może prowadzić do utraty życia lub zdrowia ludności cywilnej.

2.4 Podsumowanie

Na podstawie powyższych rozważań należy stwierdzić, że normy współczesnego MPH przewidują jedynie podstawowy standard ochrony infrastruktury krytycznej. Bez wątplenia przyczyną jej minimalnego standardu jest brak zdefiniowania pojęcia infrastruktury krytycznej w MPH. Zamiast tego postanowienia KG z 1949 roku, PD I oraz PD II odwołują się do konkretnych obiektów – medycznych, niezbędnych do przeżycia ludności cywilnej, zawierających niebezpieczne siły oraz wpływających na bezpieczeństwo środowiska naturalnego. Dopiero przyrównanie tych obiektów do definicji infrastruktury krytycznej pochodzącej spoza MPH pokazuje, że mogą one zostać zaliczone do tej infrastruktury.

Ograniczona ochrona infrastruktury krytycznej podczas konfliktu zbrojnego może wiązać się również z brakiem ochrony przewidzianej dla instytucji państwowych. Nieprzerwane i prawidłowe działanie administracji publicznej podczas konfliktu zbrojnego wpływa na skuteczną ochronę ludności cywilnej. W związku z tym, konieczne jest wprowadzenie nowych przepisów rozszerzających ochronę obiektów podczas konfliktu zbrojnego również na cywilne obiekty państwowe (na przykład urzędy nadzorujące sektory energetyczne czy medyczne).

Wyzwaniem dla ochrony infrastruktury krytycznej podczas konfliktu zbrojnego jest również rozwój nowoczesnych technologii, który wprowadza nowe kategorie obiektów, jak dobra niematerialne (np. kod źródłowy systemu zarządzania elektrownią atomową). Prawo traktatowe raczej nie reguluje nowych wynalazków, które realnie znajdują swoje zastosowanie podczas konfliktów zbrojnych, czego przykładem są wspomniane dobra niematerialne. Żaden

³⁵² A. J. Carswel, *Classifying the conflict: a soldier's dilemma*, „International Review of the Red Cross”, 2009, vol. 91, no. 873, s. 149.

akt prawny nie definiuje czym one są, ani czy można je zaliczyć do obiektów fizycznych. Nawet doktryna nie przynosi odpowiedzi co do ich charakteru. Natomiast właściwym wydaje się rozszerzenie ochrony MPH na dobra niematerialne, szczególnie w kontekście ich wykorzystania w obiektach infrastruktury krytycznej. Wspomniany kod źródłowy, czy szerzej cały system operacyjny jest potrzebny dla prawidłowego działania infrastruktury krytycznej, dlatego nawet jeśli atak nie powoduje bezpośrednich skutków w świecie fizycznym, nie oznacza to, że dobra niematerialne nie powinny podlegać ochronie MPH.

Wszystkie współczesne wyzwania wymagają wzmocnienia ochrony infrastruktury krytycznej jako czynnika bezpośrednio wpływającego na bezpieczeństwo ludności cywilnej. Określenie jedynie minimalnych standardów ochrony infrastruktury krytycznej w MPH nie oznacza, że państwa nie są w stanie zapewnić większej kontroli nad infrastrukturą krytyczną podczas konfliktu zbrojnego. Przede wszystkim państwa powinny wykorzystać pozaprawne środki ochrony infrastruktury krytycznej, obejmujące politykę bezpieczeństwa i strategię zarządzania obiektami krytycznymi, ale także działania wywiadowcze pozwalające śledzić, oceniać oraz analizować potencjalne szkody w infrastrukturze krytycznej³⁵³.

³⁵³ B. M. Figueiredo, *Strengthening the protection of civilian infrastructure in armed conflict: Practical measures to operationalize IHL and reduce civilian harm*, „International Review of the Red Cross”, 2026, s. 30.

3 Multicentryczny charakter standardu ochrony infrastruktury krytycznej

3.1 Wprowadzenie

Pomimo, że problematyką niniejszej rozprawy doktorskiej jest prawnomiędzynarodowa ochrona infrastruktury krytycznej podczas konfliktu zbrojnego, to z perspektywy właściwego ustalenia standardu ochrony konieczne jest odwołanie się do standardów ochrony przed zagrożeniami, które mają miejsce w czasie pokoju. To właśnie te regulacje są bogatsze o konkretne normy chroniące infrastrukturę krytyczną.

Ustalenie standardu ochrony infrastruktury krytycznej wobec zagrożeń w czasie pokoju wymagało przeprowadzenia dwuetapowej analizy. W pierwszym etapie skupiono się na rosyjskich działaniach hybrydowych, które od momentu wybuchu konfliktu na Ukrainie w 2014 roku są regularnie prowadzone wobec państw NATO. W ramach przeprowadzonych badań zdefiniowano zagrożenia hybrydowe oraz poddano analizie działalność dwóch organizacji międzynarodowych – UE oraz NATO, które skupiają państwa będące aktywnymi celami działalności hybrydowej ze strony Rosji.

W drugim etapie skupiono się na zagrożeniach terrorystycznych, które – pomimo wyciszenia od momentu upadku tzw. Państwa Islamskiego – w dalszym ciągu stanowią poważne zagrożenia dla infrastruktury krytycznej. W pierwszej kolejności dokonano przekrojowej analizy definicji terroryzmu, a następnie badaniu poddano dorobek prawny ONZ oraz RE w zakresie zwalczania terroryzmu. Argumentem dla wyboru tych dwóch organizacji międzynarodowych jest szeroki zakres regulacji, które zostały przyjęte na ich forach.

3.2 Ochrona infrastruktury krytycznej a zagrożenia hybrydowe

Słowniki języka polskiego zawierają zróżnicowane definicje terminu „hybryda”. Idąc za SJP PWN hybrydą jest „coś, co składa się z różnych elementów, często do siebie niepasujących”, „roślina lub zwierzę powstałe ze skrzyżowania dwóch odmian, ras lub gatunków” lub „wyraz złożony z elementów należących do dwóch różnych języków”³⁵⁴. WSJP PAN dostarcza jeszcze więcej definicji pojęcia „hybryda” wskazując, że jest to między innymi „mitologiczny potwór, którego głowa należy do innego znanego stworzenia niż

³⁵⁴ *Hybryda*, <https://sjp.pwn.pl/szukaj/hybryda.html> (dostęp: 2.06.2025).

pozostałe części ciała” czy potoczna nazwa samochodu hybrydowego³⁵⁵. Jednocześnie w WSJP PAN zawarta została definicja wojny hybrydowej, która definiuje się jako „działania wymierzone przeciw jakiemuś państwu, niemające wyłącznie charakteru bezpośredniej konfrontacji wojskowej, ale obejmujące różnego rodzaju destrukcję działania administracji państwa, blokowanie łączności, prowokowanie zamieszek i akty terrorystyczne”³⁵⁶. Również do słowników języka angielskiego wprowadzono pojęcie „wojny hybrydowej” (ang. *hybrid warfare*). W Cambridge Dictionary wojna hybrydowa została zdefiniowana jako „*the use of a range of different methods to attack an enemy, for example, the spreading of false information, or attacking important computer systems, as well as, or instead of, traditional military action*”. Porównanie powyższych definicji pozwala na określenie wojny hybrydowej jako nieregularnych działań militarnych (niekoniecznie zbrojnych), z wykorzystaniem zróżnicowanych sposobów ataku lub siły nacisku, celem destabilizacji obcego państwa. Tym samym państwo będące celem ataków hybrydowych stoi przed wielkim wyzwaniem jakim jest zidentyfikowanie tych zagrożeń, ale również podjęcie odpowiednich kroków chroniących kluczowe sektory państwa, w tym infrastrukturę krytyczną.

3.2.1 Geneza pojęcia wojny hybrydowej

Chociaż samo pojęcie „wojny hybrydowej” jest terminem nowym, wprowadzony w 2002 roku przez W. J. Nemeth w pracy „*Future War and Chechnya: A Case for Hybrid Warfare*”³⁵⁷, to jednak prowadzenie działań militarnych w sposób odpowiadający dzisiejszej definicji wojny hybrydowej jest zjawiskiem występującym już od starożytności. Jej początków można doszukiwać się już w Starożytnych Chinach, gdzie myśliciel Sun Tzu, wprowadził koncept rozmaitych forteli stosowanych na polu bitwy, mających zwiększyć szanse zwycięstwa³⁵⁸. Jednak dopiero w XX w. nastąpił intensywny rozwój koncepcji wojny hybrydowej. Postacią odgrywającą istotną rolę w rozwoju zagrożeń hybrydowych, a w zasadzie „wojen buntowniczych” był rosyjski wojskowy J. Messner³⁵⁹, według którego wojny buntownicze cechują się dwoma elementami. Po pierwsze, to ludność cywilna bierze aktywny udział

³⁵⁵ *Hybryda*, <https://wsjp.pl/haslo/podglad/81750/hybryda> (dostęp: 2.06.2025).

³⁵⁶ *Wojna hybrydowa*, <https://wsjp.pl/haslo/podglad/82200/wojna-hybrydowa> (dostęp: 2.06.2025).

³⁵⁷ W. J. Nemeth, *Future War and Chechnya: A Case for Hybrid Warfare*, Naval Postgraduate School, Monterey 2002, s. 29.

³⁵⁸ Sun Tzu, *Sztuka Wojny*, Wydawnictwo Helion S.A., Gliwice 2008.

³⁵⁹ W trakcie I Wojny Światowej brał aktywny udział w walkach w Rumunii jako żołnierz carskiej Rosji. W trakcie Rewolucji Październikowej opowiedział się po stronie „białych”, a po zwycięstwie bolszewików emigrował na Bałkany. Podczas II Wojny Światowej podjął się współpracy z III Rzeszą, a po zakończeniu wojny wyemigrował do Argentyny, gdzie mieszkał aż do śmierci, zob. L. Sykulski, *Rosyjska Koncepcja Wojen Buntowniczych Jewgienija Messnera*, „Przegląd Geopolityczny”, 2015, tom 11, s. 105.

w działaniach zbrojnych, a po drugie, wszystkie podejmowane działania muszą oddziaływać psychologicznie na przeciwnika³⁶⁰. Ponadto wojny buntownicze charakteryzują się brakiem wyraźnych linii frontu, co jest spowodowane wykorzystywaniem niekonwencjonalnych metod walki (współcześnie będzie to działalność militarna w cyberprzestrzeni)³⁶¹. Opis wojen buntowniczych wpisuje się w koncepcję wojny hybrydowej stworzonej przez W. J. Nemetha. Podstawą do zdefiniowania wojny hybrydowej przez tego amerykańskiego wojskowego był konflikt rosyjsko-czeczeński³⁶². Nierówna walka pomiędzy rosyjskimi siłami zbrojnymi a oddziałami czeczeńskimi wymuszała na tej grupie przyjęcie niekonwencjonalnych metod walki. Zgodnie z założeniami W. J. Nemetha społeczeństwo czeczeńskie funkcjonowało jako tzw. „społeczeństwo hybrydowe”, które charakteryzuje się ograniczoną władzą rządu centralnego (zamiast tego realną władzę sprawują lokalni watażkowie finansowani z działalności przestępczej) oraz słabym rozwojem gospodarczym (obywatele są wyzyskiwani oraz dyskryminowani)³⁶³. Pomimo słabej organizacji jako społeczeństwo Czeczeni byli w stanie przeciwstawić się rosyjskiej armii, do czego przyczyniły się szczególne cechy sił hybrydowych – idee, charyzmatyczni liderzy, negatywna odpowiedzialność za swoje działania, przekonanie o słuszności własnej sprawy oraz zdecentralizowana taktyka³⁶⁴.

Pojęcie wojny hybrydowej zaprezentowane przez W. J. Nemetha odnosi się przede wszystkim do sytuacji, w której strona słabsza podejmuje niekonwencjonalne działania względem strony przeciwnej, przeważnie znacznie silniejszej. Taka koncepcja działań hybrydowych nie pasuje do obecnych działań Federacji Rosyjskiej oraz innych państw je stosujących. W tej sytuacji należy pochylić się nad definicją zaproponowaną przez F. G. Hoffmana, zgodnie z którą w wojny hybrydowe mogą być zaangażowane zarówno państwa, jak i podmioty niepaństwowe, których walka opiera się na wykorzystaniu różnych modeli działań wojennych, na przykład metody konwencjonalne, nieregularna taktyka oraz formacje, masowa przemoc i przymus, ale także działalność kryminalna³⁶⁵. Tak scharakteryzowany konflikt hybrydowy wpisuje się w taktykę rosyjskich działań hybrydowych, które obejmują swym zakresem między innymi działania w cyberprzestrzeni

³⁶⁰ L. Sykulski, *Rosyjska Koncepcja...*, s. 107-108.

³⁶¹ Wytęczenie „frontu” wojny hybrydowej może mieć miejsce przy wykorzystaniu ludzi jako metody walki, czego przykładem jest masowe sprowadzanie nielegalnych imigrantów przez władze rosyjskie i białoruskie na granicę polsko-białoruską, D. Niedźwiedzki, *Kryzys humanitarny na granicy polsko-białoruskiej. Analiza zjawiska w perspektywie ładu społecznego*, „Politeja”, 2024, vol. 21, nr 1 (88/3), s. 58-59.

³⁶² W. J. Nemeth, *Future War and Chechnya...*, s. 63-64.

³⁶³ *Tamże*, s. 69.

³⁶⁴ *Tamże*, s. 71.

³⁶⁵ F. G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, Arlington 2007, s. 14.

oraz ataki na infrastrukturę krytyczną³⁶⁶. Za podstawę współczesnej rosyjskiej wojny hybrydowej należy wskazać tzw. Doktrynę Gierasimowa, czyli opracowanie Szefa Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej W. Gierasimowa dotyczące nowego spojrzenia na prowadzenie konfliktów zbrojnych³⁶⁷. W. Gierasimow, analizując konflikty zbrojne poczynając od Wielkiej Wojny Ojczyźnianej z lat 1941-1945, poprzez radziecką ofensywę w Afganistanie w latach 1979 – 1989, aż do tzw. Arabskiej Wiosny z 2010 roku, wskazuje na zmienny charakter prowadzonych konfliktów zbrojnych. Ich zakres można ograniczyć obecnie do trzech głównych celów: ochrony interesów państwa poza jego granicami, ochrony międzynarodowego pokoju oraz ochrony własnej ludności, obiektów i komunikacji³⁶⁸. Zmienny charakter konfliktu zbrojnego wymusza na państwach wprowadzenie nowych metod, mających przede wszystkim doprowadzić do osiągnięcia przewagi nad przeciwnikiem. W tym zakresie W. Gierasimow wskazuje między innymi na masowe użycie broni precyzyjnego rażenia, wykorzystanie oddziałów sił specjalnych czy redukcję potencjału militarno-ekonomicznego państwa poprzez zniszczenie krytycznie ważnych obiektów jego infrastruktury wojskowej i cywilnej w krótkim czasie³⁶⁹. Jednocześnie wskazuje na przewagę wykorzystania środków niemilitarnych, które powinny zostać użyte w stosunku 4:1 względem środków militarnych³⁷⁰.

Koncepcja zaproponowana przez W. Gierasimowa była skutecznie wdrażana od 2013 roku w Ukrainie, kiedy jej ówczesny prezydent Wiktor Janukowycz odmówił podpisania porozumienia pomiędzy Ukrainą a UE³⁷¹. Strona rosyjska sukcesywnie podsyciała wewnętrzny konflikt pomiędzy rządem a opozycją, co doprowadziło do powstania tzw. Euromajdanu, czyli społecznego ruchu oporu wobec ówczesnie urzędującego prezydenta³⁷². Przedłużające się

³⁶⁶ Polska jednym z głównych celów rosyjskich hakerów, <https://www.pap.pl/aktualnosci/polska-jednym-z-glownych-celow-rosyjskich-hakerow> (dostęp: 2.06.2025).

³⁶⁷ W. Gierasimow, *The Value of Science Is in the Foresight. New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations*, „Military Review”, January-February 2016, https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf (dostęp: 2.06.2025).

³⁶⁸ *Tamże*, s. 24-27.

³⁶⁹ *Tamże*, s. 25.

³⁷⁰ Do środków niemilitarnych W. Gierasimow zalicza przede wszystkim połączenie środków dyplomatycznych, ekonomicznych, politycznych, m.in. sankcje gospodarcze, tworzenie sojuszy, wspieranie lub tworzenie sił opozycyjnych w obcym państwie. Ponadto istotnym elementem współczesnych konfliktów, będącym na granicy zarówno środków niemilitarnych, jak i militarnych jest wojna informacyjna. Jak wskazuje W. Gierasimow, przestrzeń informacyjna umożliwia ograniczenie potencjału bojowego przeciwnika (jako przykład podaje wykorzystanie technologii informacyjnej podczas Arabskiej Wiosny), W. Gierasimow, *The Value of Science...*, s. 27-28.

³⁷¹ S. Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict*, Georgetown University Press 2020, s. 55.

³⁷² *Tamże*, s. 55-56.

protesty skutkowały wykorzystaniem siły militarnej wobec protestujących, równolegle wywierając na nich nacisk psychologiczny poprzez atakowanie ich stron internetowych i wysyłanie wiadomości sms z pogrózkami³⁷³. Destabilizacja sytuacji wewnętrznej w Ukrainie, a w późniejszym czasie obalenie prezydenta W. Janukowycza, stworzyły warunki do przejęcia przez Rosję Półwyspu Krymskiego. Wykorzystując nieoznakowane jednostki specjalne, tzw. zielone ludziki, oficjalnie przedstawiane jako lokalne siły zbrojne chroniące interes mniejszości rosyjskiej na Krymie, przejęto kontrolę nad infrastrukturą telekomunikacyjną ograniczając dostęp do sieci komórkowej oraz podmieniając ukraińskie kanały telewizyjne na rosyjskie³⁷⁴. 11 marca 2014 roku parlament Autonomicznej Republiki Krymu ogłosił niepodległość Krymu opierając swoją decyzję na opinii doradczej MTS ws. jednostronnej deklaracji niepodległości Kosowa z 2010 roku³⁷⁵. Zgodnie ze stanowiskiem zaprezentowanym przez Trybunał prawo międzynarodowe nie zakazuje ogłoszenia deklaracji niepodległości, tym samym niepodległość ogłoszona przez Kosowo nie narusza prawa międzynarodowego³⁷⁶. 16 marca 2014 roku na Krymie przeprowadzone zostało referendum, w którym jego mieszkańcy mieli opowiedzieć się za dołączeniem do Federacji Rosyjskiej. Wstępne wyniki dawały aż 93% poparcia za przyłączeniem Krymu do Rosji, a dwa dni po głosowaniu prezydent Federacji Rosyjskiej Władimir Putin podpisał traktat o włączeniu Krymu do Rosji³⁷⁷. Wydarzenia z marca 2014 roku spotkały się ze sprzeciwem społeczności międzynarodowej. 27 marca 2014 roku ZO ONZ przyjęło rezolucję odnośnie integralności terytorialnej Ukrainy, w której potwierdziło swoje zaangażowanie na rzecz suwerenności, niezależności politycznej, jedności i integralności terytorialnej Ukrainy³⁷⁸. Ponadto ZO ONZ wskazało, że referendum przeprowadzone w Autonomicznej Republice Krymu z powodu swojej nieważności nie może być podstawą do zmiany statusu Krymu oraz miasta Sewastopola, tym samym wezwano wszystkie państwa, organizacje międzynarodowe i ich agencje wyspecjalizowane do nieuznawania jakichkolwiek zmian w statusie Autonomicznej Republiki Krymu i miasta Sewastopola. Co więcej, przed samym referendumb RB ONZ podjęła próbę przygotowania rezolucji potępiającej referendum

³⁷³ *Tamże*.

³⁷⁴ *Tamże*, s. 56.

³⁷⁵ *Krym ogłosił niepodległość. Powołuje się na casus Kosowa*, <https://wiadomosci.wp.pl/krym-oglosil-niepodleglosc-powoluje-sie-na-casus-kosowa-6031313103753857a> (dostęp: 2.06.2025).

³⁷⁶ MTS, *Accordance with international law of the unilateral declaration of independence in respect of Kosovo*, Advisory Opinion, 22.07.2010, ICJ Reports 2010, s. 405-406.

³⁷⁷ S. Jasper, *Russian Cyber Operations...*, s. 57.

³⁷⁸ ZO ONZ, *Resolution 68/262*, 27.03.2014, A/RES/68/262.

w Autonomicznej Republice Krymu, jednak Federacja Rosyjska w trakcie głosowania nad projektem rezolucji skorzystała z prawa weta³⁷⁹.

Kolejnym etapem rosyjskiej wojny hybrydowej wymierzonej w Ukrainę było utworzenie Donieckiej i Ługańskiej Republiki Ludowej³⁸⁰. Tak samo jak w przypadku Autonomicznej Republiki Krymu w obwodach donieckim i ługańskim przeprowadzone zostało referendum, w którym mieszkańcy mieli opowiedzieć się za suwerennością tych regionów³⁸¹. Sfałszowane wyniki głosowania dawały około 90% poparcie dla odrębności terytorialnej obwodów donieckiego i ługańskiego, co skutkowało ogłoszeniem 12 maja 2014 roku niepodległości Donieckiej Republiki Ludowej oraz Ługańskiej Republiki Ludowej³⁸². Niespełna dwa tygodnie po ogłoszeniu niepodległości oba podmioty podpisały porozumienie o utworzeniu Federacji Republiki Noworosji, które po roku obowiązywania zostało zawieszone, a Doniecka Republika Ludowa oraz Ługańska Republika Ludowa funkcjonowały jako odrębne podmioty aż do 30 września 2022 roku, kiedy prezydent Federacji Rosyjskiej Władimir Putin podpisał traktat o przyłączeniu między innymi Doniecka oraz Ługańska do Federacji Rosyjskiej³⁸³. Rosyjska operacja prowadzona w Donbasie w latach 2014-2022 (region w Ukrainie obejmujący swym zasięgiem obwody doniecki i ługański) była skutecznym odzwierciedleniem Doktryny Gierasimowa w rzeczywistości. W ramach wykorzystania środków niemilitarnych Rosjanie utworzyli alternatywne rządy zarówno dla Donieckiej jak i Ługańskiej Republiki Ludowej, niepodporządkowane władzy w Kijowie. Dodatkowo na szeroką skalę wykorzystywane były operacje w cyberprzestrzeni, na przykład włamania do telefonów ukraińskich żołnierzy biorących udział w antyterrorystycznej operacji w Donbasie, którzy otrzymywali wiadomości z pogrózkami, ale także włamania do ukraińskich systemów zarządzania artylerią³⁸⁴. Wszystkie te środki zostały wsparte środkami militarnymi (zbrojnymi) obejmującymi między innymi ataki na ukraińską infrastrukturę krytyczną, w szczególności system telekomunikacji czy system finansowy³⁸⁵.

³⁷⁹ *UN Security Council action on Crimea referendum blocked*, <https://news.un.org/en/story/2014/03/464002-un-security-council-action-crimea-referendum-blocked> (dostęp: 2.06.2025).

³⁸⁰ S. Jasper, *Russian Cyber Operations...*, s. 57.

³⁸¹ *Farsa „referendum” w Donbasie*, <https://www.osw.waw.pl/pl/publikacje/analizy/2014-05-14/farsa-referendum-w-donbasie> (dostęp: 2.06.2025).

³⁸² A. Szumski, *Status Prawny Donieckiej Republiki Ludowej i Ługańskiej Republiki Ludowej*, „Dyplomacja i Bezpieczeństwo”, 2015, nr 1 (3), s. 151.

³⁸³ *Russia announces the annexation of four regions of Ukraine*, <https://www.osw.waw.pl/en/publikacje/analyses/2022-10-03/russia-announces-annexation-four-regions-ukraine> (dostęp: 2.06.2025).

³⁸⁴ S. Jasper, *Russian Cyber Operations...*, s. 62-63.

³⁸⁵ *Tamże*, s. 62.

Finalnym etapem wojny hybrydowej z Ukrainą jest pełnoskalowa inwazja sił zbrojnych Federacji Rosyjskiej na terytorium Ukrainy, która rozpoczęła się 22 lutego 2022 roku. Od samego początku inwazji głównymi celami ataków sił rosyjskich są obiekty infrastruktury krytycznej. Na ataki szczególnie narażony jest ukraiński system energetyczny (w tym elektrownie atomowe), który jest celem zarówno ataków konwencjonalnych, jak i ataków w cyberprzestrzeni³⁸⁶. Uszkodzenie infrastruktury energetycznej stanowi poważne zagrożenie dla ukraińskiej ludności cywilnej. Sukcesywne i metodyczne ataki na obiekty energetyczne prowadzone od października 2022 roku są odczuwalne przez ludność przede wszystkim w okresie zimowym, kiedy pozbawia się jej dostępu do prądu, często wraz z ogrzewaniem³⁸⁷. Brak dostępu do prądu negatywnie oddziałuje również na obiekty medyczne³⁸⁸, co więcej szpitale i inne placówki medyczne często same są celami ataków konwencjonalnych. Od początku inwazji do końca 2025 roku odnotowano ponad 2800 ataków na obiekty ochrony zdrowia, w większości przypadków przy użyciu ciężkiego uzbrojenia³⁸⁹.

3.2.2 Działania organizacji międzynarodowych podejmowane przeciwko zagrożeniom hybrydowym

Społeczność międzynarodowa, uznając działania hybrydowe za zagrożenie dla bezpieczeństwa państwa i bacznie obserwując rozwój sytuacji w Ukrainie (począwszy od 2014 roku), zdecydowała się podjąć kroki zmierzające do skutecznej ochrony infrastruktury krytycznej przed atakami hybrydowymi. Przed przyjęciem odpowiednich regulacji prawnych, kluczowe było zdefiniowanie konkretnych zagrożeń dla ochrony infrastruktury krytycznej płynących z działań hybrydowych. Obecnie wskazuje się na dwa główne rodzaje ataków hybrydowych na infrastrukturę krytyczną³⁹⁰. Pierwszy z nich, pośredni, ma doprowadzić do niewłaściwego zarządzania systemami infrastruktury krytycznej poprzez rozprowadzanie nieprawdziwych informacji (dezinformacja). Skuteczna obrona przed atakami pośrednimi wymaga od podmiotu zapewniającego bezpieczeństwo systemom krytycznym szybkiej

³⁸⁶ B. Pacek, P. Pacek, *Russia's devastating...*, s. 16.

³⁸⁷ *Tamże*.

³⁸⁸ Brak dostępu do prądu w szpitalu wpływa na prawidłowe działanie urządzeń podtrzymujących życie, a także innego sprzętu niezbędnego do działania placówki medycznej, np. lodówek w których przechowuje się krew lub leki. zob. *Ukraine's Health System Braces for Toughest Winter as Russia Targets Critical Infrastructure*, <https://healthpolicy-watch.news/ukraines-health-system-braces-for-toughest-winter-yet-amid-russian-attacks-on-critical-infrastructure/> (dostęp: 2.06.2025).

³⁸⁹ *Surveillance System for Attacks on Health Care (SSA)*, <https://extranet.who.int/ssa/Index.aspx> (dostęp: 12.05.2026).

³⁹⁰ M. M. Llinas, *Hybrid Attacks on Critical Infrastructure* w: P. Bargués, M. Bourekba, C. Colomina, *Hybrid threats, vulnerable order*, Barcelona Center for International Affairs, 2022, Report n°8, s. 39-40.

identyfikacji i zablokowania dystrybutorów fałszywych informacji³⁹¹. Drugi rodzaj ataku hybrydowego na infrastrukturę krytyczną to bezpośredni atak (konwencyjny lub w cyberprzestrzeni), wywołujący zmiany w świecie fizycznym³⁹².

Zidentyfikowanie zagrożeń płynących z działań hybrydowych wymierzonych w infrastrukturę krytyczną pozwoliło opracować w wymiarze międzynarodowym szereg rozwiązań mających na celu ochronę infrastruktury krytycznej, w której istotną rolę odgrywają NATO oraz UE³⁹³. Wiodąca funkcja tych dwóch organizacji międzynarodowych wynika z ich członków, ponieważ to właśnie państwa europejskie (zrzeszone w UE i NATO) oraz Stany Zjednoczone, zaraz obok Ukrainy, są głównymi celami działań hybrydowych Federacji Rosyjskiej.

Jednym z pierwszych działań Unii Europejskiej zmierzających do zabezpieczenia się przed działaniami hybrydowymi było wydanie 6 kwietnia 2016 roku Wspólnego Komunikatu do PE i Rady pt. „Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym odpowiedź Unii Europejskiej”³⁹⁴. Celem Komunikatu było określenie działań dążących do wzmocnienia współpracy pomiędzy państwami członkowskimi i UE w przeciwdziałaniu zagrożeniom hybrydowym, natomiast działania opierały się już na istniejących strategiach i politykach sektorowych. W Komunikacie wyróżniono aż 22 działania, obejmujące między innymi utworzenie komórki UE ds. syntezy informacji o zagrożeniach hybrydowych (ang. *Hybrid Fusion Cell*), której zadaniem jest analiza informacji niejawnych oraz informacji jawnych, w szczególności na temat wskaźników i ostrzeżeń dotyczących zagrożeń hybrydowych, pozyskanych między innymi od Europejskiej Służby Działań Zewnętrznych, KE i państw członkowskich. Kilka działań poświęcono usprawnieniu ochrony infrastruktury krytycznej:

Działanie 5. KE we współpracy z państwami członkowskimi i zainteresowanymi stronami ustali wspólne narzędzia, m.in. wskaźniki, w celu poprawy ochrony i odporności infrastruktury krytycznej na wypadek zagrożeń hybrydowych w istotnych sektorach – w 2008 roku przyjęto Dyrektywę w sprawie rozpoznawania i wyznaczania europejskiej

³⁹¹ *Tamże*.

³⁹² *Tamże*, s. 39.

³⁹³ H. Pillai, *Protecting Europe's critical infrastructure from Russian hybrid threats*, Center for European Reform, 2023, s. 6-8.

³⁹⁴ *Wspólny Komunikat do Parlamentu Europejskiego i Rady „Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym odpowiedź Unii Europejskiej”*, 6.04.2016, JOIN(2016) 18 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016JC0018> (dostęp: 2.06.2025).

infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony³⁹⁵, którą ustanowiono procedurę rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej i wspólne podejście do oceny potrzeb w zakresie poprawy jej ochrony. W związku z zagrożeniami hybrydowymi Wspólnota Europejska powinna przyjąć rozwiązania wzmacniające ochronę infrastruktury krytycznej, w szczególności infrastrukturę transportową (europejskie porty lotnicze i porty handlowe).

Działanie 6. KE we współpracy z państwami członkowskimi będzie wspierać wysiłki na rzecz dywersyfikacji źródeł energii i promowania norm bezpieczeństwa w celu podniesienia poziomu odporności infrastruktury jądrowej – zapewnienie bezpieczeństwa energetycznego państwom członkowskim jest jednym z najważniejszych zadań stojących przed UE. Bezpieczeństwo energetyczne wymaga podejścia dwojakiego – po pierwsze, należy przeprowadzić dywersyfikację dostaw surowców energetycznych, na przykład gazu ziemnego, a po drugie, należy zapewnić bezpieczeństwo obiektom jądrowym.

Działanie 7. KE będzie monitorować pojawiające się zagrożenia w sektorze transportu i w razie potrzeby uaktualniać przepisy. Przy wdrażaniu strategii UE w zakresie bezpieczeństwa morskiego i unijnej strategii zarządzania ryzykiem celnym i związanego z tym planu działania KE i Wysoki Przedstawiciel (w ramach swoich kompetencji), w koordynacji z państwami członkowskimi, zbadają w jaki sposób należy odpowiedzieć na złożone zagrożenia hybrydowe, zwłaszcza te dotyczące krytycznej infrastruktury transportowej – zapewnienie ciągłości trzech z czterech swobód UE – swobody przepływu towarów, swobody przepływu usług, swobody przepływu osób wymaga zapewnienia przez państwa członkowskie i UE bezpieczeństwa w zakresie infrastruktury transportowej. W tym celu UE przyjęła dwa rozporządzenia chroniące porty lotnicze³⁹⁶ i porty morskie³⁹⁷, których celem jest ustanowienie wspólnych zasad ochrony lotnictwa cywilnego przed aktami bezprawnej ingerencji zagrażającymi bezpieczeństwu lotnictwa cywilnego (w szczególności utworzenie mechanizmów monitorowania przestrzegania tych zasad) oraz wprowadzenie i wykonanie środków wspólnotowych

³⁹⁵ Dyrektywa Rady 2008/114/WE w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, 8.12.2008, Dz. Urz. L 345 z 23.12.2008.

³⁹⁶ Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 300/2008 w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002, 11.03.2008, Dz. Urz. L 97/72 z 9.04.2004.

³⁹⁷ Rozporządzenie (WE) nr 725/2004 Parlamentu Europejskiego i Rady w sprawie podniesienia ochrony statków i obiektów portowych, 31.03.2004, Dz. Urz. L 129/6 z 29.04.2004.

dla podniesienia ochrony statków używanych w handlu międzynarodowym oraz krajowej żegludze morskiej, a także stowarzyszonych obiektów portowych w świetle zagrożeń zamierzonymi aktami bezprawnymi.

Działanie 8. W kontekście zapowiadanej Strategii kosmicznej dla Europy i europejskiego planu działań w sektorze obrony KE proponuje wzmocnienie odporności infrastruktury kosmicznej na zagrożenia hybrydowe, w szczególności poprzez możliwe poszerzenie zakresu ram wsparcia obserwacji i śledzenia obiektów kosmicznych, tak by obejmowały one zagrożenia hybrydowe, przygotowania do nowej generacji rządowej łączności satelitarnej (GOVSATCOM) na europejskim poziomie i wprowadzenie systemu Galileo do infrastruktury krytycznej zależnej od synchronizacji czasu – pomimo tego, że wiele państw członkowskich UE nie posiada szeroko rozwiniętej działalności w przestrzeni kosmicznej to zapewnienie jej bezpieczeństwa w wymiarze wspólnotowym jest kluczowe dla bezpieczeństwa infrastruktury krytycznej każdego państwa z osobna. Odpowiednie zabezpieczenie łączności satelitarnej wpływa na prawidłowe działanie różnych sektorów infrastruktury krytycznej – od transportu aż po łączność.

Działanie 9. Wysoki Przedstawiciel, przy wsparciu – w stosownych przypadkach – ze strony państw członkowskich, we współpracy z KE, proponuje projekty dotyczące sposobów dostosowania zdolności obronnych oraz projekty dotyczące rozwoju mające znaczenie dla UE, w szczególności by przeciwdziałać zagrożeniom hybrydowym wymierzonym przeciwko państwu członkowskiemu lub kilku państwom członkowskim – zapewnienie bezpieczeństwa całej UE wiąże się ze zwiększeniem zdolności obronnych całej Wspólnoty oraz jej państw członkowskich. Kluczową rolę w tym zakresie pełnić może Europejska Agencja Obrony, odpowiadająca za inwestycje w nowoczesne technologie we współpracy z prywatnym biznesem.

Działanie 10. KE, we współpracy z państwami członkowskimi, zwiększy wiedzę na temat zagrożeń hybrydowych i odporność na nie w ramach istniejących mechanizmów gotowości i koordynacji, zwłaszcza w ramach Komitetu ds. Bezpieczeństwa Zdrowia – szeroki wachlarz zagrożeń hybrydowych może obejmować prowadzenie działalności przeciwko drugiemu państwu z wykorzystaniem między innymi chorób zakaźnych czy innych patogenów zagrażających zdrowiu i życiu obywateli UE, ale zwierzętom oraz roślinom. W związku z tym zagrożeniem wspólnota podjęła działania zmierzające do wyeliminowania niebezpieczeństwa chorób między innymi poprzez nadzór

nad transgranicznymi zagrożeniami dla zdrowia³⁹⁸, gdzie kluczową rolę odgrywa Komitet ds. Bezpieczeństwa Zdrowia. Komitet składa się z przedstawicieli państw członkowskich, zorganizowanych na dwóch szczeblach – pierwszy obejmuje grupę roboczą wysokiego szczebla, która będzie prowadziła regularne dyskusje na temat poważnych transgranicznych zagrożeń zdrowia oraz przyjmowała opinie i wytyczne, natomiast drugi szczebel to techniczne grupy robocze mające na celu omawianie konkretnych zagadnień, jeśli jest to konieczne.

Działanie 11. KE zachęca państwa członkowskie do utworzenia – w trybie priorytetowym – i pełnego wykorzystania sieci 28 zespołów CSIRT³⁹⁹ i CERT-UE⁴⁰⁰, a także ram współpracy strategicznej. KE, w koordynacji z państwami członkowskimi, powinna dopilnować, by inicjatywy sektorowe w dziedzinie zagrożeń cybernetycznych (np. lotniczych, energetycznych, morskich) były spójne z międzysektorowymi zdolnościami objętymi zakresem dyrektywy w sprawie NIS (ang. *Network and Information Systems*), takimi jak zdolność do gromadzenia informacji, łączenia wiedzy fachowej i szybkich reakcji – obecny poziom rozwoju technologii informacyjnej umożliwia, a niejednokrotnie wymaga, rozszerzenia usług państwowych, również tych krytycznych w cyberprzestrzeni. Powoduje to znaczny wzrost zagrożeń cybernetycznych, szczególnie w obrębie infrastruktury krytycznej, co wymusza rozwój zdolności obronnych w cyberprzestrzeni. Przejawem tego jest przyjęcie Dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)⁴⁰¹, która utworzyła między innymi sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego w celu wymiany informacji na temat cyberzagrożeń i reagowania na incydenty. Ponadto w ramach wspólnoty działania Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, do której zadań należą między innymi: pomoc i doradztwo

³⁹⁸ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2371 w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylenia decyzji nr 1082/2013/UE, 23.11.2022, Dz. Urz. L 314/26 z 6.12.2022.

³⁹⁹ Zespół reagowania na incydenty bezpieczeństwa komputerowego (ang. *Computer Security Incident Response Team*).

⁴⁰⁰ Zespół specjalistów zwalczających zagrożenia w sieciach komputerowych (ang. *Computer Emergency Response Team*). W praktyce oba terminy są stosowane zamiennie, a w ramach UE częściej stosuje się termin CERT. Zob. I. Jarosz, P. Jaroszewski, P. Kijewski, T.J. Kruk, K. Silicki, T. Grudziecki, *System bezpieczeństwa cyberprzestrzeni RP*, Naukowa i Akademicka Sieć Komputerowa (NASK/ CERT Polska), Warszawa 2015, s. 67.

⁴⁰¹ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148, 14.12.2022, Dz. Urz. L 333/80 z 27.12.2022.

w zakresie opracowywania i przeglądu polityki i prawa Unii w dziedzinie cyberbezpieczeństwa oraz w zakresie inicjatyw dotyczących polityki i prawa Unii w poszczególnych sektorach, w których występują kwestie związane z cyberbezpieczeństwem, w szczególności poprzez wydawanie niezależnych opinii i analiz, jak również prowadzenie prac przygotowawczych, pomoc państwom członkowskim przy wdrażaniu polityki i prawa Unii w dziedzinie cyberbezpieczeństwa w sposób jednolity, w szczególności w związku z dyrektywą (UE) 2016/1148, w tym za pomocą wydawania opinii, wytycznych, udzielania porad i najlepszych praktyk dotyczących takich zagadnień jak zarządzanie ryzykiem, zgłaszanie incydentów i wymiana informacji, jak również za pomocą ułatwiania wymiany najlepszych praktyk pomiędzy właściwymi organami w tym zakresie czy pomoc państwom członkowskim oraz instytucjom, organom i jednostkom organizacyjnym Unii przy opracowywaniu i propagowaniu polityk cyberbezpieczeństwa dotyczących utrzymywania ogólnej dostępności i integralności publicznego rdzenia otwartego Internetu⁴⁰².

Działanie 12. KE, w koordynacji z państwami członkowskimi, będzie współpracować z przemysłem w ramach umownego partnerstwa publiczno-prywatnego w dziedzinie bezpieczeństwa cybernetycznego, by rozwijać i testować technologie mające lepiej chronić użytkowników i infrastrukturę przed zagrożeniami hybrydowymi – zdając sobie sprawę z wrażliwości bezpieczeństwa cybernetycznego na zagrożenia hybrydowe podjęte zostaną odpowiednie kroki w celu zawarcia partnerstwa publiczno-prywatnego, którego celem będzie utworzenie odporności cybernetycznej w przemyśle.

Działanie 13. KE wyda wytyczne dla właścicieli inteligentnych sieci w celu poprawy bezpieczeństwa cybernetycznego ich instalacji. W ramach inicjatywy dotyczącej koncepcji rynku energii elektrycznej KE rozważy proponowanie „planów gotowości na zagrożenia” oraz przepisów proceduralnych dotyczących wymiany informacji i zagwarantowania solidarności między państwami członkowskimi w czasach kryzysu, w tym zasad dotyczących sposobu zapobiegania atakom cybernetycznym i ich minimalizowania – intensywny rozwój zdolności cybernetycznych, w tym pojawienie się takich usług jak „inteligentne domy” powoduje znaczny wzrost zagrożeń w zakresie bezpieczeństwa energetycznego. W celu wymiany informacji oraz dobrych praktyk

⁴⁰² Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013, 17.04.2019, Dz. Urz. L 151/15 z 7.06.2019.

stworzona została platforma mająca analizować i zbierać informacje o zagrożeniach obejmujących między innymi inteligentne sieci (obecnie Służba ds. Cyberbezpieczeństwa Instytucji, Organów i Jednostek Organizacyjnych Unii – CERT-UE⁴⁰³). Dodatkowo UE podjęła negocjacje mające na celu wypracowanie kompleksowej strategii bezpieczeństwa cybernetycznego w sektorze energetycznym w odniesieniu do działania inteligentnych sieci w celu zmniejszania podatności na zagrożenia.

Działanie 14. KE we współpracy z Agencją UE ds. Cyberbezpieczeństwa, państwami członkowskimi, odnośnymi międzynarodowymi, europejskimi i krajowymi organami i instytucjami finansowymi będzie promować platformy i sieci wymiany informacji o zagrożeniach i ułatwiać ich funkcjonowanie oraz eliminować czynniki utrudniające wymianę takich informacji – prawidłowe działanie UE jest zależne od właściwego działania sektora finansowego, natomiast podstawowym elementem w celu zapewnienia bezpieczeństwa jest współpraca. Dlatego KE podejmie współpracę na różnych forach międzynarodowych, (forum G7) aby podjąć swobodną wymianę informacji na temat zagrożeń i zaproponuje rozwiązania. Właściwa analiza zagrożeń w środowisku finansowym pozwoli odpowiednio chronić przedsiębiorców oraz całą infrastrukturę finansową.

Działanie 15. KE i Wysoki Przedstawiciel (w ramach swoich kompetencji), w koordynacji z państwami członkowskimi, zbadają w jaki sposób odpowiadać na zagrożenia hybrydowe, w szczególności te dotyczące ataków cybernetycznych w sektorze transportu – współpraca państw członkowskich UE w dużym stopniu opiera się na transporcie transgranicznym. Rozwój nowoczesnych systemów transportowych, w głównej mierze opierający się na systemach cybernetycznych jest szczególnie narażony na zagrożenia hybrydowe, które mogą osłabić UE, dlatego ważna jest szybka identyfikacja zagrożeń w transporcie.

Działanie 16. Wdrożenie planu działania w sprawie zwalczania finansowania terroryzmu także posłuży KE do przeciwdziałania zagrożeniom hybrydowym – przeprowadzenie działań hybrydowych wymaga odpowiednich nakładów finansowych, często pochodzących z nielegalnych źródeł. Finansowaniu podlegają wszelkie działania dywersyjne,

⁴⁰³ *The Cybersecurity Service for the Union institutions, bodies, offices and agencies*, <https://cert.europa.eu/> (dostęp: 2.06.2025).

ale również wykorzystanie między innymi grup terrorystycznych. W tym celu UE podjęła kroki przeciwdziałające praniu brudnych pieniędzy oraz finansowania terroryzmu.

Działanie 17. KE wdraża obecnie działania przeciwko radykalizacji postaw określonych w Europejskiej agendzie bezpieczeństwa i analizuje potrzebę wzmocnienia procedur usuwania nielegalnych treści, wzywając pośredników do zachowania należytej staranności podczas zarządzania swoimi sieciami i systemami – bezpośrednimi uczestnikami działań hybrydowych, na przykład dywersji, bardzo często są osoby niepowiązane (poprzez obywatelstwo, służbę w siłach zbrojnych lub służbach specjalnych, czy biznesowo) z państwem zlecającym takie działania⁴⁰⁴. Dlatego państwa członkowskie, we współpracy z KE, powinny podjąć odpowiednie działania zmierzające do wyeliminowania wszelkich przejawów ekstremizmu oraz fundamentalizmu tak politycznego, jak i religijnego, które mogą stanowić podstawę dla rekrutacji sprawców dywersji.

Działanie 18. Wysoki Przedstawiciel, we współpracy z KE, przeprowadzi analizę zagrożenia hybrydowego w sąsiednich regionach – UE realizująca politykę sąsiedztwa ze wschodnimi i południowymi partnerami (na przykład Ukraina, Azerbejdżan, Tunezja, Egipt, Izrael)⁴⁰⁵ dąży do pogłębienia i rozwoju współpracy w sektorze bezpieczeństwa wraz ze swoimi krajami partnerskimi. Współpraca opiera się na tak na wymianie informacji, jak i konkretnych działaniach zmierzających do przeciwdziałania terroryzmowi, handlu ludźmi czy handlu bronią. Ponadto odwołując się do Wspólnej Polityki Bezpieczeństwa i Obrony możliwe jest przeprowadzenie następujących działań: wspieranie łączności strategicznej, wsparcie doradcze dla kluczowych ministerstw narażonych na zagrożenia hybrydowe oraz dodatkowe wsparcie w zakresie zarządzania granicami w sytuacji wyjątkowej.

Jak wynika z analizy Komunikatu działania UE w budowie odporności przed zagrożeniami hybrydowymi powinny przede wszystkim skupić się na wymianie informacji dotyczących zagrożeń w ochronie infrastruktury krytycznej. W Komunikacie zaproponowano „klasyczne” ujęcie infrastruktury krytycznej z podziałem na sektory, na przykład sektor

⁴⁰⁴ *Wspólne oświadczenie Ministra Sprawiedliwości - Prokuratora Generalnego i Ministra Spraw Wewnętrznych i Administracji, Koordynatora Służb Specjalnych*, <https://www.abw.gov.pl/pl/informacje/2635,Wspolne-oswiadczenie-Ministra-Sprawiedliwosci-Prokuratora-Generalnego-i-Ministra.html> (dostęp: 2.06.2025).

⁴⁰⁵ *Europejska polityka sąsiedztwa*, https://commission.europa.eu/strategy-and-policy/policies/european-neighbourhood-policy_pl (dostęp: 2.06.2025).

energetyczny, sektor finansowy czy sektor transportu, jednak co zwraca szczególną uwagę to analiza poszczególnych zagrożeń w kontekście bezpieczeństwa cybernetycznego. Intensywny rozwój technologiczny skutecznie powiązał prawidłowe działanie infrastruktury krytycznej z systemami cybernetycznymi, tym samym wprowadzając nowe sektory wymagające ochrony przed zagrożeniami hybrydowymi.

W związku z intensyfikacją rosyjskich działań hybrydowych, UE podjęła kolejne kroki zmierzające do budowania odporności przed tymi zagrożeniami. Przejawem tego było przyjęcie 13 czerwca 2018 roku Wspólnego Komunikatu do PE, RE i Rady pt. „Zwiększenie odporności i wzmocnienie zdolności reagowania na zagrożenia hybrydowe”⁴⁰⁶. W okresie dwóch lat od przyjęcia poprzedniego Komunikatu UE zidentyfikowała kolejne zagrożenia jakim były osłabienie zaufania społecznego do instytucji publicznych i podważenie podstawowych wartości społeczeństwa. KE zidentyfikowała też trzy obszary szczególnie narażone na zagrożenia hybrydowe – po pierwsze, wspomniana już we wcześniejszym Komunikacie z 2016 roku cyberprzestrzeń⁴⁰⁷, po drugie, dezinformacja i po trzecie, zagrożenia biologiczne, chemiczne, radiologiczne i jądrowe.

Szeroki dostęp do Internetu, w tym powszechność mediów społecznościowych, spowodowały natłok wiadomości i informacji przekazywanych pomiędzy ludźmi. Wiele wiadomości, niezwłocznie udostępnianych „dalej” zawiera nieprawdziwe informacje prowadzące do niepewności i tworzenia napięć społecznych⁴⁰⁸. W celu skutecznego przeciwdziałania dezinformacji UE stworzyła „europejskie podejście do kwestii dezinformacji”⁴⁰⁹, które skupia w sobie szereg działań jak zwiększona przejrzystość, wiarygodność i odpowiedzialność platform internetowych, bezpieczniejsze i odporniejsze procesy wyborcze, wspieranie edukacji i umiejętności korzystania z mediów, wspieranie wysokiej jakości dziennikarstwa oraz zwalczanie dezinformacji dzięki komunikacji strategicznej. Kolejnym krokiem było przyjęcie w 2018 roku Kodeksu postępowania w zakresie

⁴⁰⁶ *Wspólny Komunikat do Parlamentu Europejskiego, Rady Europejskiej i Rady „Zwiększenie odporności i wzmocnienie zdolności reagowania na zagrożenia hybrydowe”* (dalej *UE JOIN(2018) 16 final*), 13.06.2018, JOIN(2018) 16 final, <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52018JC0016> (dostęp: 2.06.2025).

⁴⁰⁷ Ochrona infrastruktury krytycznej w kontekście zagrożeń w cyberprzestrzeni została opisana w podrozdziale 2.3.1.2 niniejszej rozprawy.

⁴⁰⁸ *UE JOIN(2018) 16 final*.

⁴⁰⁹ *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Zwalczanie dezinformacji w Internecie: podejście europejskie”*, 26.04.2018, COM(2018) 236 final, <https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52018DC0236> (dostęp: 28.05.2025).

zwalczania dezinformacji⁴¹⁰, którego celem było między innymi zapewnienie mechanizmów zabezpieczających przed dezinformacją, zapewnienie przejrzystości w odniesieniu do reklamy politycznej i tematycznej, również w celu umożliwienia użytkownikom zrozumienia, dlaczego dana reklama jest skierowana do nich, czy zmniejszenie widoczności dezinformacji poprzez poprawę możliwości znalezienia wiarygodnych treści. 13 lutego 2025 roku KE i Europejska Rada ds. Usług Cyfrowych zatwierdziły dokument jako Kodeks postępowania w zakresie zwalczania dezinformacji do aktu o usługach cyfrowych⁴¹¹. Kodeks reguluje między innymi obszary demonetyzacji (ograniczenie zachęt finansowych dla podmiotów rozpowszechniających dezinformację), przejrzystość reklam politycznych, zapewnienie integralności usług, wzmocnienie pozycji użytkowników i naukowców, *fact-checking* czy współpracę przy wyborach.

Kolejnym poważnym zagrożeniem dla bezpieczeństwa państw członkowskich są wszelkie działania hybrydowe z wykorzystaniem środków chemicznych, biologicznych, radioaktywnych i jądrowych (CBRJ). Już w 2017 roku UE podjęła działania zmierzające do zwiększenia gotowości na zagrożenia ze strony środków CBRJ⁴¹². Chociaż w tamtym momencie dominował pogląd, że zagrożenie ze strony CBRJ jest domeną terroryzmu dżihadystycznego⁴¹³, to niespełna kilka miesięcy później okazało się, że CBRJ może być wykorzystywane również do działań hybrydowych⁴¹⁴.

W 2017 roku UE wyznaczyła cztery cele do osiągnięcia aby uzyskać pełną ochronę przed zagrożeniami CBRJ: zmniejszenie dostępności materiałów CBRJ, zapewnienie lepszego stanu gotowości i bardziej solidnego reagowania na incydenty związane z bezpieczeństwem CBRJ, stworzenie ściślejszych wewnętrznych i zewnętrznych powiązań z kluczowymi regionalnymi i międzynarodowymi partnerami UE i zapewnienie ich zaangażowania na rzecz bezpieczeństwa CBRJ oraz poszerzenie wiedzy na temat zagrożeń w dziedzinie CBRJ⁴¹⁵.

⁴¹⁰ *2018 Code of Practice on Disinformation*, <https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation> (dostęp: 2.06.2025).

⁴¹¹ *Tamże*.

⁴¹² *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Plan działania na rzecz zwiększania gotowości na wypadek chemicznych, biologicznych, radiologicznych i jądrowych zagrożeń dla bezpieczeństwa”* (dalej *UE COM(2017) 610 final*), 18.10.2017, COM(2017) 610 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52017DC0610> (dostęp: 2.06.2025).

⁴¹³ *Tamże*.

⁴¹⁴ W marcu 2018 roku na terytorium Wielkiej Brytanii doszło do ataku z wykorzystaniem środków chemicznych, na byłego oficera rosyjskiego wywiadu wojskowego S. Skripala. Zob. I. Kanerva, *Russia and the West: An Increasingly Difficult Relationship*, „Horizons: Journal of International Relations and Sustainable Development”, 2018, nr 12, s. 112.

⁴¹⁵ *UE COM(2017) 610 final*.

Tak wyznaczone cele po raz kolejny pokazały, że kluczowymi działaniami zmierzającymi do wyeliminowania zagrożeń (pod każdą postacią) jest wymiana informacji oraz współpraca.

Tak jak w działaniach podejmowanych przez UE w ramach wyeliminowania zagrożeń hybrydowych wobec infrastruktury krytycznej w większości przebija się czynnik polityczny (można to określić jako czynnik „cywilny”), tak działania podejmowane przez NATO noszą w większości charakter militarny. Pierwsze odniesienia do zagrożeń hybrydowych w ramach NATO pojawiły się jako odpowiedź na rosyjską aneksję Krymu w 2014 roku, kiedy doszło do podpisania Deklaracji końcowej szczytu NATO w Walii z 5 września 2014 roku⁴¹⁶. W samej Deklaracji zagrożenia hybrydowe zostały zdefiniowane jako „szeroki zakres jawnych i skrytych działań militarnych, paramilitarnych i cywilnych w sposób ściśle zintegrowany”⁴¹⁷. Zagrożenia łączące ze sobą wiele elementów, zarówno tych militarnych, jak i niemilitarnych, wymagają od NATO stworzenia odpowiednich procedur oraz narzędzi, które w sposób skuteczny pozwolą na przygotowanie się, odstraszanie oraz ewentualną obronę. Przejawem takich działań jest rozwój komunikacji strategicznej, prowadzenie ćwiczeń wojskowych z uwzględnieniem elementów hybrydowych oraz podjęcie współpracy z innymi organizacjami międzynarodowymi⁴¹⁸. Szczyt w Walii skutkował również opracowaniem dwóch projektów, które w pośredni sposób przyczyniają się do przeciwdziałania zagrożeniom hybrydowym. Po pierwsze, utworzono Centrum Doskonalenia Komunikacji Strategicznej w Rydze (ang. *NATO Strategic Communications Center of Excellence*), którego zadaniem jest odpowiednie ukierunkowanie komunikacji na linii państwa członkowskie – NATO, poprzez stosowanie konkretnych narzędzi jak dyplomacja publiczna, operacje informacyjne i psychologiczne (skuteczna komunikacja pomiędzy członkami NATO oraz obywatelami przeciwdziałająca dezinformacji)⁴¹⁹. Po drugie, utworzono Plan Gotowości NATO (ang. *Readiness Action Plan*), który zawiera „niezbędne” środki do reagowania na niebezpieczeństwo wobec NATO, czego przykładem są Siły Natychmiastowego Reagowania NATO, tzw. szpica (ang. *Very High Readiness Joint Task Force*)⁴²⁰. Ich zadaniem jest odpowiedź na pojawiające się zagrożenie w ciągu kilku dni. Szpica składa się z komponentów wojsk lądowych, powietrznych, morskich oraz specjalnych.

⁴¹⁶ NATO, *Deklaracja szczytu walijskiego*, Newport, 5.09.2014, <https://www.bbn.gov.pl/pl/wydarzenia/6170,Deklaracja-koncowa-sz-czytu-NATO-w-Walii-z-2014-r-polskietlumaczenie.html> (dostęp: 2.06.2025).

⁴¹⁷ *Tamże*, par. 13.

⁴¹⁸ *Tamże*.

⁴¹⁹ *NATO Strategic Communications Center of Excellence*, <https://stratcomcoe.org/> (dostęp: 2.06.2025).

⁴²⁰ NATO, *Deklaracja szczytu walijskiego...*, par. 4.

Kolejnym kluczowym etapem w przeciwdziałaniu zagrożeniom hybrydowym w ramach NATO było przyjęcie Deklaracji końcowej szczytu NATO w Warszawie z 8 i 9 lipca 2016 roku⁴²¹, w której po raz pierwszy w oficjalnym dokumencie stwierdzono, że skierowanie działań hybrydowych wobec jednego z członków Sojuszu może skutkować obroną zbiorową przewidzianą w art. 5 Traktatu Północnoatlantyckiego z 1949 roku⁴²². Zapewnienie o zastosowaniu obrony zbiorowej z art. 5 zostało powtórzone w trakcie szczytu NATO w Brukseli w 2018 roku⁴²³. Co więcej, na szczycie zdecydowano się o powołaniu Zespołów Wsparcia Przeciwdziałania Zagrożeniom Hybrydowym (ang. *Counter Hybrid Support Teams*), których zadaniem będzie wspieranie sojuszników w identyfikacji i zwalczaniu zagrożeń hybrydowych⁴²⁴. Dotychczas Zespoły dwa razy wspierały sojuszników w zwalczaniu działań hybrydowych, pierwszy raz w 2019 roku w odpowiedzi na prośbę Czarnogóry, która obawiała się rosyjskiej ingerencji w wybory oraz w 2021 roku w odpowiedzi na prośbę Litwy mierzącej się z kryzysem migracyjnym, wywołanym przez Rosję we współpracy z Białorusią⁴²⁵.

W odpowiedzi na pełnoskalową rosyjską inwazję na Ukrainę w 2022 roku NATO, na Szczycie w Madrycie 29 czerwca 2022 roku, przyjęło nową Koncepcję Strategiczną⁴²⁶. Po raz kolejny potwierdzono konieczność zastosowania art. 5 Traktatu Północnoatlantyckiego w razie zagrożeń hybrydowych wobec jednego lub kilku sojuszników, ale również zidentyfikowano nowe zagrożenia, które mogą przyjąć formę działań hybrydowych⁴²⁷. Do tych zagrożeń zaliczono działania podejmowane przez autorytarne rządy, mające na celu podważenie zasad demokratycznych w państwa członkowskich NATO, czego przykładem są: inwestycje w zaawansowane pociski rakietowe, nuklearne oraz inne bronie konwencjonalne naruszające podstawowe zasady i normy międzynarodowe, kampanie dezinformacyjne, bezprawna ingerencja w sektor energetyczny czy wykorzystywanie migracji jako elementu wojny hybrydowej⁴²⁸. W celu przeciwdziałania tym zagrożeniom NATO w dalszym ciągu będzie

⁴²¹ NATO, *Deklaracja końcowa szczytu NATO w Warszawie*, Warszawa, 8.07.2016, https://www.bbn.gov.pl/ftp/dok/03/37-40_KBN_Deklaracja_szczytu.pdf (dostęp: 2.06.2025).

⁴²² *Traktat Północnoatlantycki*, Waszyngton, 4.04.1949, Dz. U. z 2000 r., nr 87, poz. 970.

⁴²³ NATO, *Brussels Summit Declaration*, Bruksela, 11.07.2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm#21 (dostęp: 2.06.2025).

⁴²⁴ *Tamże*, par. 21.

⁴²⁵ H. Pillai, *Protecting Europe's...*, s. 7.

⁴²⁶ NATO, *NATO 2022 Strategic Concept*, Madryt, 29.06.2022, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf (dostęp: 2.06.2025).

⁴²⁷ *Tamże*, par. 27.

⁴²⁸ *Tamże*.

podejmowało współpracę z innymi organizacjami międzynarodowymi, w szczególności z UE, a także rozwijało politykę identyfikacji i neutralizacji zagrożeń ze strony CBRJ⁴²⁹.

Podsumowując działania hybrydowe wobec infrastruktury krytycznej należy zauważyć, że obecnie jest to największe zagrożenie dla bezpieczeństwa państwa i jego obywateli. Infrastruktura krytyczna jako obiekty niezbędne do prawidłowego działania państwa jest bezsprzecznym celem ataków hybrydowych, które cechują się przede wszystkim pewnym stopniem anonimowości (przynajmniej w momencie przeprowadzenia ataku) i brakiem możliwości przypisania konkretnych podmiotów (państw lub aktorów niepaństwowych) odpowiedzialnych za ten atak. UE i NATO podejmują konkretne działania w celu skutecznego przeciwdziałania zagrożeniom hybrydowym. UE przez ostatnie lata opracowała regulacje prawne oraz instrumenty prawne niewiążące, wyraźnie dopasowane do poszczególnych sektorów infrastruktury krytycznej, które poprawiły bezpieczeństwo tych sektorów, ale nie wyeliminowały całkowicie zagrożeń hybrydowych. Inaczej kształtuje się polityka NATO w tym zakresie. Przede wszystkim z racji swojego charakteru, NATO jako organizacja wojskowa stawia na rozwiązanie militarne tworząc między innymi siły szybkiego reagowania czy organizując ćwiczenia z wykorzystaniem elementów hybrydowych. Dodatkowo, wielokrotnie podkreślano możliwość zastosowania obrony zbiorowej z art. 5 Traktatu Północnoatlantyckiego, jednak dotychczas nie zdecydowano się na podjęcie tego kroku, pomimo że państwa członkowskie NATO, szczególnie państwa flankowe, jak Polska, Rumunia czy państwa bałtyckie codziennie mierzą się z działaniami hybrydowymi (od kryzysu migracyjnego po akty dywersji).

3.3 Ochrona infrastruktury krytycznej a zagrożenia terrorystyczne

Rozważania dotyczące zagadnienia ochrony infrastruktury krytycznej przed zagrożeniami terrorystycznymi należy poprzedzić analizą etymologiczną terminu „terroryzm”, ale również „terror”. Chociaż są to terminy pokrewne, ich definicje znacznie się od siebie różnią.

3.3.1 Geneza pojęcia terroryzmu

WSJP PAN definiuje pojęcie terroru jako „stosowanie przemocy i okrucieństwa dla zastraszenia i podporządkowania sobie kogoś”, a pochodzenia tego słowa należy szukać

⁴²⁹ *Tamże*, par. 33 i 43.

w języku łacińskim, w którym terror oznaczał groźę bądź strach⁴³⁰. Podobną definicję terroru zaprezentowano w SJP PWN – „przemoc i okrucieństwo albo groźby ich użycia stosowane wobec ludzi w celu ich zastraszenia”⁴³¹. Bardziej rozbudowane definicje terroru można spotkać natomiast w słownikach języka angielskiego. Idąc za definicjami zaprezentowanymi w Cambridge Dictionary za terror uważa się: „*extreme fear*”, „*violent action or threats designed to cause fear among ordinary people, in order to achieve political aims*”, ale również „*someone, especially a child, who behaves badly and is difficult to control*”⁴³². Analogiczne definicje terroru zostały zawarte w Oxford Learner’s Dictionaries, gdzie pod pojęciem terroru rozumie się „*a feeling of extreme fear*”, „*a person, situation or thing that makes you very afraid*”, „*violent action or the threat of violent action that is intended to cause fear, usually for political purposes*” oraz „*a person (usually a child) or an animal that causes you trouble or is difficult to control*”⁴³³. Analiza pojęcia terroru pokazuje, że zarówno w języku polskim, jak i w języku angielskim jest to termin rozumiany podobnie. Terror należy rozumieć jako zjawisko polegające na osiągnięciu celu, często politycznego, z zastosowaniem przemocy i innych brutalnych działań.

Od pojęcia terroru należy odróżnić pojęcie terroryzmu. Chociaż WSJP PAN wskazuje, że termin „terroryzm” pochodzi od słowa terror, to definiuje je jako „działalność ugrupowań pozapaństwowych przejawiającą się w aktach zbrojnych, prowadzoną w celu wywarcia presji na społeczeństwa lub rządy”⁴³⁴, a SJP PWN pod pojęciem terroryzmu rozumie „planowane i zorganizowane działania pojedynczych osób lub grup usiłujących poprzez stosowanie przemocy, okrucieństwa, zastraszania wymusić na rządach państw i społeczeństwach określone ustępstwa, świadczenia”⁴³⁵. Terroryzm jednakowo jest definiowany w słownikach języka angielskiego. Cambridge Dictionary określa terroryzm jako „*violent action or threats designed to cause fear among ordinary people, in order to achieve political aims*”⁴³⁶, a Oxford Learner’s Dictionaries jako „*the use of violent action in order to achieve political aims or to force a government to act*”⁴³⁷. Powyższe definicje ukazują, że elementem niezbędnym terroryzmu jest działalność grup niepaństwowych lub jednostek niezwiązanych oficjalnie z żadnym

⁴³⁰ *Terror*, https://wsjp.pl/haslo/do_druku/13307/terror (dostęp: 2.06.2025).

⁴³¹ *Terror - znaczenie, definicja*, <https://sjp.pwn.pl/slowniki/terror.html> (dostęp: 2.06.2025).

⁴³² *Terror*, <https://dictionary.cambridge.org/dictionary/english/terror> (dostęp: 2.06.2025).

⁴³³ *Terror*, <https://www.oxfordlearnersdictionaries.com/definition/english/terror?q=terror> (dostęp: 2.06.2025).

⁴³⁴ *Terroryzm*, https://wsjp.pl/haslo/do_druku/11791/terroryzm (dostęp: 2.06.2025).

⁴³⁵ *Terroryzm - znaczenie, definicja*, <https://sjp.pwn.pl/slowniki/terroryzm.html> (dostęp: 2.06.2025).

⁴³⁶ *Terrorism*, <https://dictionary.cambridge.org/dictionary/english/terrorism> (dostęp: 2.06.2025).

⁴³⁷ *Terrorism*, <https://www.oxfordlearnersdictionaries.com/definition/english/terrorism?q=terrorism> (dostęp: 2.06.2025).

państwem (osób nie będących oficjalnymi reprezentantami państwa), które dążą do osiągnięcia własnych celów.

Rozróżnienie terroru od terroryzmu jest uwarunkowane historycznie. Pojęcie terroru w Europie zaczęło funkcjonować w XIV wieku za sprawą języka francuskiego, natomiast w języku angielskim zostało odnotowane dopiero w XVI wieku⁴³⁸. Szersze użycie pojęcia „terroru” nastąpiło za sprawą Wielkiej Rewolucji Francuskiej rozpoczętej w 1789 roku, kiedy rządy rewolucyjne pod przewodnictwem Maksymiliana Robespiera’a były nazywane Wielkim Terrorem (fr. *Regime de la Terreur*)⁴³⁹. Polityka terroru prowadzona przez rząd rewolucyjny cechowała się dobrą organizacją oraz systematycznością, szczególnie wyróżniała się wysokim poziomem agresji wobec przeciwników politycznych⁴⁴⁰. Innym, znaczącym przykładem terroru jest polityka prowadzona przez III Rzeszę w latach 1933 – 1945 oraz Związek Radziecki pod rządami Józefa Stalina w latach 30. XX wieku. W przypadku III Rzeszy polityka terroru objawiała się szeroko rozwiniętą siecią jednostek o charakterze policyjno-wojskowym, między innymi *Sturmabteilung* (SA), *Schutzstaffel* (SS) czy Gestapo, których głównym zadaniem było zwalczanie przeciwników politycznych oraz mniejszości narodowych, etnicznych i religijnych⁴⁴¹. Podobnie jak w III Rzeszy, Związek Radziecki pod rządami Józefa Stalina charakteryzował się dobrze zorganizowanym aparatem represji, który był wykorzystywany przeciwko oponentom politycznym, ale również zwykłym obywatelom (represje prowadzone były przez organy bezpieczeństwa, ale szeroko rozwinięty był również system obozów pracy przymusowej, tzw. Gułag)⁴⁴². Biorąc pod uwagę opisaną powyżej działalność władz państwowych należy przyjąć, że pojęcie terroru odnosi się przede wszystkim do sytuacji, w której to państwo (władza państwowa) stosuje opresję w sposób zorganizowany i systematyczny, w celu realizacji swoich celów politycznych oraz utrzymania władzy.

Inaczej sytuacja kształtuje się w przypadku pojęcia terroryzmu. Poddając analizie definicję tego pojęcia ze słownika języka polskiego bądź języka angielskiego wyłaniają się co najmniej trzy elementy składowe definicji. Po pierwsze, działania terrorystyczne są prowadzone przez grupy niepaństwowe lub jednostki, po drugie, działania są prowadzone

⁴³⁸ T. Aleksandrowicz, *Terroryzm międzynarodowy*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008, s. 14.

⁴³⁹ *Tamże*, s. 15.

⁴⁴⁰ *Tamże*.

⁴⁴¹ R. Gellately, H. College, *Rethinking the Nazi Terror System: A Historiographical Analysis*, „German Studies Review”, 1991, vol. 14, no. 1, s. 23-24.

⁴⁴² Y. M. Zhukov, R. Talibova, *Stalin's terror and the long-term political effects of mass repression*, „Journal of Peace Research”, 2018, vol. 55, no. 2, s. 269-271.

przy pomocy agresji bądź innych „okrutnych” form, po trzecie, działania są ukierunkowane na realizację własnych celów (najczęściej będą to cele polityczne). Oprócz definicji słownikowych wielokrotnie podejmowano próby zdefiniowania terroryzmu na różnych płaszczyznach: od definicji legalnych, przez środowisko naukowe, aż po definicje urzędowe, tworzone przez krajowe organy rządowe lub jednostki zajmujące się zwalczaniem terroryzmu.

Pierwszą, istotną próbą sformułowania definicji legalnej terroryzmu było podpisanie Konwencji dotyczącej zapobiegania i karania terroryzmu z 1937 roku⁴⁴³. W art. 1 Konwencji za akt terroryzmu uznano wszystkie działania przestępcze skierowane przeciwko państwom, których celem jest wytworzenie stanu terroru w umysłach ludzi, grup osób lub społeczeństwa. Dodatkowo państwa-strony na podstawie art. 2 Konwencji zobowiązały się do uznania za przestępstwo następujące czyny, jeśli byłyby skierowane przeciwko innemu państwu:

- każde umyślne działanie powodujące śmierć lub obrażenia ciała głowy państwa lub osoby sprawującej urząd publiczny,
- każde umyślne działanie powodujące uszkodzenie mienia publicznego innego państwa, handel bronią i amunicją w celu dokonania aktu terroryzmu, oraz
- każde umyślne działanie mające zagrozić obywatelom państwa.

Przyczyną podjęcia prac nad konwencją zakazującą aktów terroryzmu było zabójstwo w 1934 roku króla Jugosławii Aleksandra I Karadziordziewicza oraz francuskiego ministra spraw zagranicznych Jean-Louis Barthou (obaj zostali zabici przez separatystów)⁴⁴⁴. Pomimo podpisania konwencji przez 24 państwa, ostatecznie nie weszła ona w życie, a sprawą sporną pomiędzy stronami były postanowienia dotyczące ekstradycji podejrzanych o akty terroryzmu⁴⁴⁵.

Żadne prace podejmowane w późniejszym czasie nie przyniosły definicji legalnej terroryzmu, aż do 2004 roku, kiedy świat stanął na progu nowej wojny, wcześniej nieznanej. W odpowiedzi na zamach z 11 września 2001 roku prezydent Stanów Zjednoczonych G. W. Bush wypowiedział wojnę z terroryzmem (ang. *war on terrorism*)⁴⁴⁶. Jej pierwszą fazą była zbrojna interwencja państw NATO w Afganistanie, rozpoczęta w październiku 2001 roku

⁴⁴³ *Convention for the Prevention and Punishment of Terrorism*, Geneva, 16.11.1937, 19 League of Nations Official Journal 23 (1938).

⁴⁴⁴ D. Dróżdż, *Terroryzm i akt terroryzmu na świecie w świetle prawa*, Wydawnictwo My Book, Szczecin 2018, s. 20-21.

⁴⁴⁵ J. Dugard, *Towards the Definition of International Terrorism*, „The American Journal of International Law”, 1973, vol. 67, nr 5, s. 95.

⁴⁴⁶ M. Stohl, *The Global War on Terror and State Terrorism*, „Perspectives on Terrorism”, 2008, vol. 2, nr 9, Special Issue: Under-investigated topics in terrorism research, s. 4-5.

pod nazwą Trwała Wolność (ang. *Enduring Freedom*)⁴⁴⁷. Interwencja NATO została poprzedzona rezolucją RB ONZ nr 1373 z 28 września 2001 roku, zgodnie z którą państwa były zobowiązane do szeroko pojętej walki z terroryzmem, ale w samej rezolucji nie zawarto definicji terroryzmu⁴⁴⁸.

Rozwój działań podejmowanych przeciwko terroryzmowi spowodował konieczność zdefiniowania tego pojęcia, i tak 8 października 2004 roku RB ONZ przyjęła rezolucję nr 1566, zgodnie z którą za terroryzm uważa się „akty kryminalne włączające do swojego zakresu czyny przeciwko ludności cywilnej popełnione z zamiarem spowodowania śmierci albo ciężkich uszkodzeń ciała, albo wzięcie zakładników, by wywołać stan terroru w społeczeństwie lub grupie osób lub u poszczególnych osób, by przerazić społeczeństwo lub zmusić rząd lub międzynarodowe organizacje, by robiły lub powstrzymywały się od podejmowania jakiegokolwiek działania w zakresie i jak zdefiniowane w międzynarodowych konwencjach i protokołach związanych z terroryzmem i w żadnych okolicznościach nieusprawiedliwiona przez polityczne, filozoficzne, ideologiczne, rasowe, etniczne, religijne i innej podobnej natury”⁴⁴⁹.

Próby zdefiniowania terroryzmu podjęto również w aktach prawa krajowego. W Stanach Zjednoczonych wprowadzono dwa pojęcia. Pierwsze odnosi się do terroryzmu międzynarodowego i oznacza „akt przemocy lub działanie zagrażające życiu ludzkiemu, które stanowią naruszenie przepisów prawa karnego Stanów Zjednoczonych lub któregośkolwiek stanu, lub które stanowiłyby przestępstwo, gdyby zostało popełnione na terytorium Stanów Zjednoczonych lub któregośkolwiek stanu, który ma na celu zastraszanie lub wymuszanie na ludności cywilnej, wywieranie wpływu na politykę rządu poprzez zastraszanie lub wymuszanie lub wpływanie na działania rządu poprzez masowe zniszczenia, zabójstwa lub porwania a występuje głównie poza jurysdykcją terytorialną Stanów Zjednoczonych lub wykracza poza granice państwowe pod względem środków, za pomocą których jest realizowany, osób, które wydają się być przedmiotem zastraszania lub wymuszania, lub lokalizacji, w której sprawcy działają lub szukają azylu.”⁴⁵⁰. Drugim zdefiniowanym terminem jest terroryzm krajowy za który rozumie się „działania zagrażające życiu ludzkiemu, które stanowią naruszenie przepisów prawa karnego Stanów Zjednoczonych lub któregośkolwiek ze stanów, mające na celu

⁴⁴⁷ *Tamże*, s. 5.

⁴⁴⁸ RB ONZ, *Resolution 1373...*, s. 2-4.

⁴⁴⁹ RB ONZ, *Resolution 1566 (2004)*, 8.10.2004, S/RES/1566 (2004), s. 2. Tłumaczenie za D. Drózdź, *Terroryzm i akt terroryzmu...*, s. 26.

⁴⁵⁰ USA, 18 USC 2331: *Definitions, 18-Crimes and Criminal Procedure*, [https://uscode.house.gov/view.xhtml?req=\(title:18%20section:2331%20edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:18%20section:2331%20edition:prelim)) (dostęp: 2.06.2025).

zastraszanie lub wymuszanie posłuszeństwa ludności cywilnej, wywieranie wpływu na politykę rządu poprzez zastraszanie lub wymuszanie posłuszeństwa lub wpływanie na działania rządu poprzez masowe zniszczenia, zabójstwa lub porwania, a występujące głównie na terytorium podlegającym jurysdykcji Stanów Zjednoczonych”⁴⁵¹. Także w polskim systemie prawnym zdefiniowano terroryzm. W art. 115 § 20 ustawy z dnia 6 czerwca 1997 roku Kodeks karny wprowadzono pojęcie przestępstwa o charakterze terrorystycznym, za który uważa się „czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej pięć lat, popełniony w celu poważnego zastraszania wielu osób, zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności, wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej, a także groźba popełnienia takiego czynu”⁴⁵². Obie definicje zostały opracowane na potrzeby krajowego prawa karnego, którego celem jest penalizacja czynów terrorystycznych, wynikająca nie tylko z zagrożenia dla bezpieczeństwa państwa, ale także z zobowiązań międzynarodowych, jak wspomniana powyżej rezolucja RB ONZ nr 1373.

Problematyka definiowania zjawiska terroryzmu pozostaje również w zainteresowaniach przedstawicieli nauk o bezpieczeństwie, jak i nauk prawnych. Jak wskazuje T. Aleksandrowicz terroryzm „nie zastyga w czasie, lecz podlega nieustannym, różnorodnym i chaotycznym transformacjom”⁴⁵³. Różnorodność działań terrorystycznych powoduje powstanie wielu definicji, które niejednokrotnie definiują samo zjawisko terroryzmu w odmienny sposób, szczególnie za sprawą różnych metod przeprowadzenia działań terrorystycznych (obecnie można wskazać aż dwieście definicji terroryzmu)⁴⁵⁴. Pomimo tego, możliwe jest wskazanie co najmniej kilku definicji, zawierających w sobie elementy niezbędne czynów terrorystycznych. Przede wszystkim należy przywołać definicję M. Fleminga, który pod pojęciem terroryzmu rozumie „umyślne działanie stanowiące naruszenie prawa karnego i zmierzające w drodze aktów przemocy lub zagrożenia tymi aktami do zastraszania organów państwa lub znacznych odłamów społeczeństwa oraz do wymuszenia określonego postępowania”⁴⁵⁵. Definicję nie zwierającą aspektu naruszenia prawa karnego zaprezentował natomiast B. Bolechów, który terroryzmem określił formę przemocy politycznej, polegającą na

⁴⁵¹ *Tamże*.

⁴⁵² *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny*, Dz. U. z 1997 r., nr 88, poz. 553.

⁴⁵³ T. Aleksandrowicz, *Terroryzm...*, s. 12.

⁴⁵⁴ *Tamże*, s. 20.

⁴⁵⁵ M. Fleming, *Terroryzm polityczny w międzynarodowym prawodawstwie*, „Wojskowy Przegląd Prawniczy”, 1996, nr 1, s. 3.

stosowaniu morderstw lub zniszczeń (albo groźeniu zastosowaniem takich środków) w celu wywołania szoku i ekstremalnego zastraszenia jednostek, grup społecznych lub rządów, czego efektem mają być wymuszenia pożądanых ustępstw politycznych, sprowokowanie nieprzemyślanych działań lub zademonstrowanie własnych politycznych przekonań”⁴⁵⁶. Podobne definicje zaprezentowali J. Tomaszewicz, dla którego terroryzm to „systematyczne posługiwanie się aktami terroru indywidualnego dla osiągnięcia celu politycznego”⁴⁵⁷ oraz T. Białek, który terroryzm rozumie jako „wywieranie wpływu politycznego przez bezprawne stosowanie siły (przymusu lub przemocy) związane z łamaniem elementarnych norm społecznych i ustalonych w danym kręgu reguł walki politycznej, oparte na rozmyślnym zastraszeniu i manipulowaniu; osiąganie celów politycznych poprzez stwarzanie aktami przemocy atmosfery zagrożenia i utrudniania funkcjonowania wrogiego układu społecznego oraz wymuszanie decyzji, a także działań przeciwnika przez drastyczną taktykę faktów dokonanych lub szantażu siłowego”⁴⁵⁸. Analiza powyższych definicji umożliwia wyodrębnienie czterech cech charakteryzujących działania terrorystyczne⁴⁵⁹:

1. użycie przemocy lub groźba użycia przemocy;
2. zbrodnia ślepa⁴⁶⁰;
3. wywołanie określonego efektu i reakcji ze strony władz lub opinii publicznej;
4. brutalność metod terrorystycznych.

Wszystkie cztery cechy pozwalają stwierdzić, że głównym celem terroryzmu jest osiągnięcie celu politycznego przy pomocy wysokiego poziomu przemocy, nakierowanej na ludność cywilną lub obiekty cywilne.

3.3.2 Działania organizacji międzynarodowych podejmowane przeciwko zagrożeniom terrorystycznym

Chociaż główny ciężar walki z zagrożeniami terrorystycznymi spoczywa na państwach, a konkretnie na wyspecjalizowanych jednostkach policyjnych i wojskowych, a także właściwie uregulowanym prawie karnym, to sporą rolę w zwalczaniu terroryzmu odgrywa również społeczność międzynarodowa, szczególnie takie organizacje międzynarodowe jak ONZ,

⁴⁵⁶ B. Bolechów, *Terroryzm w świecie podwubiegunowym*, Wydawnictwo Adam Marszałek, Toruń 2002 r., s. 35.

⁴⁵⁷ J. Tomaszewicz, *Terroryzm na tle przemocy politycznej*, Wydawnictwo APIS, Katowice 2000, s. 12.

⁴⁵⁸ T. Białek, *Terroryzm. Manipulacja strachem*, Studio EMKA, Warszawa 2005, s. 151.

⁴⁵⁹ T. Aleksandrowicz, *Terroryzm...*, s. 20.

⁴⁶⁰ Akt przemocy polegający na przypadkowym wyborze ofiar, najczęściej w miejscu publicznym, mający na celu zwiększenie poczucie zagrożenia. Por. T. Aleksandrowicz, *Terroryzm...*, s. 20 oraz T. Walek, *Pojęcie, geneza i klasyfikacja zjawisk terrorystycznych*, „Securitologia” 2018, nr 2, s. 119.

OBWE oraz Rada Europy. Na forach tych organizacji powstawały akty prawa międzynarodowego określające sposoby identyfikacji, przeciwdziałania i zwalczania aktów terroryzmu.

Pierwsze regulacje dotyczące zwalczania aktów terroryzmu zostały podjęte na forum ONZ już w latach 60. i 70 XX wieku. 14 września 1963 roku, w ramach Organizacji Międzynarodowego Lotnictwa Cywilnego (ICAO) przyjęta została Konwencja w sprawie przestępstw i niektórych innych czynów popełnionych na pokładzie statków powietrznych (Konwencja tokijska)⁴⁶¹. Zgodnie z art. 1 tej konwencji znajduje ona swoje zastosowanie do przestępstw przewidzianych w prawie karnym oraz do czynów, które niezależnie od tego, czy są przestępstwami, mogą narażać lub narażają na niebezpieczeństwo statek powietrzny, osoby albo mienie znajdujące się na pokładzie, lub czynów, które naruszają porządek i dyscyplinę na pokładzie. Kluczowym postanowieniem konwencji z perspektywy zwalczania terroryzmu jest art. 11, który przewiduje, że państwa-strony zobowiązują się podjąć wszelkie niezbędne środki w celu przywrócenia lub utrzymania kontroli nad statkiem powietrznym, jeżeli osoba znajdująca się na pokładzie bezprawnie zakłóciła przemocą lub groźbą użycia przemocy eksploatację statku powietrznego znajdującego się w locie, zawładnęła takim statkiem lub objęła nad nim kontrolę albo gdy ma zamiar dokonać takiego czynu.

Konwencja nie zawiera definicji terroryzmu, ani też nie odwołuje się w jakikolwiek inny sposób do aktów terrorystycznych, jednak opis czynu z art. 11 Konwencji może wskazywać, że ma on charakter terrorystyczny. Kontynuując prace nad zwiększeniem bezpieczeństwa w lotnictwie cywilnym 16 grudnia 1970 roku przyjęta została Konwencja o zwalczaniu bezprawnego zawładnięcia statkami powietrznymi (Konwencja haska z 1970 roku)⁴⁶². Tak samo jak w Konwencji tokijskiej, tak w Konwencji haskiej z 1970 roku nie powołano się w żaden sposób na akt terroryzmu, jednak analiza postanowień tej Konwencji wprost wskazuje na taki charakter bezprawnego zawładnięcia statkiem powietrznym. Zgodnie z art. 1 tej konwencji każda osoba, która na pokładzie statku powietrznego będącego w locie bezprawnie, przemocą lub groźbą użycia przemocy lub w każdej innej formie zastraszenia dokonuje zawładnięcia statkiem powietrznym lub przejęcia nad nim kontroli albo też usiłuje popełnić taki czyn, lub współdziała z osobą, która popełnia lub usiłuje popełnić taki czyn, popełnia przestępstwo. Do obowiązków państw-stron konwencji należy między innymi

⁴⁶¹ Konwencja w sprawie przestępstw i niektórych innych czynów popełnionych na pokładzie statków powietrznych, Tokio, 14.09.1963, Dz. U. z 1971 r., nr 15, poz. 147.

⁴⁶² Konwencja o zwalczaniu bezprawnego zawładnięcia statkami powietrznymi, Haga, 16.12.1970, Dz. U. z 1972 r., nr 25, poz. 181.

zatrzymanie osoby lub osób podejrzanych o dopuszczenie się czynu wymienionego w art. 1 oraz niezwłoczne przystąpienie do dochodzenia mającego na celu ustalenie stanu faktycznego. Zgodnie z art. 8 Konwencji przestępstwo określone w art. 1 jest podstawą do ekstradycji.

Ostatnim aktem prawnym, przyjętym w ramach ICAO, dotyczącym bezprawnych działań na pokładzie statków powietrznych, jest przyjęta 23 września 1971 roku Konwencja o zwalczaniu bezprawnych czynów skierowanych przeciwko bezpieczeństwu lotnictwa cywilnego (Konwencja montrealaska)⁴⁶³. Ze wszystkich trzech konwencji przyjętych w ramach ICAO to Konwencja montrealaska zawiera najszerszy katalog czynów zabronionych podczas odbywania podróży statkiem pasażerskim, który zgodnie z art. 1 tej Konwencji obejmuje:

1. akt przemocy wobec osoby znajdującej się na pokładzie statku powietrznego będącego w locie, jeżeli czyn ten może zagrażać bezpieczeństwu tego statku powietrznego;
2. niszczenie statku powietrznego będącego w służbie lub powodowanie jego uszkodzenia, które czyni go niezdolnym do lotu lub które może stworzyć zagrożenie jego bezpieczeństwa w locie;
3. umieszczenie lub powodowanie umieszczenia w jakikolwiek sposób na statku powietrznym będącym w służbie urządzeń lub substancji, które mogą ten statek zniszczyć albo spowodować jego uszkodzenie czyniące go niezdolnym do lotu lub mogące stworzyć zagrożenie jego bezpieczeństwa w locie;
4. niszczenie lub uszkodzanie lotniczych urządzeń nawigacyjnych lub zakłócanie ich działania, jeżeli czyn taki może zagrozić bezpieczeństwu statku powietrznego w locie, lub
5. przekazanie informacji, o których wie, że są fałszywe, stwarzając w ten sposób zagrożenie bezpieczeństwa statku powietrznego w locie.

Konwencja przewiduje, że powyższe działania mogą zostać podjęte tylko umyślnie i bezprawnie. Analogicznie do Konwencji haskiej z 1970 roku państwo-strona jest zobowiązane do zatrzymania osoby lub osób podejrzanych o popełnienie przestępstwa z art. 1, a także do wszczęcia ewentualnej procedury ekstradycyjnej. 24 lutego 1988 roku przyjęto Protokół o zwalczaniu bezprawnych czynów przemocy w portach lotniczych obsługujących międzynarodowe lotnictwo cywilne uzupełniający Konwencję o zwalczaniu bezprawnych

⁴⁶³ Konwencja o zwalczaniu bezprawnych czynów skierowanych przeciwko bezpieczeństwu lotnictwa cywilnego, Montreal, 23.09.1971, Dz. U. z 1976 r., nr 8, poz. 37.

czynów skierowanych przeciwko bezpieczeństwu lotnictwa cywilnego podpisaną w Montrealu dnia 23 września 1971 roku (Protokół dodatkowy z 1988 roku)⁴⁶⁴. Głównym celem przyjęcia Protokołu dodatkowego z 1988 roku było rozszerzenie katalogu przestępstw przewidzianych w art. 1 Konwencji montrealskiej o bezprawne i umyślne dokonanie, przy użyciu jakiegokolwiek urządzenia, substancji lub broni:

1. aktu przemocy skierowanego przeciwko osobie w porcie lotniczym obsługującym międzynarodowe lotnictwo cywilne, który to akt powoduje lub może spowodować poważne uszkodzenia ciała lub śmierć tej osoby;
2. zniszczenia lub poważnego uszkodzenia urządzenia w porcie lotniczym obsługującym międzynarodowe lotnictwo cywilne lub statki powietrzne niebędące w użyciu a znajdujące się w tym porcie, albo powoduje przerwę w działalności tego portu lotniczego, jeśli taki czyn zagraża lub może zagrozić bezpieczeństwu w tym porcie lotniczym.

Pomimo braku zdefiniowania terroryzmu w przytoczonych konwencjach, poprzez szczegółowe opisanie czynów będących przestępstwem utworzono ramy prawne, potencjalnie pozwalające na skuteczne przeciwdziałanie aktom terrorystycznym wobec transportu lotniczego. Jednak jak wynika z danych statystycznych tylko w latach 1968 – 1970 doszło do 151 porwań samolotów, natomiast w latach 1980 – 2022 samoloty pasażerskie zostały porwane aż 553 razy, z czego najsłynniejsze porwanie dokonane 11 września 2001 roku przez terrorystów powiązanych z dżihadystycznym ugrupowaniem Al-Kaidą utratę życia 2996 osób⁴⁶⁵.

Kolejnym aktem prawnym, przyjętym na forum ONZ, ukierunkowanym *stricte* na działania terrorystyczne była Międzynarodowa konwencja w sprawie zwalczania terrorystycznych ataków bombowych z 15 grudnia 1997 roku (Konwencja o zwalczaniu terrorystycznych ataków bombowych)⁴⁶⁶. Zgodnie z art. 2 ust 1 tej Konwencji przestępstwo popełnia każdy kto bezprawnie i umyślnie dostarcza, umieszcza, wystrzeliwuje lub detonuje materiał wybuchowy, albo inne śmiertelne narzędzie w miejscu użyteczności publicznej, w kierunku takiego miejsca lub na takie miejsce, infrastrukturę państwową lub rządową, system

⁴⁶⁴ Protokół o zwalczaniu bezprawnych czynów przemocy w portach lotniczych obsługujących międzynarodowe lotnictwo cywilne uzupełniający Konwencję o zwalczaniu bezprawnych czynów skierowanych przeciwko bezpieczeństwu lotnictwa cywilnego, Montreal, 24.02.1988, Dz. U. z 2006 r., nr 48, poz. 348.

⁴⁶⁵ K. Izak, *Ataki terrorystyczne i sabotażowe na wybrane systemy infrastruktury krytycznej – perspektywa historyczna*, „Terroryzm – studia, analizy, prewencja”, 2025, wydanie specjalne, s. 93-96.

⁴⁶⁶ Międzynarodowa konwencja o zwalczaniu terrorystycznych ataków bombowych, Nowy Jork, 15.12.1997, Dz. U. z 2007 r., nr 66, poz. 438.

transportu publicznego lub infrastrukturę z zamiarem spowodowania śmierci lub poważnych obrażeń ciała albo z zamiarem spowodowania rozległych zniszczeń takiego miejsca, infrastruktury lub systemu, jeśli takie zniszczenie powoduje lub może spowodować poważne straty gospodarcze. Na podstawie art. 2 ust. 2 i 3 konwencji osoby, które usiłowały, współdziałały, organizowały lub w jakikolwiek inny sposób przyczyniły się do dokonania czynów określonych w ust. 1 również są uważane za osoby, które dopuściły się tego przestępstwa.

Chociaż w samej Konwencji nie zdefiniowano infrastruktury krytycznej, zamiast tego użyto pojęć „infrastruktury państwowej lub rządowej” oraz „infrastruktury”, to jej normy są kluczowe dla bezpieczeństwa infrastruktury krytycznej, ponieważ wprowadzają standard ochrony infrastruktury krytycznej przed zamachami bombowymi. Na podstawie art. 1 pkt 1 tej konwencji za infrastrukturę państwową lub rządową rozumie się wszelkie pomieszczenia lub pojazdy, które są stale lub czasowo wykorzystywane lub zajmowane przez przedstawicieli państwa, członków rządu, parlamentu lub sądownictwa, przez funkcjonariuszy lub pracowników państwowych lub jakichkolwiek innych władz lub instytucji publicznych, lub przez pracowników bądź funkcjonariuszy organizacji międzyrządowych w związku z pełnieniem przez nich obowiązków służbowych. Natomiast w art. 1 pkt 2 infrastrukturę zdefiniowano jako jakąkolwiek infrastrukturę stanowiącą własność publiczną lub prywatną, związaną ze świadczeniem lub dystrybucją usług dla ogółu społeczności, taką jak wodociągi, kanalizacja, elektryczność, paliwo lub łączność. Zakres obiektów obecnie uznawanych za infrastrukturę krytyczną zdecydowanie pokrywa się zarówno z definicją „infrastruktury państwowej lub rządowej” oraz „infrastruktury”, a rozbieżność definicji infrastruktury w konwencji na „państwową” oraz „cywilną/zwykłą” wynika z jednostkowego używania terminu „infrastruktura krytyczna” do obiektów zarówno należących do państwa, jak i podmiotów prywatnych.

W ONZ dostrzeżono również konieczność uregulowania kwestii związanych z wykorzystywaniem materiałów radioaktywnych i obiektów jądrowych jako potencjalnych środków lub celów aktów terrorystycznych, dlatego 13 kwietnia 2005 roku przyjęto Międzynarodową konwencję o zwalczaniu terroryzmu jądrowego⁴⁶⁷. Na podstawie art. 2 ust. 1 tej konwencji każdy kto w sposób bezprawny i świadomy posiada materiał promieniotwórczy lub wytwarza, bądź posiada urządzenie z zamiarem spowodowania śmierci lub poważnego

⁴⁶⁷ Międzynarodowa konwencja w sprawie zwalczania aktów terroryzmu jądrowego, Nowy Jork, 13.04.2005, Dz. U. z 2010 r., nr 112, poz. 740.

uszkodzenia ciała, z zamiarem spowodowania poważnej szkody w mieniu lub środowisku bądź w jakikolwiek sposób używa materiału promieniotwórczego lub urządzenia, lub używa albo powoduje szkodę w obiekcie jądrowym w sposób, który powoduje uwolnienie lub ryzyko uwolnienia materiału promieniotwórczego z zamiarem spowodowania śmierci lub poważnego uszkodzenia ciała, z zamiarem spowodowania poważnej szkody w mieniu lub środowisku lub z zamiarem zmuszenia osoby fizycznej lub prawnej, albo organizacji międzynarodowej, lub państwa do określonego działania lub zaniechania popełnia przestępstwo w rozumieniu konwencji. Dodatkowo, zgodnie z art. 2 ust. 2 konwencji przestępstwo popełnia także ten, kto grozi, w okolicznościach wskazujących na wiarygodność takiej groźby, popełnieniem przestępstwa określonego w art. 2 pkt 1 lit. b lub domaga się bezprawnie i świadomie materiału promieniotwórczego, urządzenia lub obiektu jądrowego posługując się groźbą, w okolicznościach wskazujących na wiarygodność takiej groźby, lub przy użyciu siły. Ponadto za przestępstwo uważa się również usiłowanie, pomocnictwo oraz przyczynienie się w jakikolwiek inny sposób do popełnienia przestępstwa z art. 2 ust. 1 i 2. Do podstawowych obowiązków państw-stron konwencji należy stypizowanie w systemach krajowych przestępstw określonych w art. 2 konwencji wraz z uwzględnieniem zagrożenia karami adekwatnymi do ich społecznej szkodliwości⁴⁶⁸.

Analiza wybranych konwencji międzynarodowych z zakresu ochrony przed terroryzmem, przyjętych na forum ONZ ukazuje pewien powtarzalny schemat w tworzeniu tych aktów prawnych. Chociaż każda z nich dotyczy zupełnie innego sektora (transport lotniczy, sektor jądrowy oraz szeroko rozumiana infrastruktura krytyczna), to we wszystkich określono bardzo podobne obowiązki państw będących stronami tych konwencji. Strony są przede wszystkim zobowiązane do zatrzymania osób podejrzanych o popełnienie przestępstw oraz niezwłoczne wszczęcie dochodzenia w sprawie. Jedynie Konwencja o zwalczaniu terroryzmu jądrowego zawiera postanowienia nakazujące wprowadzenie do krajowych systemów prawnych typizacji przestępstw o charakterze terroryzmu jądrowego. Tym samym normy dotyczące zupełnie odmiennych sektorów są regulowane w ten sam sposób, nie uwzględniając specyficznych wymagań poszczególnych sektorów infrastruktury krytycznej.

Działania zmierzające do zwalczania terroryzmu podjęto również na forum RE. Jednak, w porównaniu z systemem sektorowym w ONZ, regulacje RE zostały sformułowane w sposób

⁴⁶⁸ Zob. art. 184 ustawy z dnia 6 czerwca 1997 r. Kodeks karny.

ogólny⁴⁶⁹. Pierwszym aktem prawnym o zwalczaniu terroryzmu przyjętym na forum RE była Europejska konwencja o zwalczaniu terroryzmu z 27 stycznia 1977 roku⁴⁷⁰. Powodem jej przyjęcia było stworzenie ram prawnych do skutecznego ścigania sprawców ataków terrorystycznych (zob. Preambuła do Konwencji o zwalczaniu terroryzmu). W odróżnieniu od umów międzynarodowych zawartych na forum ONZ, Konwencja o zwalczaniu terroryzmu nie wprowadziła katalogu przestępstw uznanych za działania terrorystyczne, a skupiła się tylko na procedurze ekstradycyjnej. Zastosowanie ekstradycji jako formy zwalczania terroryzmu wpisuje się w szerszą koncepcję RE dotyczącą zwalczania przestępczości, która opiera się na zasadach ekstradycji oraz pomocy prawnej w sprawach karnych⁴⁷¹.

Drugim aktem prawnym o zwalczaniu terroryzmu, zawartym na forum RE, była Konwencja Rady Europy o zapobieganiu terroryzmowi z 16 maja 2005 roku⁴⁷². Przyjęcie jej stanowiło odpowiedź na zwiększone zagrożenie terrorystyczne w Europie (zob. Preambuła do Konwencji o zapobieganiu terroryzmowi). Nowa konwencja ustanowiła szereg obowiązków mających usprawnić walkę z terroryzmem. Na podstawie art. 2 tej konwencji każda strona podejmie stosowne środki, w szczególności w zakresie szkolenia organów ścigania i innych organów, a także w zakresie edukacji, kultury, informacji, mediów i podnoszenia świadomości społecznej, mając na celu zapobieganie przestępstwom o charakterze terrorystycznym i ich negatywnym skutkom, przy poszanowaniu zobowiązań dotyczących praw człowieka wyrażonych, jeżeli mają zastosowanie w stosunku do tej strony, w Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności⁴⁷³, Międzynarodowym pakcie praw obywatelskich i politycznych⁴⁷⁴ oraz innych zobowiązań wynikających z prawa międzynarodowego. Do najważniejszych środków zaliczyć można: wymianę informacji, poprawę fizycznej ochrony osób i rzeczy oraz wzmocnienie szkolenia i koordynacji zarządzania kryzysowego. Oprócz tego, strony mają obowiązek udzielać sobie wzajemnej pomocy i poparcia, mając na celu wzmocnienie swoich zdolności zapobiegania popełnianiu przestępstw o charakterze terrorystycznym, zarówno poprzez wymianę informacji i najlepszych

⁴⁶⁹ T. Aleksandrowicz, *Terroryzm...*, s. 70-71.

⁴⁷⁰ *Europejska konwencja o zwalczaniu terroryzmu*, Strasburg, 27.01.1977, Dz.U. z 1996 r., nr 117, poz. 557.

⁴⁷¹ T. Aleksandrowicz, *Terroryzm...*, s. 73.

⁴⁷² *Konwencja Rady Europy o zapobieganiu terroryzmowi*, Warszawa, 16.05.2005, Dz. U. z 2008 r., nr 161, poz. 998.

⁴⁷³ *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności, zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2*, Rzym, 4.11.1950, Dz. U. z 1993 r., nr 61, poz. 284.

⁴⁷⁴ *Międzynarodowy Pakt Praw Obywatelskich i Politycznych*, Nowy Jork, 16.12.1966, Dz. U. z 1977 r., nr 38, poz. 167.

praktyk, jak również poprzez szkolenia i inne wspólne wysiłki o charakterze zapobiegawczym (zob. art. 4 Konwencji o zapobieganiu terroryzmowi).

Postanowienia Konwencji określają również tzw. przestępstwa okołoterrorystycznych⁴⁷⁵, do których zalicza się:

1. rozpowszechnianie lub innego rodzaju udostępnianie przekazu do publicznej wiadomości z intencją podżegania do popełnienia przestępstwa o charakterze terrorystycznym, jeżeli takie zachowanie, bezpośrednio lub pośrednio stwarza niebezpieczeństwo, że jedno lub więcej takich przestępstw może zostać popełnionych,
2. rekrutację na rzecz terroryzmu,
3. szkolenie na rzecz terroryzmu.

Zupełnym *novum* wprowadzonym w Konwencji jest ochrona, odszkodowanie oraz wsparcie dla ofiar terroryzmu. Zgodnie z art. 13 konwencji każda strona przyjmie takie środki, jakie będą konieczne, aby chronić i wspierać ofiary aktu terroryzmu, jaki został popełniony na jej własnym terytorium. Środki te mogą obejmować przed wszystkim pomoc finansową i odszkodowanie dla ofiar terroryzmu oraz członków ich bliskiej rodziny.

Analiza treści Konwencji o zwalczaniu terroryzmu może doprowadzić do wniosków, że RE nie do końca zrozumiała powagę zagrożeń terrorystycznych uznając procedurę ekstradycji jako narzędzie wystarczające do zwalczania aktów terrorystycznych. Zapewne wynika to z braku doświadczenia tak krwawych ataków terrorystycznych jakie miały miejsce po 11 września 2001 roku⁴⁷⁶. Na odmienną ocenę natomiast zasługuje Konwencja o zapobieganiu terroryzmowi, która przyjęta już po doświadczeniach „11 września” opracowała regionalne standardy zwalczania aktów terrorystycznych, obejmujące na przykład rozwój współpracy międzynarodowej, ale również ustanowiła ramy prawne dla pomocy ofiarom terroryzmu.

3.4 Podsumowanie

Na podstawie powyższych ustaleń należy stwierdzić, że infrastruktura krytyczna jest zdecydowanie częściej celem ataków w czasie pokoju poprzez działalność hybrydową oraz działalność terrorystyczną, niż w trakcie konfliktu zbrojnego. Taki stan rzeczy wymusza na państwach oraz na społeczności międzynarodowej wypracowanie standardów skutecznej ochrony infrastruktury krytycznej przed tymi zagrożeniami.

⁴⁷⁵ T. Aleksandrowicz, *Terroryzm...*, s. 77.

⁴⁷⁶ W. Szewko, *Księga Dżihadu*, Alt.pl Sp. z o.o., Warszawa 2024, s. 328-330.

W przypadku zagrożeń hybrydowych widać szczególną aktywność państw zgromadzonych w UE oraz NATO. Oczywiście nie powinno budzić to zdziwienia, ponieważ państwa te stanowią przeciwwagę dla Rosji, która jest państwem wiodącym w działaniach hybrydowych. Regulacje unijne charakteryzują się typowym podziałem infrastruktury krytycznej, uwzględniając każdy sektor, na przykład energetyczny, transportu czy finansowy. Jednocześnie uwaga skupia się na zagadnieniach bezpieczeństwa cybernetycznego poszczególnych sektorów infrastruktury krytycznej, co świadczy o dużej świadomości przedstawicieli unijnych o zagrożeniach hybrydowych. Obecnie działalność w cyberprzestrzeni stanowi jeden z głównych elementów działań hybrydowych. Inny model ochrony infrastruktury krytycznej prezentuje NATO, który nie wprowadza rozwiązań sektorowych, ale skupia się na rozwoju zdolności militarnych w zakresie ochrony infrastruktury krytycznej, uwzględniających zagrożenia hybrydowe.

W obliczu aktywnych konfliktów zbrojnych, między innymi pomiędzy Rosją a Ukrainą czy Izraelem a Hamasem, wydaje się, że działalność terrorystyczna zeszła na dalszy plan i nie stanowi obecnie poważnego zagrożenia. Jak pokazują jednak ataki przeprowadzone w 2024 roku na centrum handlowe w Moskwie⁴⁷⁷ oraz w Nowym Orleanie⁴⁷⁸ zagrożenie terrorystyczne ciągle pozostaje na wysokim poziomie. Infrastruktura krytyczna obejmująca w swym zakresie obiekty kluczowe dla bezpieczeństwa państwa stanowi doskonały cel dla terrorystów. Uszkodzenie sieci energetycznej lub pozbawienie dostępu do opieki medycznej bez wątpienia wzbudzą niepokój i strach wśród ludzi. W odróżnieniu od zagrożeń hybrydowych terroryzm był zjawiskiem znanym społeczeństwu już od dawna, dlatego zarówno państwa, jak i organizacje międzynarodowe prowadziły intensywne prace nad ustanowieniem norm zwalczających terroryzm. Największy dorobek prawny w tym zakresie należy do ONZ, na forum której przyjęto szereg umów międzynarodowych sektorowych, zobowiązujących strony do przeciwdziałania terroryzmowi. Dodatkowo organizacje regionalne, jak RE opracowały własne regulacje, usprawniające zwalczanie międzynarodowego terroryzmu.

Dorobek prawny zarówno w zakresie zwalczania zagrożeń hybrydowych, jak i zagrożeń terrorystycznych, powinien stanowić inspirację dla poszerzenia regulacji ochrony infrastruktury krytycznej podczas konfliktu zbrojnego, zważywszy, że tak zagrożenia

⁴⁷⁷ *Zamach w Moskwie*, <https://www.pism.pl/publikacje/zamach-w-moskwie> (dostęp: 2.06.2025).

⁴⁷⁸ *Zamachy w Nowym Orleanie i Las Vegas. Islamiści wrócili do USA*, <https://www.rp.pl/przesteczosc/art41639921-zamachy-w-nowym-orleanie-i-las-vegas-islamisci-wrocili-do-usa> (dostęp: 2.06.2025).

hybrydowe, jak i terrorystyczne nierzadko mają ścisły związek z konfliktem zbrojnym – stanowią jego zapowiedź, poprzedzają go lub występują równolegle z nim.

4 Obowiązki stron konfliktu zbrojnego w zakresie ochrony infrastruktury krytycznej

4.1 Wprowadzenie

Infrastruktura krytyczna jako jeden z najważniejszych elementów bezpieczeństwa państwa pozostaje podczas konfliktu zbrojnego częstym celem ataków. Z uwagi na to, że obiekty infrastrukturalne służą zarówno państwu jako instytucji, ale również wpływają na bezpieczeństwo ludności cywilnej, ich atakowanie podlega ścisłym regulacjom MPH.

Ustalenie obowiązków stron konfliktu zbrojnego w zakresie ochrony infrastruktury krytycznej wymaga przeprowadzenia trzyczęściowej analizy norm prawa humanitarnego. W pierwszej części dokonana będzie analiza obowiązków ochrony infrastruktury krytycznej zgodnie z wymaganiami podstawowych zasad MPH – rozróżniania, proporcjonalności, konieczności wojskowej oraz humanitaryzmu.

Druga część analizy dotyczy ustalenia środków ostrożności, którymi powinna kierować się strona atakująca infrastrukturę krytyczną. W szczególności przeanalizowano obowiązek wyboru i weryfikacji celu, ocenę skutków ataku, kontrolę nad atakiem oraz ostrzeżenia przed atakiem. Jednak MPH przewiduje obowiązki nie tylko dla strony atakującej, ale również dla strony broniącej, dlatego analizie poddano również prewencyjny środek ostrożności w postaci lokalizacji obiektów infrastruktury krytycznej.

W trzeciej części dokonano analizy obowiązków stron konfliktu w zakresie doboru odpowiednich środków walki wykorzystanych do ataku na infrastrukturę krytyczną. Punktem wyjścia była interpretacja zakazu powodowania nadmiernego i zbędnego cierpienia, następnie analiza obowiązku dokonywania przeglądu uzbrojenia przez strony konfliktu legalności użycia poszczególnych środków walki wykorzystywanych w ataku na infrastrukturę krytyczną, jak broń masowego rażenia, broń zapalająca oraz broń kasetowa.

4.2 Ochrona infrastruktury krytycznej przez pryzmat fundamentalnych zasad MPH

Prowadzenie działań zbrojnych wymaga od strony atakującej, nawet jeśli działania te są podjęte w sposób niezgodny z prawem międzynarodowym, poddania się rygorowi MPH. Jako trzon tego rygoru należy uznać cztery podstawowe zasady MPH, tj. zasadę rozróżniania, zasadę

proporcjonalności, zasadę konieczności wojskowej oraz zasadę humanitaryzmu⁴⁷⁹. Jako normy prawa zwyczajowego podstawowe zasady MPH są istotnym punktem odniesienia przy interpretacji obowiązków stron konfliktu, szczególnie w zakresie doboru metody i środków walki⁴⁸⁰.

Przez zasadę rozróżniania należy rozumieć odróżnienie ludności cywilnej od kombatanów, a dobra cywilne od celów wojskowych (zob. rozdział II tej rozprawy). Jednak współcześnie granica pomiędzy obiektem cywilnym a celem wojskowym może się zacierać. Przykładem tego jest infrastruktura krytyczna, która służy zarówno ludności cywilnej, jak i państwu, w tym jego siłom zbrojnym. Z tego powodu jest postrzegana jako obiekt podwójnego znaczenia (ang. *dual-use object*), chociaż to określenie wprost nie wynika z aktów normatywnych. Chodzi bowiem o rolę jaką odgrywa dla bezpieczeństwa ludności cywilnej i państwa. Właśnie ochrona obiektów podwójnego zastosowania, w szczególności infrastruktury krytycznej, stanowi obecnie jeden z głównym tematów dyskusji tak przedstawicieli doktryny, jak również praktyków pola walki. Podstawą dyskusji jest możliwość legalnego zaatakowania infrastruktury krytycznej gdy spełnia ona funkcje zarówno cywilne, jak i wojskowe. Zgodnie ze stanowiskiem reprezentowanym głównie przez amerykańskich czy izraelskich wojskowych, jeżeli obiekt podwójnego zastosowania spełnia przesłanki celu wojskowego (obiekty, które ze swojej natury, swego rozmieszczenia, swego przeznaczenia lub wykorzystania wnoszą istotny wkład do działalności wojskowej i których całkowite lub częściowe zniszczenie, zajęcie lub zneutralizowanie daje określoną korzyść w danej sytuacji) to *per se* nie stanowi obiektu cywilnego, tym samym jest legalnym celem ataku⁴⁸¹. Jednak zakwalifikowanie obiektu podwójnego zastosowania jako celu wojskowego wymaga dodatkowej weryfikacji w zakresie potencjalnych negatywnych skutków dla ludności cywilnej. Tym samym kolejnym etapem jest analiza ataku pod kątem zasady proporcjonalności.

Zgodnie z zasadą proporcjonalności przeprowadzony atak nie może cechować się nadmierną szkodą (w szczególności stratą wśród ludności cywilnej czy uszkodzeniem dóbr o charakterze cywilnym) w porównaniu z oczekiwaną konkretną i bezpośrednią korzyścią wojskową (zob. art. 51 ust. 5 lit. b PD I). Zasada proporcjonalności, wynikająca także z norm prawa zwyczajowego, znajduje swoje zastosowanie w konflikcie zbrojnym o charakterze

⁴⁷⁹ Por. MTS, *Case concerning military...*, par. 215-218 oraz MTS, *Legality of the threat...*, par. 78

⁴⁸⁰ M. Marcinko, *Podstawowe zasady międzynarodowego prawa humanitarnego konfliktów zbrojnych*, w: Z. Falkowski, M. Marcinko (red.), *Międzynarodowe prawo humanitarne konfliktów zbrojnych*, Wojskowe Centrum Edukacji Obywatelskiej, Warszawa 2014, s. 60.

⁴⁸¹ O. A. Hathaway, A. Khan, M. R. Revekin, *The Dangerous Rise of "Dual-Use" Objects in War*, „The Yale Law Journal”, 2025, vol. 134, s. 2734-2735.

międzynarodowym, jak i w konflikcie zbrojnym o charakterze niemiędzynarodowym. Dodatkowo zasadę proporcjonalności można wyprowadzić z art. 3 pkt 3 Protokołu w sprawie zakazów lub ograniczeń użycia min, min-pułapek i innych urządzeń z 1980 r. (Protokół II do Konwencji CCW)⁴⁸² i art. 3 pkt 8 Poprawionego Protokołu w sprawie zakazów lub ograniczeń użycia min, min-pułapek i innych urządzeń zgodnie z poprawkami z 1996 r. (Poprawiony Protokół II do Konwencji CCW)⁴⁸³. Obie regulacje wprowadzają zakaz niekontrolowanego użycia broni, co może skutkować utratą życia lub zranieniem ludności cywilnej, jak i uszkodzeniem obiektów cywilnych. Dodatkowo skutki niekontrolowanego użycia broni powinny być niewspółmierne w stosunku do przewidywanej korzyści wojskowych. Dopiero takie działanie będzie stanowiło naruszenie zasady proporcjonalności.

Zasada proporcjonalności należy do głównych zasad MPH i stanowi połączenie zasady rozróżniania z obowiązkiem ochrony ludności cywilnej⁴⁸⁴. Każdy atak, zgodnie z założeniami „racjonalnego dowodzenia” powinien być podejmowany z jej uwzględnieniem, a dowództwo uchylające się od jej stosowania naraża się na odpowiedzialność karną za bezprawny atak na ludność cywilną⁴⁸⁵. Kluczowe w tym przypadku jest prawidłowe rozpatrzenie przez dowództwo, czy atak może spowodować szkody wśród ludności cywilnej. Jeżeli odpowiedź jest twierdząca, to powinno się odstąpić od przeprowadzenia tego ataku. Dla ustalenia proporcjonalności należy rozpatrzyć czy osoba podejmująca decyzję o ataku, korzystając w rozsądny sposób z dostępnych informacji, mogła przewidzieć, że atak spowoduje nadmierne ofiary wśród ludności cywilnej⁴⁸⁶.

Chociaż normy MPH zakazują bezpośredniego atakowania ludności cywilnej i obiektów cywilnych, to pośrednim skutkiem ataku może być utrata życia lub poważne uszkodzenie zdrowia ludności cywilnej albo zniszczenie dóbr o charakterze cywilnym⁴⁸⁷.

⁴⁸² Konwencja o zakazie lub ograniczeniu użycia pewnych broni konwencjonalnych, które mogą być uważane za powodujące nadmierne cierpienia lub mające niekontrolowane skutki, wraz z załącznikami, Genewa, 10.10.1980, Dz. U. 1984 r., nr 23, poz. 104.

⁴⁸³ Pierwotnie postanowienia Protokołu II do Konwencji CCW z 1980 r. odnosiły się wyłącznie do konfliktów zbrojnych o charakterze międzynarodowym, dopiero poprawka z 1996 r. objęła swoimi postanowieniami również konflikt zbrojny o charakterze nie międzynarodowym. Zob. *Poprawiony Protokół II w sprawie zakazów lub ograniczeń użycia min, min-pułapek i innych urządzeń zgodnie z poprawkami z dnia 3 maja 1996 r. (Protokół II zgodnie z poprawkami z dnia 3 maja 1996 r.) załączony do Konwencji o zakazie lub ograniczeniu użycia pewnych broni konwencjonalnych, które mogą być uważane za powodujące nadmierne cierpienia lub mające niekontrolowane skutki, sporządzony w Genewie dnia 10 października 1980 r.*, Genewa, 3.05.1996, Dz. U. z 2005 r., nr 125, poz. 1048.

⁴⁸⁴ MTS, *Legality of the threat...*, par. 78.

⁴⁸⁵ MTKJ, *Final Report...*, par. 28 i 50.

⁴⁸⁶ MTKJ, *Prosecutor v. Stanislav Galić*, Judgment, 5.12.2003, IT-98-29, par. 58-60.

⁴⁸⁷ Ch.P. Trumbull IV, *Collateral damage and individual rights in armed conflict*, „Fordham Journal of International Law”, 2024, vol. 48, no. 2, s. 527

W takiej sytuacji domniemywa się zachowanie proporcji pomiędzy powstałą szkodą (utrata życia lub zdrowia) a osiągniętą korzyścią wojskową (eliminacja celu wojskowego)⁴⁸⁸. Jest to zjawisko tzw. szkód ubocznych (ang. *collateral damages*). Jedna z definicji określa szkody uboczne jako niezamierzone lub przypadkowe obrażenia lub szkody wobec osób lub przedmiotów, które w danych okolicznościach nie byłyby zgodnie z prawem celami wojskowymi⁴⁸⁹. W tym przypadku utrata życia lub zdrowia ludności cywilnej albo zniszczenie dóbr o charakterze cywilnym nie powoduje braku legalności działań sił zbrojnych⁴⁹⁰. Oznacza to, że atak został przeprowadzony zgodnie z wymaganiami MPH, a szkody powstałe podczas ataku, nie były jego głównym celem. Skutki ataków wymierzonych w obiekty infrastruktury krytycznej są przykładem potencjalnych szkód ubocznych ze względu na funkcję jaką infrastruktura krytyczna pełni dla bezpieczeństwa ludności cywilnej, ale także jej kluczowej roli we wsparciu sił zbrojnych (na przykład sektor energetyczny). Infrastruktura energetyczna jest częstym celem ataku w konflikcie zbrojny pomiędzy Ukrainą a Rosją. Atak wypełnia swój cel jakim jest korzyść militarna, w szczególności kiedy jego skutkiem jest obniżone morale strony przeciwnej, jednak jego skutki dotyczą również ludność cywilną⁴⁹¹. Szczególnie jest to odczuwalne w okresie jesienno-zimowym, kiedy przerwy w dostawie prądu uniemożliwiają prawidłowe działanie systemu grzewczego i dostaw wody⁴⁹². Szkody uboczne w atakach na obiekty infrastruktury krytycznej mogą doprowadzić również do długotrwałych i rozległych skutków, jak miało to miejsce w Sudanie⁴⁹³. Od 2023 roku w Sudanie trwa międzynarodowy konflikt zbrojny pomiędzy siłami rządowymi *Sudanese Armed Forces* (SAF) a siłami rozłamowymi, zjednoczonymi i sprzymierzonymi w grupie *Rapid Support Forces* (RSF). Intensywność konfliktu pomiędzy obiema grupami prowadzi do poważnych naruszeń MPH, zarówno ze strony SAF, jak i RSF. Działania dotknęły szczególnie obiekty infrastruktury krytycznej, co spowodowało konieczność udzielenia pomocy humanitarnej aż 30 milionom osób⁴⁹⁴. Naloty bombowe ze strony SAF doprowadziły do zniszczenia obiektów zaopatrzenia

⁴⁸⁸ MTKJ, *Prosecutor v. Stanislav Galić*, Judgement on Appeal..., par. 190.

⁴⁸⁹ USA, *DOD Dictionary of Military and Associated Terms*, Washington DC, The Joint Staff, November 2021, https://www.supremecourt.gov/opinions/URLs_Cited/OT2021/21A477/21A477-1.pdf (dostęp: 21.12.2025), s. 36.

⁴⁹⁰ B. Cronin, *Reckless endangerment warfare: Civilian casualties and the collateral damage exception in international humanitarian law*, „Journal of Peace Research”, 2013, vol. 50, nr 2, s. 176.

⁴⁹¹ F. Capone, *The Wave of Russian Attacks on Ukraine's Power Infrastructures: An Opportunity to Infuse Meaningfulness into the Notion of "Dual-use Objects"?*, „European Papers - A Journal on Law and Integration”, 2023, vol. 8, nr 2, s. 742.

⁴⁹² *Tamże*.

⁴⁹³ *IHL in Focus: Spot Report Weaponizing Water and Humanitarian Collapse in Sudan: An International Humanitarian Law Assessment*, The Geneva Academy of International Humanitarian Law and Human Rights, Geneva 2025, <https://geneva-academy.ch/wp-content/uploads/2025/09/IHL-Spot-Report-Weaponizing-Water-and-Humanitarian-Collapse-in-Sudan.pdf> (dostęp: 21.12.2025), s. 5-8.

⁴⁹⁴ *Tamże*, s. 5.

w wodę, co skutkowało rozwojem epidemii cholery (w samym regionie stołecznym w maju 2025 roku było potwierdzonych ponad 7 tysięcy przypadków zarażeń). Jak pokazują powyższe przykłady, skutki uboczne, szczególnie w stratach ludności cywilnej są nieodłącznym elementem ataków na infrastrukturę krytyczną. Chociaż MPH nakłada obowiązek każdorazowego weryfikowania zgodnie z zasadą rozróżnienia, to nawet atak na cel wojskowy może doprowadzić do cywilnych skutków ubocznych, co niekoniecznie będzie stanowiło naruszenie prawa międzynarodowego⁴⁹⁵. Dlatego obecnie postuluje się wprowadzenie nowych rozwiązań prawnych mających na celu uszczelnienie ochrony infrastruktury krytycznej w zgodzie z zasadą proporcjonalności⁴⁹⁶. Po pierwsze, atak na obiekt podwójnego zastosowania (infrastrukturę krytyczną), w perspektywie proporcjonalności, powinien uwzględniać nie tylko ofiary śmiertelne wśród ludności cywilnej, ale także szkody spowodowane utratą dostępu do takich obiektów. Po drugie, obiekty które bezpośrednio nie wpływają na zdolność do prowadzenia działań zbrojnych, a jedynie stanowią obiekty podtrzymujące działania zbrojne (ang. *war-sustaining object*)⁴⁹⁷ nie powinny być rozpatrywane jako cele wojskowe⁴⁹⁸. Powyższe rozważania pozwalają stwierdzić, że współczesne konflikty zbrojne coraz częściej będą skupiały się na zniszczeniach w infrastrukturze krytycznej. Tym samym niezbędne jest zapewnienie jej skutecznej ochrony, przy jednoczesnym osiągnięciu korzyści wojskowej.

Trzecią zasadą, którą strony powinny kierować się podczas konfliktu zbrojnego, jest zasada konieczności wojskowej. Jako jedna z podstawowych zasad prowadzenia działań zbrojnych została wprowadzona już podczas wojny secesyjnej w Stanach Zjednoczonych w XIX wieku⁴⁹⁹. Zgodnie z art. 14 Kodeksu Liebera konieczność wojskowa to podjęcie takich środków, które są niezbędne do zapewnienia zakończenia wojny i które są zgodne z prawem i zwyczajami wojennymi. Obecnie pojęcie konieczności wojskowej jest rozumiane jako uzasadnienie stosowania wszelkich niezbędnych środków pozwalających jak najszybciej i jak najskuteczniej pokonać stronę przeciwną, ale w granicach prawa⁵⁰⁰. Problemem z dopuszczeniem tych wszelkich niezbędnych środków jest ich kontrola zgodności z MPH,

⁴⁹⁵ MTKJ, *Prosecutor v. Dario Kordić and Mario Čerkez*, Judgment on Appeal, 17.12.2004, IT-95-14/2-A, par. 52.

⁴⁹⁶ O. A. Hathaway, A. Khan, M. R. Revekin, *The Dangerous...*, s. 2734-2735.

⁴⁹⁷ Jako obiekty podtrzymujące działania zbrojne należy rozumieć wszystkie obiekty zapewniające finansowanie działań zbrojnych zob. N. S. Reetz, *Same Same but Different Why War-Sustaining Objects Can Be Destroyed but Not Targeted*, „Journal of Conflict & Security Law”, 2022, vol. 27, nr 3, s. 439-440.

⁴⁹⁸ O. A. Hathaway, A. Khan, M. R. Revekin, *The Dangerous...*, s. 2733-2734.

⁴⁹⁹ M. N. Schmitt, *Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance*, „Virginia Journal of International Law”, 2010, vol. 50, nr 4, s. 801.

⁵⁰⁰ USA, *Department of Defense Law of War Manual*, June 2015 (Updated July 2023), <https://media.defense.gov/2023/Jul/31/2003271432/-1/-1/0/DOD-LAW-OF-WAR-MANUAL-JUNE-2015-UPDATED-JULY%202023.PDF> (dostęp: 21.12.2025), s. 52.

przede wszystkim w zachowaniu bezpieczeństwa ludności cywilnej. Jak pokazuje praktyka wojskowa badanie konieczności wojskowej przechodzi przez trójstopniowy proces⁵⁰¹. Po pierwsze, najszybsze i najskuteczniejsze zakończenie konfliktu zbrojnego jest podstawowym celem prowadzenia konfliktu z militarnego punktu widzenia. Po drugie, niektóre działania podejmowane przez siły zbrojne są z natury niezbędne do osiągnięcia korzyści wojskowej. Po trzecie, osoby oceniające konieczność wojskową powinny podejmować decyzje na podstawie informacji posiadanych podczas podejmowania decyzji, i nie należy ich oceniać na podstawie informacji ujawnionych w późniejszym czasie. Przykładem procesu decyzyjnego, uwzględniającego konieczność wojskową, jest przygotowanie amerykańskiej armii do połączonej operacji w Iraku pomiędzy lutym i marcem 1991 roku, podjętej na podstawie rezolucji RB ONZ nr 678 z 29 października 1990 roku⁵⁰². Operacja połączonych sił amerykańskich i pozostałych 26 sojuszników stanowiła odpowiedź na iracką inwazję na Kuwejt w sierpniu 1990 roku, która została przeprowadzona z naruszeniem z Karty Narodów Zjednoczonych. Opracowując strategię operacji wojskowej amerykańska armia wyznaczyła pięć głównych celów, które powinny zostać osiągnięte poprzez zniszczenia wskazanych obiektów za pomocą lotnictwa:

1. izolowanie i unieszkodliwienie irackiego reżimu (obiekty dowodzenia, obiekty energetyczne zasilające irackie siły zbrojne, obiekty telekomunikacyjne);
2. zdobycie i utrzymanie przewagi w powietrzu (systemy radarowe, lotniska);
3. zniszczenie zdolności bojowych w zakresie broni masowego rażenia (obiekty badawcze, produkcyjne i magazyny broni masowego rażenia);
4. wyeliminowanie ofensywnych zdolności irackiej armii (fabryki i magazyny wojskowe, obiekty rafinacji i dystrybucji ropy naftowej);
5. zniszczenie zdolności armii irackiej w zakresie zmechanizowanym (koleje i mosty)⁵⁰³.

Powyższe cele w znacznym stopniu skupiały się na zniszczeniu obiektów infrastruktury krytycznej, głównie obiektów energii elektrycznej, systemów telekomunikacji oraz dróg i mostów. Amerykańskie dowództwo uznało ich zniszczenie jako działanie przynoszące znaczną korzyść militarną, tym samym postępując w zgodzie z zasadą konieczności wojskowej. Każdy z tych obiektów w znacznym stopniu wspierał iracką działalność militarną w Kuwejcie.

⁵⁰¹ *Tamże*, s. 56.

⁵⁰² RB ONZ, *Resolution 678 (1990)*, 29.11.1990, S/RES/678(1990), s. 27-28.

⁵⁰³ USA, *Conduct of the Persian Gulf War*, Final Report to Congress, 1.04.1992, <https://apps.dtic.mil/sti/pdfs/ADA249270.pdf> (dostęp: 21.12.2025), s. 125-126.

Na konieczność wojskową może powołać się nie tylko strona atakująca, ale również strona broniąca. Zgodnie z art. 54 ust. 5 PD I ze względu na istotne interesy każdej strony konfliktu podczas obrony własnego terytorium przeciwko inwazji, strona konfliktu może na takim terytorium, jeżeli znajduje się pod jej kontrolą, odstąpić od zakazów przewidzianych w ustępie 2 (zakaz atakowania, niszczenia, zabierania lub czynienia nieużytecznymi dóbr niezbędnych dla przetrwania ludności cywilnej), jeżeli stanowcza konieczność wojskowa tego wymaga. Przedstawiona sytuacja jest przeciwieństwem tak zwanej taktyki spalonej ziemi, gdzie okupant wycofując się z zajmowanego terytorium dokonuje zniszczeń w infrastrukturze państwa okupowanego, między innymi mostów, dróg, portów lotniczych czy morskich⁵⁰⁴. Stosując taktykę spalonej ziemi, okupant nie może jednak zniszczyć obiektów niezbędnych dla przetrwania ludności cywilnej, obejmujących przede wszystkim magazyny żywnościowe czy urządzanie i zbiorniki z wodą pitną. Wyjątkiem od tej zasady, na podstawie art. 54 ust. 2 PD I, jest zniszczenie tych obiektów przez stronę broniącą. Natomiast jest to obwarowane dwoma warunkami⁵⁰⁵. Po pierwsze, terytorium, na którym znajdują się te obiekty musi być jej własnym terytorium, nad którym sprawuje rzeczywistą kontrolę, a to oznacza wyłączenie terytorium znajdującego się pod okupacją. Drugim warunkiem jest istnienie stanowczej konieczności wojskowej. Termin ten nie został jednak zdefiniowany, ale można przyjąć, że stanowcza konieczność wojskowa zachodzi wtedy, gdy nie ma żadnej innej możliwości aby osiągnąć korzyść wojskową, a zniszczenie wymienionych obiektów stanowi jedyne rozwiązanie⁵⁰⁶. Każda taka sytuacja powinna być rozpatrywana indywidualnie. Należy przy tym pamiętać, że osiągnięcie korzyści wojskowej nie może być usprawiedliwieniem do podejmowania ataku bez wcześniejszej jego weryfikacji przez pryzmat wszystkich fundamentalnych zasad MPH. Dotyczy to również ostatniej, czwartej zasady – humanitaryzmu.

Zasada humanitaryzmu jest uznawana nie tylko za jedną z podstawowych zasad MPH, ale również za jedną z podstawowych zasad prawa międzynarodowego w całości⁵⁰⁷. Pierwszych odwołań do humanitaryzmu należy doszukiwać się już w Deklaracji Petersburskiej z 1868 roku, która zakazywała używania broni sprzecznej z prawami ludzkości⁵⁰⁸. Jednak kluczowym momentem dla zasady humanitaryzmu było przyjęcie IV Konwencji

⁵⁰⁴ Y. Sandoz et al., *Commentary to APs...*, s. 659.

⁵⁰⁵ *Tamże*.

⁵⁰⁶ MTK, *Situation in the Democratic Republic of the Congo in the Case of the Prosecutor v. Germain Katanga*, Judgment pursuant to article 74 of the Statute, 7.03.2014, ICC-01/04-01/07, par. 894.

⁵⁰⁷ I. Brownlie, *Principles of Public International Law*, Clarendon Press, Oxford 1998, s. 28. por. MTS, *Corfu Channel (United Kingdom v. Albania)*, Judgment, 9.04.1949, ICJ Reports 1949, s. 22,

⁵⁰⁸ *Deklaracja wyrzeczenia się użycia, w czasie wojny, pocisków wybuchających o wadze poniżej 400 gramów*, Sankt Petersburg, 11.12.1868, w: P. K. Marszałek, *Międzynarodowe prawo...*, s. 605.

haskiej z 1899 roku. Zgodnie z jej preambułą w przypadkach nieuregulowanych przepisami konwencji, ludność i strony konfliktu pozostają pod opieką i władzą zasad prawa narodów oraz zasad humanitarności i wymagań społecznego sumienia. Powyższy fragment zwany Klauzulą Martensa wprowadził pewnego rodzaju „kompas moralny” do cechującego się brakiem obiektywizmu prawa naturalnego w postaci wymagań społecznego sumienia⁵⁰⁹. Klauzula Martensa została powtórzona w art. 1 ust. 2 PD I, co było podyktowane jej elastycznym charakterem. Pomimo kodyfikacji coraz szerszego zakresu MPH, żadne normy traktatowe nie zapewniają pełnej ochrony. Dodatkowo klauzula jako element dynamiczny, może objąć swoją ochroną skutki stosowania nowych technologii, nieuregulowanych jeszcze normami traktatowymi⁵¹⁰. Jednocześnie Klauzula Martensa stanowi potwierdzenie zastosowania zasad MPH we wszystkich konfliktach zbrojnych, i to niezależnie od tego czy dany przypadek byłby uregulowany w prawie traktatowym, czy też nie⁵¹¹. Chociaż wydaje się, że zasada humanitaryzmu stanowi całkowite zaprzeczenie zasady konieczności wojskowej, to należy ją interpretować nie tylko jako ograniczenie, ale możliwe jest również jej uzasadnienie⁵¹². Zasadę humanitaryzmu należy traktować jako podstawę do interpretacji pozostałych zasad (rozdzielenia, proporcjonalności oraz konieczności wojskowej), ponieważ stanowi etyczny i moralny wyznacznik norm MPH⁵¹³.

4.3 Środki ostrożności podczas ataku na infrastrukturę krytyczną

W celu wyeliminowania niepożądanych skutków ataków na cele wojskowe strony konfliktu zbrojnego powinny podjąć odpowiednie środki ostrożności. W art. 57 PD I sformułowano środki ostrożności, którymi powinna się kierować strona atakująca. Jako główną zasadę wskazano ogólną troskę o ludność cywilną oraz dobra o charakterze cywilnym, natomiast środki ostrożności można skategoryzować w następujący sposób: wybór i weryfikacja celu, wybór środków i metod walki, ocena skutków ataku, kontrola nad atakiem oraz ostrzeżenie przed atakiem. W przypadku strony broniącej, środki ostrożności jakimi powinna się kierować zostały sformułowane w art. 58 PD I i zbiorczo można je określić jako

⁵⁰⁹ R. Coupland, *Humanity: What is it and how does it influence international law?*, „International Review of the Red Cross”, 2001, vol. 83, no. 844, s. 975.

⁵¹⁰ Y. Sandoz et al., *Commentary to APs...*, s. 39.

⁵¹¹ *Tamże*.

⁵¹² E. Winter, *Pillars not Principles: The Status of Humanity and Military Necessity in the Law of Armed Conflict*, „Journal of Conflict and Security Law”, 2020, vol. 25, iss. 1, s. 30-31.

⁵¹³ R. Coupland, *Humanity...*, s. 988-989.

lokalizację celów wojskowych poza terenem gęsto zaludnionym ludnością cywilną i z dala od dóbr o charakterze cywilnym.

Pomimo wyraźnego rozróżnienia na obowiązki strony atakującej i obowiązki strony broniącej, oba te aspekty powinny być rozpatrywane wspólnie, odnosząc się przede wszystkim do zapewnienia bezpieczeństwa ludności cywilnej⁵¹⁴. Co więcej, wskazuje się, że zastosowanie środków ostrożności jest komplementarne z zasadą rozróżniania, a obowiązek zapewnienia bezpieczeństwa ludności cywilnej i obiektów infrastruktury cywilnej jest zasadą nadrzędna dla obu stron konfliktu⁵¹⁵.

4.3.1 Wybór i weryfikacja celu

Podczas planowania lub decydowania o podjęciu ataku strona atakująca powinna uczynić wszystko, co jest praktycznie możliwe, dla sprawdzenia, czy celami ataku nie są osoby cywilne ani dobra o charakterze cywilnym i czy nie korzystają ze szczególnej ochrony, a czy stanowią one cele wojskowe (art. 57 ust. 2 lit a pkt i PD I). Ponadto, jeżeli możliwy jest wybór między kilkoma celami wojskowymi dla osiągnięcia jednakowej korzyści wojskowej, wybrany powinien być cel, którego zaatakowanie stanowi najmniejsze niebezpieczeństwo dla osób cywilnych lub dóbr o charakterze cywilnym (art. 57 ust. 3 PD I).

Wybór celu przed atakiem wiąże się bezpośrednio z praktycznym zastosowaniem zasady rozróżnienia, strona atakująca przede wszystkim musi wybrać i potwierdzić wojskowy charakter swojego celu⁵¹⁶. Oznacza to, że dokonujący ataku musi mieć całkowitą pewność, a każda wątpliwość co do statusu celu powinna być interpretowana jako przeszkoda w ataku⁵¹⁷. Dalsza dyspozycja art. 57 PDI I ukazuje również ograniczony charakter w wyborze pomiędzy celami wojskowymi. Kierując się zasadą „mniejszego zła” dokonujący ataku powinien wybrać taki cel wojskowy, którego zniszczenie nie przyczyni się, albo przyczyni się w nieznacznym stopniu, do pogorszenia sytuacji ludności cywilnej i dóbr o charakterze cywilnym.

Wybór i weryfikacja celu jest istotnym elementem środków ostrożności podejmowanych przed atakiem na infrastrukturę krytyczną. Szczególnie jest to widoczne w przypadku infrastruktury krytycznej charakteryzującej się podwójnym zastosowaniem

⁵¹⁴ E. J. Breeze, *Duty to act on knowledge: precautions, intelligence and the law of armed conflict*, „Journal of Conflict & Security Law”, 2024, vol. 29, iss. 3, s. 314.

⁵¹⁵ M. Bothe, K. J. Partsch, W. A. Solf, *New Rules for Victims of Armed Conflicts. Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949. Second Edition*, Brill, Nijhoff 2013, s. 413.

⁵¹⁶ MTKJ, *Prosecutor v. Stanislav Galić*, Judgment..., par. 58.

⁵¹⁷ P. Grzebyk, *Cele osobowe...*, s. 208.

(wojskowym i cywilnym). W przypadku konieczności zniszczenia infrastruktury komunikacyjnej, wybierając pomiędzy dworcem kolejowym, a drogą publiczną, dowództwo powinno przeanalizować jakie skutki odniesie atak na dworzec kolejowy, zazwyczaj znajdujący się w centrum miasta i czy podobnych korzyści wojskowych nie przyniosłoby zniszczenie torów kolejowych lub drogi publicznej poza terenem miasta⁵¹⁸.

4.3.2 Ocena skutków ataku

Strona atakująca powinna powstrzymać się od podjęcia ataku, który mógłby spowodować niezamierzone straty w życiu ludzkim wśród ludności cywilnej, ranienia osób cywilnych, szkody w dobrach o charakterze cywilnym lub takie straty i szkody łącznie, których rozmiary byłyby nadmierne do oczekiwanej konkretnej i bezpośredniej korzyści wojskowej (art. 57 ust. 3 lit. a pkt iii PD I).

Ocena skutków ataku jest powiązana z zasadą proporcjonalności, zgodnie z którą osiągnięty cel wojskowy nie może pozostawiać nieproporcjonalnie duży względem negatywnych skutków wobec ludności cywilnej i dóbr o charakterze cywilnym. Po pozytywnym wyborze i weryfikacji celu wojskowego następnym krokiem jaki powinno podjąć dowództwo jest określenie ewentualnych szkód wśród ludności cywilnej. Jeżeli dowództwo spodziewa się lub może się spodziewać ofiar wśród ludności cywilnej, powinno odstąpić od przeprowadzenia ataku⁵¹⁹.

Ocena skutków ataku stanowi kluczowy element podczas planowania i wykonania ataku na infrastrukturę krytyczną. Po raz kolejny jako problem jawi się jej podwójny charakter, który w znaczny sposób może uniemożliwić prawidłową ocenę skutków ataku na obiekty infrastruktury krytycznej. Za przykład wątpliwości w ocenie skutków ataku może posłużyć atak na mosty w trakcie kampanii NATO przeciwko Federalnej Republice Jugosławii w 1999 roku, którego skutkiem była śmierć cywili⁵²⁰. NATO potwierdziło uzyskanie korzyści militarnej, w formie przerywania komunikacji wśród przeciwników. Innego zdania byli natomiast niezależni obserwatorzy, którzy wskazali, że wybrane mosty nie miały istotnego znaczenia dla

⁵¹⁸ Y. Sandoz et al., *Commentary to APs...*, s. 687.

⁵¹⁹ MTKJ, *Prosecutor v. Stanislav Galić*, Judgment..., par. 58.

⁵²⁰ Human Rights Watch, *Civilian Deaths in the NATO Air Campaign*, New York, 7.02.2000, <https://www.hrw.org/reports/pdfs/g/general/natbm002.pdf> (dostęp: 21.12.2025), s. 24.

transportu, a prawdziwym celem ataku na nie był efekt psychologiczny (obniżone morale przeciwnika)⁵²¹.

4.3.3 Kontrola nad atakiem

Kolejnym środkiem ostrożności, który powinien zostać podjęty przez stronę atakującą jest odstąpienie lub przerwanie ataku, jeżeli okazałoby się, że jego cel nie ma charakteru wojskowego lub korzysta ze szczególnej ochrony albo że można oczekiwać, iż wywoła on niezamierzone straty w życiu ludzkim wśród ludności cywilnej, ranienia osób cywilnych lub szkody w dobrach o charakterze cywilnym albo takie straty i szkody łącznie, których rozmiary byłyby nadmierne w stosunku do oczekiwanej konkretnej i bezpośredniej korzyści wojskowej (art. 57 ust. 2 lit b PD I).

W odróżnieniu od dwóch pierwszych środków ostrożności kontrola nad atakiem jest wymagana przez cały okres trwania operacji. Strona atakująca nie tylko musi podjąć określone środki jeszcze przed rozpoczęciem ataku, ale również w trakcie jego trwania powinna być zdolna do ewentualnego zaprzestania atakowania, jeżeli okazałoby się, że cel utracił swój charakter wojskowy lub można oczekiwać strat po stronie ludności cywilnej⁵²². Szczególna uwaga w sprawowaniu kontroli nad atakiem powinna być uwzględniona przy wykorzystaniu armii lądowej⁵²³. Prowadzenie działań zbrojnych na lądzie może doprowadzić do ograniczonych zdolności rozpoznania wynikających z ukształtowania terenu czy ograniczeń pola widzenia, dlatego dowództwo powinno zachować szczególną kontrolę nad atakiem. Bardziej skuteczne w zachowaniu ciągłej kontroli nad atakiem wydaje się wykorzystanie lotnictwa, którego zasięg widzenia i ogólne rozpoznania są dużo większe niż armii lądowej. Nie oznacza to jednak, że i ten rodzaj wojska nie może naruszyć zasady kontroli nad atakiem. W trakcie kampanii NATO w Kosowie w 1999 roku doszło do zbombardowania przez siły sojusznicze między innymi mostu kolejowego w Grdelicy oraz mostu samochodowego w Lužane pomimo tego, że na tych mostach znajdowała się ludność cywilna⁵²⁴. Pilot odpowiedzialny za zbombardowanie mostu kolejowego przyznał, że przed dokonaniem

⁵²¹ Tamże, s. 24. Mieszkańcy Nowego Sadu wspominali, że atak między innymi na most Petrovaradina zniszczył nie tylko sam obiekt, ale także ich „wspomnienia z dzieciństwa”, które spędzali w okolicach tego obiektu, zob. P. Ramadanovic, *When Bombs Fall: Becoming American During the NATO Bombing of Yugoslavia*, „Discourse”, 2003, vol. 25, no. 1/2, s. 276.

⁵²² P. Grzebyk, *Cele osobowe...*, s. 209.

⁵²³ Y. Sandoz et al., *Commentary to APs...*, s. 687.

⁵²⁴ Amnesty International, *NATO/Federal Republic of Yugoslavia: „Collateral Damage” or Unlawful Killings? Violations of the Laws of War by NATO during Operation Allied Force*, London, 5.06.2000, <https://www.amnesty.org/en/documents/eur70/018/2000/en/> (21.12.2025), s. 32-34.

ataku nie dostrzegł pociągu pasażerskiego, jednak po ostrzale zorientował się co znajdowało się na moście i mimo tego dokonał kolejnego ostrzału doprowadzając do całkowitego zniszczenia mostu. Skutkiem ataku była śmierć co najmniej 10 cywili, a 15 z nich zostało poważnie rannych⁵²⁵. W Raporcie końcowym komitetu powołanego przez Prokuratora MTKJ dotyczącym bombardowań przeprowadzonych przez NATO wobec Federalnej Republiki Jugosławii⁵²⁶ potwierdzono wojskowy charakter mostu, jednocześnie nie wskazując argumentów, które by to potwierdziły⁵²⁷. Pomimo, że wśród członków komitetu istniała rozbieżność w poglądach co do lekkomyślności pilota, nie zdecydowano się zbadać tego incydentu jako potencjalnego naruszenia MPH⁵²⁸.

4.3.4 Ostrzeżenie przed atakiem

Ostatnim środkiem ostrożności koniecznym do podjęcia przez stronę atakującą jest ostrzeżenie przed atakiem. W porównaniu do poprzednich środków ostrzeżenie przed atakiem zostało uregulowane już Regulaminie haskim z 1907 roku. Zgodnie z art. 26 Regulaminu dowódca wojsk napadających zanim przystąpi do bombardowania, za wyjątkiem szturm, powinien uczynić wszystko, co jest w jego mocy, aby uprzedzić o tym władze. Ostrzeżenie przed atakiem zostało powtórzone w art. 57 ust. 2 lit c PD I, jednak w Protokole zaakcentowano szczególną ochronę ludności cywilnej – w wypadku gdy ataki mogą zagrozić ludności cywilnej, należy wydać w odpowiednim czasie skuteczne ostrzeżenie, chyba że okoliczności na to nie pozwalają.

Przepisy nie wskazują konkretnie jaką formę powinny przybrać ostrzeżenia, jednak przyjmuje się, że mogą to być między innymi ulotki, komunikaty radiowe lub telewizyjne, wiadomości sms⁵²⁹. Z perspektywy osiągnięcia celu militarnego, z uwzględnieniem elementu „zaskoczenia” możliwym jest dokonanie tylko ogólnego ostrzeżenia przed atakiem, kiedy strona atakująca poda informacje o miejscu ataku, potencjalnym celu, z ogólnym wskazaniem daty⁵³⁰. W trakcie operacji militarnych prowadzonych przez Izrael w Strefie Gazy, w okresie od grudnia 2008 roku do stycznia 2009 roku, izraelskie siły zbrojne wykorzystywały do

⁵²⁵ L. Hamourtziadou, J. Jackson, *Winning wars: the triumphs and myths of technology*, „Journal of Global Faultlines”, 2019, vol. 6, iss. 2, s. 130.

⁵²⁶ 14 maja 1999 roku Prokurator MTKJ powołał Komitet, którego celem było zbadanie czy działania NATO wymierzone w Federalną Republikę Jugosławii nie naruszyły MPH. Zob. MTKJ, *Final Report...*, par. 2-4.

⁵²⁷ P. Benvenuti, *The ICTY Prosecutor and the Review of the NATO Bombing Campaign against the Federal Republic of Yugoslavia*, „European Journal of International Law”, 2001, vol. 12, no. 3, s. 520-521.

⁵²⁸ MTKJ, *Final Report...*, par. 62.

⁵²⁹ P. Grzebyk, *Cele osobowe...*, s. 210.

⁵³⁰ Y. Sandoz et al., *Commentary to APs...*, s. 687.

ostrzegania między innymi rozgłoszenie radiowe, połączenia telefoniczne, ale także ulotki z informacjami o ataku w języku arabskim⁵³¹. Zastosowane ostrzeżenia pozwoliły ograniczyć ofiary wśród ludności cywilnej. Większość z nich opuściła obiekty przed atakiem, co zostało potwierdzone przez izraelskie siły zbrojne, stale monitorujące sytuację za pomocą podglądu z powietrza⁵³².

4.3.5 Lokalizacja celów wojskowych

Przedstawione dotychczas środki ostrożności dotyczyły działań podejmowanych przez stronę atakującą (środki czynne), jednak MPH przewiduje również środki prewencyjne, które powinny być zastosowane przez potencjalną stronę broniącą (środki bierne). Strony konfliktu powinny podjąć wysiłki aby oddalić z sąsiedztwa celów wojskowych pozostające pod ich władzą ludność cywilną, osoby cywilne i dobra o charakterze cywilnym (art. 58 lit. a PD I). Ponadto, strony powinny unikać umieszczenia celów wojskowych wewnątrz lub w sąsiedztwie stref gęsto zaludnionych (art. 58 lit. b PD I).

Oddalenie celów wojskowych od stref zamieszkałych przez ludność cywilną pozwala wyeliminować potencjalne skutki uboczne w życiu lub zdrowiu osób cywilnych. Szczególnie ważne jest zapewnienie ochrony placówkom medycznym, które powinny znajdować się z dala od celów wojskowych, żeby nie narażać pacjentów⁵³³.

4.4 Środki walki wykorzystywane do ataków na infrastrukturę krytyczną

Podstawowym narzędziem wykorzystywanym przez strony konfliktu zbrojnego jest broń. Jednak na próżno szukać jej definicji legalnej. WSJP definiuje broń jako „rzecz służącą do walki lub do zabijania”⁵³⁴. SJP PWN natomiast wskazuje aż trzy definicje broni: narzędzie walki, środek lub sposób walki z kimś lub z czymś, formacja wojskowa⁵³⁵. Bardziej rozbudowane, wyróżniające konkretne rodzaje broni definicje można znaleźć w języku angielskim. Zgodnie z definicją Cambridge Dictionary termin *weapon* oznacza „*any object used in fighting or war, such as a gun, bomb, knife, etc.*” oraz „*an object used in fighting or war, such as a gun or a bomb, or something used against someone*”⁵³⁶. W Oxford Dictionary

⁵³¹ Izrael, *Briefing to the Diplomatic Corps by the Vice Prime Minister and Minister of Foreign Affairs*, 3.03.2008, <https://www.gov.il/en/pages/briefing-by-fm-livni-to-the-diplomatic-corps-3-mar-2008> (dostęp: 14.05.2026).

⁵³² Izrael, *The Operation in Gaza...*, s. 99

⁵³³ P. Grzebyk, *Cele osobowe...*, s. 206.

⁵³⁴ *Broń palna*, <https://wsjp.pl/haslo/podglad/18340/bron/2577109/palna> (dostęp: 21.12.2025).

⁵³⁵ *Broń - znaczenie, definicja*, <https://sjp.pwn.pl/slowniki/bro%C5%84.html> (dostęp: 21.12.2025).

⁵³⁶ *Weapon*, <https://dictionary.cambridge.org/english/weapon> (dostęp: 21.12.2025).

pojęcie *weapon* jest rozumiane jako „*an object such as a knife, gun, bomb, etc. that is used for fighting or attacking somebody*”⁵³⁷.

Zamiast pojęcia „broni” w MPH zastosowano pojęcie „środków i metod walki”, gdzie jako środki rozumie się broń, natomiast metody odnoszą się do taktyk i strategii. Chociaż żaden akt prawny nie definiuje pojęcia środków i metod walki, to możliwym jest wyodrębnienie trzech grup środków, które MPH zakazuje⁵³⁸. Po pierwsze, będą to środki, których produkcja i użycie są całkowicie zakazane, takie jak broń biologiczna⁵³⁹ i chemiczna⁵⁴⁰. Do drugiej grupy zakazanych środków walki należy zaliczyć te środki, które zostały zakazane ze względu na pewne swoje cechy konstrukcyjne, np. miny, gdzie istotny jest sposób ich detonacji (aktywacja miny następuje poprzez bezpośredni kontakt z ofiarą)⁵⁴¹. Ostatnią, trzecią grupą zakazanych środków są te, powodujące określony, niepożądany skutek, jak oślepiająca broń laserowa, której użycie może doprowadzić do nieodwracalnej ślepoty⁵⁴².

4.4.1 Zakaz powodowania nadmiernego i zbędnego cierpienia

Przyjęcie PD I wprowadziło nowy wymiar regulacji użycia środków walki. Przede wszystkim wprowadzono zasadę ograniczonego doboru środków i metod walki (art. 35 ust. 1 PD I). Oznacza to, że wybrany środek lub metoda walki nie mogą pozostawać w sprzeczności z wymaganiami MPH. W szczególności oznacza to, że wybrana broń, pocisk lub materiał nie mogą powodować zbędnego cierpienia (art. 35 ust. 2 PD I). Źródła zakazu należy doszukiwać się już w XIX wieku. W Deklaracji petersburskiej z 1868 roku określono, że jedynym słusznym celem, do którego państwa powinny dążyć podczas wojny, jest osłabienie sił militarnych nieprzyjaciela. Tym samym użycie broni, która niepotrzebnie zwiększa cierpienie osób obezwładnionych lub doprowadza do ich śmierci byłoby sprzeczne z podstawowym celem wojny jakim jest osłabienie sił militarnych nieprzyjaciela. Pomimo utrwalonego zwyczaju przestrzegania zakazu, problemem jest zdefiniowanie nadmiernego

⁵³⁷ *Weapon*, <https://www.oxfordlearnersdictionaries.com/definition/english/weapon?q=weapon> (dostęp: 21.12.2025).

⁵³⁸ K. Kowalczevska, *Sztuczna Inteligencja na wojnie. Perspektywa Międzynarodowego Prawa Humanitarnego Konfliktów Zbrojnych*, Wydawnictwo Naukowe Scholar Spółka z o.o., Warszawa 2021, s. 68-69.

⁵³⁹ *Konwencja o zakazie prowadzenia badań, produkcji i gromadzenia zapasów broni bakteriologicznej (biologicznej) i toksycznej oraz o ich zniszczeniu*, Moskwa, Londyn i Waszyngton, 10.04.1972, Dz. U. z 1976 r., nr 1, poz. 1.

⁵⁴⁰ *Konwencja o zakazie prowadzenia badań, produkcji, składowania i użycia broni chemicznej oraz o zniszczeniu jej zapasów*, Paryż, 13.01.1993, Dz. U. z 1999 r., nr 63, poz. 703.

⁵⁴¹ Protokół II zgodnie z poprawkami z 3 maja 1996 roku.

⁵⁴² *Protokół w sprawie laserowych broni oślepiających (Protokół IV) do Konwencji o zakazie lub ograniczeniu pewnych broni konwencjonalnych, które mogą być uznawane za powodujące nadmierne cierpienia lub z natury nierozróżniające*, Wiedeń, 12.10.1995, Dz. U. z 2007 r., nr 215, poz. 1583.

obrażenia i niepotrzebnego cierpienia. W opinii doradczej w sprawie legalności groźby lub użycia broni jądrowej z 1996 roku MTS określił, że niepotrzebnym cierpieniem są szkody większe niż te, których nie da się uniknąć przy osiągnięciu celu wojskowego⁵⁴³. Natomiast w dokumencie przedłożonym po Konferencji Ekspertów Rządowych z 1971 roku, MKCK zdefiniował niepotrzebne cierpienie jako oszczędzanie, nawet kombatantom, bezcelowych obrażeń lub cierpień wykraczających poza to, co jest konieczne do wyeliminowania przeciwnika z walki⁵⁴⁴. Brak definicji legalnej nadmiernego i zbędnego cierpienia i pozostawienie interpretacji tych pojęć *case by case*, może powodować jedynie pozorną ochronę wynikającą z tego zakazu, bez skutecznych mechanizmów kontroli⁵⁴⁵. Rozwiązaniem mogącym wspierać skuteczność zakazu powodowania nadmiernego i zbędnego cierpienia jest trzyetapowy proces przedstawiony przez J. Picteta, którego celem jest zminimalizowanie szans na wystąpienie nadmiernego cierpienia podczas działań zbrojnych:

1. przy wyborze i użyciu środka walki należy uwzględniać względy humanitaryzmu i konieczności wojskowej;
2. jeżeli możliwe jest wyeliminowanie przeciwnika przez schwytanie, nie należy go ranić, a jeżeli można osiągnąć ten sam efekt przez ranienie go, nie należy go zabijać;
3. jeżeli do osiągnięcia tej samej korzyści wojskowej dysponuje się dwoma środkami, z których jeden powoduje mniejsze szkody i cierpienia, to należy wybrać i użyć ten drugi środek⁵⁴⁶.

Zobowiązania wynikające z art. 35 PD I wymagają od państwa podjęcia odpowiednich kroków, które we właściwy sposób pomogą je wykonać. Tymi krokami jest procedura tzw. przeglądu uzbrojenia określona w art. 36 PD I. Oznacza to, że państwo przed włączenia do swojego arsenału określonego typu uzbrojenia musi zweryfikować czy jego użycie nie jest zakazane *per se* lub czy użycie go w inny sposób nie będzie stanowiło naruszenia MPH⁵⁴⁷.

⁵⁴³ MTS, *Legality of the threat...*, par. 78.

⁵⁴⁴ MKCK, *Rules Relative to Behaviour of Combatants, Submitted to the First Session of the Conference of Government Experts*, 24.05-12.06.1971, Geneva, https://library.icrc.org/library/docs/CD/CEG_1971_DOCUMENTS_ENG_4.pdf (dostęp: 21.12.2025), s. 6.

⁵⁴⁵ K. Kowalczevska, *Sztuczna Inteligencja...*, s. 90.

⁵⁴⁶ J. Pictet, *Le droit humanitaire et la protection des victimes de la guerre*, Institut Henry-Dunant, Geneve 1973, s. 91.

⁵⁴⁷ R. Łasa, *Military review in the context of cyber-warfare. Article 36 of 1977 Additional Protocol I in practice*, „Acta Iuridica Resoviensia”, 2023, t. 43, nr 125, s. 52.

4.4.2 Przegląd uzbrojenia

Chociaż przegląd uzbrojenia jest mechanizmem stworzonym dla ograniczenia negatywnych skutków podczas konfliktu zbrojnego, to wykracza on poza ramy MPH, odnosząc się również do prawa kontroli zbrojeń. Celem przeglądu jest wyeliminowanie środków i metod walki zakazanych przez MPH, co pośrednio przyczynia się do rozbrojenia⁵⁴⁸. Dla ustalenia szczegółowego wykazu środków walki objętych przeglądem uzbrojenia należy odwołać się do Instrukcji MKCK⁵⁴⁹. Publikacja stanowi zbiór dobrych praktyk w zakresie przeglądu uzbrojenia, jednocześnie wskazując katalog uzbrojenia, który podlega temu przeglądowi:

- wszystkie rodzaje broni oraz sposoby ich użycia,
- broń nabytą przez siły zbrojne państwa,
- broń nabytą przez państwo, która nie jest nowa (w technicznym tego słowa znaczeniu),
- broń, która wcześniej została poddana przeglądowi, ale została znacznie zmodyfikowana,
- broń, która poprzez przystąpienie państwa do konkretnego traktatu międzynarodowego może zostać uznana za nielegalną⁵⁵⁰.

Kwestią budzącą wątpliwości jest uznanie przeglądu wojskowego jako normy prawa zwyczajowego. Chociaż praktyka państw, w szczególności Stanów Zjednoczonych oraz Izraela, a więc państw, które nie są stroną PD I, wskazuje na powszechność tego przeglądu, to w doktrynie przeważa stanowisko zgodnie, z którym przegląd uzbrojenia nie przekształcił się w normę prawa zwyczajowego⁵⁵¹. Jednocześnie ta sama praktyka może świadczyć o potencjalnym powstaniu normy zwyczajowej w przyszłości. Jednak brak jednolitej regulacji co do sposobu przeprowadzenia przeglądu może opóźnić powstanie tej normy⁵⁵².

Odmienne zdania jest MKCK, który uważa przegląd uzbrojenia za koncepcję sięgającą jeszcze XIX wieku, co jednoznacznie wskazywałoby na zwyczajowy charakter normy art. 36 PD I⁵⁵³. Jako uzasadnienie swojej tezy podaje liczne akty prawne potwierdzające

⁵⁴⁸ A. Dienelt, *The Shadowy Existence of the Weapons Review and Its Impact on Disarmament*, „Sicherheit und Frieden (S+F)/Security and Peace”, 2018, vol. 36, no. 3, s. 131.

⁵⁴⁹ MKCK, *Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977*, „International Review of the Red Cross”, 2006, vol. 88, no 864.

⁵⁵⁰ *Tamże*, s. 937-938.

⁵⁵¹ N. Jevglevskaja, *Weapons Review Obligation under Customary International Law*, „International Law Studies”, 2018, vol. 94, s. 213.

⁵⁵² *Tamże*, s. 209.

⁵⁵³ MKCK, *Guide to the Legal...*, s. 932.

ewolucję przeglądu uzbrojenia⁵⁵⁴. Jednak pogląd MKCK należy uznać za błędny, ponieważ wskazane konwencje nie dotyczą przeglądu uzbrojenia, a odnoszą się do redukcji użycia konkretnych środków walki.

Postanowienia PD I w żaden sposób nie określają konkretnej procedury przeglądu uzbrojenia. Jedyne wytyczne w tym zakresie odnaleźć można w Instrukcji MKCK. Co do zasady, ciężar realizacji tego obowiązku spoczywa na organie administracji rządowej właściwym dla obronności państwa⁵⁵⁵. W strukturach tego organu należy utworzyć wyspecjalizowany departament obsługi prawnej, w ramach którego zadania będą wykonywać doradcy prawni (zob. art. 82 PD I). W trakcie prac nad Tallinn Manual 2.0 sformułowano regułę, zgodnie z którą państwo jest zobowiązane do zapewnienia zgodności środków i metod walki z postanowieniami MPH, co w praktyce oznaczałoby możliwość stworzenia alternatywnego procesu weryfikacji uzbrojenia, który jednocześnie spełniałby warunki przewidziane w art. 36 PD I⁵⁵⁶.

Kluczowym zagadnieniem pozostaje ustalenie terminu, w jakim należy dokonać przeglądu uzbrojenia. Artykuł 36 nie określa ram czasowych, dlatego domniemywa się, że procedura powinna rozpocząć się na możliwie jak najwcześniejszym etapie. W przypadku państw będących producentami uzbrojenia wskazuje się już etap projektowania⁵⁵⁷. Z kolei w przypadku państw importujących broń, optymalnym momentem na realizację tego obowiązku jest etap weryfikacji ofert⁵⁵⁸.

Wątpliwości budzi możliwość utajnienia przez państwo ustaleń dotyczących legalności danego uzbrojenia. Postanowienia MPH nie wymagają od państwa upublicznienia wyników przeglądu uzbrojenia, nawet jeśli przeprowadzona procedura potwierdzi, że broń jest nielegalna *per se* bądź jej użycie w konkretnym przypadku mogłoby się okazać nielegalne⁵⁵⁹. Pomimo braku jednoznacznych postanowień nakazujących ujawnianie wyników przeglądu, dominuje praktyka publikowania raportów z badań, co wpływa na zwiększenie transparentności MPH⁵⁶⁰.

Obecna forma przeglądu uzbrojenia zawiera luki wpływające na prawidłowe działanie mechanizmu kontrolnego. Kluczową kwestią pozostaje wskazania instytucji odpowiedzialnych

⁵⁵⁴ *Tamże*, s. 941-942.

⁵⁵⁵ MKCK, *Guide to the Legal...*, s. 949-950.

⁵⁵⁶ N. Jevglevskaja, *Weapons Review...*, s. 215.

⁵⁵⁷ MKCK, *Guide to the Legal...*, s. 951.

⁵⁵⁸ *Tamże*, s. 952.

⁵⁵⁹ Y. Sandoz et al., *Commentary to APs...*, par. 1481.

⁵⁶⁰ L. Wexler, *International Humanitarian Law Transparency*, „Journal of Transnational Law & Policy”, 2014, vol. 23, iss. 1, s. 116.

za przeprowadzenie tego przeglądu⁵⁶¹. Czy powinni to być prawnicy zatrudnieni w administracji cywilnej (ministerstwo właściwe ds. wojskowych) czy administracji wojskowej (sztab generalny)? Czy powinna zostać powołana specjalna organizacja międzynarodowa, której zadaniem będzie kontrola legalności uzbrojenia państw członkowskich, między innymi poprzez analizę corocznych sprawozdań? Wątpliwości wzbudza również brak wymogu informowania o wyniku przeprowadzonego przeglądu, szczególnie gdy uzbrojenie okaże się nielegalne.

4.4.3 Broń masowego rażenia

Problematyka regulacji broni masowego rażenia łączy się z jej śmiertelnościami charakterem i negatywnym oddziaływaniem na środowisko naturalne. W celu jej całkowitego wyeliminowania zdecydowano się na wprowadzenie szeregu regulacji prawnych. Początkowo przybierały one postać umów międzynarodowych, wprowadzających ogólne zakazy użycia poszczególnych rodzajów broni masowego rażenia, jednak w późniejszym czasie przyjęto konwencje, które – oprócz zakazu ich użycia – wprowadziły zakaz prowadzenia badań nad taką bronią, jej produkowania, testowania, przechowywania, a ponadto stworzyły odpowiednie mechanizmy, mające zapewnić szczegółową kontrolę nad wykonywaniem postanowień tych konwencji.

4.4.3.1 Broń biologiczna

Broń biologiczna jest jednym z najstarszych rodzajów broni masowego rażenia, jednocześnie wzbudzając największy postrach ze wszystkich jej rodzajów⁵⁶². Broń biologiczna jest nazywana „bronią biednych”, ponieważ cechuje się łatwością uzyskania czynników biologicznych, nie zawsze wymagając do tego warunków laboratoryjnych, tym samym koszty jej wyprodukowania są niskie⁵⁶³. Dzięki temu była wykorzystywana przez wszystkie strony konfliktów, tak armie państwowe, jak i niepaństwowe grupy zbrojne.

Próby zdefiniowania broni biologicznej podejmowano zarówno w gronie ekspertów wojskowych, jak i w środowisku naukowym. W Słowniku Terminów i Definicji NATO

⁵⁶¹ R. Łasa, *Military review in the context...*, s. 59.

⁵⁶² D. A. Henderson, *Bioterroryzm. Pierwsza linia naszego reagowania w ocenie gotowości amerykańskiej publicznej służby zdrowia i medycyny*, w: Y. Alexander, M. Koenig (red.), *Superterroryzm biologiczny, chemiczny i nuklearny*, Wydawnictwo Bellona, Warszawa 2001, s. 116.

⁵⁶³ B. Michailiuk, *Broń biologiczna i bioterroryzm*, „Zeszyty Naukowe AON”, 2016, nr 1(102), s. 17.

z 2013 roku⁵⁶⁴ broń biologiczną zdefiniowano jako środki materiałowo-techniczne, które przenoszą, rozprzestrzeniają lub rozsiewają środki biologiczne, w tym również stawonogi⁵⁶⁵. B. Michailiuk definiuje broń biologiczną jako „rodzaj broni masowego rażenia, w której ładunek bojowy stanowią różnego rodzaju drobnoustroje chorobotwórcze (bakterie, wirusy, riketsje, pierwotniaki) oraz ich toksyny odpowiedzialne za epidemie chorób wśród ludzi i ich otoczenia”⁵⁶⁶, natomiast J. Pięta określił broń biologiczną jako „żywe organizmy (bakterie, wirusy, pierwotniaki, grzyby) oraz wytwarzane przez nie substancje, a także niektóre organizmy wyższe (zakażone gryzonie, owady) wraz ze środkami ich przenoszenia i rozprzestrzeniania, przeznaczone do wywoływania masowych chorób zakaźnych (epidemii ludzi, zwierząt i roślinności)”⁵⁶⁷. Elementem niezbędnym broni biologicznej są mikroorganizmy, które można podzielić na trzy główne kategorie: wirusy (np. ospa prawdziwa, gorączka krwotoczna tzw. Ebola), bakterie (np. dżuma, wąglik) oraz toksyny (np. rycyna, jad kielbasiany)⁵⁶⁸.

Pierwsza regulacja międzynarodowa dotycząca zakazu użycia broni biologicznej została przyjęta w 1925 roku w formie Protokołu dotyczącego zakazu używania na wojnie gazów duszących, trujących lub podobnych oraz środków bakteriologicznych (Protokół genewski z 1925 roku)⁵⁶⁹. Celem protokołu było wzmocnienie już istniejącego zakazu stosowania gazów duszących i trujących, ale również wprowadzenie zakazu stosowania broni masowego rażenia w konfliktach zbrojnych o kolejny rodzaj broni – bakteriologicznej.

Kluczowym aktem prawnym regulującym zakaz użycia broni biologicznej jest Konwencja o zakazie broni biologicznej. Jej przyjęcie było poprzedzone wieloletnimi negocjacjami, a istotną rolę odegrało opracowanie wspólnego stanowiska Stanów Zjednoczonych i Związku Radzieckiego we wrześniu 1961 roku, nazywanego Deklaracją McCloy-Zorin (John McCloy był doradcą amerykańskiego prezydenta ds. rozbrojenia a Valerian Zorian był radzieckim ambasadorem przy ONZ)⁵⁷⁰. Natomiast bezpośrednio

⁵⁶⁴ Najnowsza wersja Słownika terminów i definicji NATO pochodzi z 2020 r., jednak ostatnia wersja Słownika zawierająca definicję broni biologicznej pochodzi z 2013 r.

⁵⁶⁵ NATO, *Słownik terminów i definicji NATO*, AAP-6(2013), s. 75.

⁵⁶⁶ B. Michailiuk, *Broń biologiczna...*, s. 19.

⁵⁶⁷ J. Pięta, *Broń masowego rażenia*, WSBIO, Warszawa 2006, s. 7.

⁵⁶⁸ M. Żuber, *Broń masowego rażenia w działalności terrorystycznej*, Wydawnictwo Difin S.A., Warszawa 2015, s. 50-51.

⁵⁶⁹ *Protokół dotyczący zakazu używania na wojnie gazów duszących, trujących lub podobnych oraz środków bakteriologicznych*, Genewa, 17.06.1925, Dz. U. z 1929 r., nr 28, poz. 278.

⁵⁷⁰ We wspólnym oświadczeniu Stany Zjednoczone oraz Związek Radziecki zaapelowały do całkowitej likwidacji zapasów broni biologicznej, chemicznej oraz jądrowej, a także do zaprzestania jej produkcji. Zob. A. Joshi, *BTWC: The History of Early Negotiations*, w: A. Lele (ed.), *50 Years of the Biological Weapons Convention. Tracking the Journey*, Pentagon Press LLP, New Delhi 2025, s. 96.

negocjacje nad projektem konwencji toczyły się w latach 1969-1971 na forum Konferencji Komitetu ds. Rozbrojenia ONZ.

Celem przyjęcia konwencji była chęć efektywnego postępu na drodze do powszechnego i całkowitego rozbrojenia, obejmującego zakaz i likwidację wszystkich rodzajów broni masowej zagłady. Osiągnięcie tego celu wiązało się z wprowadzeniem szeregu zobowiązań dla stron konwencji. Przede wszystkim strony konwencji zobowiązały się do powstrzymania się od prowadzenia badań, produkcji, gromadzenia, nabywania, oraz przechowywania mikrobiologicznych lub innych biologicznych środków czy toksyn, poza celami profilaktycznymi, ochronnymi lub w innych celami pokojowymi (art. 1 Konwencji o zakazie broni biologicznej). Konwencja zawiera również zobowiązania dla stron, które były już posiadaczami broni biologicznej i zobowiązała je do zniszczenia lub przekształcenia na cele pokojowe (w terminie do 9 miesięcy od wejścia w życie Konwencji) wszystkich środków, toksyn, broni, urządzeń oraz środków ich przenoszenia (art. 2 Konwencji o zakazie broni biologicznej). Na podstawie konwencji wprowadzono system współpracy międzynarodowej, polegającej po pierwsze na konsultacjach⁵⁷¹, a po drugie na skargach⁵⁷². Wadą konwencji jest brak mechanizmów pozwalających skutecznie kontrolować strony w zakresie wypełniania przez nie zobowiązań konwencji, czego przykładem było stworzenie przez Związek Radziecki projektu „Biopreparat” mającego na celu opracowanie środków bakteriologicznych i toksyn, możliwych do wykorzystania w trakcie konfliktu zbrojnego⁵⁷³.

Obecnie broń biologiczna nie znajduje zastosowania w konfliktach zbrojnych, jednak sporadycznie jest wykorzystywana przez grupy terrorystyczne. W latach 80. XX wieku w Stanach Zjednoczonych sekta Rajneeshee dokonała ataku z wykorzystaniem salmonelli⁵⁷⁴. Do ataku doszło w dzień wyborów poprzez zarażenie bakterią salmonelli baru sałatkowego oraz miejskiej stacji wodociągowej, zarażonych zostało ponad 750 osób. Wybór stacji wodociągowej jako cel ataku pokazuje, że infrastruktura krytyczna jest szczególnie narażona na bezpośrednie zagrożenia ze strony broni biologicznej⁵⁷⁵. Jednak prawidłowe

⁵⁷¹ Konsultacje i współpraca dotyczy ewentualnych trudności z wypełnieniem celu lub konkretnych postanowień Konwencji. Strony Konwencji mogą wykorzystać istniejące już procedury, m.in. w ONZ jako forum do konsultacji i współpracy.

⁵⁷² W przypadku stwierdzenia naruszenia postanowień Konwencji strona może wnieść skargę do RB ONZ, jednocześnie wskazując wszystkie możliwe dowody potwierdzające jej zasadność i prośbę o jej rozpatrzenie.

⁵⁷³ R. Kopeć, *Zastosowanie broni biologicznej w konfliktach zbrojnych i atakach terrorystycznych*, „Annales Universitatis Paedagogicae Cracoviensis Studia de Securitate et Educatione Civili IV”, 2014, s. 55.

⁵⁷⁴ Ch. M. Thompson, *The Bioterrorism Threat by Non-State Actors: Hype Or Horror?*, Naval Postgraduate School, Monterey, December 2006, s. 18-28.

⁵⁷⁵ J-E. S. Hansen, *Concepts of offensive use of biological weapons*, „Militært Tidsskrift”, 2006, vol. 135, s. 349.

funkcjonowanie infrastruktury krytycznej może zostać także zakłócone jako efekt pośredni działania broni biologicznej. Wykorzystanie tej broni może doprowadzić do paraliżu placówek medycznych, które w niewystarczający sposób będą przygotowane na leczenie osób poszkodowanych czynnikami biologicznymi, na przykład ze względu na małą liczbę personelu medycznego lub brak odpowiednich środków leczniczych⁵⁷⁶.

4.4.3.2 Broń chemiczna

Obok broni biologicznej broń chemiczna stanowi najczęściej używany rodzaj broni masowego rażenia. Po raz pierwszy została użyta na przełomie VII i VI wieku p.n.e. przez wojska ateńskie, dowodzone przez Solona, które zatruiły rzekę korzeniami ciemniaka⁵⁷⁷. Jednak do najpowszechniejszego użycia środków chemicznych w trakcie konfliktu zbrojnego doszło podczas I wojny światowej, między innymi w bitwie pod Ypres w 1915 roku.⁵⁷⁸ W trakcie II wojny światowej ofiarą broni chemicznej była przede wszystkim ludność cywilna, wobec której zarówno Niemcy, jak i Japończycy wykorzystywali środki chemiczne do prowadzenia badań i masowej eksterminacji⁵⁷⁹. Współcześnie broń chemiczna, w związku z wprowadzeniem całkowitego jej zakazu, jest rzadko używanym środkiem walki, a jej ostatnie masowe wykorzystanie miało miejsce w trakcie wojny domowej w Syrii⁵⁸⁰. Wszystkie te przykłady wiązały się z użyciem broni chemicznej przez podmioty państwowe, jednak środki chemiczne równie często stosowane były przez grupy terrorystyczne. 20 marca 1995 roku radykalne ugrupowanie religijne Najwyższa Prawda (jap. *Aum Shinrikyō*), przy użyciu Sarinu (gazu paraliżującego), dokonało zamachu na tokijskie metro⁵⁸¹. W wyniku ataku zmarło 12 osób, a kilka tysięcy zostało rannych.

Pierwszy powszechny zakaz użycia broni chemicznej w trakcie konfliktu zbrojnego wprowadzono w art. 23 Regulaminu haskiego z 1907 roku, zgodnie z którym strony wojujące nie mogły wykorzystywać trucizn oraz broni zatrutej. Dodatkowo zakaz użycia broni chemicznej został powtórzony w Protokole genewskim z 1925 roku.

⁵⁷⁶ D. P. Fidler, *Facing the global challenges posed by biological weapons*, „Microbes and Infection”, 1999, vol. 1, iss. 12, s. 1061.

⁵⁷⁷ J. Boczek, M. Lewandowski, *Wykorzystanie owadów i innych organizmów w akcjach terroru i konfliktach zbrojnych*, „Zagadnienia Doradztwa Rolniczego”, 2015, 82(4), s. 141.

⁵⁷⁸ J. E. van Courtland Moon, *Chemical Weapons and Deterrence: The World War II Experience*, „International Security”, 1984, vol. 8, no. 4, s. 5.

⁵⁷⁹ J. Boczek, M. Lewandowski, *Wykorzystanie owadów...*, s. 142.

⁵⁸⁰ R. Barber, *Uniting for Peace Not Aggression: Responding to Chemical Weapons in Syria Without Breaking the Law*, „Journal of Conflict and Security Law”, 2019, vol. 24, iss. 1, s. 71-72.

⁵⁸¹ M. Żuber, *Broń masowego rażenia...*, s. 132-133.

Obecnie fundamentem nieprolifracji broni chemicznej jest Konwencja o zakazie broni chemicznej z 1993 roku, w której broń chemiczną zdefiniowano jako toksyczne związki chemiczne i ich prekursory (występujące razem lub osobno) specjalnie zaprojektowane dla spowodowania śmierci lub innej szkody poprzez toksyczne właściwości związków chemicznych, wyzwalanych w rezultacie zastosowania takiej amunicji i urządzeń oraz wszelki sprzęt specjalnie zaprojektowany do użycia w bezpośrednim związku z zastosowaniem tej amunicji i urządzeń (art. II ust. 1 lit a-c Konwencji o zakazie broni chemicznej). Oprócz tego konwencja w art. II ust. 2 i 7 zdefiniowała dwa terminy: toksyczny związek chemiczny oraz chemiczny środek policyjny. Za toksyczny związek chemiczny uważa się dowolny związek chemiczny, który przez swoje działanie na procesy życiowe może spowodować śmierć, czasowe obezwładnienie lub trwałą szkodę ludziom lub zwierzętom. Obejmuje to wszystkie tego rodzaju związki chemiczne, niezależnie od ich pochodzenia lub metody ich produkcji, bez względu na zastosowanie ich w obiektach, w amunicji lub gdzie indziej. Natomiast pod pojęciem chemicznego środka policyjnego rozumie się każdy związek chemiczny nie umieszczony w wykazach, który może szybko wywołać w organizmie człowieka podrażnienie narządów zmysłów lub fizyczne obezwładnienie, zanikające w krótkim czasie po zaprzestaniu działania.

Na podstawie art. I ust. 1 lit. a-d oraz ust. 2 i 3 konwencji strony zobowiązały się do:

1. nie prowadzenia badań, produkowania, nabywania, gromadzenia lub przechowywania broni chemicznej lub przekazywania jej pośrednio lub bezpośrednio komukolwiek,
2. nie używania jej ani nie podejmowania jakichkolwiek wojskowych przygotowań do jej użycia,
3. nie pomagania, nie zachęcania ani nie skłaniania kogokolwiek do podejmowania jakiejkolwiek działalności zabronionej postanowieniami konwencji,
4. zniszczenia broni chemicznej oraz obiektów służących do jej produkcji, których są właścicielami albo znajdują się w ich posiadaniu,
5. zniszczenia broni chemicznej, którą porzuciły na terytorium innego państwa.

Zniszczenie arsenału broni chemicznej oznacza, że związki chemiczne przyjmują formę niezdatną do użycia w broni chemicznej, a amunicję oraz inne urządzenia czyni się bezwartościowymi. Strony konwencji same decydują o sposobie zniszczenia broni chemicznej w specjalnie do tego przygotowanych ośrodkach. Cały proces musi się odbyć z poszanowaniem dla środowiska naturalnego oraz ochrony ludności, a konwencja wyróżnia trzy metody, które

są zakazane: zatapianie w jakimkolwiek środowisku wodnym, zakopywanie w ziemi oraz spalanie na otwartej przestrzeni (część IV Załącznika do Konwencji o zakazie broni chemicznej). Ponadto traktat określa sztywne ramy czasowe, w których strony muszą dokonać zniszczenia swoich zasobów broni chemicznej. Proces niszczenia nie może rozpocząć się później niż dwa lata od wejścia w życie Traktatu, a zakończyć się dziesięć lat po dacie wejścia do życia Konwencji. Dopuszczono jednak możliwość przedłużenia dziesięcioletniego terminu, jeżeli państwo-strona nie będzie w stanie zniszczyć broni chemicznej w tym terminie. Przedłużenie następuje po złożeniu wniosku, zawierającego informacje nt. okresu, na jaki ma nastąpić przedłużenie, szczegółowe wyjaśnienie przyczyn przedłużenia oraz szczegółowy plan zniszczenia pozostałych zasobów broni chemicznej.

Konwencja o zakazie broni chemicznej przewiduje system weryfikacji, który nadzoruje strony oraz ich postępy w zakresie niszczenia broni chemicznej (część IV Załącznika do Konwencji o zakazie broni chemicznej). Pierwszym etapem weryfikacji jest sprawdzenie przez inspektorów prawdziwości danych zawartych w deklaracjach stron. Kontroli podlega ilość i rodzaj związków chemicznych, typ i ilość amunicji, urządzeń i innego sprzętu. Podczas tej fazy inspektorom przysługuje możliwość systematycznej weryfikacji miejsc składowania, co ma uniemożliwić niezauważone przenoszenie broni chemicznej. Inspekcje zapowiada się na 48 godzin przed jej przeprowadzeniem. Drugim etapem jest systematyczna weryfikacja niszczenia broni chemicznej. Jego celem jest określenie charakteru i ilości zapasów broni chemicznej do zniszczenia oraz potwierdzenie, że te zapasy zostały zniszczone. Ponadto dla kontroli przestrzegania postanowień Konwencji powołano do życia Organizację ds. Zakazu Broni Chemicznej, z siedzibą w Hadze (art. VIII Konwencji o zakazie broni chemicznej). Członkami Organizacji są wszystkie państwa będące stroną Konwencji o zakazie broni chemicznej.

Pomimo powszechnego zakazu użycia broni chemicznej jest ona w dalszym ciągu wykorzystywana podczas konfliktów zbrojnych. Szczególnie narażone na jej użycie są obiekty infrastruktury krytycznej. Na przełomie 2006 i 2007 roku Al-Kaida porwała cysterny z chlorem przeznaczone do wykorzystania w stacjach uzdatniania wody⁵⁸². Cysterny wypełnione duszącym gazem zostały wykorzystane jako bomby do przeprowadzenia zamachu w centrum miast. Natomiast w 2018 roku rządowe wojska syryjskie przypuściły atak bombowy

⁵⁸² J. P. Zanders, *Preventing the Re-Emergence of Chemical Weapons. The evolution of chemical weapon use since 1990*, European Union Institute for Security Studies, Report 2019, s. 4.

z wykorzystaniem gazów bojowych na szpital znajdujący się w strefie „rebeliantów”⁵⁸³. W wyniku ataku ponad 500 osób zostało hospitalizowanych z objawami zatrucia gazem, z czego około 70 z nich zmarło. Tak samo, jak w przypadku broni biologicznej, broń chemiczna została wykorzystana do ataku na urządzenia związane z dostawami wody pitnej. Atak na systemy wodociągowe stanowi szczególne niebezpieczeństwo dla ludności cywilnej, ograniczając jej dostęp do realizacji podstawowych potrzeb człowieka. Również placówki medyczne, ze względu na swoją dostępność oraz ograniczoną ochronę, są obiektami narażonymi na ataki ze strony broni chemicznej⁵⁸⁴, a jego skutki paraliżują funkcjonowanie państwa, ale także wpływają na życie i zdrowie ludności cywilnej.

4.4.3.3 Broń jądrowa

Ostatnim rodzajem broni masowego rażenia jest broń jądrowa. Jej pierwszy test zakończony sukcesem przeprowadzono 16 lipca 1945 roku na terytorium Stanów Zjednoczonych⁵⁸⁵. Natomiast do pierwszego ataku z wykorzystaniem broni nuklearnej doszło 6 sierpnia 1945 roku w Hiroszimie, co skutkowało śmiercią ponad 100 tysięcy osób⁵⁸⁶. Drugi atak nastąpił trzy dni później – 9 sierpnia 1945 roku – a jego celem było Nagasaki, co przyczyniło się do śmierci prawie 75 tysięcy osób⁵⁸⁷.

Po 1945 roku kluczową rolę w próbach ograniczenia produkcji i użycia broni nuklearnej odegrała nowopowstała Organizacja Narodów Zjednoczonych. Już w pierwszej rezolucji ZO ONZ wezwało do całkowitego wyeliminowania broni nuklearnej oraz powołała komisję, zajmującą się problematyką nuklearną⁵⁸⁸. Pomimo podejmowanych działań, mocarstwa nuklearne – Stanów Zjednoczonych, Związku Radzieckiego, Francji oraz Wielka Brytania – nie wykazywały żadnej woli politycznej do pozbycia się broni nuklearnej z własnego arsenału⁵⁸⁹. Co więcej, 30 października 1961 roku Związek Radziecki, w ramach testu, zdetonował ówczesnie najsilniejszą bombę termojądrową⁵⁹⁰.

⁵⁸³ R. Barber, *Uniting for Peace*..., s. 73-74.

⁵⁸⁴ K. Vichová, M. Hromada, F. Paulus, J. Valasek, *CBRN Weapons as a Threat to Critical Infrastructure Elements*, 2022 6th International Conference on Medical and Health Informatics (ICMHI 2022), 13–15.05.2022, https://www.researchgate.net/publication/364557657_CBRN_Weapons_as_a_Threat_to_Critical_Infrastructure_Elements (dostęp: 15.05.2026).

⁵⁸⁵ *The road to a world free of nuclear weapons*, https://www.icanw.org/nuclear_weapons_history (dostęp: 4.03.2026).

⁵⁸⁶ *Tamże*.

⁵⁸⁷ *Tamże*.

⁵⁸⁸ ZO ONZ, *Resolution 1(I)*, 24.01.1946, A/RES/1(I).

⁵⁸⁹ *The road to a world....*

⁵⁹⁰ *Tamże*.

Pod pojęciem broni nuklearnej rozumie się ładunki jądrowe lub termojądrowe oraz systemy urządzeń zdolne do przenoszenia tych ładunków, jak rakiety czy pociski artyleryjskie⁵⁹¹. Połączenie tych składników prowadzi do wybuchu, który powoduje reakcję jądrową polegającą na rozpadzie izotopów ciężkich pierwiastków – uranu lub plutonu (bomba atomowa) lub połączenie izotopów, np. wodoru (bomba termojądrowa)⁵⁹².

Ładunki wykorzystywane w broni jądrowej należy podzielić na cztery generacje. Pierwszą generację stanowią bomby, których działanie opiera się na rozszczepieniu pierwiastków ciężkich. Są one łatwe w wytworzeniu, przez co są najczęściej produkowanym rodzajem broni nuklearnej. Druga generacja stanowią bomby termojądrowe oraz bomby wodorowe. Trzecią generacją są bomby neutronowe, które nie prowadzą do skażenia promieniotwórczego, co wiąże się z ich określeniem jako „czystych bomb”. Ostatnią generację stanowi broń, która będzie opierała się na najnowszych badaniach oraz doświadczeniach⁵⁹³.

W drugiej połowie XX wieku państwa, dostrzegając zagrożenie płynące z wykorzystania broni jądrowej, sukcesywnie wprowadzały prawne ograniczenia jej wykorzystania, zarówno na poziomie ogólnoświatowym, jak i regionalnym. Pierwszy traktatem międzynarodowym tak szeroko regulującym problematykę broni jądrowej był Układ o nierozprzestrzenianiu broni jądrowej z 1968 roku (NPT)⁵⁹⁴. Celem NPT była kontrola materiałów nuklearnych oraz całkowite wykluczenie użycia broni nuklearnej. Wiązało się to z koniecznością opracowania procedur z zakresu nieprolifracji, rozbrojenia oraz wykorzystanie energii jądrowej w celach pokojowych⁵⁹⁵. Przystępując do NPT państwa nuklearne zobowiązały się do nieprzekazywania, w sposób bezpośredni jak i pośredni, komukolwiek broni jądrowej lub innych jądrowych urządzeń wybuchowych, a także kontroli nad taką bronią lub urządzeniami (art. I NPT). Ponadto zobligowały się do niezachęcania, nieokazywania pomocy oraz do nienakłaniania państw nienuklearnych do produkowania broni jądrowej lub innych urządzeń jądrowych lub zdobycia ich w jakikolwiek inny sposób. Natomiast państwa nienuklearne zobowiązały się do nieprzyjmowania od kogokolwiek, w sposób bezpośredni lub pośredni, broni jądrowej ani jądrowych urządzeń wybuchowych,

⁵⁹¹ USA, *Operations in Chemical, Biological, Radiological, and Nuclear Environments*, Joint Publication 3-11, 4 October 2013, https://edocs.nps.edu/2012/December/jp3_11.pdf, (dostęp: 4.01.2026), s. Appendix C-1.

⁵⁹² *Tamże*, s. Appendix C-1.

⁵⁹³ M. Żuber, *Broń masowego rażenia...*, s. 14.

⁵⁹⁴ *Układ o nierozprzestrzenianiu broni jądrowej*, Moskwa, Waszyngton i Londyn, 1.07.1968, Dz. U. z 1970 r., nr 8, poz. 60.

⁵⁹⁵ R. Kopeć, *Traktat o nierozprzestrzenianiu broni nuklearnej jako prawnomiędzynarodowy reżim zapobiegania proliferacji*, „Annales Universitatis Paedagogicae Cracoviensis Studia de Securitate et Educatione Civili V”, 2015, s. 87.

a także powstrzymanie się od produkcji i nabywania w inny sposób wspomnianej wcześniej broni oraz urządzeń (art. II NPT). Jako, że jednym z fundamentów NPT jest wykorzystanie energii atomowej w celach pokojowych, państwa-strony zobowiązane są wymieniać się informacjami, wyposażeniem oraz materiałami, które mogą przysłużyć się do pokojowego wykorzystania energii jądrowej (art. IV NPT). Ponadto państwa nuklearne zobligowały się do udostępniania państwom nienuklearnym potencjalnych korzyści wynikających z pokojowego zastosowania wybuchów jądrowych (art. V NPT).

Dla właściwego nadzoru nad postanowieniami NPT zdecydowano się na podjęcie współpracy z Międzynarodową Agencją Energii Atomowej (MAEA). Agencja została powołana w 1957 roku jako organizacja wyspecjalizowana ONZ w zakresie pokojowego wykorzystania energii jądrowej. Jej zadaniem jest nadzór nad działalnością państw-stron w zakresie zgodności z postanowieniami traktatu⁵⁹⁶. Kontrole są prowadzone na podstawie porozumień zawartych pomiędzy stronami NPT a MAEA i nie mogą powodować trudności w ekonomicznym i technicznym rozwoju państw-stron oraz międzynarodowej współpracy w dziedzinie pokojowego wykorzystania energii jądrowej (art. III NPT).

NPT nie spełniło jednak swojej roli jaką było całkowite wyeliminowanie proliferacji broni jądrowej, a jedynie wzmocniło rolę Stanów Zjednoczonych oraz Związku Radzieckiego jako mocarstw atomowych⁵⁹⁷. W późniejszym czasie, pomimo postanowień NPT, kolejne państwa weszły w posiadanie tej broni, na przykład Indie i Pakistan, tym samym ukazując słabość mechanizmów przewidzianych w traktacie⁵⁹⁸.

W porównaniu z NPT skuteczniejsze w tym względzie okazały się porozumienia regionalne. Możliwość przyjęcia regionalnych układów tworzących strefy wolne od broni jądrowej przewidywał już art. VII NPT. Obecnie na świecie istnieje sześć stref bezatomowych – Antarktyka, Afryka (cały kontynent), Ameryka Łacińska, obszar południowego Pacyfiku, Azja Południowo-Wschodnia oraz Azja Centralna⁵⁹⁹.

Pierwsza strefa bezatomowa powstała po przyjęciu Układu w sprawie Antarktyki z 1959 roku (Układ Antarktyczny)⁶⁰⁰. Geneza powstania Układu łączy się z roszczeniami

⁵⁹⁶ D. Fischer, *History of the International Atomic Energy Agency. The First Forty Years*, Division of Publications International Atomic Energy Agency, Vienna 1998, s. 59-60.

⁵⁹⁷ R. Kopeć, *Traktat o nierozprzestrzenianiu broni...*, s. 96.

⁵⁹⁸ *The Legacy of India's Nuclear Weapons Test*, <https://www.armscontrol.org/act/2024-11/features/legacy-indias-nuclear-weapons-test#:~:text=Fifty%20years%20ago%2C%20on%20May,1> (dostęp: 7.01.2026).

⁵⁹⁹ M. Żuber, *Broń masowego rażenia...*, s. 156.

⁶⁰⁰ *Układ w sprawie Antarktyki*, Waszyngton, 1.12.1959, Dz. U. z 1961 r., nr 46, poz. 237.

terytorialnymi Australii, Argentyny, Chile, Francji, Nowej Zelandii, Norwegii oraz Wielkiej Brytanii do terytorium Antarktyki. Każde z tych państw wysuwało swoje żądania na podstawie potrzeby eksploracji lub bliskości geograficznej Antarktyki⁶⁰¹. Chociaż działalność tych państw (wraz z pozostałymi państwami prowadzącymi badania naukowe, na przykład Stanami Zjednoczonymi, Związkiem Radzieckim czy Polską) odbywała się pokojowo, to podjęto decyzję o zwołaniu konferencji dyplomatycznej, w ramach której omówione zostały następujące tematy: niezmiennosc statusu prawnego Antarktyki, współpraca naukowa oraz wykorzystanie Antarktyki tylko do celów pokojowych⁶⁰². Założenia konferencji znalazły swoje odzwierciedlenie w art. I Układu, zgodnie z którym Antarktyka będzie wykorzystywana tylko w celach pokojowych a wszelkie przedsięwzięcia militarnych, między innymi tworzenia baz wojskowych czy wykorzystywania personelu lub sprzętu wojskowego do prowadzenia badań naukowych, będą zabronione. Na podstawie art. V ust. 1 Układu wprowadzono zakaz wszelkich wybuchów jądrowych w Antarktyce oraz usuwania w tym rejonie odpadów promieniotwórczych. Zgodnie z ust. 2 tego artykułu państwa-strony Układu miałyby w przyszłości stworzyć system umożliwiający ewentualne wykorzystanie energii jądrowej w Antarktyce, jednak nigdy nie doszło do jego stworzenia⁶⁰³. Przyjęcie Układu pozwoliło Antarktyce uniknąć losu Arktyki, która regularnie jest terytorium sporów pomiędzy państwami położonymi w graniach koła podbiegunowego północnego, ale również pozwoliło zachować środowisko naturalne w nienaruszonym stanie. Zarówno Stany Zjednoczone, jak i Rosja, czy wcześniej Związek Radziecki, wykorzystują tereny koła podbiegunowego północnego do tworzenia baz wojskowych, w których operują okręty podwodne z napędem atomowym czy do składowania broni jądrowej⁶⁰⁴.

Druga strefa bezatomowa powstała wraz z przyjęciem Traktatu o zakazie broni jądrowej w Ameryce Łacińskiej i na Karaibach z 1967 roku (Traktat z Tlatelolco)⁶⁰⁵. Traktat powstał z inicjatywy Brazylii, która obserwując rosnące napięcie pomiędzy Stanami Zjednoczonymi i Związkiem Radzieckim, obawiała się wojny nuklearnej na obszarze Ameryki Łacińskiej

⁶⁰¹ T. Graham, D. J. LaVera, *Cornerstones of Security: Arms Control Treaties in the Nuclear Era*, University of Washington Press, Washington DC 2002, s. 13.

⁶⁰² *Tamże*, s. 14.

⁶⁰³ A. D. Hemmings, *The 1959 Antarctic Treaty and Subsequent Antarctic Treaty System*, w: A. D. Hemmings, K. Offerdal, N. Oral, H. A. Conley (ed.), *History Lessons for the Arctic: What International Maritime Disputes Tell Us about a New Ocean*, Center for Strategic and International Studies (CSIS), Washington DC 2016, s. 41-42.

⁶⁰⁴ *Tamże*, s. 42.

⁶⁰⁵ *Układ o zakazie broni jądrowych w Ameryce Łacińskiej i na Karaibach*, Tlatelolco, 14.02.1967, United Nations Treaty Series, 1967, vol. 634, nr 326.

(w 1962 roku Związek Radziecki rozmieścił na Kubie rakiety strategiczne)⁶⁰⁶. Do Traktatu mogą przystąpić tylko państwa położone na określonej szerokości geograficznej, obejmującej swoim zasięgiem obszar od północy Meksyku, aż po południowe rejony Argentyny i Chile (art. 4 ust. 2 Traktatu). Strony Traktatu zobowiązały się do zakazu testowania, używania, produkcji, wytwarzania lub nabywania w jakikolwiek sposób broni jądrowej, pośrednio lub bezpośrednio oraz do zakazu otrzymywania, przechowywania, instalowania, rozmieszczania i wszelkich innych sposobów posiadania broni jądrowej, w tym tworzenia baz wojskowych obcych państw⁶⁰⁷. W Traktacie zdefiniowano pojęcie broni jądrowej, za którą uznano „każde urządzenie, które może wyzwalać energię jądrową w sposób niekontrolowany i które posiada zestaw cech odpowiednich do wykorzystania w celach wojennych” (art. 5 Traktatu). Co więcej, w ramach sprawowania kontroli nad wykonaniem postanowień Traktatu powołano do życia Agencję do spraw Zakazu Broni Jądrowej w Ameryce Łacińskiej i na Karaibach (ang. *Agency for the Prohibition of Nuclear Weapons in Latin America and the Caribbean*). Do jej głównych zadań należy kontrola realizacji postanowień Traktatu oraz organizacja cyklicznych lub nadzwyczajnych konsultacji pomiędzy stronami Traktatu (art. 7 Traktatu). Traktat jest pierwszą umową międzynarodową wprowadzającą regionalną ochronę przed bronią jądrową, nie tylko zakazującą produkowania czy używania tej broni przez państwa-strony, ale również zakazującą tworzenia baz wojskowych państw trzecich, które składowałyby w tych bazach broń jądrową. W następnych latach Traktat z Tlatelolco posłużył jak wzór do tworzenia kolejnych stref bezaatomowych⁶⁰⁸.

Trzecia strefa bezaatomowa została utworzona wraz z przyjęciem Traktatu o strefie bezaatomowej na Południowym Pacyfiku w 1985 roku (Traktat z Rarotonga)⁶⁰⁹. Traktat stanowił odpowiedź na wieloletnie wykorzystywanie obszaru Południowego Pacyfiku jako poligonu nuklearnego, w szczególności przez Francję, Wielką Brytanię oraz Stany Zjednoczone⁶¹⁰. W samej preambule Traktatu znajdują się odniesienia do zapewnienia bezpieczeństwa środowisku naturalnemu, będącego dziedzictwem ludności tubylczej. W odróżnieniu od Traktatu z Tlatelolco, Traktat z Rarotonga nie zdefiniował pojęcia broni jądrowej, a zamiast

⁶⁰⁶ D. R. Robinson, *The Treaty of Tlatelolco and the United States: A Latin American Nuclear Free Zone*, „The American Journal of International Law”, 1970, vol. 64, no. 2, s. 283.

⁶⁰⁷ J. R. Redick, *Regional Nuclear Arms Control in Latin America*, „International Organization”, 1975, vol. 29, no. 2, s. 435.

⁶⁰⁸ E. Mendenhall, *Nuclear-Weapon-Free Zones and Contemporary Arms Control*, „Strategic Studies Quarterly”, 2020, vol. 14, no. 4, s. 145-146.

⁶⁰⁹ *Traktat o strefie bezaatomowej na Południowym Pacyfiku*, Rarotonga, 6.08.1985, United Nations Treaty Series, 1987, vol. 1445, nr 178.

⁶¹⁰ N. Maclellan, *The Nuclear Age in the Pacific Islands*, „The Contemporary Pacific”, 2005, vol. 17, no. 2, s. 363.

tego wprowadził pojęcie jądrowego urządzenia wybuchowego (ang. *nuclear explosive device*), za które rozumie się „każdą broń jądrową lub inne urządzenie wybuchowe zdolne do uwolnienia energii jądrowej, niezależnie od celu, do którego mogłoby zostać wykorzystane” (art. 1 lit. c Traktatu z Rarotonga). Oprócz tego za jądrowe urządzenie wybuchowe należy uznać wszystkie części składowe, bez których urządzenie nie może prawidłowo działać. Do samych urządzeń nie zalicza się środków transportujących te urządzenia. Powyższa definicja jest szersza niż ta przedstawiona w Traktacie z Tlatelolco, ponieważ obejmuje również inne części konieczne do prawidłowego działania broni jądrowej. Postanowienia art. 3 Traktatu nakładają na strony zakaz produkowania, nabywania lub posiadania jądrowych urządzeń wybuchowych, poszukiwania lub przyjmowania pomocy przy produkcji takich urządzeń oraz zakazują podejmowania jakichkolwiek działań zmierzających do pomocy lub zachęcania do nabycia lub produkcji jądrowych urządzeń wybuchowych przez inne państwo. Co więcej, strony zobowiązały się do nierozmieszczania żadnych jądrowych urządzeń wybuchowych na swoim terytorium (art. 5 Traktatu). Dodatkowo, uwzględniając bezpieczeństwo środowiska naturalnego strony zobowiązały się, że nie będą utylizować odpadów radioaktywnych w morzach obszaru południowego Pacyfiku, a także będą przeciwdziałały składowaniu odpadów radioaktywnych przez inne państwa na ich wodach terytorialnych (art. 7 lit. a i b Traktatu). W celu prawidłowego wykonania Traktatu wprowadzono system kontroli w zakres którego wchodzi: raporty i wymiana informacji, konsultacje, współpraca z MAEA oraz procedura skargowa (art. 8 Traktatu). Wprawdzie, z militarnego punktu widzenia, testowanie broni jądrowej na atolach Południowego Pacyfiku pozwoliło na osiągnięcie sukcesu w badaniach nad tą bronią, to z punktu widzenia ludności tubylczej działania wojskowych doprowadziły do poważnych skutków w postaci nie tylko zmian w środowisku naturalnym, ale również problemów zdrowotnych związanych z chorobą popromienną, w tym zgonów⁶¹¹.

Czwartą strefę bezatomową utworzono na obszarze Azji Południowo-Wschodniej dzięki przyjęciu Traktatu o strefie bezatomowej w Azji Południowo-Wschodniej z 1995 roku (Traktat z Bangkoku)⁶¹². Geneza Traktatu sięga jeszcze wczesnych lat 70. XX wieku kiedy Stowarzyszenie Narodów Azji Południowo-Wschodniej przyjęło deklarację o utworzeniu w przyszłości Strefy Pokoju, Wolności i Neutralności w Azji Południowo-Wschodniej

⁶¹¹ E. L. Winterer, *Nuclear Bomb Testing*, w: R. G. Gillespie, D. A. Clague (ed.) *Encyclopedia of Islands*, University of California Press, Berkley, Los Angeles and London 2009, s. 685.

⁶¹² *Traktat o strefie bezatomowej w Azji Południowo-Wschodniej*, Bangkok, 15.12.1995, „International Legal Materials”, 1996, vol. 35, nr 635.

(ang. *Zone of Peace, Freedom and Neutrality in Southeast Asia*)⁶¹³. Była to odpowiedź na narastające zagrożenie wpływami światowych mocarstw (Stanów Zjednoczonych i Związku Radzieckiego) na obszarze Azji Południowo-Wschodniej, w szczególności Wietnamu, Kambodży i Laosu⁶¹⁴. Prace nad utworzeniem Stefy zostały zawieszone w związku z konfliktem pomiędzy Wietnamem a Kambodżą z 1979 roku, jednak w dalszym ciągu prowadzono negocjacje nad utworzeniem strefy bezatomowej. Przełomem było zakończenie zimnej wojny i przyjęcie Porozumienia w sprawie kompleksowego rozwiązania politycznego konfliktu w Kambodży (Porozumienie paryskie z 1991 roku) kończącego konflikt pomiędzy Kambodżą a Wietnamem⁶¹⁵. Osiągnięcie pokoju i względnej stabilności w tym rejonie pozwoliło na dalsze prowadzenie prac w zakresie utworzenia strefy bezatomowej, czego skutkiem było przyjęcie 15 grudnia 1995 roku Traktatu z Bangkoku. W Traktacie wprowadzono definicję broni jądrowej, za którą uważa się „każde urządzenie wybuchowe zdolne do uwolnienia energii jądrowej w sposób niekontrolowany, z wyłączeniem środków transportu lub dostarczania takiego urządzenia, jeżeli można je od niego oddzielić i nie stanowią one jego nieodłącznej części”. Oprócz tego zdefiniowano dwa dodatkowe pojęcia – materiały radioaktywne oraz odpady radioaktywne. Za materiały radioaktywne uważa się materiały zawierające radionuklidy (izotopy promieniotwórcze) powyżej poziomów dopuszczalnych lub zwolnionych z kontroli zalecanych przez MAEA, natomiast odpadami radioaktywnymi są materiały zawierające lub zanieczyszczone radionuklidami w stężeniach lub o aktywności przekraczającej poziom dopuszczalny przez MAEA (art. 1 lit. c, e, f Traktatu). Na podstawie art. 3 Traktatu państwa zobowiązały się nie opracowywać, nie produkować ani w inny sposób nie nabywać, nie posiadać ani nie sprawować kontroli nad bronią jądrową, nie rozmieszczać jej, nie transportować, nie testować ani nie używać. Zobowiązały się również nie zezwalać żadnemu innemu państwu na opracowywanie, produkcję lub nabywanie w inny sposób, posiadanie lub sprawowanie kontroli nad bronią jądrową, rozmieszczanie jej, testowanie lub używanie na swoim terytorium. Ponadto zakazano składowania odpadów radioaktywnych na lądzie, w morzu lub w atmosferze. Zamiast tego, na podstawie art. 4 Traktatu państwa mogą rozwijać energetykę jądrową w pokojowych celach, dla rozwoju gospodarczego. Jednak wymaga to od nich restrykcyjnej kontroli bezpieczeństwa systemu jądrowego, z koniecznością informowania innych państw-stron o tym systemie i ewentualnych awariach systemu

⁶¹³ A. Acharya, J. D. K. Boutin, *The Southeast Asia Nuclear Weapon-Free Zone Treaty*, „Security Dialogue”, 1998, vol. 29, no. 2, s. 219.

⁶¹⁴ *Tamże*, s. 219-220.

⁶¹⁵ *Agreement on a comprehensive political settlement of the Cambodia conflict*, Paryż, 23.10.1991, United Nations Treaty Series, 1992, vol. 1663, nr 28613.

jądrowego. W ramach Traktatu ustanowiono system kontroli, którego celem jest nadzór nad prawidłowym wykonaniem postanowień Traktatu. System opiera się na trzech filarach: procedurach MAEA, wzajemnym zgłaszaniu i wymianie informacji pomiędzy stronami Traktatu oraz wnioskach i procedurach misji wyjaśniającej (art. 10 Traktatu). Oprócz tego systemu na mocy Traktatu utworzono Komisję Strefy Bezaatomowej w Azji Południowo-Wschodniej (ang. *Commission for the Southeast Asia Nuclear Weapon-Free Zone*), do zadań której należy nadzorowanie prawidłowego wdrożenia postanowień Traktatu oraz przestrzeganie zgodności działań państw z postanowieniami Traktatu. Przyjęcie Traktatu z Bangkoku wpisywało się w trend tworzenia regionalnych stref bezaatomowych, ale przyczyniło się także do rozwoju ekonomicznego i społecznego regionu Azji Południowo-Wschodniej⁶¹⁶.

Piąta strefa bezaatomowa powstała na obszarze całego kontynentu afrykańskiego wraz z przyjęciem Traktatu o strefie bezaatomowej w Afryce w 1996 roku (Traktat z Pelindaby)⁶¹⁷. Geneza Traktatu z Pelindaby wykazuje pewne podobieństwa z Traktatem z Rarotonga, ponieważ także w przypadku Afryki państwa kolonialne prowadziły testy z bronią jądrową (Francja testowała broń jądrową na Saharze)⁶¹⁸. 24 listopada 1961 roku ZO ONZ przyjęło rezolucję nr 1652 (XVI) wzywającą do powstrzymania się od testowania, przechowywania lub transportowania przez terytorium Afryki broni jądrowej⁶¹⁹. Cztery lata później, 3 grudnia 1965 roku ZO ONZ przyjęło rezolucję 2033 (XX), deklarując Afrykę strefą zdenuklearyzowaną⁶²⁰. Pomimo wielu politycznych deklaracji, dopiero Traktat z Pelindaby dał prawne podstawy do utworzenia w Afryce strefy bezaatomowej. Traktat zakazuje państwom-stronom przeprowadzenia testów nuklearnych urządzeń wybuchowych, ale także ich nabywania, składowania czy przeprowadzania badań nad takimi urządzeniami (art. 3-5 Traktatu). Oprócz tego państwa-strony nie mogą sprowadzać do Afryki odpadów radioaktywnych, w celu ich składowania, a także zobowiązują się do kontroli transgranicznego przemieszczania odpadów radioaktywnych (art. 7 Traktatu). Na podstawie art. 11 Traktatu państwa-strony zobowiązują się do nieatakowania obiektów nuklearnych podczas konfliktu zbrojnego. Postanowienia Traktatu wspierają rozwój energii jądrowej wykorzystywanej w celu

⁶¹⁶ S. P. Subedi, *Problems and Prospects for the Treaty on the Creation of a Nuclear-Weapon-Free Zone in Southeast Asia*, „International Journal of Peace Studies”, 1999, vol. 4, no. 1, s. 73-74.

⁶¹⁷

⁶¹⁸ S. Ogunbanwo, *The Treaty of Pelindaba: Africa Is Nuclear-Weapon-Free*, „Security Dialogue”, 1996, vol. 27, no. 2, s. 186.

⁶¹⁹ ZO ONZ, *Resolution 1652 (XVI)*, 24.11.1961, A/RES/1652(XVI).

⁶²⁰ ZO ONZ, *Resolution 2033 (XX)*, 3.12.1965, A/RES/2033(XX).

rozwoju gospodarczego i społecznego (art. 8 Traktatu). Ponadto w art. 12 Traktat przewiduje system kontroli jego postanowień, w tym utworzenie Afrykańskiej Komisji ds. Energii Jądrowej (ang. *African Commission on Nuclear Energy*). Traktat z Pelindaby stanowi zwięźczenie wielu deklaracji politycznych dotyczących utworzenia na terytorium Afryki strefy bezatomowej. Same postanowienia Traktatu wykazują wiele podobieństw, a miejscami są wręcz identyczne jak postanowienia przyjętych już wcześniej traktatów tworzących strefy bezatomowe. Chociaż Traktat nie jest pierwszą umową międzynarodową w tym zakresie, to wielokrotnie wskazywano, że powinien stanowić impuls do powstania następnych stref bezatomowych, obejmujących między innymi obszar Bliskiego Wschodu⁶²¹.

Ostatnia, szósta strefa bezatomowa została utworzona na obszarze Azji Centralnej wraz z przyjęciem Traktatu o strefie bezatomowej w Azji Centralnej w 2006 roku (Traktat z Semipałatyńska)⁶²². Podobnie jak Południowy Pacyfik i Afryka, obszar Azji Centralnej również był wykorzystywany jako poligon broni nuklearnej. Na obszarze dzisiejszego Kazachstanu Związek Radziecki prowadził testy z bronią jądrową⁶²³. Traktat, jak pozostałe traktaty tworzące strefy bezatomowe, zdefiniował pojęcie broni jądrowej, za którą rozumie się każdą broń lub inne urządzenie wybuchowe zdolne do uwolnienia energii jądrowej, niezależnie od wojskowego lub cywilnego przeznaczenia. Traktat zakazuje państwom-stronom rozwoju, produkowania, gromadzenia lub w jakikolwiek inny sposób nabywania broni nuklearnej lub innego nuklearnego urządzenia wybuchającego, przeprowadzania testów broni jądrowej, a także prowadzenia takiej działalności przez inne państwo na terytorium państwa-strony (art. 3 Traktatu). Na podstawie art. 6 Traktatu państwa-strony są zobowiązane do podjęcia niezbędnych kroków w celu rekultywacji środowiska naturalnego, które zostało zniszczone przez wykorzystywanie terenów Azji Centralnej w przeszłości jako miejsca produkcji i przechowywania broni jądrowej. W ramach zapewnienia systemu kontroli nad postanowieniami Traktatu państwa-strony zgodziły się na przyjęcie procedur MAEA (art. 8 Traktatu) oraz organizację konsultacji stron Traktatu (art. 10 Traktatu).

Jak do tej pory Traktat z Semipałatyńska jest ostatnim traktatem tworzącym strefę bezatomową. Połowę stref bezatomowych (Południowy Pacyfik, Afrykę i Azję Centralną) łączy wspólna historia wykorzystywanie tych obszarów przez światowe mocarstwa (Francję, Wielką

⁶²¹ B. Griffith, *African Nuclear-Weapon-Free Zone Nears Realization*, „Arms Control Today”, 2008, vol. 38, no. 4, s. 44.

⁶²² *Traktat o strefie bezatomowej w Azji Centralnej*, Semipałatyńsk, 08.09.2006, United Nations Treaty Series, vol. 2970, nr 51633.

⁶²³ *Semipalatinsk Test Site*, <https://www.nti.org/education-center/facilities/semipalatinsk-test-site/> (dostęp: 13.01.2026).

Brytanię, ale również Stany Zjednoczone i Związek Radziecki) w charakterze poligonów nuklearnych. Zdając sobie sprawę z katastrofalnych skutków testów broni jądrowej, chcąc naprawić zniszczone środowisko naturalne, państwa leżące na tych obszarach zdecydowały się nadać ramy prawne systemowi mającemu wyeliminować całkowite wykorzystanie broni jądrowej na ich terenie. Obecnie na obszarach objętych strefami bezatomowymi nie odbywają się żadne testy broni jądrowej, a państwa-strony tych traktatów powstrzymują się od produkcji broni jądrowej, dlatego należy uznać, że traktaty tworzące strefy bezatomowe odniosły sukces⁶²⁴.

Na obszarze Europy nie utworzono żadnej strefy bezatomowej, jednak UE podejmuje działania mające na celu zapewnienie bezpieczeństwa jądrowego, na przykład poprzez przyjęcie 12 i 13 grudnia 2003 roku przez Radę Europejską Europejskiej Strategii Przeciwko Proliferacji Broni Masowego Rażenia (ang. *EU Strategy Against Proliferation of Weapons of Mass Destruction*)⁶²⁵. Dostrzegając rosnące zagrożenie międzynarodowego bezpieczeństwa i pokoju UE przedstawiła szereg działań, które powinny zostać podjęte w celu wyeliminowania zagrożenia jakim jest broń masowego rażenia. Przede wszystkim wskazuje się na międzynarodową współpracę w zwalczaniu broni masowego rażenia (każde państwo członkowskie UE jest stroną NPT) oraz rozwój regionalnych porozumień w zakresie kontroli zbrojeń⁶²⁶. Oprócz tego Strategia przewiduje między innymi rozszerzenie nadzoru nad „wrażliwymi” materiałami (obejmującymi między innymi materiały radioaktywne) czy zwiększenie kontroli nad nielegalnym handlem materiałami masowego rażenia⁶²⁷. Pomimo, że Strategia była jedynie aktem politycznym, nie kreującym żadnych ram prawnych w zakresie ochrony przed bronią jądrową, to w późniejszym czasie Unia Europejska przyjęła szereg dyrektyw i rozporządzeń, które wyznaczały ramy prawne szeroko rozumianego bezpieczeństwa jądrowego w Europie. Przede wszystkim należy wskazać Dyrektywę Rady 2009/7/EURATOM z 25 września 2009 roku ustanawiającą wspólnotowe ramy bezpieczeństwa jądrowego obiektów jądrowych (Dyrektywa 2009/7/EURATOM)⁶²⁸. Celem dyrektywy było stworzenie ram wspólnotowych mających poprawić i promować bezpieczeństwo jądrowe wraz z jego regulacją oraz zapewnienie wprowadzenia przez państwa członkowskie krajowych

⁶²⁴ E. Mendenhall, *Nuclear-Weapon-Free...*, s. 144-146.

⁶²⁵ UE, *Europejska Strategia Przeciwko Proliferacji Broni Masowego Rażenia*, <https://data.consilium.europa.eu/doc/document/ST-15708-2003-INIT/en/pdf> (dostęp: 7.01.2026).

⁶²⁶ *Tamże*.

⁶²⁷ *Tamże*.

⁶²⁸ *Dyrektywa Rady 2009/7/EURATOM ustanawiająca wspólnotowe ramy bezpieczeństwa jądrowego obiektów jądrowych*, 25.06.2009, Dz. Urz. UE L 172/18 z 2.7.2009.

regulacji, tworzących odpowiedni poziom bezpieczeństwa jądowego. W art. 3 Dyrektywy zdefiniowano między innymi pojęcie bezpieczeństwa jądowego jako „osiągnięcie odpowiednich warunków eksploatacji, zapobieganie awariom i łagodzenie ich skutków, czego wynikiem jest ochrona pracowników i ludności przed zagrożeniami wynikającymi z promieniowania jonizującego z obiektów jądowych”. Jednak należy zauważyć, że chociaż sama Dyrektywa szeroko odnosiła się do bezpieczeństwa jądowego, to nie regulowała kwestii broni jądowej. Krokiem w stronę regulacji potencjalnej broni jądowej było przyjęcie Rozporządzenia Rady (WE) NR 428/2009 z dnia 5 maja 2009 roku ustanawiające wspólnotowy system kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania (Rozporządzenie 428/2009)⁶²⁹. W Rozporządzeniu zdefiniowano produkty podwójnego zastosowania jako „produkty, włącznie z oprogramowaniem i technologią, które mogą być stosowane zarówno w celach cywilnych, jak i wojskowych, oraz obejmują wszystkie towary, które mogą być użyte zarówno w zastosowaniach niewybuchowych, jak i w jakikolwiek sposób do wspomagania wytwarzania broni jądowej lub innych urządzeń do wybuchu jądowego”. Celem Rozporządzenia było utworzenie ram kontroli nad produktami podwójnego zastosowania potencjalnie wykorzystywanymi do produkcji broni jądowej. 20 maja 2021 roku przyjęto nowe rozporządzenie zastępujące Rozporządzenie 428/2009, ustanawiające unijny system kontroli wywozu, pośrednictwa, pomocy technicznej, tranzytu i transferu produktów podwójnego zastosowania (Rozporządzenie 2021/821)⁶³⁰. W Rozporządzeniu powtórzono definicję produktów podwójnego zastosowania, jednak w szerszym stopniu uregulowano kwestię zezwoleń na wywóz tych produktów.

W ramach unijnego systemu prawnego wprowadzono szereg regulacji mających na celu ograniczenie broni jądowej na terytorium Europy, ale nie zdecydowano się na całkowite jej wyeliminowanie. Należy wskazać, że Francja i Wielka Brytania dysponują własną bronią jądową, a państwa takie jak Niemcy czy Włochy biorą aktywny udział w programie współdzielenia broni jądowej Stanów Zjednoczonych w ramach NATO (ang. *Nuclear Sharing*

⁶²⁹ Rozporządzenia Rady (WE) NR 428/2009 ustanawiające wspólnotowy system kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania, 5.05.2009, Dz. Urz. UE L 134/1 z 29.05.2009.

⁶³⁰ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/821 ustanawiające unijny system kontroli wywozu, pośrednictwa, pomocy technicznej, tranzytu i transferu produktów podwójnego zastosowania, 20.05.2021, Dz. Urz. UE L 206/1 z 11.06.2021.

Policy)⁶³¹. Oznacza to, że główne europejskie państwa nie będą zainteresowane całkowitym wyeliminowaniem broni jądrowej z terytorium Europy, ponieważ straciłyby możliwość aktywnego działania w programie NATO, tym samym pozbywając się systemu odstraszenia potencjalnych wrogów.

Pomimo szeroko rozwiniętego systemu antynuklearnego na poziomie regionalnym, również na poziomie ogólnoświatowym starano się wprowadzić regulacje całkowicie eliminujące broń jądrową. W 1996 roku ZO ONZ przyjęło Traktat o całkowitym zakazie prób jądrowych⁶³². Traktat zobowiązywał strony do całkowitego zaprzestania oraz zapobiegania wykonywania prób z bronią nuklearną lub jakichkolwiek innych eksplozji nuklearnych na terytorium podległemu ich jurysdykcji lub kontroli, zarówno tych o charakterze militarnym jak i cywilnym. Pomimo, że Traktat został podpisany przez ponad 180 państwo, to nigdy nie wszedł w życie, ponieważ jego postanowienia wymagają ratyfikacji przez państwa będące członkami Konferencji Rozbrojeniowej, posiadające broń jądrową oraz elektrownie jądrowe⁶³³.

Przyjęcie Traktatu o całkowitym zakazie prób jądrowych zbiegło się w czasie z wydaną przez MTS opinią doradczą w sprawie legalności groźby użycia lub użycia broni nuklearnej z 8 lipca 1996 roku⁶³⁴. W Rezolucji nr 49/75 K ZO ONZ sformułowało zapytanie do MTS czy groźba użycia lub użycie broni jądrowej jest w jakichkolwiek okolicznościach dozwolone na mocy prawa międzynarodowego⁶³⁵. W swojej opinii Trybunał podniósł, że w skrajnych przypadkach samoobrony nie można wykluczyć legalności użycia broni jądrowej, jednak potencjalna legalność powinna być rozstrzygnięta na podstawie skutków użycia broni jądrowej zgodnie z MPH.

W 2017 roku, na podstawie Rezolucji ZO ONZ nr 71/258⁶³⁶, zwołano konferencję, której zadaniem było przyjęcie prawnie wiążącego dokumentu zakazującego broni nuklearnej. Traktat o zakazie broni nuklearnej został zawarty 7 lipca 2017 roku⁶³⁷. Umowa zobowiązuje strony do całkowitego zaprzestania produkowania, testowania, posiadania i gromadzenia broni

⁶³¹ A. Mattelaer, *Nuclear Sharing and NATO as a 'Nuclear Alliance'* w: S. Frühling, A. O'Neil (ed.), *Alliances, Nuclear Weapons and Escalation: Managing Deterrence in the 21st Century*, Australian National University Press, Acton 2021, s. 123-125.

⁶³² Ustawa z dnia 22 stycznia 1999 r. o ratyfikacji Traktatu o całkowitym zakazie prób jądrowych, przyjętego przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 10 września 1996 r., 22.01.1999, Dz. U. z 1999 r., nr 15, poz. 136.

⁶³³ S. Zarychta, *Kontrola zbrojeń i traktaty rozbrojeniowe dotyczące broni jądrowej*, „Rocznik Bezpieczeństwa Morskiego”, 2015, rok IX, cz. IV, s. 299.

⁶³⁴ MTS, *Legality of the threat...*, 1996.

⁶³⁵ ZO ONZ, *Resolution 49/75 K*, 15.12.1994, A/RES/49/75.

⁶³⁶ ZO ONZ, *Resolution 71/258*, 11.01.2017, A/RES/71/258.

⁶³⁷ *Traktat o zakazie broni nuklearnej*, Nowy Jork, 7.07.2017, United Nations Documents A/CONF.229/2017/8.

jądrowej, w tym także rozmieszczania tej broni na terytorium innego państwa. Strony Traktatu zobligowały się również do pomocy osobom, które ucierpiały na skutek użycia lub testowania broni jądrowej. Traktat wszedł w życie 90 dni po złożeniu pięćdziesiątego dokumentu ratyfikacyjnego, tj. 22 stycznia 2021 roku wraz z ratyfikacją traktatu przez Republikę Hondurasu⁶³⁸.

Użycie broni nuklearnej wiąże się tylko z dwoma atakami na Hiroszimę i Nagasaki w 1945 roku, podczas których zniszczeniu uległy całe miasta. Atak szczególnie wpłynął na sektor ochrony zdrowia, który był kluczowy dla zapewnienia opieki medycznej osobom poszkodowanym w wybuchach, a skutki można podzielić na dwie kategorie⁶³⁹. Po pierwsze, w związku z wybuchem bomby jądrowej życie straciła większość personelu medycznego, a szpitale zostały całkowicie zniszczone. Po drugie, nastąpił całkowity paraliż pomocy medycznej. Władze zdecydowały się na organizację tymczasowego szpitala, jednak ze względu na braki w personelu medycznym oraz w sprzęcie medycznym, wielu rannych pozostało bez odpowiedniej opieki. Chociaż w przywołanym przykładzie skutki dotknęły przede wszystkim sektor medyczny, należy pamiętać, że w przypadku ataku nuklearnego wszystkie sektory infrastruktury krytycznej są zagrożone. Użycie broni jądrowej doprowadziłoby do zniszczenia źródeł energii elektrycznej oraz przerwania dostaw z wodą pitną⁶⁴⁰. Co więcej, sama woda pitna, ale także żywność byłaby skażone radioaktywnie. Wszystkie te skutki doprowadziłyby do załamania się podstawowej funkcji infrastruktury krytycznej, czyli bezpieczeństwa państwa i jego obywateli.

4.4.4 Broń zapalająca

Kolejnym środkiem walki wykorzystywanym już od starożytności jest ogień⁶⁴¹. Jego niszczycielski charakter pozwala nie tylko szybko osiągnąć cel wojskowy, ale przede wszystkim wywołać strach i poruszenie u przeciwnika. Do masowego wykorzystania broni zapalającej (w postaci napalmu) dochodziło podczas wojny wietnamskiej⁶⁴², a wojska

⁶³⁸ *Treaty on the Prohibition of Nuclear Weapons (TPNW)*, <https://www.nti.org/education-center/treaties-and-regimes/treaty-on-the-prohibition-of-nuclear-weapons/> (dostęp: 1.03.2026).

⁶³⁹ MKCK, *ICRC report on the effects of the atomic bomb at Hiroshima*, „International Review of the Red Cross”, 2015, vol. 97, no. 899, s. 868-869.

⁶⁴⁰ WHO, *Effects of Nuclear War on Health and Health Services*, Report of the WHO Management Group on Follow-up of Resolution WHA36.28, Geneva 1987, <https://iris.who.int/server/api/core/bitstreams/ba2bd9fd-1d75-4672-a3e9-b66df956ec1f/content> (dostęp: 15.05.2026), par. 69.

⁶⁴¹ M. Piątkowski, *Międzynarodowe prawo humanitarne wobec zastosowania broni zapalającej w konflikcie zbrojnym*, „Bezpieczeństwo – Teoria i Praktyka”, 2017, nr 2, s. 148.

⁶⁴² *Tamże*, s. 149.

izraelskie wykorzystywały biały fosfor do atakowania obiektów zajmowanych przez Hezbollah w Libanie⁶⁴³.

Powszechność w korzystaniu z broni zapalającej spowodowała, że przez długie lata państwa nie podejmowały jakichkolwiek prób zmierzających do utworzenia uniwersalnego zakazu stosowania tej broni. Dopiero wraz z przyjęciem Konwencji CCW broń zapalająca została zakazana na podstawie Protokołu III do Konwencji CCW.

W art. 1 Protokołu III zdefiniowano pojęcie broni zapalającej, za którą rozumie się broń lub amunicję, która zasadniczo przeznaczona jest do powodowania pożarów obiektów lub oparzeń osób wskutek działania płomieniowego lub cieplnego albo obu jednocześnie, wywołanych przez reakcję chemiczną substancji przeniesionych do celu, na przykład poprzez miotacze ognia, fugasy, rakiety czy granaty. Zgodnie z art. 2 Protokołu broń zapalająca nie może być w żaden sposób użyta wobec ludności cywilnej oraz obiektów cywilnych. Co więcej również obiekty wojskowe nie mogą być atakowane przy pomocy broni zapalającej, z wyjątkiem obiektów położonych poza skupiskiem ludności cywilnej.

Infrastruktura krytyczna pozostaje szczególnie narażona na ataki z wykorzystaniem broni zapalającej. W maju 2022 roku wojska rosyjskie ostrzelały ukraińską fabrykę stali w Mariupolu z wykorzystaniem rakiet 9M22S, zawierających w sobie łatwopalną substancję - termit⁶⁴⁴. Broń zapalająca w postaci białego fosforu była również regularnie wykorzystywana do atakowania infrastruktury krytycznej przez izraelskie wojska w Gazie, na przykład 15 stycznia 2009 roku wojska izraelskie ostrzelały szpital Al-Quds w Gazie⁶⁴⁵. W momencie ataku w szpitalu leczono 50 osób, a ponad 500 znalazło w tym miejscu schronienie. Użycie w ostrzale białego fosforu doprowadziło do całkowitego zniszczenia placówki medycznej, pozbawiając tym samym ludność cywilną stałego dostępu do opieki lekarskiej. Kilka dni później izraelskie wojska zaatakowały szkołę podstawową w Beit Lahiya⁶⁴⁶. W momencie ataku szkoła pełniła funkcję tymczasowego schronienia dla 1600 osób.

⁶⁴³ *Lebanon: Israel's White Phosphorous Use Risks Civilian Harm*, <https://www.hrw.org/news/2024/06/05/lebanon-israels-white-phosphorous-use-risks-civilian-harm> (dostęp: 1.03.2026).

⁶⁴⁴ *Russian War Report: Russian forces use incendiary munitions in Mariupol*, <https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-incendiary-munitions-in-mariupol/> (dostęp: 1.03.2026).

⁶⁴⁵ Human Rights Watch, *Rain of Fire Israel's Unlawful Use of White Phosphorus in Gaza*, Report, March 2009, <https://www.hrw.org/reports/iot0309webwcover.pdf> (dostęp: 1.03.2026), s. 39-41.

⁶⁴⁶ *Tamże*, s. 39-41.

4.4.5 Amunicja kasetowa

Amunicja kasetowa stanowi jeden z najpowszechniejszych środków walki używanych w konflikcie zbrojnym. Od czasu II wojny światowej była wykorzystywana we wszystkich największych konfliktach zbrojnych, między innymi podczas alianckich nalotów na Drezno w 1945 roku, amerykańskich nalotów w Azji Południowo-Wschodniej w latach 60. i 70. XX wieku, czy podczas nalotów NATO na Kosowo i Serbię w 1999 roku⁶⁴⁷. Systematyczne użycie amunicji kasetowej w konfliktach zbrojnych sprawiło, że państwa nie były zainteresowane wprowadzeniem uniwersalnego zakazu jej użycia, w odróżnieniu od przedstawicieli organizacji pozarządowych⁶⁴⁸. Jednak długotrwałe negocjacje doprowadziły do przyjęcia w 2008 roku Konwencji o amunicji kasetowej⁶⁴⁹.

W Konwencji amunicję kasetową zdefiniowano jako amunicję konwencjonalną zaprojektowaną do rozpraszania się lub uwalniania ładunków wybuchowych, o masie mniejszej niż 20 kilogramów, i obejmującej te ładunki wybuchowe. Wraz z przyjęciem Konwencji strony zobowiązały się do nieużywania amunicji kasetowej, do zaprzestania opracowywania, produkowania lub pozyskiwania w inny sposób amunicji kasetowej oraz do zaprzestania pomocy czy nakłaniania do angażowania się w jakąkolwiek działalność sprzeczną z postanowieniami Konwencji (art. 1 Konwencji o amunicji kasetowej). Ponadto Konwencja wprowadziła nakaz zniszczenia zapasów amunicji kasetowej (w terminie 8 lat od przystąpienia do Konwencji) oraz oczyszczenia swojego terytorium z niewybuchów (w terminie 10 lat od przystąpienia do Konwencji). Elementem szczególnie zasługującym na uwagę w Konwencji o amunicji kasetowej jest jej artykuł 5 stanowiący o pomocy ofiarom tej broni. Zgodnie z jego treścią strony Konwencji zapewniają szeroko rozumianą pomoc ofiarom amunicji kasetowej, obejmującą między innymi opiekę medyczną, rehabilitację oraz wsparcie psychologiczne.

Pomimo wprowadzenia uniwersalnego systemu przeciwdziałania amunicji kasetowej wiele państw nie przystąpiło do Konwencji, przede wszystkim z powodów biznesowych⁶⁵⁰. Połowa państw produkujących amunicję kasetową, w tym Polska, nie podpisały Konwencji o amunicji kasetowej ze względu na potencjalną utratę korzyści z handlu tą amunicją. Co więcej, sama amunicja jest systematycznie wykorzystywana do rosyjskich ataków na

⁶⁴⁷ J. Borrie, *Banning cluster munitions*, „New Zealand International Review”, 2010, vol. 35, no. 5, s. 3-4.

⁶⁴⁸ B. Docherty, *Breaking New Ground: The Convention on Cluster Munitions and the Evolution of International Humanitarian Law*, „Human Rights Quarterly”, 2009, vol. 31, no. 4, s. 936-937.

⁶⁴⁹ *Konwencja o amunicji kasetowej*, Dublin, 30.05.2008, United Nations Treaty Series, vol. 2688, no. 47713.

⁶⁵⁰ N. van Woudenberg, *The Long and Winding Road Towards an Instrument on Cluster Munitions*, „Journal of Conflict & Security Law”, 2008, vol. 12, no. 3, s. 448-449.

obiekty infrastruktury krytycznej, przede wszystkim sektora energetycznego⁶⁵¹. Użycie amunicji kasetowej w konflikcie zbrojnym stwarza szczególne zagrożenie dla infrastruktury krytycznej, ponieważ ze względu na swoją charakterystykę niemożliwe jest dokonanie rozróżnienia pomiędzy celami wojskowymi a obiektami cywilnymi⁶⁵².

4.5 Podsumowanie

Na podstawie powyższych rozważań należy wskazać, że MPH w precyzyjny sposób określa obowiązki stron w zakresie podejmowanych ataków. Jeżeli strony konfliktu decydują się w pełni wykonywać swoje obowiązki narzucone przez MPH możliwe jest wyeliminowanie skutków ubocznych ataku, a na pewno ich znaczne ograniczenie.

Szczególnie ważne jest to w przypadku ataków wymierzonych w infrastrukturę krytyczną. Atak na obiekty podwójnego zastosowania, jakimi są obiekty infrastruktury krytycznej, z jednej strony przyczyni się do osiągnięcia korzyści wojskowej, jednak z drugiej strony atak może przyczynić się do powstania negatywnych skutków wśród ludności cywilnej. Dlatego każdy atak powinien być indywidualnie rozważany przez pryzmat podstawowych zasad MPH. Co więcej, strona atakująca powinna za każdym razem przeprowadzić proces angażowania celu, zaczynając od prawidłowego wyboru i weryfikacji celu, przez ocenę skutków ataku, aż po wysłanie odpowiednich ostrzeżeń przed atakiem. Tak podjęte działanie pozwoli zminimalizować ryzyko utraty kontroli nad obiektami infrastruktury krytycznej.

Istotnym problemem przy ataku na infrastrukturę krytyczną są również środki walki wybierane przez stronę atakującą. Wykorzystanie broni masowego rażenia czy amunicji kasetowej nie tylko narusza podstawową zasadę MPH jaką jest zasada rozróżniania, ale przede wszystkim realnie wpływa na zagrożenie obiektów infrastruktury krytycznej. Atak z wykorzystaniem takiego uzbrojenia szczególnie zagraża sektorowi medycznemu, który nie tylko może sam stać się celem ataku, ale dostęp do natychmiastowej opieki medycznej może zostać ograniczony ze względu na potencjalną ilość ofiar i poszkodowanych. W związku z tym państwa powinny dążyć nie tylko do opracowywania norm prawnych chroniących infrastrukturę krytyczną, ale także powinny podjąć działania bardziej „praktyczne”. Obejmować to może między innymi zarządzanie kryzysowe, zwiększające odporność obiektów

⁶⁵¹ *Russia using cluster bombs to kill Ukrainian civilians, analysis suggests*, <https://www.theguardian.com/world/2022/apr/21/russia-using-banned-weapons-to-kill-ukrainian-civilians-pictures-suggest> (dostęp: 1.03.2026).

⁶⁵² Pocisk kasetowy zawiera w sobie małe pociski, rozrzucone po całym obszarze. Zob. V. Poposka, A. Nuredin, *Legality of the use of cluster bombs in international law: a short overview*, „Journal of Liberty and International Affairs”, 2024, vol. 10, nr. 1, s. 254.

krytycznych (na przykład działalność kontrwywiadowcza) czy szkolenia personelu obsługującego te obiekty oraz samej ludności cywilnej w zakresie zachowania się przy potencjalnym ataku⁶⁵³.

⁶⁵³ Por. J. Guź, *Rola Agencji Bezpieczeństwa Wewnętrznego w zwalczaniu zagrożeń terrorystycznych na terytorium Rzeczypospolitej Polskiej*, „Studia nad Autorytaryzmem i Totalitaryzmem”, 2015, vol. 37, nr 3, s. 74-75 oraz J. Grębowski, M. Skalski, M. Bijak, *The threat of weapons of mass destruction in the context of the conflict in Ukraine and its impact on battlefield medicine*, „Lekarz Wojskowy” 2025, vol. 103, no. 2, s. 102

5 Skutki niezapewnienia ochrony infrastrukturze krytycznej podczas konfliktu zbrojnego

5.1 Wprowadzenie

MPH zapewnia systemowe ramy ochrony poszczególnych obiektów oraz środowiska naturalnego, jednak państwa żeby skutecznie realizować tę ochronę potrzebują do tego odpowiednich narzędzi. Infrastruktura krytyczna jest jednym z takich narzędzi, a jej uszkodzenie lub zniszczenie wywołuje negatywne skutki zarówno w świecie fizycznym, oddziałując na osoby i środowisko naturalne, ale także w sferze prawnej, implikując odpowiedzialność państwa i jednostki.

Ustalenie skutków niezapewnienia ochrony infrastrukturze krytycznej podczas konfliktu zbrojnego wymaga przeprowadzenia dwuetapowej analizy. W pierwszej części skupiono się na skutkach ataku w sferze zewnętrznej, faktycznie wpływającej na ludność cywilną oraz środowisko naturalne. Analizie poddano ataki skierowane na obiekty szczególnie chronione w MPH, jak obiekty medyczne, dobra niezbędne dla przetrwania ludności cywilnej (przede wszystkim żywność, dostęp do wody pitnej oraz sektor energetyczny), obiekty zawierające niebezpieczne siły (elektrownie jądrowe i zapory wodne), ale także ataki wymierzone w środowisko naturalne. Ostatnia kategoria jest rozpatrywana w kontekście infrastruktury krytycznej i potencjalnych skutków jej ataku, ponieważ w ramach normy art. 55 PD I powinno się rozpatrywać ataki na niektóre obiekty infrastruktury krytycznej, jak szyby naftowe⁶⁵⁴.

Druga część analizy została poświęcona ustaleniu przesłanek odpowiedzialności za ataki wymierzone w infrastrukturę krytyczną podczas konfliktu zbrojnego. W pierwszej kolejności nakreślono przesłanki przypisania winy państwu za działania niezgodne z prawem międzynarodowym. Następnie wskazano potencjalne formy naprawienia szkody powstałej w wyniku ataków nakierowanych na infrastrukturę krytyczną. Dodatkowo ustalono możliwość przypisania odpowiedzialności karnej jednostce, która dopuściła się ataku na infrastrukturę krytyczną. W tym celu analizie poddano przesłanki zbrodni wojennych określonych w art. 8 Statutu MTK.

⁶⁵⁴ P. Grzebyk, *Cele osobowe...*, s. 191.

5.2 Skutki ataku na obiekty infrastruktury krytycznej chronione przez międzynarodowe prawo humanitarne

MPH wskazuje szereg obiektów oraz dóbr, które ze względu na potencjalne skutki ataku podlegają szczególnej ochronie podczas konfliktu zbrojnego. Do kategorii tych obiektów należy zaliczyć:

- obiekty medyczne (art. 25, 26 KG I, art. 36 KG II, art. 20 KG IV, art. 15 ust. 1 PD I, art. 9 ust. 1 PD II),
- pomoc humanitarną (art. 17 ust. 2, art. 71 ust. 2 PD I),
- dobra niezbędne dla przetrwania ludności cywilnej (art. 54 ust. 2 PD I i art. 14 PD II),
- środowisko naturalne (art. 55 PD I), oraz
- obiekty zawierające niebezpieczne siły (art. 56 ust. 1 PD I i art. 15 PD II).

Atak na jakąkolwiek z tych grup powoduje naruszenia międzynarodowego prawa humanitarnego. Jednak sytuacja powyższych obiektów powinna być rozpatrywana nie tylko jako bezpośredni atak na te obiekty, ale również jako ewentualne skutki uboczne ataku na infrastrukturę krytyczną. Oprócz tego na negatywne skutki ataków wymierzonych w infrastrukturę krytyczną, szczególnie narażone są trzy grupy osób: personel medyczny, personel pomocy humanitarnej oraz ludność cywilna.

5.2.1 Skutki ataku na obiekty medyczne i pomoc humanitarną

Udział, a zarazem ochrona obiektów medycznych i personelu medycznego podczas konfliktu zbrojnego leży u podstaw rozwoju MPH. To właśnie zapewnienie specjalistycznej opieki medycznej stanowiło impuls do powołania pierwszej uniwersalnej umowy międzynarodowej regulującej los rannych kombatantów – Konwencji o polepszeniu losu rannych w armiach w polu, która jednocześnie wprowadzała ochronę personelu medycznego⁶⁵⁵.

Zgodnie z obowiązującymi regulacjami międzynarodowymi wszyscy ranni, chorzy, rozbitkowie, niezależnie od tego, do jakiej strony należą powinni być szanowani i chronieni, co powinno przekładać się na natychmiastową pomoc medyczną, obejmującą najszerszy zakres i najszybszy czas leczenia (art. 10 PD I i art. 7 PD II). Dla stron konfliktu nieistotny powinien być status rannych i chorych, ponieważ opieką medyczną powinni objąć zarówno osoby wojskowe oraz cywili, którzy zmagają się z urazami, chorobami lub innymi ułomnościami czy

⁶⁵⁵ M. Goniewicz, K. Goniewicz, *Protection of medical personnel in armed conflicts—case study: Afghanistan*, "European Journal of Trauma and Emergency Surgery", 2013, vol. 39 (2), s. 108.

zakłóceniami czynności fizycznych lub umysłowych (art. 8 lit. a PD I). W celu zapewnienia skutecznego leczenia, strony konfliktu korzystają z wykwalifikowanego personelu medycznego, tak cywilnego, jak i wojskowego, jednak mogą być ponadto wspierane lekarzami organizacji pozarządowych (art. 8 lit. c pkt i-ii PD I). Ochrona została również rozszerzona na jednostki medyczne, w zakres których zaliczyć należy między innym szpitale, ośrodki zaopatrzenia medycznego czy magazyny materiałów medycznych i artykułów farmaceutycznych (art. 8 lit e PD I). Co jest istotne, ochronę sektora służby zdrowia należy wywieść bezpośrednio z zapewnienia ochrony ludności cywilnej, ponieważ personel medyczny, przy prawidłowo zaopatrzonych jednostkach medycznych, odpowiada za ochronę życia i zdrowia osób cywilnych⁶⁵⁶, dlatego dopuszczenie się ataku na sektor opieki zdrowotnej wywołuje negatywne skutki. Po pierwsze, sam personel oraz obiekty medyczne stają się celem ataku, co w świetle MPH stanowi poważne naruszenie prawa. Po drugie, przemoc wobec personelu medycznego i obiektów medycznych powoduje utratę możliwości świadczenia usług zdrowotnych wobec osób szczególnie potrzebujących pomocy⁶⁵⁷.

Rola jaką odgrywa służba zdrowia w systemie bezpieczeństwa państwa wymaga od społeczności międzynarodowej objęcia tego sektora szczególnym nadzorem, przede wszystkim w obliczu konfliktu zbrojnego⁶⁵⁸. W 2019 roku WHO uruchomiło system monitorowania ataków na służbę zdrowia (ang. *surveillance system for attacks on health care, SSA*)⁶⁵⁹. Jego celem jest gromadzenie danych dotyczących ataków na służbę zdrowia działającą na obszarach dotkniętych sytuacjami kryzysowymi, w szczególności konfliktami zbrojnymi. W ramach metodologii działań Systemu WHO stworzyła rozwiniętą definicję ataku na służbę zdrowia⁶⁶⁰. Atak został podzielony na dwie kategorie – atak bezpośredni i pośredni (ang. *direct, indirect*). W ramach ataku bezpośredniego wyróżniono dwa typy:

- ukierunkowany (ang. *targeted*), który oznacza celowy atak na wybrany obszar systemu opieki zdrowia, pośrednio wpływając na jakość i dostępność świadczonych usług medycznych, na przykład: zamach bombowy na placówkę medyczną,

⁶⁵⁶ Y. Sandoz et al., *Commentary to APs...*, s. 124.

⁶⁵⁷ MKCK, *Researching Violence Against Health Care: Gaps and Priorities*, Report, March 2026, <https://healthcareindanger.org/wp-content/uploads/2022/06/elrha-and-icrc-violence-against-health-care-full-report-010720-digital.pdf> (dostęp: 8.04.2026), s. 11.

⁶⁵⁸ RB ONZ, *Resolution 2286 (2016)*, 3.05.2016, S/RES/2286 (2016), s. 4.

⁶⁵⁹ WHO, *Surveillance System for Attacks on Health Care (SSA). Methodology Version 1.0*, Geneva 2018, WHO/WHE/EMO/2019.2/BRO, <https://iris.who.int/server/api/core/bitstreams/6be521b9-cc94-4609-9c50-def0e470a5bb/content> (dostęp: 8.04.2026), s. 3.

⁶⁶⁰ *Tamże*, s. 21.

- nieukierunkowany (ang. *non targeted*), za który rozumie się działanie nieukierunkowane w system opieki zdrowia, ale bezpośrednio wpływające na jakość i dostępność świadczonych usług medycznych, na przykład: lekarz zostaje zabity w incydencie ulicznym, niezwiązanym z jego pracą.

W ramach ataku pośredniego WHO również wskazuje typ ukierunkowany oraz nieukierunkowany. W przypadku tego pierwszego znowu działania mają charakter wymierzony bezpośrednio w wybrany obszar systemu opieki zdrowia, ale pośrednio wpływają na jakość i dostępność świadczonych usług medycznych, na przykład zatrzymanie personelu medycznego ze względu na pełnioną funkcję. Natomiast w przypadku ataku pośredniego ukierunkowanego uważa się, że są to działania pozbawione przemocy i nie są wymierzone w wybrane obszary opieki medycznej. Dodatkowo nie wpływają bezpośrednio na jakość i dostępność świadczonych usług medycznych, na przykład zatrzymanie członka personelu medycznego na punkcie kontrolnym.

Od pierwszego dnia raportowania, tj. 1 stycznia 2020 roku, do 31 marca 2026 roku SSA odnotowała 7990 ataków wymierzonych w służbę zdrowia, co doprowadziło do śmierci prawie 5000 członków personelu medycznego⁶⁶¹. Ponad połowa ataków odbyła się z wykorzystaniem ciężkiego uzbrojenia⁶⁶² i objęła 25 państw (głównie Ukrainę, Palestynę, Liban oraz Mjanmę).

Pomimo szeroko rozwiniętego prawnego systemu ochrony personelu medycznego, ataki stanowią stały element prowadzenia konfliktu zbrojnego, zarówno o charakterze międzynarodowym, jak i niemiędzynarodowym. Jednym z głównych skutków ataków na personel medyczny jest tworzenie się tzw. medycznych pustyni, za które uważa się regiony, w których potrzeby zdrowotne ludności pozostają częściowo lub całkowicie niezaspokojone z powodu braku odpowiedniego dostępu do usług zdrowotnych lub ich niewystarczającej jakości, co wynika z niedoboru kadr medycznych lub placówek, długiego czasu oczekiwania, nieproporcjonalnie wysokich kosztów usług lub innych barier społeczno-kulturowych⁶⁶³. W trwającym od 2023 roku konflikcie zbrojnym pomiędzy sudańską armią a siłami rozłamowymi RSF, personel medyczny jest regularnym celem ataków ze strony RSF. Tylko w 2024 roku śmierć poniosło 66 członków personelu medycznego, w większości byli to

⁶⁶¹ *Surveillance System for Attacks on Health Care (SSA)*, <https://extranet.who.int/ssa/Index.aspx> (dostęp: 8.04.2026).

⁶⁶² SSA za ciężkie uzbrojenie (ang. *heavy weapons*) uważa broń palną, rakiety, bomby, moździerz oraz czołgi.

⁶⁶³ M. G. Brinzac, E. Kuhlmann, G. Dussault, M. I. Ungureanu, R. M. Chereches, C. O. Baba, *Defining medical deserts—an international consensus-building exercise*, „European Journal of Public Health”, 2023, vol. 33 (5), s. 786.

lekarze, pielęgniarki oraz ratownicy medyczni⁶⁶⁴. Skierowanie ataków na personel medyczny doprowadziło do załamania się sudańskiego sektora służby zdrowia. Na podstawie informacji udostępnionych przez sudańskie ministerstwo zdrowia, w związku z konfliktem większość pracowników medycznych zdecydowała się opuścić terytorium Sudanu⁶⁶⁵. Olbrzymie braki kadrowe wśród personelu medycznego, wraz ze zwiększeniem osób rannych w wyniku konfliktu przyczyniły się do rozwoju epidemii cholery⁶⁶⁶.

Odminną sytuację można zaobserwować w Ukrainie, gdzie od rozpoczęcia pełnoskalowej inwazji przez Rosję w 2022 roku dochodzi do regularnych ataków na personel medyczny. W 2024 roku 78 członków personelu medycznego zostało zabitych w rosyjskich atakach⁶⁶⁷. Ukraińscy medycy są celami ataków rosyjskich dronów, rakiet oraz ostrzałów artyleryjskich. Pomimo poważnych problemów z funkcjonowaniem sektora medycznego w początkowych miesiącach inwazji na Ukrainę, obecnie sektor medyczny, w tym personel medyczny wykazuje się dużą odpornością na ataki ze strony Rosji⁶⁶⁸. Według oficjalnych danych w 2024 roku tylko 7% wszystkich placówek medycznych było całkowicie niezdolnych do świadczenia usług medycznych, a 4% placówek ograniczyło świadczenie tych usług.

Chociaż po stronie państwa leży obowiązek zapewnienia skutecznego systemu opieki zdrowotnej, nawet podczas konfliktu zbrojnego, to regularne ataki wymierzone w ten sektor mogą osłabić lub całkowicie wyeliminować zdolności państwa w świadczeniu opieki zdrowotnej⁶⁶⁹, dlatego w konflikty zbrojne często zaangażowane są instytucje oraz organizacje pozarządowe świadczące pomoc humanitarną. Taka pomoc obejmuje dostawy medykamentów, leczenie oraz ewentualną rehabilitację. Pomoc humanitarna stanowi tylko uzupełnienie opieki zdrowotnej i należy pamiętać, że to na władzy państwowej w dalszym ciągu spoczywa obowiązek jej zapewnienia.

MPH nie definiuje pojęcia pomocy humanitarnej, natomiast Instytut Prawa Międzynarodowego zaproponował definicję, zgodnie z którą za pomoc humanitarną uważa się wszelkie działania, przedsięwzięcia oraz zasoby ludzkie i materialne służące dostarczaniu dóbr

⁶⁶⁴ Safeguarding Health in Conflict Coalition, *Epidemic of Violence: Attacks on Health Care in 2024*, Baltimore 2024, <https://insecurityinsight.org/wp-content/uploads/2025/04/2024-SHCC-Annual-Report.pdf> (dostęp: 8.04.2026), s. 27.

⁶⁶⁵ *Tamże*, s. 28.

⁶⁶⁶ *Tamże*.

⁶⁶⁷ *Tamże*, s. 122.

⁶⁶⁸ *Tamże*, s. 123.

⁶⁶⁹ E. Mikos-Skuza, *Pomoc humanitarna w świetle międzynarodowego prawa humanitarnego konfliktów zbrojnych*, w: P. Grzebyk, E. Mikos-Skuza (red.), *Pomoc humanitarna w świetle prawa i praktyki*, Wydawnictwo Naukowe SCHOLAR, Warszawa 2016, s. 39.

i świadczeniu usług o charakterze wyłącznie humanitarnym, niezbędnych do przetrwania i zaspokojenia podstawowych potrzeb ofiar katastrof⁶⁷⁰. Instytut podzielił pomoc humanitarną na dwie kategorie: dóbr oraz usług. Do kategorii dóbr należy zaliczyć przede wszystkim żywność, wodę pitną oraz produkty farmaceutyczne. Natomiast w kategorii usług znajdują się między innymi pomoc medyczna, wsparcie psychologiczne i duchowe, transport. Tak szeroki zakres pomocy humanitarnej znajduje odzwierciedlenie również w doktrynie MPH, gdzie przyjmuje się, że pomoc humanitarna przybiera szerszy zakres niż tylko uzupełnienie pomocy medycznej, co więcej pomoc medyczna została uregulowana w innych przepisach niż pomoc humanitarna⁶⁷¹.

Na podstawie art. 17 PD I i art. 18 PD II personel pomocy humanitarnej podlega takiej samej ochronie jak personel i obiekty medyczne. Strony konfliktu powinny umożliwić działanie na swoim terytorium oraz na terenach okupowanych organizacjom humanitarnym, jak stowarzyszenia Czerwonego Krzyża i Czerwonego Półksiężyca czy inne organizacje pozarządowe. Normy wynikające z art. 71 PD I i art. 18 PD II warunkują jednak udzielenie pomocy humanitarnej od uzyskania zgody strony, na terytorium której pomoc humanitarna będzie świadczona.

Współczesne konflikty zbrojne cechują się odmiennym podejściem do ograniczenia świadczenia pomocy humanitarnej. Przede wszystkim zainteresowane strony wskazują, że personel humanitarny oraz jego wyposażenie i obiekty są wykorzystywane przez drugą stronę konfliktu lub otwarcie z nimi współpracują⁶⁷². Tym samym ataki na personel humanitarny ograniczają dostęp do tej pomocy. Chociaż ograniczenie to, ze względów na bezpieczeństwo państwa wydaje się zgodne z prawem międzynarodowym, to jest ono nadużywane w sposób budzący wątpliwości. Należy zauważyć, że ograniczenie dostępu do pomocy humanitarnej nie zawsze znajduje uzasadnienie w interesie państwa, a raczej jest nieregularną metodą prowadzenia walki. Na początku 2026 roku Biuro Wysokiego Komisarza Narodów Zjednoczonych do spraw Praw Człowieka poinformowało, że z dniem 30 grudnia 2025 roku Izrael przyjął nowe prawo zakazujące działalności ponad 30 organizacjom pozarządowym świadczącym pomoc humanitarną na terytorium Strefy Gazy, co było podyktowane

⁶⁷⁰ International Law Institute, *Sixteenth Commission Humanitarian Assistance. Resolution of The International Law Institute*, 2.09.2003, <https://www.ifrc.org/Docs/idrl/I318EN.pdf> (dostęp: 8.04.2026).

⁶⁷¹ P. Grzebyk, *Cele osobowe...*, s. 188.

⁶⁷² A. P. Marin, R. Ben Ali, *Guilt by association: Restricting humanitarian assistance in the name of counterterrorism*, „International Review of the Red Cross”, 2021, no. 916-917, s. 543-542.

bezpieczeństwem narodowym⁶⁷³. Co więcej, podaje się, że od października 2023 roku siły zbrojne Izraela zabiły ponad 500 pracowników humanitarnych⁶⁷⁴. Działania Izraela polegające na blokowaniu pomocy humanitarnej dla Strefy Gazy doprowadziły do załamania się systemu opieki zdrowia, tym samym pozbawiając ludność terytoriów palestyńskich pomocy medycznej⁶⁷⁵.

Pomimo ochrony MPH personel i obiekty medyczne pozostają celem ataków podczas konfliktu zbrojnego. Wywiera to negatywne skutki szczególnie dla ludności cywilnej, która zostaje odcięta od podstawowej opieki zdrowotnej, tak bardzo potrzebnej podczas konfliktu zbrojnego. Co więcej, również organizacje pomocowe często podają ofiarą działań stron konfliktu. Chociaż sam personel humanitarny nie zawsze jest atakowany w rozumieniu ataku kinetycznego, to pod przykryciem legalnego działania strony konfliktu blokują dostęp do pomocy humanitarnej.

5.2.2 Skutki ataku na dobra niezbędne do przetrwania ludności cywilnej

MPH na podstawie art. 54 ust. 2 PD I i art. 14 PD II wprowadziło ochronę dóbr niezbędnych do przetrwania ludności cywilnej. Za takie dobra uznano przede wszystkim żywność, urządzenia i zbiorniki z wodą pitną oraz urządzenia nawadniające. Ochrona tych dóbr obejmuje nie tylko skutki ataku, skutki wszystkich działań, które doprowadziłyby do ich zniszczenia lub uczynienia nieużytecznymi.

Zapewnienie bezpieczeństwa żywnościowego powinno być rozpatrywane w dwóch aspektach – pozytywnym i negatywnym⁶⁷⁶. Aspekt pozytywny określa „prawo do czegoś”, a więc w tym przypadku będzie się odnosił do prawa do wyżywienia. Regulacje wywodzą się z międzynarodowego prawa praw człowieka. Podstawy prawa do wyżywienia należy szukać już w art. 25 Powszechnej Deklaracji Praw Człowieka z 1948 roku⁶⁷⁷, w której dostęp do wyżywienia został uznany za jedną z podstawowych potrzeb człowieka, wpływającą na jego

⁶⁷³ *Israel: Ban on 37 aid groups makes life unbearable for genocide survivors in Palestine, say UN experts*, <https://www.ohchr.org/en/press-releases/2026/01/israel-ban-37-aid-groups-makes-life-unbearable-genocide-survivors-palestine> (dostęp: 8.04.2026).

⁶⁷⁴ *Tamże*.

⁶⁷⁵ *Safeguarding Health in Conflict Coalition, Epidemic of Violence...*, s. 108.

⁶⁷⁶ Ch. Sova, *Starvation Crimes and International Law: A New Era*, Center for Strategic and International Studies (CSIS), December 2024, s. 2.

⁶⁷⁷ ZO ONZ, *Resolution 217/III A*, 10.12.1948, A/RES/217(III). Deklaracja została przyjęta jako rezolucja ZO ONZ, a więc formalnie nie posiada wiążącego charakteru. Jednak ze względu na jej rozpowszechnione stosowanie przez państwa oraz powoływanie jej postanowień w orzecznictwie przyjmuje się, że Deklaracja stała się prawem zwyczajowym, zob.: W. Czapliński, A. Wyrozumski, *Prawo międzynarodowe publiczne. Zagadnienia systemowe*, Wydawnictwo C.H. Beck, Warszawa 2014, s. 550.

poziom życia. Prawo do wyżywienia zostało następnie powtórzone w art. 11 Międzynarodowego Paktu Praw Gospodarczych, Społecznych i Kulturalnych, na podstawie którego strony Paktu są zobowiązane do zapewnienia każdemu odpowiedniego poziomu życia, włączając w to między innymi wyżywienie. Co więcej, strony Paktu uznają, że każdy człowiek powinien być wolny od głodu, a to zobowiązuje strony do podjęcia współpracy międzynarodowej w celu stworzenia programów obejmujących:

- ulepszenia metod produkcji, konserwacji i dystrybucji żywności przez pełne wykorzystanie wiedzy technicznej i naukowej, przez rozpowszechnianie wiedzy o zasadach żywienia oraz przez rozwijanie lub reformowanie systemów rolnych w taki sposób, aby osiągnąć najbardziej sprawny rozwój i wykorzystanie zasobów naturalnych (art. 11 ust. 2 pkt 1 MPPGSiK);
- zapewnienia sprawiedliwego podziału światowych zasobów żywności stosownie do potrzeb, uwzględniając problemy krajów importujących i krajów eksportujących żywność (art. 11 ust. 2 pkt 2 MPPGSiK).

Należy jednak zauważyć, że zobowiązania wynikające z MPPGSiK są zależne od woli państw, ponieważ zgodnie z art. 2 MPPGSiK państwa będą podejmowały kroki indywidualnie lub we współpracy międzynarodowej, w celu stopniowego osiągnięcia pełnej realizacji praw uznanych w Pakcie. Oznacza to, że prawa wynikające z MPPGSiK cechują się progresywnością, a ich wykonanie jest zależne między innymi od możliwości finansowych państwa⁶⁷⁸.

Natomiast aspekt negatywny w kontekście bezpieczeństwa żywnościowego odnosi się do zakazów, a więc określenia „czego nie można robić”⁶⁷⁹. W tym przypadku kluczową rolę odgrywają normy MPH, a w szczególności art. 54 PD I i art. 14 PD II. Systematyczne ataki bądź niszczenie obiektów składowania żywności, upraw rolnych czy urządzeń uzdatniania wody pitnej mogą zostać uznane za prowadzenie działań zbrojnych z wykorzystaniem zakazanej metody walki jaką jest głód (art. 54 ust. 1 PD I i art. 14 PD II). Długotrwałe stosowanie głodu jako metody walki skutkuje nie tylko trwałym niedożywieniem, ale może również przyczynić się do rozwoju chorób i innych poważnych dolegliwości związanych z brakiem dostępu do najpotrzebniejszych artykułów żywnościowych⁶⁸⁰. W rezolucji nr 2417

⁶⁷⁸ W. Czapliński, A. Wyrozumski, *Prawo międzynarodowe...*, s. 553.

⁶⁷⁹ Ch. Sova, *Starvation Crimes...*, s. 3-4.

⁶⁸⁰ N. Durhin, *Protecting civilians in urban areas: A military perspective on the application of international humanitarian law*, „International Review of the Red Cross”, 2016, vol. 98, iss. 901, s. 180.

z 24 maja 2024 roku RB ONZ wskazała, że w owym czasie 74 miliony osób cierpiało z powodu zagrożenia bezpieczeństwa żywnościowego związanego z konfliktami zbrojnymi⁶⁸¹. Rada jednoznacznie potępiła stosowanie głodu jako metody prowadzenia walki i wskazała, że kryzys bezpieczeństwa żywnościowego może skutkować przymusowymi przesiedleniami.

Pomimo istnienia traktatowego systemu ochrony dóbr niezbędnych do przetrwania ludności cywilnej, przede wszystkim żywności i dostępu do wody pitnej, przeszłe oraz obecne konflikty zbrojne ukazują brak skuteczności w egzekwowaniu tej ochrony. Konflikt zbrojny o charakterze niemiędzynarodowym rozpoczęty w Somali w 1991 roku, w związku z obaleniem dyktatury prezydenta Mohammeda Siad Barre, doprowadził do poważnych zniszczeń w cywilnej infrastrukturze krytycznej, skutkującej między innymi poważnymi niedoborami w żywności⁶⁸². W związku z brakami żywności wielu Somalijczyków zdecydowało się na przesiedlenie na południowe terytoria Somalii oraz do Kenii⁶⁸³. Z badań przeprowadzonych przez MKCK wynika, że w 1992 roku na terenach środkowej i południowej Somalii 95% ludności cierpiało z powodu ogólnego niedożywienia, z czego 75% to przypadki ciężkiego niedożywienia⁶⁸⁴. W celu przeciwdziałania negatywnym skutkom braku żywności w regionie RB ONZ, na podstawie rezolucji nr 751 z 24 kwietnia 1992 roku, podjęła decyzję o utworzeniu misji pokojowej UNOSOM I⁶⁸⁵. Jej celem było rozmieszczenie nieuzbrojonych obserwatorów wojskowych ONZ, których zadaniem było nadzorowanie zawieszenia broni w Somali oraz zabezpieczenie dostaw pomocy humanitarnej i żywności. Rok później, wraz z wygaśnięciem mandatu UNOSOM I, Rada na mocy rezolucji nr 814 z 26 marca 1993 roku utworzyła kolejną misję pokojową UNOSOM II⁶⁸⁶. Zadania misji skupiały się między innymi na pomocy w odbudowie infrastruktury Somalii oraz jej potencjału gospodarczego oraz na wsparciu w repatriacji osób przesiedlonych w Somalii.

Obecnie głód jako metoda walki jest szeroko stosowana przez Izrael w Strefie Gazy. Od października 2023 r. wojska izraelskie regularnie blokują dostawy żywności do Strefy Gazy⁶⁸⁷. Świadcowie zeznawali, że brakowało dla nich wystarczającej ilości wyżywienia, musieli też udać się kilka kilometrów po wodę pitną. Zgodnie z informacjami przekazanymi

⁶⁸¹ RB ONZ, *Resolution 2417 (2018)*, 24.05.2024, S/RES/2417 (2018).

⁶⁸² *Starvation and Terror in Somalia*, Foreign Policy Bulletin, 1992, vol. 3, iss. 2, s. 22.

⁶⁸³ *Tamże*.

⁶⁸⁴ *Tamże*.

⁶⁸⁵ RB ONZ, *Resolution 751 (1992)*, 24.04.1992, S/RES/751 (1992).

⁶⁸⁶ RB ONZ, *Resolution 814 (1993)*, 26.03.1993, S/RES/814 (1993).

⁶⁸⁷ *Israel: Starvation Used as Weapon of War in Gaza*, <https://www.hrw.org/news/2023/12/18/israel-starvation-used-weapon-war-gaza> (dostęp: 8.04.2026).

przez Światowy Program Żywnościowy przez pierwszy miesiąc konfliktu (od października do listopada 2023 roku) do Strefy Gazy dotarło tylko 10% dostaw żywności⁶⁸⁸. Utrzymujące się ataki na infrastrukturę związaną z wyżywieniem oraz wodą pitną mogą prowadzić do wzrostu zachorowań oraz zwiększać niedożywienie wśród ludności cywilnej⁶⁸⁹. Na początku 2024 roku Minister Zdrowia Strefy Gazy poinformował, że w szpitalu im. Nassera odnotowano śmierć 8 pacjentów w związku brakiem dostępu do tlenu, ponadto placówka znajdowała się pod oblężeniem sił zbrojnych Izraela, co skutkowało brakiem dostępu do żywności i wody pitnej przeznaczonej dla pacjentów⁶⁹⁰. 13 marca 2024 roku wojska izraelskie przeprowadziły atak na centrum dystrybucji żywności prowadzone przez Agencję Narodów Zjednoczonych dla Pomocy Uchodźcom Palestyńskim na Bliskim Wschodzie (UNRWA) powodując śmierć kilku pracowników Agencji oraz raniąc ponad 20 osób⁶⁹¹. Komisarz Generalny UNRWA podał, że atak zniszczył jeden z ostatnich centrów dystrybucyjnych żywności, czego skutkiem będzie pogłębienie się klęski głodowej w Strefie Gazy.

Poważnym zagrożeniem dla ludności cywilnej podczas konfliktu zbrojnego jest również ograniczenie dostępu do wody pitnej. Tak samo jak prawo do wyżywienia, prawo do świeżej wody jest uznawane za jedno z podstawowych praw człowieka⁶⁹². Działania zbrojne zagrażają instalacjom i urządzeniom zaopatrującym w wodę pitną. Dotyczy to przede wszystkim bezpośredniego ataku na te cele. Jednak należy również zwrócić uwagę na czas trwania konfliktu zbrojnego. Jego wydłużenie sprzyja regularnym atakom na urządzenia z wodą pitną, tym samym doprowadzając do załamania się tego systemu⁶⁹³. Jak pokazuje praktyka konfliktów zbrojnych, brak dostępu do wody pitnej może powodować śmierć takiej samej liczby osób jak w przypadku użycia konkretnego rodzaju broni⁶⁹⁴. W celu przeciwdziałania atakom na urządzenia zapewniające dostęp do wody pitnej, społeczność międzynarodowa, wielokrotnie podejmowała próby opracowania zasad regulujących sytuację dostępu do wody w konflikcie zbrojnym. Jednym z przykładów są Berlińskie Zasady dotyczące Zasobów

⁶⁸⁸ *Gaza faces widespread hunger as food systems collapse, warns WFP*, <https://www.wfp.org/news/gaza-faces-widespread-hunger-food-systems-collapse-warns-wfp> (dostęp: 8.04.2026).

⁶⁸⁹ MKCK, *Food Security and Armed Conflict*, Policy Brief, Geneva 2022, https://www.developmentaid.org/api/frontend/cms/file/2022/10/4662_002-ebook.pdf (dostęp: 8.04.2026), s. 4

⁶⁹⁰ *UNRWA Situation Report #80 on the situation in the Gaza Strip and the West Bank, including East Jerusalem*, <https://www.unrwa.org/resources/reports/unrwa-situation-report-80-situation-gaza-strip-and-west-bank-including-east-jerusalem> (dostęp: 8.04.2026).

⁶⁹¹ *At least one UNRWA staff killed when Israeli Forces hit UNRWA centre used for food and lifesaving supplies*, <https://www.unrwa.org/newsroom/official-statements/least-one-unrwa-staff-killed-when-israeli-forces-hit-unrwa-centre-used> (dostęp: 8.04.2026).

⁶⁹² *Letter dated 8 July 2025 from the Permanent Representative of Slovenia to the United Nations addressed to the Secretary-General*, 9 July 2025, S/2025/453, s. 8.

⁶⁹³ *Tamże*.

⁶⁹⁴ P. Grzebyk, *Cele osobowe...*, s. 186.

Wodnych (BZZW), przyjęte przez Stowarzyszenie Prawa Międzynarodowego w 2004 roku⁶⁹⁵. W BZZW sformułowano zobowiązania dla stron konfliktu dotyczące relacji działań zbrojnych z zasobami wodnymi. Zobowiązania obejmują między innymi zakaz zatruwania oraz czynienia niezdatnym do użytku w jakikolwiek inny sposób wody niezbędnej do przetrwania ludności cywilnej (art. 50 BZZW) czy zakaz atakowania, niszczenia, usuwania lub unieruchamiania zasobów wodnych i instalacji wodnych niezbędnych dla zdrowia i przetrwania ludności cywilnej, jeżeli można oczekiwać, że takie działania pozostawią ludność cywilną z tak niewystarczającą ilością wody, że spowoduje to jej śmierć z powodu braku wody lub zmusi ją do przemieszczenia się (art. 51 ust. 2 BZZW).

W związku z tym, że katalog dóbr niezbędnych do przetrwania ludności cywilnej zawarty w art. 54 ust. 2 PD I i art. 14 PD II ma charakter otwarty, przyjęto również możliwość zakwalifikowania do tych dóbr sektora energetycznego, którego prawidłowe działanie wpływa bezpośrednio na bezpieczeństwo ludności cywilnej, poprzez dostarczanie światła oraz ciepła do domostw⁶⁹⁶.

Jednak sam status sektora energetycznego podczas konfliktu zbrojnego nie jest jednoznaczny, co wynika z podwójnego przeznaczenia obiektów energetycznych. W 1956 roku MKCK przyjęło Projekt Zasad dotyczących ograniczenia zagrożeń dla ludności cywilnej w czasie wojny (ang. *Draft Rules for the Limitation of the Dangers incurred by the Civilian Population in Time of War*)⁶⁹⁷. Zgodnie z art. 7 ust. 2 Projektu za cele wojskowe w konflikcie zbrojnym należy uznać tylko takie obiekty, które ze względu na swoje zasadnicze cechy są powszechnie uznawane za mające znaczenie wojskowe. Konkretnie kategorie tych obiektów wymieniono w załączniku do Projektu i zaliczono do nich między innymi obiekty wytwarzające energię głównie na potrzeby obrony narodowej, np. z węgla, innych paliw lub energii jądrowej, oraz zakłady produkujące gaz lub energię elektryczną głównie na potrzeby wojskowe⁶⁹⁸. W przypadku kiedy infrastruktura energetyczna jest bezsprzecznie wykorzystywana dla celów wojskowych staje się legalnym celem ataku. Tym samym historia ataków na infrastrukturę energetyczną podczas konfliktu zbrojnego jest bardzo bogata⁶⁹⁹.

⁶⁹⁵ International Law Association, *Berlin Rules on Water Resources*, International Law Association Berlin Conference (2004), https://www.cawater-info.net/library/eng/1/berlin_rules.pdf (dostęp: 8.04.2026).

⁶⁹⁶ Y. Sandoz et al., *Commentary to APs...*, s. 655.

⁶⁹⁷ MKCK, *Draft Rules for the Limitation of the Dangers incurred by the Civilian Population in Time of War*, 1956, <https://ihl-databases.icrc.org/assets/treaties/420-Draft-ICRC-Rules-1956-EN.pdf> (dostęp: 8.04.2026).

⁶⁹⁸ Y. Sandoz et al., *Commentary to APs...*, s. 632.

⁶⁹⁹ J. W. Crawford, *The Law of Noncombatant Immunity and the Targeting of National Electrical Power Systems*, „The Fletcher Forum of World Affairs”, 1997, vol. 21, no. 2, s. 101.

Jednak należy pamiętać, że bezpieczeństwo sektora energetycznego bezpośrednio wpływa również na bezpieczeństwo ludności cywilnej. Infrastruktura energetyczna wywiera podwójny wpływ na ludność cywilną. Po pierwsze, energia elektryczna jest niezbędna do prawidłowego działania dóbr niezbędnych do przetrwania ludności cywilnej, jak wodociągi czy urządzenia sanitarne, ale także obiekty medyczne⁷⁰⁰. Po drugie, w warunkach zimowych sektor energetyczny jest niezbędny dla dostarczania ciepła.

Infrastruktura energetyczna stała się regularnym celem ataków podczas pełnoskalowej inwazji rosyjskiej na Ukrainę od 2022 roku⁷⁰¹. W okresie od października 2022 roku do lutego 2023 roku wojska rosyjskie przeprowadziły co najmniej 13 ataków na elektrownie energetyczne, obejmujące swym zasięgiem 19 na 24 regiony Ukrainy. Ataki doprowadziły do śmierci ponad 100 cywilów, a prawie 400 cywilów zostało rannych. Przeciętne ukraińskie gospodarstwo domowe, w okresie pomiędzy październikiem a grudniem 2022 roku, pozostawało bez dostępu do energii elektrycznej łącznie przez pięć tygodni⁷⁰². Ataki na infrastrukturę energetyczną wywołują obszerne skutki zarówno dla działalności państwa (zakłócenia w dostawie wody, ogrzewania centralnego, transportu publicznego)⁷⁰³, ale również wpływają bezpośrednio na ludność cywilną (ograniczenia w gotowaniu, sprzątaniu czy przechowywaniu żywności, dodatkowo osoby zamieszkujące wieżowce, a zmagające się z trudnościami w poruszaniu zostały pozbawione możliwości korzystania z wind)⁷⁰⁴.

Ataki wymierzone w dobra niezbędne dla przetrwania ludności cywilnej stanowią poważne zagrożenie dla bezpieczeństwa cywilów podczas konfliktu zbrojnego. Szczególnie narażone na działania zbrojne są dobra związane z wyżywieniem oraz dostępem do wody pitnej. Przykłady bieżących konfliktów zbrojnych pokazują, że stosowanie głodu jako metody prowadzenia wojny staje się regularną praktyką mającą na celu obniżenia morale strony przeciwnej. Również ataki na sektor energetyczny implikują poważne skutki dla ludności

⁷⁰⁰ International Bank for Reconstruction and Development, *Joining Forces to Combat Protracted Crises. Humanitarian and Development Support for Water and Sanitation Providers in the Middle East and North Africa*, Washington D.C. 2021, https://www.icrc.org/sites/default/files/document_new/file_list/joining_forces_to_combat_protracted_crisis.pdf (dostęp: 8.04.2026), s. 38.

⁷⁰¹ OHCHR, *Attacks on Ukraine's Energy Infrastructure: Harm to the Civilian Population*, Bulletin, September 2024, s. 2.

⁷⁰² *Tamże*.

⁷⁰³ *Tamże*.

⁷⁰⁴ *Tamże*.

cywilnej. Strony konfliktu powinny jednak pamiętać o podstawowych obowiązkach wynikających z MPH, a przede wszystkim bezpieczeństwie ludności cywilnej⁷⁰⁵.

5.2.3 Skutki ataku na obiekty zawierające niebezpieczne siły

Katalog obiektów zawierających niebezpieczne siły został ustalony w art. 56 ust. 1 PD I i art. 15 PD II. W przeciwieństwie do dóbr niezbędnych do przetrwania ludności cywilnej, katalog obiektów zawierających niebezpieczne siły ma charakter zamknięty i składa się z trzech budowli: zapór, grobli oraz elektrowni jądrowych. Atak skierowany na jakikolwiek z tych obiektów może spowodować wyzwolenie niebezpiecznych sił (promieniowanie lub olbrzymie ilości wody) i tym samym skutkować poważnymi stratami wśród ludności cywilnej, dlatego żaden z tych obiektów co do zasady nie może być celem ataku, nawet jeśli stanowiłby cel wojskowy. Jednak w przypadku konfliktu zbrojnego o charakterze międzynarodowym (art. 56 ust. 2 PD I) wprowadzono pewne ograniczenia w zakresie ochrony obiektów zawierających niebezpieczne siły. Zapory i groble mogą stać się celem ataku, jeżeli są używane do innych celów niż ich normalne przeznaczenie i do regularnego, istotnego i bezpośredniego wsparcia operacji wojskowych oraz gdy atak jest jedynym możliwym środkiem mogącym spowodować ustanie takiego wsparcia (art. 56 ust. 2 lit. a PD I). Natomiast elektrownia jądrowa może stać się legalnym celem ataku, jeśli dostarcza prąd elektryczny dla regularnego, istotnego i bezpośredniego wsparcia operacji wojskowych oraz jeżeli atak jest jednym możliwym środkiem do spowodowania ustania takiego wsparcia (art. 56 ust. 2 lit. b PD I). Należy tutaj zaznaczyć, że ochrona ludności cywilnej i obiektów cywilnych pozostaje dalej w mocy, nawet jeśli dochodzi do ataku na któryś z powyższych obiektów. W takim przypadku strony konfliktu powinny powziąć odpowiednie środki ostrożności przewidziane w art. 57 PD I (art. 56 ust. 3 PD I).

W historii konfliktów zbrojnych elektrownie jądrowe wielokrotnie stawały się celami ataków. W 1980 roku, w trakcie konfliktu zbrojnego pomiędzy Iranem a Irakiem, siły irańskie zbombardowały irański ośrodek badawczy Osirak, niszcząc wiele budynków, jednak sam reaktor nie został zniszczony⁷⁰⁶. W 2010 roku irańskie władze poinformowały o wykryciu złośliwego oprogramowania w systemie ośrodka nuklearnego w Natanz⁷⁰⁷. Oprogramowanie,

⁷⁰⁵ E. Wicks, *The Meaning of 'Life': Dignity and the Right to Life in International Human Rights Treaties*, „Human Rights Law Review”, 2012, vol. 12, iss. 2, s. 219.

⁷⁰⁶ SIPRI, *Nuclear Security During Armed Conflict: Lessons from Ukraine*, Policy Paper, 2023, s. 3.

⁷⁰⁷ R. Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, „Journal of Conflict & Security Law”, 2012, vol. 17, iss. 2, s. 219.

nazwane „Stuxnet”, miało pokazywać fałszywe informacje o prędkości wirników doprowadzając do uszkodzenia reaktora.

Jednak dopiero po 2022 roku miała miejsce wzmożona dyskusja na temat ochrony obiektów jądrowych podczas konfliktu zbrojnego. Zwiększenie efektywności ochrony elektrowni jądrowych było związane z regularnymi atakami rosyjskimi na ukraińskie obiekty jądrowe. W ciągu pierwszego roku konfliktu, od lutego 2022 roku do lutego 2023 roku, Rosja zaatakowała pięć ukraińskich elektrowni jądrowych: w Czarnobylu, w Chmielnickim, w Równym, w Zaporozżu oraz w Mikołajowie⁷⁰⁸. Każdy z tych ataków doprowadził do zerwania linii przesyłowej, tym samym powodując zakłócenia w dostawie energii elektrycznej. W odpowiedzi na te ataki, Dyrektor Generalny MAEA wskazał siedem filarów, których przestrzeganie gwarantuje bezpieczeństwo nuklearne podczas konfliktu zbrojnego⁷⁰⁹. Zaliczono do nich:

1. integralność fizyczną – integralność obejmuje reaktory, baseny na paliwo oraz magazyny odpadów radioaktywnych. Kierowanie ataków na obiekty elektrowni jądrowych może doprowadzić do uszkodzenia jej budynków i infrastruktury, a także realnie wpływać na wystąpienie incydentu lub awarii jądrowej;
2. bezpieczeństwo i ochrona sprzętu oraz systemów – wszystkie sprzęty oraz systemy działające w ramach elektrowni jądrowej muszą pozostawać sprawne cały czas. Podejmowanie działań zbrojnych w okolicach elektrowni jądrowej destabilizuje bezpieczeństwo tego obiektu. Prowadzenie ostrzału elektrowni jądrowej może uszkodzić krytyczne systemy obiektu, doprowadzając do negatywnych skutków radiologicznych;
3. zespół operacyjny – zespół pracujący w elektrowni jądrowej musi być zdolny do zapewnienia bezpieczeństwa elektrowni jądrowej. Ciągły ostrzał obiektu oraz obecność sił zbrojnych na jego terenie mogą wywierać negatywne skutki na działania zespołu operacyjnego elektrowni jądrowej. Ciągły stres oraz niepokój zwiększa ryzyko wystąpienia błędu ludzkiego, wpływając na możliwość wystąpienia zagrożenia radiologicznego;

⁷⁰⁸ SIPRI, *Nuclear Security...*, s. 2.

⁷⁰⁹ MAEA, *Nuclear Safety, Security and Safeguards in Ukraine. February 2022–February 2023*, <https://www.iaea.org/sites/default/files/documents/nuclear-safety-security-and-safeguards-in-ukraine-feb-2023.pdf> (dostęp: 8.04.2026), s. 6-7.

4. zasilanie zewnętrzne – obiekty jądrowe powinny mieć alternatywną, zewnętrzną sieć zasilania. Zapewnienie zewnętrznego źródła zasilania zmniejsza szansę wystąpienia incydentu radiologicznego związanego z wyłączeniem reaktorów jądrowych;
5. łańcuch dostaw – należy zapewnić nieprzerwany łańcuch dostaw do elektrowni jądrowej wszystkich elementów, które wpływają na prawidłowe działanie obiektu i jego ewentualną naprawę;
6. systemy monitorowania promieniowania oraz gotowość i reagowanie na sytuacje awaryjne – zespół elektrowni jądrowej musi być przygotowany na wystąpienie sytuacji awaryjnych, które bezpośrednio lub pośrednio mogą wpływać na prawidłowe działanie obiektu, na przykład uszkodzenie zasilania elektrowni lub uszkodzenie pozostałej infrastruktury krytycznej;
7. komunikację – zespół obsługujący elektrownię jądrową powinien posiadać ciągły i stabilny system komunikacji z władzami publicznymi (na każdym szczeblu zarządzania). Brak odpowiedniej komunikacji może wpłynąć na utratę kontroli nad obiektem.

Pomimo ustalenia przejrzystego planu działania, Siedem Filarów jest stosowane w ograniczonym zakresie. ZO ONZ wystosowało zalecenia do obu stron konfliktu o jak najszybsze wprowadzenie filarów w życie, co pozwoli zabezpieczyć ukraińskie elektrownie jądrowe⁷¹⁰.

Kolejnym zagrożeniem dla bezpieczeństwa ludności cywilnej jest uszkodzenie lub zniszczenie zapory wodnej. Wykorzystanie w konflikcie zbrojnym żywiołu jakim jest woda, jest metodą znaną już od starożytności, to jednak działania zbrojne w tym kierunku przybierają przede wszystkim postać zatrucia źródła wody czy niszczenia obiektów i urządzeń poboru lub uzdatniania wody⁷¹¹.

W historii konfliktów zbrojnych ataki wymierzone w zapory wodne były stosowane w ograniczony sposób, jednakże ich skutki były poważne i rozległe. Podczas II wojny światowej brytyjskie wojska przeprowadziłyby operacje bombardowania niemieckich tam⁷¹². Na skutek przerywania zapór wodnych ponad tysiąc niemieckich cywilów straciło życie.

⁷¹⁰ ZO ONZ, *Safety and security of nuclear facilities of Ukraine, including the Zaporizhzhia nuclear power plant*, 5.07.2024, A/78/L.90.

⁷¹¹ Ch. Kohler, *An Ancient Practice with a New Face: The Use of Water as a Weapon in Times of Climate Change*, Peace Research Institute Frankfurt, Frankfurt 2020, s. 1.

⁷¹² A. Szpak, *The Use of Water as a Weapon Under International Humanitarian Law with Special Emphasis on the Destruction of the Nova Kakhovka Dam*, „Studia Iuridica”, 2024, vol. 103, s. 63.

Do tragicznego w skutkach ataku na zaporę wodną doszło w 1938 roku podczas Drugiej Wojny Chińsko-Japońskiej⁷¹³. Na skutek zniszczenia tamy na Żółtej Rzece przez grupę chińskich nacjonalistów śmierć poniosło prawie 900 tysięcy cywilów (w konsekwencji zniszczenia domostw, zanieczyszczenia wody, braku dostępu do żywności). Dodatkową konsekwencją było przesiedlenie od trzech do dwunastu milionów osób. Również we współczesnych konfliktach zbrojnych dochodzi do atakowania tam. 6 czerwca 2023 roku przerwana została zapora wodna w Nowej Kachowce w Ukrainie⁷¹⁴. W wyniku przedostania się olbrzymich ilości wody śmierć poniosły 84 osoby⁷¹⁵, a ponad 4 tysiące musiało zostać przesiedlonych⁷¹⁶. Zniszczenie zapory skutkowało ograniczeniem dostępu do czystej wody oraz do energii elektrycznej i gazu⁷¹⁷.

Jak pokazują powyższe przykłady skierowanie ataku na zapory wodne oraz tamy grozi poważnymi i rozległymi konsekwencjami po stronie ludności cywilnej. Przede wszystkim uwolnienie w jednej chwili tak dużych ilości wody prowadzi do natychmiastowej powodzi, która zagraża bezpośrednio życiu i zdrowiu cywili⁷¹⁸. Powódź przynosi również długotrwałe skutki pośrednie. W głównej mierze będzie to dotyczyło bezpieczeństwa żywnościowego. Wskazuje się, że powódź może doprowadzić do strat lub uszkodzeń w uprawach rolnych oraz żywym inwentarzu, ale także zanieczyszczać wody gruntowe⁷¹⁹. Wystąpienie skutków w postaci naruszenia bezpieczeństwa żywnościowego stanowi podstawę do wskazania art. 54 ust. 2 PD I i art. 14 PD II jako dodatkowego naruszenia MPH atakiem ukierunkowanym na zapory wodne⁷²⁰. Co więcej, systematyczne niszczenie infrastruktury krytycznej w postaci między innymi zapór wodnych pogłębia kryzys humanitarny oraz pozbawia ludność cywilną stabilnych źródeł utrzymania⁷²¹.

Ataki skierowane w obiekty zawierające niebezpieczne siły są poważnym zagrożeniem dla bezpieczeństwa ludności cywilnej. Obranie za cel zapór wodnych może przyczynić się nie tylko do śmierci cywilów, ale również obejmuje wiele skutków pośrednich, jak naruszenie

⁷¹³ *Tamże*.

⁷¹⁴ United Nations Environment Programme, *Rapid Environmental Assessment of Kakhovka Dam Breach*, Nairobi 2023, <https://wedocs.unep.org/rest/api/core/bitstreams/d16d8f8a-ee13-463e-b051-448ddbf1577e/content> (dostęp: 8.04.2026), s. 6

⁷¹⁵ *Dwa lata od zniszczenia zapory w Nowej Kachowce. Oto skutki ekobójstwa*, <https://energetyka24.com/klimat/wiadomosci/dwa-lata-od-zniszczenia-zapory-w-nowej-kachowce-oto-skutki-ekobojstwa> (dostęp: 8.04.2026).

⁷¹⁶ United Nations Environment Programme, *Rapid Environmental Assessment...*, s. 6

⁷¹⁷ *Tamże*.

⁷¹⁸ A. Szpak, *The Use of Water...*, s. 69.

⁷¹⁹ C. Reed, W. Anderson, A. Kruczkiewicz, J. Nakamura, D. Gallo, R. Seager, S. S. McDermid, *The impact of flooding on food security across Africa*, „Proceedings of the National Academy of Sciences of the United States of America”, 2022, vol. 119 (43), s. 1.

⁷²⁰ P. Grzebyk, *Cele osobowe...*, s. 179.

⁷²¹ RB ONZ, *Protection of civilians in armed conflict*, 22.05.2024, S/PV.9921.

bezpieczeństwa żywnościowego czy uszkodzenie sektora energetycznego. Szczególnym rodzajem zagrożenia jest atak skierowany w elektrownię jądrową. Niebezpieczna siła w postaci skażenia radiologicznego wywiera negatywne skutki nie tylko wobec ludzi, ale również dla środowiska naturalnego.

5.2.4 Skutki ataku na środowisko naturalne

Środowisko naturalne pozostaje pod ochroną MPH na podstawie art. 55 PD I, która obejmuje przeciwdziałanie rozległym, długotrwałym i poważnym szkodami w środowisku naturalnym. Warunkiem koniecznym dla uznania ochrony z art. 55 PD I jest wystąpienie powyższych przesłanek kumulatywnie⁷²². Co więcej, zakazane jest stosowanie metod lub środków walki, które wywołując rozległe, długotrwałe i poważne szkody mogłyby zagrozić zdrowiu lub przetrwaniu ludności. Wskazuje się, że zwrot „zdrowie” został ujęty tutaj w kontekście przyszłościowym potencjalnych skutków, na przykład powodując zwyrodnienia lub wady wrodzone⁷²³.

Konieczność usprawnienia ochrony środowiska naturalnego uwidocznili konflikt zbrojny w Zatoce Perskiej z lat 1990-1991. W celu powstrzymania wsparcia międzynarodowego dla Kuwejtu, Saddam Husajn wystosował groźby wypuszczenia kuwejckiej ropy do morza⁷²⁴. W związku z rozpoczęciem operacji Pustynna Burza prezydent Iraku zrealizował swoją groźbę, doprowadzając do wycieku 460 milionów galonów ropy naftowej do Zatoki Perskiej. Konsekwencje wycieku były rozległe, a jego największymi ofiarami padły zwierzęta morskie Zatoki. Oprócz wycieków ropy do morza, armia irakijska prowadziła kampanię podpalania kuwejckich odwiertów naftowych, powodując ich zniszczenie w około 85%⁷²⁵. Na skutek pożarów do powietrza przedostało się 50 tysięcy ton dwutlenku siarki, 100 tysięcy ton węgla w postaci sadzy oraz 800 tysięcy ton dwutlenku węgla. Zanieczyszczenie powietrza taką ilością związków chemicznych było przyczyną choroby układu oddechowego mieszkańców Kuwejtu oraz nietypowych zjawisk pogodowych, jak czarny deszcz lub śnieg. Chociaż działania Saddama Husajna spotkały się ze stanowczą reakcją

⁷²² P. Grzebyk, *Cele osobowe...*, s.190-191.

⁷²³ Y. Sandoz et al., *Commentary to APs...*, s. 663-664.

⁷²⁴ K. Hulme, *Armed Conflict, Wanton Ecological Devastation and Scorched Earth Policies: How the 1990-91 Gulf Conflict Revealed the Inadequacies of the Current Laws to Ensure Effective Protection and Preservation of the Natural Environment*, „Journal of Armed Conflict Law”, 1997, vol. 2, no. 1, s. 46.

⁷²⁵ *Tamże*.

ze strony społeczności międzynarodowej, to po raz kolejny uwidocznił się problem egzekwowania ochrony przewidzianej w MPH⁷²⁶.

Wprowadzenie w art. 56 ust. 1 PD I zamkniętego katalogu obiektów zawierających niebezpieczne siły nie pozwala na objęcie ochroną tej normy zakładów chemicznych. Dlatego norma wynikająca z art. 55 PD I, przy łącznym spełnieniu przesłanek rozległości, długotrwałości oraz poważności skutków, może zostać również wykorzystana do ochrony obiektów chemicznych w trakcie konfliktu zbrojnego. Praktyka obecnych konfliktów zbrojnych pokazuje, że ośrodki chemiczne równie często jak inne obiekty, w tym elektrownie jądrowe stają się celami ataku.

W 2022 roku rosyjskie wojska co najmniej trzy razy dopuściły się ataków na ukraińskie zakłady chemiczne⁷²⁷. W marcu zaatakowano zakłady chemiczne Sumychimprom, co spowodowało uwolnienie się toksycznego gazu amoniakowego. W maju rosyjskim celem była fabryka nawozów w Iziumie, co skutkowało uwolnieniem kwasu azotowego. Najpoważniejszy atak miał miejsce w czerwcu na zakłady chemiczne Azot w Siewierodonecku. Ostrzał zakładów doprowadził do wybuchu pożaru, który potencjalnie mógł uwolnić toksyczne związki chemiczne do powietrza⁷²⁸.

Działania podejmowane przez społeczność międzynarodową zwiększające ochronę środowiska naturalnego w czasie pokoju, powinny skłaniać te same strony do podejmowania co najmniej tego samego zakresu ochrony podczas konfliktu zbrojnego. Należy zauważyć, że wymagania stawiane przez art. 55 PD I względem ochrony środowiska cechuje bardzo wysoki próg zastosowania. Warunki, którym powinny sprostać strony konfliktu są rygorystyczne, jednocześnie ich treść i zakres pozostają nieprecyzyjne⁷²⁹. Niemniej państwa powinny pamiętać, że poszanowanie środowiska naturalnego jest jednym z elementów oceny zgodności działania z zasadą konieczności, a więc każde ich działanie, potencjalnie oddziałujące na środowisko naturalne, powinno być oceniane w kontekście konieczności i proporcjonalności osiągniętych celów wojskowych⁷³⁰.

⁷²⁶ ZO ONZ, *Resolution 47/37*, 9.02.1993, A/RES/47/37.

⁷²⁷ K. Burck, S. Veini, *Attacks on chemical and nuclear facilities in Ukraine—legal frameworks and protections*, „Journal of Conflict & Security Law”, 2023, vol. 30, s. 329.

⁷²⁸ *Tamże*.

⁷²⁹ MTKJ, *Final Report...*, § 15.

⁷³⁰ MTS, *Legality of the threat...*, par. 30.

5.3 Odpowiedzialność za atak na infrastrukturę krytyczną

Ataki na obiekty medyczne, pomoc humanitarną, dobra niezbędne do przetrwania ludności cywilnej, obiekty zawierające niebezpieczne siły lub skutkujące poważnymi szkodami w środowisku naturalnym stanowią naruszenie postanowień konwencji genewskich oraz protokołów dodatkowych.

W KG wyróżniono dwa typy naruszeń: ciężkie naruszenia (ang. *grave breaches*) oraz wszystkie inne, które nie zostały precyzyjnie zdefiniowane⁷³¹. W przypadku ciężkich naruszeń strona konfliktu nie tylko ma obowiązek zaprzestania tych naruszeń, ale przede wszystkim powinna dążyć do zidentyfikowania i ukarania sprawcy⁷³². Natomiast w przypadku pozostałych naruszeń KG na stronach konfliktu spoczywa jedynie obowiązek zaprzestania naruszeń, bez konieczności odszukania i ukarania ich sprawcy. Różnice w konsekwencjach egzekwowania poszczególnych naruszeń prowadzą do powstania luki prawnej, co może przyczynić się do ograniczonego przeciwdziałania innym naruszeniom niż ciężkie⁷³³.

Również w PD I zdecydowano się na wprowadzenie dualizmu naruszeń, dzieląc je na ciężkie naruszenia oraz wszystkie pozostałe. W art. 85 ust. 2 PD I wskazano, że działania określone w KG jako ciężkie naruszenia stanowią również ciężkie naruszenia PD I. jeżeli zostały popełnione między innymi na szkodę osób znajdujących się we władzy strony przeciwnej, na szkodę jeńców wojennych, kombatantów wyłączonych z walki, uchodźców i bezpaństwowców, albo przeciwko personelowi medycznemu, formacjom medycznym lub środkom transportu medycznego, znajdującym się pod kontrolą strony przeciwnej. Ponadto, w art. 85 ust. 3 PD I rozszerzono katalog ciężkich naruszeń MPH, o czyny takie jak⁷³⁴: czynienie ludności cywilnej lub osób cywilnych celami ataku (art. 85 ust. 3 lit. a PD I), podejmowanie ataku bez rozróżnienia, dotyczącego ludność cywilną lub dobra o charakterze cywilnym, ze świadomością, że taki atak wywoła straty w życiu ludzkim, ranienie osób cywilnych oraz szkody w dobrach cywilnych, nadmierne do oczekiwanej konkretnej i bezpośredniej korzyści militarnej (art. 85 ust. 3 lit. b PD I), podejmowanie ataku przeciwko budowlom lub urządzeniom zawierającym siły niebezpieczne ze świadomością, że taki atak spowoduje straty w życiu

⁷³¹ Y. Sandoz, *The History of the Grave Breaches Regime*, „Journal of International Criminal Justice”, 2009, vol. 7, no. 4, s. 673-674.

⁷³² *Tamże*, s. 674.

⁷³³ L. Moir, *Grave Breaches and Internal Armed Conflicts*, „Journal of International Criminal Justice”, 2009, vol. 7, no. 4, s. 785.

⁷³⁴ Autor ograniczył się do wskazania tylko tych ciężkich naruszeń, które można wywieść z ataku na infrastrukturę krytyczną podczas konfliktu zbrojnego.

ludzkim, ranienie osób cywilnych lub szkody w dobrach o charakterze cywilnym, nadmierne do oczekiwanej konkretnej i bezpośredniej korzyści militarnej (art. 85 ust. 3 lit. c PD I).

Aby powyższe naruszenia zakwalifikować jako ciężkie, każde z nich musi zostać popełnione z winy umyślnej, z naruszeniem odpowiednich postanowień PD I oraz pociągać za sobą śmierć lub powodować poważne uszkodzenie ciała lub rozstroju zdrowia (art. 85 ust. 3 PD I). Wina umyślna oznacza, że sprawca działa świadomie i z zamiarem, czyli mając na uwadze czyn i jego konsekwencje chce go popełnić⁷³⁵. Działanie z winą umyślną obejmuje również czyny lekkomyślne, a więc sytuację, w której sprawca nie będąc pewnym określonego rezultatu, akceptuje możliwość jego zajścia⁷³⁶. Ponadto działanie sprawcy musi spowodować naruszenie odpowiednich postanowień PD I, na przykład art. 55 PD I odnoszącego się do ochrony środowiska naturalnego⁷³⁷. Ostatnim warunkiem ciężkiego naruszenia MPH jest śmierć ludności cywilnej lub powstanie negatywnych skutków, które długotrwale będą wpływały na zdrowie fizyczne lub psychiczne cywilów⁷³⁸.

Naruszenie MPH jako czyn bezprawny powoduje powstanie odpowiedzialności międzynarodowej. W klasycznym ujęciu, wyrażonym między innymi przez D. Anzilotti, za czyn bezprawny rozumie się takie naruszenie prawa międzynarodowego, które powoduje powstanie nowego stosunku prawnego pomiędzy państwami, gdzie strona dopuszczająca się czynu bezprawnego jest zobowiązana do naprawienia powstałej szkody, a strona pokrzywdzona jest upoważniona do dochodzenia roszczenia o jej naprawę⁷³⁹. Obowiązek naprawienia szkody, jako konsekwencja naruszeń zobowiązań międzynarodowych, został potwierdzony przez Stały Trybunał Sprawiedliwości Międzynarodowej w wyroku z 13 września 1928 roku w sprawie fabryki w Chorzowie. W wyroku Trybunał wskazał, że obowiązek naprawienia szkody wynika wprost z zasad prawa międzynarodowego, ale również z samej koncepcji prawa⁷⁴⁰.

Zdefiniowanie odpowiedzialności międzynarodowej wymaga ustalenia jej kluczowych elementów. Po pierwsze, należy ustalić jaki jest zakres podmiotowy odpowiedzialności międzynarodowej⁷⁴¹. Obecnie naruszenia prawa międzynarodowego, w tym MPH, nie dotyczą

⁷³⁵ Y. Sandoz et al., *Commentary to APs*, s. 994.

⁷³⁶ *Tamże*.

⁷³⁷ *Tamże*, s. 995.

⁷³⁸ *Tamże*.

⁷³⁹ D. Anzilotti, *Cours de Droit International*, <https://archive.org/details/in.ernet.dli.2015.475454/page/n7/mode/1up> (9.04.2026), s. 467.

⁷⁴⁰ STSM, *Case concerning factory at Chorzów (Germany v. Poland)*, Judgment, 13.09.1928, Publications of the Permanent Court of International Justice, 1928, series A – no. 13, s. 29.

⁷⁴¹ A. Pellet, *The Definition of Responsibility in International Law*, w: J. Crawford, A. Pellet, S. Olleson (ed.), *The Law of International Responsibility*, Oxford University Press, New York 2010, s. 6.

wyłącznie państwa, ale również organizacji międzynarodowych czy jednostek. Odpowiedzialność jednostki ogranicza się jednak do naruszeń MPH, w konsekwencji czego powstaje po jej stronie odpowiedzialność karna, która jest realizowana przez sądy krajowe oraz międzynarodowe trybunały karne i musi wynikać wprost z traktatów międzynarodowych⁷⁴². Po drugie, należy ustalić zakres przedmiotowy odpowiedzialności międzynarodowej⁷⁴³. Doktryna określiła trzy pojęcia związane z odpowiedzialnością międzynarodową: *responsibility*, *liability*, *accountability*⁷⁴⁴. Wszystkie trzy terminy w języku polskim oznaczają odpowiedzialność, jednak w znaczeniu odpowiedzialności międzynarodowej każde z nich będzie charakteryzowało się innym zakresem przedmiotowym. Termin *responsibility* związany jest z odpowiedzialnością deliktową państwa, co wiąże się z przypisaniem mu czynu bezprawnego, a także z indywidualną odpowiedzialnością karną jednostki⁷⁴⁵. Termin *liability* związany jest z odpowiedzialnością odszkodowawczą państwa w związku z czynami niezabronionymi⁷⁴⁶. Zastosowanie tego rodzaju odpowiedzialności wiąże się z trudnościami interpretacyjnymi, ponieważ powstały dwie szkoły rozumienia *liability*⁷⁴⁷. Pierwsza z nich uznaje, że tego rodzaju odpowiedzialność przybiera formę obiektywną i jest związana z każdym rodzajem szczególnie niebezpiecznej działalności państwa. Natomiast druga z nich wiąże odpowiedzialność z obowiązującymi umowami międzynarodowymi, a więc z odpowiedzialnością, która *de facto* już obowiązuje. Istotą *liability* jest tak naprawdę skutek działania państwa, a nie sama jego działalność w formie naruszenia prawa⁷⁴⁸. Termin *accountability* odnosi się do odpowiedzialności państw w relacjach z organizacjami międzynarodowymi, w szczególności w sprawach związanych z raportowaniem i składaniem sprawozdań związanych z wykonywaniem obowiązków wynikających z umów międzynarodowych⁷⁴⁹.

Dla potrzeb niniejszej rozprawy przyjęto rozumienie odpowiedzialności międzynarodowej jako odpowiedzialności deliktowej państwa za czyn bezprawny (naruszenie MPH) oraz działanie bezprawne jednostki skutkujące powstaniem międzynarodowej odpowiedzialności karnej za zbrodnie wojenne.

⁷⁴² *Tamże*,

⁷⁴³ *Tamże*,

⁷⁴⁴ D. Iwan-Sojka, *Responsibility of war industry for lethal autonomous weapons systems*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2024, s. 58.

⁷⁴⁵ *Tamże*, s. 58-59.

⁷⁴⁶ *Tamże*, s. 62.

⁷⁴⁷ W. Czapliński, A. Wyrozumska, *Prawo międzynarodowe...*, s. 773.

⁷⁴⁸ A. Pellet, *The Definition of Responsibility...*, s. 10.

⁷⁴⁹ D. Iwan-Sojka, *Responsibility of war...*, s. 63.

5.3.1 Odpowiedzialność państwa

Uznanie odpowiedzialności państwa za naruszenia prawa międzynarodowego (zarówno polegającej na działaniu, jak i zaniechaniu właściwego działania), w tym MPH, wymaga łącznego wystąpienia dwóch elementów, jakimi są naruszenie prawa międzynarodowego oraz przypisanie działania państwu⁷⁵⁰. Stwierdzenie istnienia obu tych przesłanek skutkować będzie możliwością dochodzenia odpowiedzialności międzynarodowej w formie restytucji, rekompensaty lub satysfakcji⁷⁵¹.

Zgodnie z art. 12 Artykułów o odpowiedzialności państw za akty międzynarodowo bezprawne z 2001 roku (ARSIWA)⁷⁵² naruszenie prawa międzynarodowego przez państwo ma miejsce wtedy, gdy działanie państw jest niezgodne z wymaganiami zobowiązania prawnego, niezależnie od jego pochodzenia lub charakteru. Postępowanie niezgodne z prawem międzynarodowym jest przesłanką obiektywną, co oznacza, że przypisanie naruszenia tego zobowiązania nie wymaga ustalenia winy państwa⁷⁵³. Co więcej, państwo może naruszyć tylko takie zobowiązania międzynarodowe, którymi jest związane w momencie powstania naruszenia (por. art. 3 i 13 ARSIWA). Jak wskazano w art. 12 ARSIWA nieważne jest pochodzenie lub charakter tego zobowiązania, co wydaje się być istotne w kontekście MPH. Nie każde bowiem państwo jest stroną np. Protokołów dodatkowych, a jednak istnieje możliwość przypisania mu naruszeń tych postanowień. Zwyczajowy charakter postanowień KG nie budzi żadnych zastrzeżeń i uznaje się, że są one skuteczne wobec wszystkich podmiotów prawa międzynarodowego⁷⁵⁴. Inaczej sytuacja kształtuje się w przypadku PD I oraz PD II. Pomimo tego, że w Protokołach skodyfikowano już wiele istniejących norm zwyczajowych, to co do charakteru zwyczajowego całego aktu pozostaje wiele wątpliwości⁷⁵⁵. Przyjmuje się, że tylko niektóre postanowienia PD I oraz PD II przyjęły charakter zwyczajowy, a więc są skuteczne *erga omnes*⁷⁵⁶. Zaliczyć do nich należy zasadę rozróżnienia, zasadę proporcjonalności czy normy regulujące ochronę ludności cywilnej.

⁷⁵⁰ W. Czapliński, A. Wyrozumski, *Prawo międzynarodowe...*, s. 738.

⁷⁵¹ P. Grzebyk, *Cele osobowe...*, s. 253.

⁷⁵² ZO ONZ, *Resolution 56/83*, 28.01.2002, A/RES/56/83 (2002).

⁷⁵³ B. Stern, *The Elements of an Internationally Wrongful Act*, w: J. Crawford, A. Pellet, S. Olleson (ed.), *The Law of International Responsibility*, Oxford University Press, New York 2010, s. 209.

⁷⁵⁴ P. Grzebyk, *Cele osobowe...*, s. 259.

⁷⁵⁵ J-M. Henckaerts, *Study on customary international humanitarian law: A contribution to the understanding and respect for the rule of law in armed conflict*, „International Review of the Red Cross”, 2005, vol. 87, no. 857, s. 187-188.

⁷⁵⁶ *Tamże*.

W przypadku istnienia przepisów specjalnych, art. 55 ARSIWA wyłącza zastosowanie artykułów dotyczących odpowiedzialności państwa, wskazując *lege speciales* jako normy właściwe do dochodzenia odpowiedzialności międzynarodowej. Znajduje to odniesienie szczególnie w przypadku istnienia tzw. reżimów zamkniętych (ang. *self-contained regims*). Pierwsze wskazanie na istnienie reżimów zamkniętych miało miejsce w wyroku STSM z 17 sierpnia 1923 roku w sprawie Wimbledon, w którym Trybunał wskazał, że postanowienia dotyczące Kanału Kilońskiego zawarte w Traktacie Wersalskim⁷⁵⁷ stanowią reżim zamknięty względem postanowień traktatu, które mają ogólne zastosowanie do śródlądowych dróg wodnych i są mniej restrykcyjne dla niemieckiej suwerenności⁷⁵⁸. Do reżimów zamkniętych odniósł się również MTS w wyroku z 24 maja 1980 roku w sprawie zakładników amerykańskich w Teheranie⁷⁵⁹. Zgodnie ze stanowiskiem zaprezentowanym przez Trybunał prawo dyplomatyczne w wyczerpujący sposób zdefiniowało środki konieczne do obrony przed nielegalnym działaniem przedstawicieli dyplomatycznych i w związku z tym nie jest wymagane odwołanie się do ogólnych zasad odpowiedzialności. Tak ukształtowane orzecznictwo sądów międzynarodowych daje podstawę do uznania, że reżim zamknięty jest używany w znaczeniu: wyznaczającym charakter konkretnych postanowień traktatu, celem uwypuklenia ich zamknięcia (samowykonalności) względem innych norm prawnych, wyznaczającym charakter działu prawa międzynarodowego (i tworzących ten dział instytucji prawnych), który posiadając pewną autonomię względem ogólnego prawa międzynarodowego jest z nim wielostronnie powiązany lub wyznaczającym charakter organów sądowych, z których każdy stanowiąc całość ma zdolność do samodzielnego funkcjonowania, w oparciu o normy prawne, które organ ten kreują⁷⁶⁰.

Czy wobec powyższego należy uznać, że MPH stanowi reżim zamknięty? Według Raportu Komisji Prawa Międzynarodowego dotyczącego fragmentacji prawa międzynarodowego z 2006 roku, MPH stanowi reżim zamknięty, ponieważ reguluje pewną określoną sytuację jaką jest konflikt zbrojny, w której ogólne normy prawa międzynarodowego zostaną ograniczone albo nawet wyłączone z użycia⁷⁶¹. Dodatkowo KPM podkreśla specjalny

⁷⁵⁷ *Traktat pokoju między mocarstwami sprzymierzonymi i skojarzonymi i Niemcami*, Wersal, 28.06.1919, Dz. U. z 1920 r., nr 35, poz. 200.

⁷⁵⁸ STSM, *Case of the S.S. "Wimbledon" (United Kingdom, France, Italy & Japan v. Germany)*, Judgment, 17.08.1923, Publications of the Permanent Court of International Justice, 1923, series A – no. 1, s. 23-24.

⁷⁵⁹ MTS, *Case concerning United States diplomatic and consular staff in Tehran (USA v. Iran)*, Judgment, 24.05.1980, ICJ Reports, 1980, par. 86.

⁷⁶⁰ E. Cała-Wacinkiewicz, *Fragmentacja prawa międzynarodowego*, Wydawnictwo C.H. Beck, 2018, s. 365.

⁷⁶¹ ZO ONZ, *Report of the Study Group of the International Law Commission: Fragmentation of International Law: Difficulties Arising From the Diversification and Expansion of International Law*, 13.04.2006, A/CN.4/L.682, par. 129.

charakter MPH ze względu na nieformalne działania między innymi prawników i dyplomatów, wynikające bardziej z potrzeby specjalizacji niż świadomego tworzenia reżimów⁷⁶². Odmienne stanowisko zaprezentował Ch. Greenwood, według którego określenie MPH reżimem zamkniętym może być mylące⁷⁶³. Zamiast tego wskazuje, że MPH nie jest samoistnym reżimem, ale raczej częścią składową czegoś większego⁷⁶⁴. Powyższe sugeruje, że MPH nie wypełnia wszystkich przesłanek wymaganych do uznania za reżim zamknięty, dlatego że wiele jego mechanizmów tylko modyfikuje ogólne zasady dotyczące odpowiedzialności, a trybunały międzynarodowe wielokrotnie stosowały ogólne zasady odpowiedzialności w związku z naruszeniami MPH⁷⁶⁵.

Drugim elementem uznania odpowiedzialności państwa za naruszenia prawa międzynarodowego jest przypisanie działania temu państwu. Zgodnie z art. 4 ARSIWA za działalność państwa uważa się działania podejmowane przez organy centralne tego państwa, skupione wokół władzy ustawodawczej oraz wykonawczej, ale także działalność organów jednostek samorządu terytorialnego oraz władzy sądowniczej. Odpowiedzialność państwa za działania każdego swojego organu zostało potwierdzone w postanowieniu MTS w sprawie środków tymczasowych z 3 marca 1999 roku w sprawie braci La Grand⁷⁶⁶. Trybunał wskazał, że Gubernator Arizony jako przedstawiciel rządu centralnego Stanów Zjednoczonych jest zobowiązany do działania zgodnie z międzynarodowymi zobowiązaniami Stanów Zjednoczonych. Powyższe stanowisko wpisuje się w zasadę jedności państwa, zgodnie z którą działania lub zaniechania jednego z jego organów należy traktować jako działania lub zaniechania państwa w kontekście odpowiedzialności międzynarodowej⁷⁶⁷. Wiąże się to również z tym, że różnorodność zobowiązań międzynarodowych nie pozwala na jakiegokolwiek rozróżnienie między organami państwa, które mogą popełniać czyny międzynarodowo bezprawne, a tymi, które tego zrobić nie mogą.

Państwo odpowiada również za działania podejmowane przez osoby lub podmioty, które nie sprawują władzy, ale działają na zlecenie powyższych organów (art. 5 ARSIWA).

⁷⁶² *Tamże*, par. 158.

⁷⁶³ Ch. Greenwood, *International Humanitarian Law in Context*, w: Ch.-J. Cheng (ed.), *A New International Legal Order*, Brill | Nijhof, 2016, s. 312-313.

⁷⁶⁴ „an island entire of itself” but rather each is “a piece of the continent, a part of the main”, zob. Ch. Greenwood, *International Humanitarian Law...*, s. 313.

⁷⁶⁵ M. Sassòli, *State responsibility for violations of international humanitarian law*, „International Review of the Red Cross”, 2002, vol. 84, no. 846, s. 404.

⁷⁶⁶ MTS, *LaGrand Case (Germany v. United States Of America)*, Request for the Indication of Provisional Measures, 3.03.1999, ICJ Reports, 1999, par. 28.

⁷⁶⁷ *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, Yearbook of the International Law Commission, 2011, vol. II, Part Two, s. 40.

Katalog podmiotów objętych art. 5 jest otwarty, natomiast jedyną przesłanką wymaganą dla uznania podmiotu za działający na zlecenie organów państwowych jest posiadanie odpowiedniego umocowania do działania⁷⁶⁸.

Na podstawie art. 8 ARSIWA odpowiedzialność państwa może być również przypisana za działania osoby lub grupy osób, które w rzeczywistości działają na podstawie instrukcji, pod kierownictwem lub kontrolą tego państwa. Kwestia odpowiedzialności państwa za wsparcie działalności wywrotowej lub partyzanckiej była rozpatrywana przez MTS w wyroku z 27 czerwca 1986 w sprawie Nikaragui⁷⁶⁹. W tej sprawie Trybunał musiał rozpatrzyć, czy bojówki *Contras* pozostawały pod takim wpływem Stanów Zjednoczonych, że można było obciążyć Stany Zjednoczone odpowiedzialnością za naruszenia MPH. Trybunał orzekł, że w sprawie nie występują jednoznaczne dowody wskazujące na tak dużą kontrolę na bojówkami ze strony Stanów Zjednoczonych.

Dla przypisania odpowiedzialności państwu za naruszenia MPH kluczowym może okazać się również art. 10 ARSIWA, zgodnie z którym jeśli działania powstańcze doprowadzą do powstania nowego państwa (choćby stało się to na części terytorium państwa już istniejącego), to uważa się, że nowo powstałe państwo ponosi odpowiedzialność za działania partyzanckie. Elementami kluczowymi do przypisania odpowiedzialności nowo powstałemu państwu jest ciągłość władzy (rozumiana jako utworzenie nowego rządu z władz partyzanckich) oraz działanie w imieniu ruchu partyzanckiego jako grupy, a nie poszczególnych osób indywidualnie⁷⁷⁰.

Uznanie odpowiedzialności państwa za bezprawne naruszenie prawa międzynarodowego rodzi po stronie pokrzywdzonej możliwość dochodzenia roszczenia o naprawę wyrządzonej krzywdy. Artykuł 34 ARSIWA przewiduje trzy formy naprawienia szkody wyrządzonej przez bezprawne działanie państwa: restytucję, kompensację oraz satysfakcję. Podstawową formą odpowiedzialności jest restytucja, czyli przywrócenie stanu sprzed popełnienia czynu bezprawnego (art. 35 ARSIWA). Często wskazuje się, że restytucja może być jedyną realną formą naprawy wyrządzonej szkody, jak w przypadku naruszenia zwierzchnictwa terytorialnego⁷⁷¹. Możliwość dokonania restytucji jest ograniczona

⁷⁶⁸ *Tamże*, s. 43.

⁷⁶⁹ MTS, *Case Concerning Military...*, par. 28.

⁷⁷⁰ *Draft articles on Responsibility of States...*, s. 50.

⁷⁷¹ W. Czapliński, A. Wyrozumska, *Prawo międzynarodowe...*, s. 763.

tylko do sytuacji, w której jest ona materialnie możliwa oraz nie pociąga za sobą obciążenia niewspółmiernego do korzyści potencjalnie wynikającej z tej restytucji.

Drugą formą odpowiedzialności jest kompensacja, a więc wypłacenie odszkodowania, które pokryje zarówno rzeczywiście powstałą stratę, ale również utracone zyski (art. 36 ARSIWA). W przypadku opisanym w art. 36 ARSIWA wykluczeniu podlega wypłacenie odszkodowania za tzw. straty moralne, które są związane z kolejną formą odpowiedzialności jaką jest satysfakcja⁷⁷². Zgodnie z art. 37 ust. 2 ARSIWA satysfakcja może przybrać formę przyznania się do naruszenia, wyrażenia żalu lub formalnych przeprosin. Wskazuje się, że satysfakcja nie należy do standardowych form odszkodowania międzynarodowego i jest związana z pewną formą komplementarności względem restytucji i kompensacji⁷⁷³.

Naruszenie zobowiązań międzynarodowych powoduje po stronie państwa powstanie odpowiedzialności międzynarodowej i konieczność naprawienia wyrządzonej szkody. W przypadku ataków na infrastrukturę krytyczną szczególnie ważne wydaje się dokonanie restytucji, czyli przywrócenie stanu faktycznego sprzed dokonania czynu bezprawnego. Jako przykład może posłużyć odpowiedzialność rosyjska za zniszczenie zapory wodnej w Nowej Kachowce⁷⁷⁴. Niemniej przywrócenie stanu poprzedniego, a więc odtworzenie infrastruktury krytycznej może być fizycznie niemożliwe lub powodować skutki niewspółmiernie wysokie, dlatego państwa powinny rozpatrywać również zastosowanie innych form odpowiedzialności, jak odszkodowanie lub zadośćuczynienie⁷⁷⁵.

5.3.2 Odpowiedzialność jednostki

W klasycznym ujęciu prawa międzynarodowego jednostka może stać się podmiotem ochrony prawa międzynarodowego, w szczególności międzynarodowej ochrony praw człowieka⁷⁷⁶. Jednak obecnie przyjmuje się, że prawo międzynarodowe może w ograniczonym zakresie tworzyć też pewne obowiązki dla jednostki. Zmiana w podejściu do praw i obowiązków wynikających z prawa międzynarodowego względem jednostki jest konsekwencją wprowadzenia międzynarodowej odpowiedzialności karnej.

⁷⁷² *Draft articles on Responsibility of States...*, s. 98-99.

⁷⁷³ *Tamże*, s. 106.

⁷⁷⁴ Y. Gunawan, Mhd. E. R. Pane, *Responsibility for Excessive Infrastructure Damage in Attacks: Analyzing Russia's Attack in Ukraine*, „PETITA Jurnal Kajian Ilmu Hukum dan Syariah”, 2024, vol. 9, no. 1, s. 227-228.

⁷⁷⁵ MTS, *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, Judgment, 20.04.2010, ICJ Reports, 2010, par. 273.

⁷⁷⁶ Ch. Tomuschat, *The Responsibility of the Other Entities*, w: J. Crawford, A. Pellet, S. Olleson (ed.), *The Law of International Responsibility*, Oxford University Press, New York 2010, s. 318.

Rozwój odpowiedzialności karnej jednostki wiąże się z zakończeniem II wojny światowej i powołaniem dwóch pierwszych międzynarodowych trybunałów karnych, których zadaniem było osądzenie zbrodni popełnionych przez nazistów i siły zbrojne Japonii podczas II wojny światowej⁷⁷⁷. 8 sierpnia 1945 roku państwa alianckie podpisały Porozumienie w przedmiocie ścigania i karania głównych przestępców wojennych Osi Europejskiej, tym samym powołując do życia Międzynarodowy Trybunał Wojskowy w Norymberdze (MTW)⁷⁷⁸. Integralną częścią porozumienia była Karta MTW. Jurysdykcją Trybunału objęto trzy rodzaje zbrodni:

- zbrodnie przeciwko pokojowi, w tym planowanie, przygotowywanie, początkowanie lub prowadzenie wojny napastniczej albo wojny będącej pogwałceniem traktatów, porozumień lub gwarancji międzynarodowych albo współudział w planie lub zмовie w celu dokonania jednego z powyższych czynów (art. VI lit. a Statutu MTW);
- zbrodnie wojenne, w tym pogwałcenie praw i zwyczajów wojennych. Pogwałcenie będzie obejmowało, ale nie będzie ograniczone do morderstw, złego obchodzenia się lub deportacji na roboty przymusowe albo w innym celu ludności cywilnej na okupowanym obszarze lub z tego obszaru, do mordowania lub złego obchodzenia się z jeńcami wojennymi lub osobami na morzu, do zabijania zakładników, do rabunku własności publicznej lub prywatnej, do bezmyślnego burzenia osiedli, miast lub wsi albo do spustoszeń nie usprawiedliwionych koniecznością wojenną (art. VI lit. b Statutu MTW);
- zbrodnie przeciw ludzkości, w tym morderstwa, wytępienie, obracanie ludzi w niewolników, deportacja i inne czyny nieludzkie, których dopuszczono się przeciwko jakiegokolwiek ludności cywilnej, przed wojną lub podczas niej, albo prześladowania ze względów politycznych, rasowych lub religijnych przy popełnianiu jakiegokolwiek zbrodni wchodzącej w zakres kompetencji Trybunału lub w związku z nią, niezależnie od tego, czy było to zgodne, czy też stało w sprzeczności z prawem kraju, w którym zbrodni dokonano (art. VI lit. c Statutu MTW).

⁷⁷⁷ E. van Sliedregt, *Individual Criminal Responsibility in International Law*, Oxford University Press, New York 2012, s. 4.

⁷⁷⁸ Porozumienie międzynarodowe w przedmiocie ścigania i karania głównych przestępców wojennych Osi Europejskiej, Londyn, 8.08.1945, Dz. U. z 1947 r., nr 63, poz. 367.

Karta MTW była pierwszym aktem prawnym o randze międzynarodowej, w którym zbrodnie wojenne zostały uznane za podstawę odpowiedzialności karnej jednostki⁷⁷⁹.

Kamieniem milowym w regulacjach odpowiedzialności karnej jednostki było utworzenie dwóch międzynarodowych trybunałów karnych do zbadania i osądzenia zbrodni popełnionych w byłej Jugosławii oraz w Rwandzie⁷⁸⁰. Jednak należy zaznaczyć, że oba Trybunały były organami doraźnymi, utworzonymi w celu osądzenia osób odpowiedzialnych za zbrodnie w byłej Jugosławii i Rwandzie⁷⁸¹. RB ONZ rezolucją nr 827 z 25 maja 1993 roku powołała do życia MTKJ, którego zadaniem było ściganie osób odpowiedzialnych za poważne naruszenia MPH popełnione na terytorium byłej Jugosławii od 1991 roku⁷⁸². Trybunał swoją jurysdykcją objął cztery zbrodnie:

- ciężkie naruszenia KG, obejmujące między innymi torturowanie, branie cywilów za zakładników (art. 2 Statutu MTKJ),
- naruszenia praw i zwyczajów wojennych, obejmujące między innymi atakowani lub bombardowanie niebronionych miast, wsi, domów lub budynków (art. 3 Statutu MTKJ),
- ludobójstwo, popełnione z zamiarem zniszczenia w całości lub w części grupy narodowej, etnicznej, rasowej lub religijnej, jako takiej, między innymi poprzez zabijanie członków grupy czy wprowadzanie środków mających ograniczyć urodzenia wśród grupy (art. 4 Statutu MTKJ),
- zbrodnie przeciwko ludzkości, obejmujące między innymi morderstwa, eksterminację czy deportacje (art. 5 Statutu MTKJ).

8 grudnia 1994 roku RB ONZ przyjęła rezolucję nr 955 tworzącą Międzynarodowy Trybunał Karny dla Rwandy, którego zadaniem było ściganie osób odpowiedzialnych za poważne naruszenia MPH popełnione na terytorium Rwandy oraz obywateli Rwandy odpowiedzialnych za takie naruszenia popełnione na terytorium państw sąsiednich, między 1 stycznia 1994 roku a 31 grudnia 1994 roku⁷⁸³. Trybunał swoją jurysdykcją objął trzy typy zbrodni:

⁷⁷⁹ J. Nowakowska-Małusecka, *Sytuacja dziecka w konflikcie zbrojnym. Studium prawnomiędzynarodowe*, Oficyna Wydawnicza BRANTA, Bydgoszcz 2011, s. 116.

⁷⁸⁰ K. Masło, *Międzynarodowa odpowiedzialność karna jednostek za zbrodnie przeciwko ludzkości*, Wydawnictwo Instytutu Wymiaru Sprawiedliwości, Warszawa 2020, s. 45-46.

⁷⁸¹ J. Nowakowska-Małusecka, *Odpowiedzialność karna jednostek za zbrodnie popełnione w byłej Jugosławii i w Rwandzie*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2000, s. 42 i 49.

⁷⁸² RB ONZ, *Resolution 827 (1993)*, 25.05.1993, S/RES/827 (1993), z późn. zmianami.

⁷⁸³ RB ONZ, *Resolution 955 (1994)*, 8.12.1994, S/RES/955 (1994), z późn. zmianami.

- ludobójstwo (art. 2 Statutu MTKR),
- zbrodnie przeciwko ludzkości, popełniane w ramach szeroko zakrojonego lub systematycznego ataku na ludność cywilną z powodów narodowych, politycznych, etnicznych, rasowych lub religijnych, obejmujące między innymi morderstwa, tortury czy zgwałcenie (art. 3 Statutu MTKR),
- naruszenia wspólnego artykułu 3 dla KG i PD II, obejmujące między innymi kary zbiorowe, branie zakładników czy plądrowanie (art. 4 Statutu MTKR).

Zwieńczeniem kształtowania się odpowiedzialności karnej jednostki w prawie międzynarodowym było powołanie w 1998 roku stałego Międzynarodowego Trybunału Karnego (MTK)⁷⁸⁴. Trybunał rozpoczął swoją działalność w 2002 roku, a zakresem jego jurysdykcji są objęte cztery kategorie zbrodni: ludobójstwo, zbrodnie przeciwko ludzkości, zbrodnie wojenne oraz zbrodnie agresji⁷⁸⁵.

Analiza statutów międzynarodowych trybunałów karnych ukazuje ewolucyjny charakter pojęcia zbrodni wojennych⁷⁸⁶. W Karcie MTW oraz Statucie MTKJ zdecydowano się na sformułowanie „naruszenia praw i zwyczajów wojennych”, natomiast Statut MTKR nie posługuje się ani pojęciem zbrodni wojennych, ani pojęciem naruszeń praw i zwyczajów wojennych. Dopiero w Statucie MTK precyzyjnie określono zbrodnie wojenne, wprowadzając ich obszerny katalog.

Przypisanie jednostce odpowiedzialności karnej za zabrodnie wojenne wymaga zaistnienia związku pomiędzy dokonaną zbrodnią a konfliktem zbrojnym⁷⁸⁷. Ustalenie takiego związku pozwala na odróżnienie zbrodni wojennych od przestępstw pospolitych. W myśl Elementów Zbrodni⁷⁸⁸ nie wymaga się od sprawcy oceny prawnej istnienia konfliktu zbrojnego, ani jego międzynarodowego czy niemiedzynarodowego charakteru. Sprawca powinien jedynie być świadomy faktycznego istnienia konfliktu zbrojnego, co pozwoli mu

⁷⁸⁴ H. J. A. N. Mensa-Bonsu, *The ICC, International Criminal Justice and International Politics*, „Africa Development”, 2015, vol. XL, no. 2, s. 36.

⁷⁸⁵ J. Nowakowska-Małusecka, *Sytuacja dziecka w konflikcie zbrojnym. Studium prawnomiędzynarodowe*, Oficyna Wydawnicza BRANTA, Bydgoszcz 2011, s. 302.

⁷⁸⁶ *Tamże*, s. 116.

⁷⁸⁷ H. van der Wilt, *War Crimes and the Requirement of a Nexus with an Armed Conflict*, „Journal of International Criminal Justice”, 2012, vol. 10, iss. 5, s. 1116.

⁷⁸⁸ MTK, *Elements of Crimes, 2011*, „Official Records of the Assembly of States Parties to the Rome Statute of the International Criminal Court”, First session, New York, 3-10.09.2002, United Nations Publications, Sales No. E.03.V.2 and corrigendum, part II.B.

ocenić, że jego czyn został popełniony w związku z konfliktem zbrojnym i jest z nim związany, nawet jeśli popełniono go na obszarze nieobjętym działaniami zbrojnymi⁷⁸⁹.

Odpowiedzialność karna jednostki za zbrodnie wojenne wymaga przypisania sprawcy spełnienia określonych przesłanek strony podmiotowej (*actus reus*), a także istnienia winy (*mens rea*)⁷⁹⁰. Należy tutaj zaznaczyć, że zbrodnie wojenne co do zasady popełniane są z zamiarem bezpośrednim (*dolus directus*), natomiast część z nich może zostać popełniona również w zamiarze ewentualnym (*dolus eventualis*), ale także poprzez lekkomyślność⁷⁹¹. MTKJ w wyroku z 2 sierpnia 2001 roku w sprawie *Krstić* zdefiniował pojęcie „popełnić” jako fizyczne popełnienie przestępstwa lub spowodowanie zawinione go zaniechania z naruszeniem prawa karnego⁷⁹². Dodatkowo Statut MTK dopuszcza możliwość odpowiedzialności karnej nie tylko za popełnienie zbrodni, ale także za usiłowanie, pomocnictwo czy podżeganie do jej popełnienia (art. 25 Statutu MTK).

Ponadto w art. 28 Statutu MTK przewiduje się możliwość odpowiedzialności dowódcy lub innego przełożonego za zbrodnie dokonane przez podwładnych, o których zamiarze popełnienia wiedział i nie podjął działań ani środków, które zmierzałyby do powstrzymania podwładnych od ich popełnienia.

W katalogu zbrodni wojennych określonych w art. 8 Statutu MTK należy wyróżnić kilka z nich, potencjalnie uprawniających do odpowiedzialności karnej jednostki za ataki ukierunkowane na infrastrukturę krytyczną. W art. 8 ust. 2 lit. b (iii) Statutu MTK⁷⁹³ określono zbrodnię wojenną polegającą na naruszeniu praw i zwyczajów prawa międzynarodowego mających zastosowanie do konfliktów zbrojnych o międzynarodowym charakterze obejmującą zamierzone kierowanie ataków na personel, instalacje, materiały, oddziały lub pojazdy związane z pomocą humanitarną lub misjami pokojowymi działającymi w oparciu o Kartę NZ tak długo, jak są one uprawnione do ochrony przysługującej osobom cywilnym i obiektom cywilnym na podstawie międzynarodowego prawa konfliktów zbrojnych. Elementy Zbrodni wymagają, aby sprawca zamierzał zaatakować personel, instalacje, materiały, jednostki lub pojazdy biorące udział w misji pomocy humanitarnej lub pokojowej⁷⁹⁴. Z punktu widzenia

⁷⁸⁹ D. Iwan-Sojka, *Responsibility of war...*, s. 175.

⁷⁹⁰ P. Grzebyk, *Cele osobowe...*, s. 231.

⁷⁹¹ M. N. Schmitt, *Tallinn Manual 2.0...*, s. 392.

⁷⁹² MTKJ, *Krstić case*, Judgment, 2.08.2001, IT-98-33-T, par. 601.

⁷⁹³ Dla konfliktów zbrojnych o charakterze niemiędzynarodowym zastosowanie znajdzie art. 8 ust. 2 lit. e (iii) Statutu MTK.

⁷⁹⁴ MTK, *Elements of Crimes...*, s. 12-13.

ochrony personelu i obiektów humanitarnych nie jest wymagane, aby doszło do faktycznych strat po ich stronie. Przesłanką odpowiedzialności w tym zakresie będzie sam fakt ataku⁷⁹⁵. Dodatkowo wymaga się, aby sprawca był świadomy ochrony tego personelu i tych obiektów⁷⁹⁶.

Współczesne konflikty zbrojne są przykładem tego, że pomimo ochrony przewidzianej w MPH, ale także pośredniej ochrony wynikającej z międzynarodowego prawa karnego⁷⁹⁷, pracownicy oraz obiekty pomocy humanitarnej są nieustannie celami ataku. Od początku konfliktu pomiędzy Izraelem a Hamasem (od 7 października 2023 roku) pomoc humanitarna skierowana do mieszkańców Strefy Gazy⁷⁹⁸ była wielokrotnie atakowana przez siły zbrojne Izraela, co doprowadziło do poważnych zakłóceń w dostępie ludności cywilnej do żywności, wody pitnej oraz medykamentów⁷⁹⁹. W okresie od 6 października 2024 roku do 19 stycznia 2025 roku izraelskie wojska dokonały całkowitej blokady pomocy humanitarnej przeznaczonej dla mieszkańców Strefy Gazy, co skutkowało przesiedleniem niemal całej ludności jej północnej części⁸⁰⁰. Społeczność międzynarodowa dostrzegając pogłębiający się kryzys humanitarny w Strefie Gazy podjęła środki zaradcze zmierzające do zwiększenia dostępności pomocy humanitarnej. Przede wszystkim środki te objęły naciski dyplomatyczne tak ze strony RB ONZ i innych organizacji międzynarodowych, jak i ze strony najbliższego sojusznika Izraela – Stanów Zjednoczonych. Wielokrotnie jednak podkreślano, że tymczasowe zwiększenie dostępności pomocy humanitarnej ze strony Izraela nie wynikało ze zobowiązań MPH, a właśnie ze względu na naciski dyplomatyczne⁸⁰¹. Pomimo zaistnienia przesłanek określonych w art. 8 ust. 2 lit. b (iii) Statutu MTK śledztwo wobec premiera B. Netanjahu

⁷⁹⁵ SCSL, *Sesay case*, Judgment, 2.03.2009, SCSL-04-15-T, par. 220.

⁷⁹⁶ *Tamże*, par. 235.

⁷⁹⁷ Obok celu sprawiedliwościowego (zaspokojenia poczucia sprawiedliwości) oraz celu kompensacyjnego (naprawienia powstałej szkody) kara spełnia co najmniej jeszcze dwa dodatkowe cele – ogólnoprewencyjny, dotyczący całego społeczeństwa oraz szczególnoprewencyjny, odnoszący się konkretnie do sprawcy przestępstwa. Oba te cele wiążą się z działaniem prewencyjnym kary, a więc przeciwdziałaniem popełnienia przestępstwa, jako formy odstraszającej, zob. K. Kulig, *Teoria pracowniczej odpowiedzialności porządkowej*, Wydawnictwo C.H. Beck, Warszawa 2017, s. 27.

⁷⁹⁸ Pomoc humanitarna obejmująca między innymi żywność, wodę pitną, leki, odzież oraz miejsca schronienia należy kierować tylko i wyłącznie do ludności cywilnej. Kombatanci oraz osoby bezpośrednio zaangażowane w działania zbrojne powinni być wyłączone z dostępu do pomocy humanitarnej, zob. Y. Dinstein, *The Right to Humanitarian Assistance*, „Naval War College Review”, 2000, vol. 53, no. 4, s. 77.

⁷⁹⁹ *Situation in the State of Palestine: ICC Pre-Trial Chamber I rejects the State of Israel's challenges to jurisdiction and issues warrants of arrest for Benjamin Netanyahu and Yoav Gallant*, <https://www.icc-cpi.int/news/situation-state-palestine-icc-pre-trial-chamber-i-rejects-state-israels-challenges> (dostęp: 24.05.2026).

⁸⁰⁰ OHCHR, *Overview Report. Practices and policies affecting human rights in the Occupied Palestinian Territory, including East Jerusalem (7 October 2023 – 31 May 2025)*, 18.05.2026, <https://www.ohchr.org/sites/default/files/documents/countries/opt/occupied-palestinian-territory-overview-report-east-jerusalem-practices-en.pdf> (dostęp: 24.05.2026), s. 28.

⁸⁰¹ *Situation in the State of Palestine: ICC Pre-Trial Chamber I...*

ani byłego ministra obrony Izraela J. Gallanta nie objęło ataków na pomoc humanitarną⁸⁰², a personel i obiekty wykorzystywane do pomocy humanitarnej w dalszym ciągu pozostają celem działań izraelskich sił zbrojnych⁸⁰³.

Z kolei zbrodnią wojenną, określoną w art. 8 ust. 2 lit. b (iv) Statutu MTK⁸⁰⁴, jest atak przeprowadzony ze świadomością, że spowoduje on przypadkową utratę życia lub zdrowia osób cywilnych, szkodę w obiektach cywilnych lub rozległą, długotrwałą i poważną szkodę w środowisku naturalnym, które byłyby wyraźnie nadmierne w stosunku do konkretnej, bezpośredniej i całkowitej spodziewanej korzyści wojskowej. Zgodnie z Elementami Zbrodni sprawca kierujący atakiem musi wiedzieć, że atak spowoduje utratę życia ludności cywilnej, zniszczenie lub uszkodzenie obiektów cywilnych lub będzie powodował rozległą, długotrwałą i poważną szkodę w środowisku naturalnym⁸⁰⁵. Dlatego nawet jeśli obiekt stanowi cel wojskowy, a pojawiłaby się obawa wystąpienia powyższych skutków, to osoba odpowiedzialna za przeprowadzenie ataku powinna od niego odstąpić⁸⁰⁶.

Postanowienia art. 8 ust. 2 lit. b (iv) Statutu MTK w najszerszym stopniu odpowiadają potencjalnemu naruszeniu MPH jako skutku ataku na infrastrukturę krytyczną. Do obiektów cywilnych wymienionych w tych postanowieniach należy zaliczyć infrastrukturę energetyczną, która jest regularnym celem ataków podczas konfliktu zbrojnego pomiędzy Ukrainą a Rosją. 28 listopada 2024 roku wojska rosyjskie dokonały zmasowanego ataku wymierzonego w ukraińską sieć energetyczną największych ośrodków miejskich, takich jak Kijów, Lwów czy Odessa⁸⁰⁷. Skutkiem ataku było pozbawienie ponad miliona gospodarstw domowych dostępu do elektryczności, ogrzewania oraz wody pitnej. Rosja nieprzerwanie podtrzymuje, że ataki wymierzone w ukraińską sieć energetyczną są atakami skierowanymi na cele wojskowe (co najmniej obiekty o podwójnym zastosowaniu), ponieważ ich działalność przyczynia się do korzyści militarnej przeciwnika (dostarczają energię elektryczną ukraińskim siłom zbrojnym),

⁸⁰² *Statement of ICC Prosecutor Karim A.A. Khan KC: Applications for arrest warrants in the situation in the State of Palestine*, <https://www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-kc-applications-arrest-warrants-situation-state> (dostęp: 24.05.2026).

⁸⁰³ *Israel intercepts Gaza flotilla near Crete and detains 175 activists*, <https://www.bbc.com/news/articles/c4g4lk9m77vo> (dostęp: 24.05.2026).

⁸⁰⁴ Dla konfliktów zbrojnych o charakterze międzynarodowym zastosowanie znajduje art. 8 ust. 2 lit. e (i) Statutu MTK, przy czym jego zakres jest ograniczony w porównaniu do sytuacji konfliktu zbrojnego o charakterze międzynarodowym – powyższe postanowienia bezpośrednio nie sankcjonują ataków wymierzonych w środowisko naturalne.

⁸⁰⁵ MTK, *Elements of Crimes...*, s. 13.

⁸⁰⁶ MTKJ, *Final Report...*, § 22.

⁸⁰⁷ *Russia/Ukraine: Latest massive missile strike on critical infrastructure is a war crime*, <https://www.amnesty.org/en/latest/news/2024/11/russia-ukraine-latest-massive-missile-strike-on-critical-infrastructure-is-a-war-crime/> (dostęp: 24.05.2026).

a więc stanowią legalny cel ataku⁸⁰⁸. Rosyjska argumentacja jakoby ukraińska sieć energetyczna stanowiła obiekt podwójnego zastosowania, tym samym stając się legalnym celem ataku, zdaje się być w pewnym stopniu prawidłowa. Wydaje się to racjonalne w kontekście wykorzystywanych współcześnie technologii militarnych i ich całkowitego uzależnienia od energii elektrycznej, gdzie pozbawienie dostępu do niej pozwoliłoby na szybkie zwycięstwo w konflikcie zbrojnym⁸⁰⁹. Takie samo stanowisko zaprezentowano w amerykańskich podręcznikach wojskowych, jednak w odpowiedzi na rosyjskie ataki na ukraińską sieć energetyczną amerykański Przewodniczący Połączonych Szefów Sztabów M. Milley określił je jako zbrodnie wojenne⁸¹⁰. Potwierdzeniem, że atak na infrastrukturę energetyczną strony przeciwnej może stanowić zbrodnię wojenną są działania podjęte przez MTK wobec rosyjskich przedstawicieli państwowych i wojskowych. 5 marca 2024 roku MTK wydał nakaz aresztowania dowódcy rosyjskiego lotnictwa dalekiego zasięgu generała S. Kobylasza oraz dowódcy Floty Czarnomorskiej admirała W. Sokołowa⁸¹¹. Obaj zostali oskarżeni między innymi o zbrodnie wojenne polegające na spowodowaniu nadmiernych obrażeń wśród ludności cywilnej oraz szkód wśród obiektów cywilnych, co bezpośrednio wiąże się z atakami na ukraińskie elektrownie. 24 czerwca 2024 roku MTK, w tym samym zakresie, wydał nakazy aresztowania rosyjskiego ministra obrony S. Szojgu oraz Szefa Sztabu Generalnego rosyjskiej armii W. Gierasimowa⁸¹².

Obok obiektów cywilnych postanowieniami art. 8 ust. 2 lit. b (iv) Statutu MTK objęte zostało również środowisko naturalne. W doktrynie podkreśla się, że jest to jedyny przepis międzynarodowego prawa karnego odnoszący się do ochrony środowiska naturalnego, zwracając uwagę na jego „ekocentryczny” charakter⁸¹³. Konieczność ochrony środowiska naturalnego postanowieniami międzynarodowego prawa karnego wynika z konsekwencji z jakimi wiąże się atak na ten cel, mianowicie z rozległymi, długotrwałymi i poważnymi

⁸⁰⁸ *Ukraine Symposium – Attacking Power Infrastructure under International Humanitarian Law*, <https://lieber.westpoint.edu/attacking-power-infrastructure-under-international-humanitarian-law/> (dostęp: 24.05.2026).

⁸⁰⁹ H. Shue, D. Wippman, *Limiting Attacks on Dual-Use Facilities Performing Indispensable Civilian Functions*, „Cornell International Law Journal”, 2002, vol. 35, iss. 3, s. 575.

⁸¹⁰ O. A. Hathaway, A. Khan, M. R. Revekin, *The Dangerous Rise...*, s. 2655.

⁸¹¹ *Situation in Ukraine: ICC judges issue arrest warrants against Sergei Ivanovich Kobylash and Viktor Nikolayevich Sokolov*, <https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-sergei-ivanovich-kobylash-and> (dostęp: 24.05.2026).

⁸¹² *Situation in Ukraine: ICC judges issue arrest warrants against Sergei Kuzhugetovich Shoigu and Valery Vasilyevich Gerasimov*, <https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-sergei-kuzhugetovich-shoigu-and> (dostęp: 24.05.2026).

⁸¹³ S. Maruf, *Environmental Damage in Ukraine as Environmental War Crime under the Rome Statute*, „Journal of International Criminal Justice”, 2024, vol. 22, iss. 1, s. 100.

szkodami. Przykładem takiego ataku jest wysadzenie tamy w Nowej Kachowce, który spowodował śmierć ponad 50 osób, jednak do bezpośrednich skutków należy zaliczyć również rozległe szkody w środowisku naturalnym, jak zniszczenie naturalnych siedlisk zwierząt oraz roślinności⁸¹⁴. Chociaż wydaje się, że atak spełnia przesłanki zbrodni wojennej określonej w art. 8 ust. 2 lit. b (iv) Statutu MTK, a ponadto zwraca się uwagę, że Rosjanie byli świadomi szkód, do których potencjalnie może doprowadzić zniszczenie tamy, to przypisanie odpowiedzialności za ten atak wiąże się z pewnymi trudnościami⁸¹⁵. Po pierwsze, problemem jest ustalenie „długotrwałości” tej szkody. Ani Statut MTK, ani dotychczasowe orzecznictwo trybunałów międzynarodowych nie określają, co to znaczy, że okres jest „długotrwały”. W związku z tym osoba potencjalnie odpowiedzialna za atak mogłaby kontrargumentować, że nie była świadoma długotrwałości tego skutku, gdyż w jej przekonaniu powinno to być co najmniej sto lat⁸¹⁶. Po drugie, w momencie wysadzenia tama znajdowała się na terytorium okupowanym przez Rosjan, a więc problemem może okazać się zakwalifikowanie jej zniszczenia jako ataku w świetle art. 49 PD I, czyli aktu przemocy skierowanego wobec strony przeciwnej⁸¹⁷. Rozwiązaniem może być uznanie tego terytorium jako linii frontu co umożliwiłoby uznanie tego zniszczenia jako ataku zgodnie z art. 49 PD I⁸¹⁸.

Kolejną zbrodnią wojenną, potencjalnie odnoszącą się do obiektów infrastruktury krytycznej, jest określony w art. 8 ust. 2 lit. b (ix) Statutu MTK zamierzony atak na budynki przeznaczone na cele religijne, edukacyjne, artystyczne, naukowe lub charytatywne, pomniki historyczne, szpitale oraz miejsca, gdzie gromadzeni są ranni i chorzy, pod warunkiem że nie są one celami wojskowymi. Elementy Zbrodni wymagają aby sprawca kierujący atakiem działał z zamiarem zniszczenia jednego lub więcej budynków obejmujących między innymi obiekty medyczne lub miejsca gromadzenia się rannych i chorych⁸¹⁹. Dla zaistnienia przesłanki odpowiedzialności karnej za atak wymagane jest aby atakowany obiekt nie stanowił celu wojskowego. MPH dopuszcza sytuację, w której obiekty takie jak szpitale utracą swoją ochronę i staną się legalnymi celami ataku, szczególnie w przypadku gdy są wykorzystywane do dokonywania czynów szkodliwych dla wroga⁸²⁰.

⁸¹⁴ K. Gavrysh, *Prosecuting Individuals for Environmental Harm in the Armed Conflict Between Russia and Ukraine: The Case of Destruction of the Kakhovka Dam*, „Polish Yearbook of International Law”, 2023, vol. XLIII, s. 275-276.

⁸¹⁵ S. Maruf, *Environmental Damage in Ukraine...*, s. 125.

⁸¹⁶ W szczególności należy tutaj uwzględnić zasadę „*in dubio pro reo*”, zob. *tamże*, s. 125.

⁸¹⁷ K. Gavrysh, *Prosecuting Individuals for Environmental Harm...*, s. 277.

⁸¹⁸ *Tamże*, s. 278.

⁸¹⁹ MTK, *Elements of Crimes...*, s. 15.

⁸²⁰ MTKJ, *Prosecutor v. Stanislav Galić*, Judgment on Appeal..., par. 341.

Jednak jak pokazują współczesne konflikty zbrojne obiekty medyczne, w tym personel medyczny, pozostają częstymi celami ataków. W trakcie wojny domowej w Syrii, w latach od 2011 do 2013, siły rządowe przeprowadziły serię ataków na szpitale, między innymi w Aleppo, co doprowadziło do śmierci pacjentów i personelu medycznego, ale też zniszczenia infrastruktury szpitalnej wstrzymując dostęp do pomocy medycznej w mieście⁸²¹. Placówki medyczne są również regularnym celem ataku izraelskich sił zbrojnych w Strefie Gazy. Od października 2023 roku *Ahli Baptist Hospital* był atakowany pięciokrotnie, co było uzasadniane potencjalnym centrum dowodzenia Hamasu znajdującym się w szpitalu⁸²². Ponadto Izrael oświadczył, że do ataku użył „precyzyjnej amunicji”, co miało zminimalizować ewentualne skutki uboczne. Niemniej z oświadczenia dyrektorki szpitala wynika, że w trakcie ataków dochodziło między innymi do zniszczenia szpitalnego oddziału ratunkowego. 25 sierpnia 2025 roku izraelskie siły zbrojne zaatakowały jeden z największych szpitali w Strefie Gazy – Nasser, co doprowadziło do śmierci ponad 20 osób, w tym personelu medycznego⁸²³. Choć ataki na obiekty medyczne oraz personel medyczny w konflikcie pomiędzy Izraelem a Hamasem są dobrze udokumentowane, to MTK nie zdecydowało się rozszerzyć śledztwa w tym kierunku. Brak reakcji ze strony społeczności międzynarodowej, w szczególności MTK, może doprowadzić do całkowitego załamania się sektora zdrowia w Strefie Gazy.

Ostatnią zbrodnią wojenną, potencjalnie mogącą odnosić się do ataków na infrastrukturę krytyczną, jest zamierzone głodzenie osób cywilnych jako metoda prowadzenia działań wojennych poprzez pozbawianie tych osób środków niezbędnych do życia, w tym umyślne pozbawianie racji żywnościowych przewidzianych w KG (art. 8 ust. 2 lit. b (xxv) Statutu MTK⁸²⁴). Elementy Zbrodni wymagają, aby sprawca, zamierzając zagłodzić ludność cywilną pozbawił ją dostępu do dóbr niezbędnych do jej przetrwania⁸²⁵, czyli przede wszystkim do żywności, wody pitnej oraz leków. W konflikcie zbrojnym z Palestyną Izrael regularnie

⁸²¹ Rada Praw Człowieka ONZ, *Assault on medical care in Syria*, 13.09.2013, A/HRC/24/CRP.2, s. 3.

⁸²² *Hospital Attacks in Gaza and Israel: What Counts as a War Crime?*, <https://www.thinkglobalhealth.org/article/hospital-attacks-gaza-and-israel-what-counts-war-crime> (dostęp: 24.05.2026).

⁸²³ Izrael argumentował atak obecnością w szpitalu 6 członków Hamasu, jednak niezależni eksperci nie potwierdzili tych doniesień, zob. L. Rubenstein, R. J. Haar, J. J. Amon, *Attacks on healthcare in war are being steadily normalized—we need to end impunity*, *Opinion*, *BMJ*, 2025, no. 390 (1964), <https://www.bmj.com/content/390/bmj.r1964> (dostęp: 24.05.2026).

⁸²⁴ Statut MTK nie przewiduje karalności głodu jako metody walki w konflikcie zbrojnym o charakterze międzynarodowym. Obecnie podejmowane są działania dyplomatyczne, szczególnie przez rząd Szwajcarii, zmierzające do przyjęcia poprawek w Statucie MTK w tym zakresie, zob. F. D'Alessandra, M. Gillett, *The War Crime of Starvation in Non-International Armed Conflict*, „*Journal of International Criminal Justice*”, 2019, vol. 17, iss. 4, s. 816-817.

⁸²⁵ MTK, *Elements of Crimes*..., s. 21.

wykorzystuje głód jako metodę prowadzenia walki. Zgodnie z udokumentowanymi działaniami izraelskie siły zbrojne od października 2023 roku wielokrotnie wstrzymywały na przejściach granicznych przekazanie żywności, a także blokowały transgraniczne rurociągi z wodą pitną (łącznie Izrael ze Strefą Gazy)⁸²⁶. Powyższe zostało potwierdzone przez MTK, tym samym wobec B. Netanjahu oraz J. Gallanta wydano nakazy aresztowania obejmujące między innymi zbrodnie wojenne określone w art. 8 ust. 2 lit. b (xxv) Statutu MTK.

5.4 Podsumowanie

Na podstawie powyższych rozważań należy przyjąć, że ataki na obiekty infrastruktury krytycznej podczas konfliktu zbrojnego powodują powstanie dwóch rodzajów skutków. Do pierwszej kategorii należy zaliczyć skutki bezpośrednie, związane z utratą życia lub zdrowia ludności cywilnej lub długotrwałymi, rozległymi i poważnymi szkodami w środowisku naturalnym. Infrastruktura krytyczna rozumiana jako struktura połączonych ze sobą urządzeń, obiektów oraz systemów, wpływa na bezpieczeństwo państwa oraz jego ludności w trzech głównych kategoriach – schronienia, zaopatrzenia oraz bezpieczeństwa. Jak wspomniano już wielokrotnie, MPH nie zawiera definicji infrastruktury krytycznej; zamiast tego wprowadziło rozproszoną ochronę sektorową, obejmującą swym zakresem: obiekty medyczne, dobra niezbędne do przeżycia ludności cywilnej, obiekty zawierające niebezpieczne siły oraz środowisko naturalne, w ramach którego należy rozpatrywać obiekty, jak fabryki chemiczne oraz inne budowle przemysłowe. Dokonanie ataku na każdy z tych obiektów doprowadzi do powstania negatywnych skutków w innej kategorii infrastruktury krytycznej. Najszersze skutki wywoływać będzie atak na dobra niezbędne dla przetrwania ludności cywilnej, ponieważ pozbawienie jej dostępu żywności, wody pitnej, lekarstw, energii elektrycznej czy odzieży wpływa na wszystkie trzy kategorie, a więc schronienie, zaopatrzenie oraz bezpieczeństwo. Także atak na obiekty zawierające niebezpieczne siły oraz środowisko naturalne przyczynia się do utraty schronienia, zaopatrzenia oraz bezpieczeństwa. Natomiast wydaje się, że atak na obiekty medyczne skutkują brakami tylko w jednej kategorii – bezpieczeństwa. Jednak należy rozpatrywać to dwuetapowo, a więc jako utraty bezpieczeństwa fizycznego (jako dostępu do ciągłej opieki medycznej) oraz bezpieczeństwa psychicznego (dobrostanu psychicznego człowieka).

Druga kategoria skutków wiąże się z potencjalną odpowiedzialnością za ataki na infrastrukturę krytyczną. W tym zakresie należy wyróżnić dwa typy odpowiedzialności –

⁸²⁶ *Statement of ICC Prosecutor Karim A.A. Khan....*

państwa oraz jednostki. W przypadku odpowiedzialności państwa jej głównym celem jest naprawienie szkody powstałej w związku z atakiem na infrastrukturę krytyczną. Odpowiedzialność powinna przyjąć formę restytucji, czyli przywrócenia stanu poprzedniego, jednak zniszczenia dokonane w obiektach infrastruktury krytycznej mogą okazać się na tyle poważne, że niemożliwe będzie przywrócenie stanu poprzedniego, więc należy doszukiwać się innych form odpowiedzialności, takich jak odszkodowanie lub zadośćuczynienie. Natomiast w przypadku odpowiedzialności jednostki, głównym celem jest ukaranie sprawcy dopuszczającego się zbrodni wojennej w rozumieniu Statutu MTK. Jednak co łączy obie te formy odpowiedzialności, to sposób na egzekwowanie norm ochronnych infrastruktury krytycznej wynikających z MPH. Niestety, jak pokazują przywołane postępowania sprzed MTK, skuteczność wykonywania nakazów aresztowania, a tym samym wykonania kroku ku rzeczywistemu pociągnięciu do odpowiedzialności karnej osób odpowiedzialnych za ataki na obiekty infrastruktury krytycznej, jest praktycznie niemożliwe. Pokazuje to słabość systemu prawa międzynarodowego, szczególnie w kontekście egzekwowania norm ochronnych między innymi infrastruktury krytycznej.

Zakończenie

Zrekonstruowany standard ochrony infrastruktury krytycznej

W pracy podjęto próbę odpowiedzi na pytanie czy kategoria infrastruktury krytycznej, dająca się zrekonstruować z międzynarodowego prawa humanitarnego, jest zakresowo wystarczająca, by współcześnie chronić tę infrastrukturę, uwzględniając dynamicznie zmieniającą się rzeczywistość. Przeprowadzone badania pozwalają uznać, że MPH tylko w sposób minimalny przewiduje ochronę dla obiektów infrastruktury krytycznej. Minimalna ochrona infrastruktury krytycznej w MPH wynika z dwóch powodów. Po pierwsze, samo MPH nie definiuje infrastruktury krytycznej oraz zawiera rozproszoną ochronę jej poszczególnych obiektów, a po drugie obowiązujące normy MPH nie w każdym przypadku odpowiadają współczesnym wymaganiom pola walki.

Jako główny problem ograniczonej ochrony obiektów infrastruktury krytycznej w MPH ustalono brak właściwego zdefiniowania pojęcia infrastruktury krytycznej. Zamiast tego przepisy MPH wprowadzają sektorową ochronę obiektów, takich jak obiekty medyczne, dobra niezbędne do przetrwania ludności cywilnej czy obiekty zawierające niebezpieczne siły, które dopiero po zestawieniu z definicją infrastruktury krytycznej pochodzącą z innych działów prawa międzynarodowego lub prawa krajowego mogą zostać potencjalnie uznane za jej kategorie. Z racji tego, w trakcie badań powstała konieczność zrekonstruowania pojęcia infrastruktury krytycznej, odwołując się do innych systemów prawnych, uwzględniając tak prawo międzynarodowe, jak i prawo wewnętrzne wybranych państw.

Problem ze zdefiniowaniem pojęcia infrastruktury krytycznej powoduje również infrastruktura krytyczna sama w sobie, a właściwie funkcje, które spełnia w bezpieczeństwie państwa i jego obywateli. Należy pamiętać, że infrastruktura krytyczna przede wszystkim jest zbiorem obiektów niezbędnych dla prawidłowego funkcjonowania państwa, tak w czasie pokoju, jak i w czasie konfliktu zbrojnego. Dlatego zapewnienie bezpieczeństwa obywatelom przez obiekty infrastruktury krytycznej jest tak naprawdę skutkiem pośrednim działania samej infrastruktury.

Wsparciem dla zrekonstruowania tego pojęcia była działalność organizacji międzynarodowych, ale także dorobek doktryny oraz orzecznictwo trybunałów międzynarodowych. Odtworzenie pojęcia infrastruktury krytycznej doprowadziło do wniosku, że sam ten termin jest nieostry i wydaje się niemożliwe opracowanie jednej, uniwersalnej

definicji, która będzie wykorzystywana zarówno w prawie krajowym, jak i w prawie międzynarodowym. Jednak dla potrzeb niniejszej rozprawy przyjęto, że infrastruktura krytyczna jest strukturą połączonych ze sobą urządzeń, obiektów oraz systemów (w tym dóbr o charakterze niematerialnym), które wpływają na bezpieczeństwo państwa oraz ludności, oddziałując na trzy główne kategorie, jakimi są schronienie, zaopatrzenie oraz bezpieczeństwo. Każda z tych kategorii obejmuje swoim zakresem inne sektory, które potencjalnie mogą zostać uznane za infrastrukturę krytyczną.

Zakreślenie definicji infrastruktury krytycznej jako funkcjonalnie powiązanych ze sobą systemów zapewniających bezpieczeństwo zarówno państwu, jak i obywatelom wiązało się z wyzwaniem dopasowania norm międzynarodowego prawa humanitarnego względem instytucji i obiektów państwowych. Należy tutaj zaznaczyć, że za instytucje i obiekty państwowe w rozumieniu infrastruktury krytycznej należy rozumieć przede wszystkim systemy i sektory związane z ciągłością administracji publicznej, bez których państwo traci rzeczywistą kontrolę nad wykonywaną władzą. Tym samym domniemywa się utratę zdolności do zapewnienia bezpieczeństwa obywatelom (ludności cywilnej), co w kontekście konfliktu zbrojnego stanowi jeden z podstawowych obowiązków stron konfliktu.

Obiekty administracji publicznej nie są objęte ochroną MPH, a często, w perspektywie podstawowych zasad, takich jak zasada proporcjonalności i konieczności wojskowej, stają się legalnym celem ataku. Implikuje to negatywne skutki dla ludności cywilnej, która staje się pośrednią ofiarą ataków na obiekty państwowe.

Kolejnym problemem zidentyfikowanym na podstawie przeprowadzonych badań jest rozwój nowoczesnych technologii i dostosowanie ich do istniejących, może się wydawać, już przestarzałych norm MPH. Szczególnie widoczne staje się to w przypadku dóbr niematerialnych. Bez wątpienia kod źródłowy (będący przykładem dobra niematerialnego) może być traktowany jako część składowa infrastruktury krytycznej, a jego uszkodzenie lub zmiana wpłynie na prawidłowe działanie systemu jako całości. Jednak na próżno szukać odpowiedniej normy MPH, która rozstrzygałaby legalność ataku na taki kod źródłowy. Co więcej, nawet doktryna nie przynosi jednoznacznej odpowiedzi, zmagając się ze sporem w tej materii.

Luki w międzynarodowym prawie humanitarnym zakresie ochrony infrastruktury krytycznej zmuszają do rekonstrukcji standardu ochrony tej infrastruktury na podstawie innych działów prawa międzynarodowego. Na pozór może się to wydawać błędnym założeniem,

ponieważ to MPH stanowi system szczególnej ochrony ludności cywilnej i obiektów jej służących w konflikcie zbrojnym, jednak współczesna działalność hybrydowa oraz terrorystyczna pokazuje, że to w czasie pokoju dochodzi częściej do naruszeń w bezpieczeństwie infrastruktury krytycznej. Z racji tego możliwe jest wypracowanie dobrych praktyk, szczególnie z obszaru działalności organizacji międzynarodowych. Organizacje takie jak NATO czy UE wiodą prym w zwalczaniu zagrożeń hybrydowych między innymi poprzez zwiększanie odporności infrastruktury krytycznej. Szczególną uwagę należy w tym zakresie zwrócić na UE, której regulacje przyjmują charakter sektorowy. To oznacza, że prawo unijne, w porównaniu z międzynarodowym prawem humanitarnym, nie traktuje infrastruktury krytycznej wybiórczo, a jednak dostrzega połączenia systemowe każdego sektora i rozumie, że bezpieczne i prawidłowe działanie każdego sektora z osobna wpływa na bezpieczeństwo i prawidłowe działanie infrastruktury krytycznej jako całości.

Z powodu swojego newralgicznego charakteru infrastruktura krytyczna wielokrotnie padała również ofiarą ataków terrorystycznych. To sprawiło, że społeczność międzynarodowa żywo pozostawała zainteresowana i aktywnie działała w kierunku zwiększenia odporności infrastruktury krytycznej na zagrożenia tego rodzaju (szczególnie bogaty dorobek w tym zakresie wykazuje ONZ oraz RE). Obszerne regulacje pozostałych działów prawa międzynarodowego, wspierane doktryną bezpieczeństwa wewnętrznego i zewnętrznego, powinny stanowić źródło inspiracji dla MPH w zakresie rozszerzenia ochrony infrastruktury krytycznej.

Przeprowadzone badania pozwalają wywnioskować, że standard ochrony infrastruktury krytycznej, oparty na współczesnych normach międzynarodowego prawa humanitarnego nie odpowiada współczesnym wyzwaniom, a co więcej, realnie pozbawia ludność cywilną skutecznej ochrony podczas konfliktu zbrojnego. Zrekonstruowany standard ochrony infrastruktury krytycznej w MPH obejmuje tylko wybiórcze sektory, które potencjalnie mogą zostać zaliczone do tej infrastruktury. Wskazać tutaj należy obiekty medyczne, personel oraz obiekty związane z pomocą humanitarną, dobra niezbędne dla przetrwania ludności cywilnej, obiekty zawierające niebezpieczne siły oraz środowisko naturalne w kontekście potencjalnych szkód wyrządzonych przez działalność fabryk i innych obiektów chemicznych.

Pomimo ograniczonej ochrony tylko wybranych sektorów potencjalnie zaliczanych do infrastruktury krytycznej, może się okazać, że wyegzekwowanie już istniejącej ochrony będzie niemożliwe. Jako przykład mogą posłużyć postanowienia art. 55 PD I, które dla uznania

ochrony środowiska naturalnego wymagają, żeby potencjalny atak doprowadził do rozległych, długotrwałych i poważnych szkód. Takie podejście wydaje się stać w całkowitej sprzeczności z obecnymi standardami ochrony środowiska naturalnego w czasie pokoju. Jak słusznie zauważył MTS w opinii doradczej z 8 czerwca 1996 roku w sprawie legalności groźby lub użycia broni jądrowej, środowisko naturalne nie jest abstrakcją, lecz stanowi rzeczywistą przestrzeń życiową, wpływając na jakość życia obecnych oraz przyszłych pokoleń, a mimo to zmagają się z codziennymi zagrożeniami⁸²⁷. Dlatego państwa, w ramach swojej jurysdykcji, ale również w ramach prawa międzynarodowego, powinny zapewnić konkretne ramy jego ochrony.

O tym, jak istotne jest prawidłowe współdziałanie wszystkich sektorów infrastruktury ze sobą, niech posłuży porównanie infrastruktury do ciała człowieka. Ciało człowieka, tak jak infrastruktura krytyczna, składa się z wielu powiązanych ze sobą organów/systemów. Jeżeli dojdzie do krótkotrwałego uszkodzenia organu, to organizm sobie z tym poradzi. Natomiast jeżeli uszkodzenie będzie długotrwałe, to z czasem dojdzie do zapaści całego organizmu. Tak samo jest z infrastrukturą krytyczną. Niezapewnienie jej poszczególnym sektorom ochrony krótkotrwałej, co do zasady, nie wpłynie na jej prawidłowe i ciągłe działanie. Ale trwałe pozbawienie ochrony poszczególnych sektorów będzie miało swoje długofalowe konsekwencje.

Wnioski *de lege ferenda*

Odpowiedzią na ograniczoną ochronę infrastruktury krytycznej w MPH powinno być znówelizowanie obowiązujących postanowień MPH w tym zakresie, a być może przyjęcie całkowicie nowego aktu prawnego, regulującego tylko i wyłącznie status infrastruktury krytycznej podczas konfliktu zbrojnego. Jednak uwzględniając sytuację polityczną oraz charakter samej infrastruktury krytycznej, w szczególności jej funkcje, jakie pełni w bezpieczeństwie narodowym, państwa nie wykazują woli uregulowania tak ważnej kwestii na poziomie międzynarodowym. Wynika to z kilku powodów. Po pierwsze, już początkowym problemem jest zdefiniowanie pojęcia infrastruktury krytycznej. Jak przedstawiono w niniejszej rozprawie, każde państwo, w szczególności potęgi militarne – Stany Zjednoczone, Federacja Rosyjska oraz Chińska Republika Ludowa – w odmienny sposób definiują infrastrukturę krytyczną⁸²⁸. Brak porozumienia na tak wczesnym etapie negocjacji treści

⁸²⁷ MTS, *Legality of the threat...*, par. 29.

⁸²⁸ Wyjątkiem jest opracowanie na forum UE definicji europejskiej infrastruktury krytycznej, a następnie zdefiniowanie podmiotów i usług krytycznych. Jednak osiągnięcie porozumienia w tym zakresie wynikało

umowy międzynarodowej doprowadziłby do impasu w dalszych rokowaniach, co potencjalnie mogłoby przełożyć się na zaprzestanie dalszych prac nad traktatem.

Po drugie, nawet jeśli państwa określiłyby zakres przedmiotowy takiej umowy międzynarodowej (w tym definicję infrastruktury krytycznej), kolejnym problemem byłoby ustalenie zasad angażowania infrastruktury krytycznej jako celu ataku. W tym zakresie wyłaniają się dwa stanowiska. Pierwsze, reprezentowane przez światowe mocarstwa militarne, w szczególności Stany Zjednoczone oraz Izrael, dopuszcza atakowanie poszczególnych sektorów infrastruktury krytycznej jako obiektów wspierających działania militarne przeciwnika. Dotyczy to przede wszystkim sektora energetycznego, teleinformatycznego czy łączności, często określanych jako obiekty podwójnego zastosowania, a więc obiektów wspierających tak ludność cywilną, jak i państwo oraz jego instytucje. Co więcej, te same państwa – w sytuacji konfliktu zbrojnego – z racji swojego rozwoju gospodarczego są w stanie zapewnić skuteczną ochronę tych obiektów na swoim terytorium. Odmienne stanowisko w tym zakresie prezentują państwa rozwijające się, dla których atak wymierzony w obiekty ich infrastruktury krytycznej, obejmujące przede wszystkim obiekty podwójnego zastosowania, jak sektor energetyczny czy zaopatrzenia w wodę, może doprowadzić do całkowitego paraliżu państwa, pośrednio hamując jego rozwój gospodarczy⁸²⁹.

Czy przedstawione dylematy oznaczają, że ochrona infrastruktury krytycznej podczas konfliktu zbrojnego pozostanie nadal ograniczona, czy może istnieją alternatywne sposoby rozszerzenia tej ochrony? Szukając tych sposobów, społeczność międzynarodowa powinna zwrócić się w kierunku prawa miękkiego (*soft law*), które co prawda nie jest prawnie wiążące, jednak zapewnia większą elastyczność w jego stosowaniu. Instrumenty prawa miękkiego mają za zadanie tylko wskazać państwom kierunek działania w określonej materii. Obecnie należy wyróżnić trzy główne elementy prawa miękkiego: rezolucje organów organizacji

z konieczności współpracy gospodarczej państw europejskich. Inaczej sytuacja kształtuje się w przypadku ochrony infrastruktury krytycznej podczas konfliktu zbrojnego – porozumienie musiałyby osiągnąć państwa, które są dla siebie potencjalnymi wrogami, tym samym nie powinna dziwić niechęć państw do uregulowania tej materii.

⁸²⁹ B. Ngalim, *Towards the Legal Protection of Critical Infrastructure in Africa against Cyberwar and Cyberterrorism*, „Journal of Cyberspace Studies”, 2023, vol. 7, no. 2, s. 142.

międzynarodowych⁸³⁰, porozumienia pomiędzy państwami⁸³¹ oraz rekomendacje pozarządowych organizacji międzynarodowych⁸³².

Współcześnie, miękkie prawo odgrywa coraz większą rolę w regulacjach konkretnych obszarów prawa międzynarodowego, co widoczne jest zwłaszcza w przypadku ochrony środowiska naturalnego oraz zdrowia publicznego⁸³³. Czy zatem miękkie prawo może wpłynąć na rozszerzenie ochrony infrastruktury krytycznej podczas konfliktu zbrojnego? Zdecydowanie tak, a szczególna rola w tym zakresie powinna spoczywać na MKCK. Jednym z podstawowych zadań tej organizacji jest działalność zmierzająca do rozwijania MPH oraz jego upowszechniania, między innymi poprzez podejmowanie tzw. dyplomacji humanitarnej⁸³⁴, ale także poprzez opracowywanie wytycznych oraz dobrych praktyk w zakresie stosowania MPH⁸³⁵. Zatem dla zwiększenia skuteczności ochrony infrastruktury krytycznej podczas konfliktu zbrojnego MKCK powinien sporządzić wytyczne uwzględniające:

Definicję pojęcia infrastruktury krytycznej – rozumianej jako struktura połączonych ze sobą urządzeń, obiektów oraz systemów, które wpływają na bezpieczeństwo państwa oraz ludności, oddziałując na trzy główne kategorie – schronienie, zaopatrzenie oraz bezpieczeństwo;

⁸³⁰ Obejmują wszystkie decyzje oraz rekomendacje organizacji międzynarodowych, które na mocy ich statutu nie są wiążące dla państw członkowskich. Jednak ich prawnie niewiążący charakter nie skutkuje brakiem znaczenia prawnego, co widać szczególnie w przypadku przestrzegania Powszechnej Deklaracji Praw Człowieka z 1948 roku (przyjętej jako rezolucja ZO ONZ), zob. D. Thürer, *Soft Law*, Encyclopedia entries, Max Planck Encyclopedias of International Law, 2009, <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1469> (dostęp: 21.05.2026).

⁸³¹ Wszystkie porozumienia nie posiadające prawnie wiążącego charakteru, jednak dzięki znaczeniu prawnemu wpływające na relacje międzynarodowe, np. Akt końcowy Konferencji Bezpieczeństwa i Współpracy w Europie z 1975 roku, zob. D. Thürer, *Soft Law*....

⁸³² Dobre praktyki, wytyczne oraz wszystkie inne formy rekomendacji wystosowane przez pozarządowe organizacje międzynarodowe, jak MKCK, zob. L. Blumman, *In the trap of a legal metaphor: International soft law*, „The International and Comparative Law Quarterly”, 2010, vol. 59, no. 3, s. 607-608.

⁸³³ Por. D. Bodansky, *The Legal Character of the Paris Agreement*, „Review of European Community & International Environmental Law”, 2016, vol. 25, iss. 2, s. 149 oraz *Overcoming the “Soft vs Hard Law” Debate in the Development of New Global Health Instruments*, <https://opiniojuris.org/2021/11/30/overcoming-the-soft-vs-hard-law-debate-in-the-development-of-new-global-health-instruments/> (dostęp: 21.05.2026).

⁸³⁴ M. Marcinko, *Międzynarodowy Ruch Czerwonego Krzyża i Czerwonego Półksiężycy*, w: Z. Falkowski, M. Marcinko (red.), *Międzynarodowe prawo humanitarne konfliktów zbrojnych*, Wojskowe Centrum Edukacji Obywatelskiej, Warszawa 2014, s. 116.

⁸³⁵ Por. MKCK, *Guidelines on the protection of the natural environment in armed conflict. Rules and recommendations relating to the protection of the natural environment under international humanitarian law, with commentary*, International Committee of the Red Cross, Geneva 2020 oraz MKCK, *Guidelines on investigating violations of international humanitarian law: law, policy, and good practice*, The Geneva Academy of International Humanitarian Law and Human Rights/International Committee of the Red Cross, Geneva 2019.

Przedmiotowo-podmiotowy charakter infrastruktury krytycznej – ochrona powinna objąć swoim zakresem nie tylko same obiekty infrastruktury krytycznej, ale także personel zatrudniony w tych obiektach, który jest niezbędny do prawidłowego ich funkcjonowania;

Status obiektów podwójnego zastosowania – rekomendacje powinny uwzględnić szczególny status obiektów podwójnego zastosowania, w tym wskazywać konkretnie środki ostrożności, które strony konfliktu powinny podjąć w celu wyeliminowania lub znacznego obniżenia skutków ubocznych ataku dla ludności cywilnej.

Chociaż niedostosowanie się do wytycznych prawa miękkiego charakteryzuje się odpowiedzialnością polityczną, a nie prawnomiędzynarodową, to na obecnym etapie rozwoju MPH tylko rekomendacje i dobre praktyki, wypracowane przede wszystkim przez MKCK, są szansą na uszczelnienie i potencjalne rozszerzenie ochrony infrastruktury krytycznej podczas konfliktu zbrojnego.

Bibliografia

1. Umowy międzynarodowe

- Treaty of Nanjing (Nanking), 29.08.1842, <https://china.usc.edu/treaty-nanjing-nanking-1842> (dostęp: 27.10.2024)
- Deklaracja poszanowania prawa morskiego, Paryż, 16.04.1856, w: P. K. Marszałek, Międzynarodowe prawo humanitarne konfliktów zbrojnych. Dokumenty, Wydawnictwo C.H. Beck, Warszawa 2019
- Rezolucja Międzynarodowej Konferencji w Genewie, Genewa, 29.10.1863, w: P. K. Marszałek, Międzynarodowe prawo humanitarne konfliktów zbrojnych. Dokumenty, Wydawnictwo C.H. Beck, Warszawa 2019
- Konwencja o polepszeniu losu rannych w armiach w polu, Genewa, 22.08.1864, w: P. K. Marszałek, Międzynarodowe prawo humanitarne konfliktów zbrojnych. Dokumenty, Wydawnictwo C.H. Beck, Warszawa 2019
- Deklaracja wyrzeczenia się użycia, w czasie wojny, pocisków wybuchających o wadze poniżej 400 gramów, Sankt Petersburg, 11.12.1868, w: P. K. Marszałek, Międzynarodowe prawo humanitarne konfliktów zbrojnych. Dokumenty, Wydawnictwo C.H. Beck, Warszawa 2019
- Konwencja o poszanowaniu praw i zwyczajów wojny na lądzie i załącznik do niej: Regulamin dotyczący praw i zwyczajów wojny na lądzie, Haga, 29.07.1899, w: P. K. Marszałek, Międzynarodowe prawo humanitarne konfliktów zbrojnych. Dokumenty, Wydawnictwo C.H. Beck, Warszawa 2019
- Konwencja dotycząca praw i zwyczajów wojny lądowej, podpisana wraz z odnośnym Regulaminem, Haga, 18.10.1907, Dz. U. z 1927 r., nr 21, poz. 161
- Konwencja o bombardowaniu przez morskie siły zbrojne w czasie wojny, Haga, 18.10.1907, Dz. U. z 1936 r., nr 6 poz. 66
- Traktat pokoju między mocarstwami sprzymierzonymi i skojarzonymi i Niemcami, Wersal, 28.06.1919, Dz. U. z 1920 r., nr 35, poz. 200.
- Protokół dotyczący zakazu używania na wojnie gazów duszących, trujących lub podobnych oraz środków bakteriologicznych, Genewa, 17.06.1925, Dz. U. z 1929 r., nr 28, poz. 278
- Konwencja Genewska o polepszeniu losu chorych i rannych w armjach czynnych, Genewa, 27.07.1929, Dz. U. z 1932 r., nr 103, poz. 864
- Konwencja dotycząca traktowania jeńców wojennych, Genewa, 27.07.1929, Dz. U. z 1932 r., nr 103, poz. 866
- Convention for the Prevention and Punishment of Terrorism, Geneva, 16.11.1937, 19 League of Nations Official Journal 23 (1938)

Porozumienie międzynarodowe w przedmiocie ścigania i karania głównych przestępców wojennych Osi Europejskiej, Londyn, 8.08.1945, Dz. U. z 1947 r., nr 63, poz. 367

Traktat Północnoatlantycki, Waszyngton, 4.04.1949, Dz. U. z 2000 r., nr 87, poz. 970

Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności, zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2, Rzym, 4.11.1950, Dz. U. z 1993 r., nr 61, poz. 284

Konwencja o polepszaniu losu rannych i chorych w armiach czynnych, Genewa, 12.08.1949, Dz. U. z 1956 r., nr 56, poz. 175

Konwencja o polepszaniu losu rannych, chorych i rozbitków sił zbrojnych na morzu, Genewa, 12.08.1949, Dz. U. z 1956 r., nr 56, poz. 175

Konwencja o traktowaniu jeńców wojennych, Genewa, 12.08.1949, Dz. U. z 1956 r., nr 56, poz. 175

Konwencja o ochronie osób cywilnych podczas wojny, Genewa, 12.08.1949, Dz. U. z 1956 r., nr 56, poz. 175

Układ w sprawie Antarktyki, Waszyngton, 1.12.1959, Dz. U. z 1961 r., nr 46, poz. 237

Konwencja w sprawie przestępstw i niektórych innych czynów popełnionych na pokładzie statków powietrznych, Tokio, 14.09.1963, Dz. U. z 1971 r., nr 15, poz. 147

Międzynarodowy Pakt Praw Obywatelskich i Politycznych, Nowy Jork, 19.12.1966, Dz. U. z 1977 r., nr 38, poz. 167

Międzynarodowy Pakt Praw Gospodarczych, Społecznych i Kulturalnych, Nowy Jork, 19.12.1966, Dz. U. z 1977, nr 38, poz. 169

Układ o zakazie broni jądrowych w Ameryce Łacińskiej i na Karaibach, Tlatelolco, 14.02.1967, United Nations Treaty Series, 1967, vol. 634, nr 326

Układ o nierozprzestrzaniu broni jądrowej, Moskwa, Waszyngton i Londyn, 1.07.1968, Dz. U. z 1970 r., nr 8, poz. 60

Konwencja Wiedeńska o Prawie Traktatów, Wiedeń, 23.05.1969, Dz. U. z 1990 r., nr 74, poz. 439

Konwencja o zwalczaniu bezprawnego zawładnięcia statkami powietrznymi, Haga, 16.12.1970, Dz. U. z 1972 r., nr 25, poz. 181

Konwencja o zwalczaniu bezprawnych czynów skierowanych przeciwko bezpieczeństwu lotnictwa cywilnego, Montreal, 23.09.1971, Dz. U. z 1976 r., nr 8, poz. 37.

Konwencja o zakazie prowadzenia badań, produkcji i gromadzenia zapasów broni bakteriologicznej (biologicznej) i toksycznej oraz o ich zniszczeniu, Moskwa, Londyn i Waszyngton, 10.04.1972, Dz. U. z 1976 r., nr 1, poz. 1

Europejska konwencja o zwalczaniu terroryzmu, Strasburg, 27.01.1977, Dz.U. z 1996 r., nr 117, poz. 557

- Protokół dodatkowy do Konwencji genewskich z 12 sierpnia 1949 roku, dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych (Protokół dodatkowy I), Genewa, 08.06.1977, Dz. U. z 1992 r., nr 41, poz. 175
- Protokół dodatkowy do Konwencji genewskich z 12 sierpnia 1949 roku, dotyczący ochrony ofiar konfliktów zbrojnych niemających charakteru międzynarodowego (Protokół dodatkowy II), Genewa, 08.06.1977, Dz. U. z 1992 r., nr 41, poz. 175
- Konwencja o zakazie lub ograniczeniu użycia pewnych broni konwencjonalnych, które mogą być uważane za powodujące nadmierne cierpienia lub mające niekontrolowane skutki, wraz z załącznikami, Genewa, 10.10.1980, Dz. U. 1984 r., nr 23, poz. 104
- Protokół w sprawie zakazów lub ograniczeń użycia broni zapalających (Protokół III), załączony do Konwencji o zakazie lub ograniczeniu użycia pewnych broni konwencjonalnych, które mogą być uważane za powodujące nadmierne cierpienia lub mające niekontrolowane skutki, Genewa, 10.10.1980, Dz. U. z 1984 r., nr 23, poz. 104
- Traktat o strefie bezatomowej na Południowym Pacyfiku, Rarotonga, 6.08.1985, United Nations Treaty Series, 1987, vol. 1445, nr 178
- Protokół o zwalczaniu bezprawnych czynów przemocy w portach lotniczych obsługujących międzynarodowe lotnictwo cywilne uzupełniający Konwencję o zwalczaniu bezprawnych czynów skierowanych przeciwko bezpieczeństwu lotnictwa cywilnego, Montreal, 24.02.1988, Dz. U. z 2006 r., nr 48, poz. 348
- Agreement on a comprehensive political settlement of the Cambodia conflict, Paryż, 23.10.1991, United Nations Treaty Series, 1992, vol. 1663, nr 28613
- Agreement Relating to the Establishment of a Protected Zone around the Hospital of Osijek, between the Federal Republic of Yugoslavia and Croatia, Pècs, 27.12.1991, https://theirwords.org/media/transfer/doc/sc_yu_croatia_serbia_1991_05-a9cc261d359aa66dc002e823921202f6.pdf (dostęp: 15.05.2026)
- Konwencja o zakazie prowadzenia badań, produkcji, składowania i użycia broni chemicznej oraz o zniszczeniu jej zapasów, Paryż, 13.01.1993, Dz. U. z 1999 r., nr 63, poz. 703
- Protokół w sprawie laserowych broni oślepiających (Protokół IV) do Konwencji o zakazie lub ograniczeniu pewnych broni konwencjonalnych, które mogą być uznawane za powodujące nadmierne cierpienia lub z natury nierozróżniające, Wiedeń, 12.10.1995, Dz. U. z 2007 r., nr 215, poz. 1583
- Traktat o strefie bezatomowej w Azji Południowo-Wschodniej, Bangkok, 15.12.1995, International Legal Materials, 1996, vol. 35, nr 635
- Poprawiony Protokół II w sprawie zakazów lub ograniczeń użycia min, min-pułapek i innych urządzeń zgodnie z poprawkami z dnia 3 maja 1996 r. (Protokół II zgodnie z poprawkami z dnia 3 maja 1996 r.) załączony do Konwencji o zakazie lub ograniczeniu użycia pewnych broni konwencjonalnych, które mogą być uważane za powodujące nadmierne cierpienia lub mające niekontrolowane skutki, sporządzonej w Genewie dnia 10 października 1980 r., Genewa, 3.05.1996, Dz. U. z 2005 r., nr 125, poz. 1048

Międzynarodowa Konwencja o zwalczaniu terrorystycznych ataków bombowych, Nowy Jork, 15.12.1997, Dz. U. z 2007 r., nr 66, poz. 438

Rzymski Statut Międzynarodowego Trybunału Karnego, Rzym, 17.07.1998, Dz. U. z 2003 r., nr 78, poz. 708

Międzynarodowa Konwencja w sprawie zwalczania aktów terroryzmu jądrowego, Nowy Jork, 13.04.2005, Dz. U. z 2010 r., nr 112, poz. 740

Konwencja Rady Europy o zapobieganiu terroryzmowi, Warszawa, 16.05.2005, Dz. U. z 2008 r., nr 161, poz. 998

Traktat o strefie bezatomowej w Azji Centralnej, Semipałatyńsk, 08.09.2006, United Nations Treaty Series, vol. 2970, nr 51633

Konwencja o amunicji kasetowej, Dublin, 30.05.2008, United Nations Treaty Series, vol. 2688, no. 47713

Traktat o zakazie broni nuklearnej, Nowy Jork, 7.07.2017, United Nations Documents A/CONF.229/2017/8

2. Uchwały i inne akty organów organizacji międzynarodowych

2.1. ONZ

2.1.1. Zgromadzenie Ogólne

Resolution 1(I), 24.01.1946, A/RES/1(I)

Resolution 217/III A, 10.12.1948, A/RES/217(III)

Resolution 1652 (XVI), 24.11.1961, A/RES/1652(XVI)

Resolution 2033 (XX), 3.12.1965, A/RES/2033(XX)

Resolution 47/37, 9.02.1993, A/RES/47/37

Resolution 49/75 K, 15.12.1994, A/RES/49/75

Resolution 56/83, 28.01.2002, A/RES/56/83

Resolution 68/262, 27.03.2014, A/RES/68/262

Resolution 71/258, 11.01.2017, A/RES/71/258

2.1.2. Rada Bezpieczeństwa

Resolution 678 (1990), 29.11.1990, S/RES/678(1990)

Resolution 751 (1992), 24.04.1992, S/RES/751 (1992)

Resolution 814 (1993), 26.03.1993, S/RES/814 (1993)

Resolution 827 (1993), 25.05.1993, S/RES/827 (1993), z późn. zmianami.

Resolution 955 (1994), 8.12.1994, S/RES/955 (1994), z późn. zmianami.

Resolution 1368 (2001), 12.09.2001, S/RES/1368 (2001)

Resolution 1373 (2001), 28.09.2001, S/RES/1373 (2001)

Resolution 1535 (2004), 26.03.2004, S/RES/1535 (2004)

Resolution 1566 (2004), 8.10.2004, S/RES/1566 (2004)

Resolution 2286 (2016), 3.05.2016, S/RES/2286 (2016)

Resolution 2341 (2017), 13.02.2017, S/RES/2341 (2017)

Resolution 2417 (2018), 24.05.2018, S/RES/2417 (2018)

2.1.3. Komisja Prawa Międzynarodowego

Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, Yearbook of the International Law Commission, 2011, vol. II, Part Two

Draft principles on protection of the environment in relation to armed conflicts, Yearbook of the ILC, 2022, vol. II, Part Two

2.2. Zgromadzenie państw-stron Statutu MTK

Elements of Crimes, 2011, "Official Records of the Assembly of States Parties to the Rome Statute of the International Criminal Court", First session, New York, 3-10.09.2002, United Nations Publications, Sales No. E.03.V.2 and corrigendum, part II.B

2.3. NATO

Deklaracja szczytu walijskiego, Newport, 5.09.2014,
<https://www.bbn.gov.pl/pl/wydarzenia/6170,Deklaracja-koncowa-sz-czytu-NATO-w-Walii-z-2014-r-polskielumaczenie.html> (dostęp: 2.06.2025)

Deklaracja końcowa szczytu NATO w Warszawie, Warszawa, 8.07.2016,
https://www.bbn.gov.pl/ftp/dok/03/37-40_KBN_Deklaracja_szczytu.pdf (dostęp: 2.06.2025)

Brussels Summit Declaration, Bruksela, 11.07.2018,
https://www.nato.int/cps/en/natohq/official_texts_156624.htm#21 (dostęp: 2.06.2025)

NATO 2022 Strategic Concept, Madryt, 29.06.2022,
https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf (dostęp: 2.06.2025)

2.4. Międzynarodowy Komitet Czerwonego Krzyża

Draft Rules for the Limitation of the Dangers incurred by the Civilian Population in Time of War, 1956, <https://ihl-databases.icrc.org/assets/treaties/420-Draft-ICRC-Rules-1956-EN.pdf> (dostęp: 8.04.2026)

Rules Relative to Behaviour of Combatants, Submitted to the First Session of the Conference of Government Experts, 24.05-12.06.1971, Geneva, https://library.icrc.org/library/docs/CD/CEG_1971_DOCUMENTS_ENG_4.pdf (dostęp: 21.12.2025)

Declaration Agenda for Humanitarian Action Resolutions, 28th International Conference of the Red Cross and Red Crescent Geneva, 2-6 December 2003, <https://library.icrc.org/library/docs/DOC/icrc-1103-002.pdf> (dostęp: 21.12.2025)

Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977, „International Review of the Red Cross”, 2006, vol. 88, no 864

ICRC report on the effects of the atomic bomb at Hiroshima, „International Review of the Red Cross”, 2015, vol. 97, no. 899

Statutes of the International Committee of the Red Cross, 21.12.2017, <https://www.icrc.org/en/document/statutes-international-committee-red-cross-0> (dostęp: 27.10.2024)

Guidelines on the Protection of the Natural Environment in Armed Conflict. Rules and Recommendations Relating to the Protection of the Natural Environment Under International Humanitarian Law, with Commentary, International Committee of the Red Cross, Geneva 2020

Food Security and Armed Conflict, Policy Brief, Geneva 2022, https://www.developmentaid.org/api/frontend/cms/file/2022/10/4662_002-ebook.pdf (dostęp: 8.04.2026)

Researching Violence Against Health Care: Gaps and Priorities, Report, March 2026, <https://healthcareindanger.org/wp-content/uploads/2022/06/elrha-and-icrc-violence-against-health-care-full-report-010720-digital.pdf> (dostęp: 8.04.2026)

The statement of ICRC President Mirjana Spoljaric, 23.03.2026, <https://www.icrc.org/en/statement/icrc-president-war-on-essential-infrastructure-is-war-on-civilians> (dostęp: 15.05.2026)

2.5. Pozostale dokumenty

ZO ONZ, Report of the Study Group of the International Law Commission: Fragmentation of International Law: Difficulties Arising From the Diversification and Expansion of International Law, 13.04.2006, A/CN.4/L.682

ZO ONZ, Letter from the Permanent Representative of Spain to the United Nations addressed to the Secretary-General, 1.04.2019, A/73/822–S/2019/285

- ZO ONZ, Safety and security of nuclear facilities of Ukraine, including the Zaporizhzhia nuclear power plant, 5.07.2024, A/78/L.90
- RB ONZ, Letter from the Chairman of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Security Council, 19.02.2004, S/2004/124
- RB ONZ, Letter dated 8 July 2025 from the Permanent Representative of Slovenia to the United Nations addressed to the Secretary-General, 9 July 2025, S/2025/453
- Rada Praw Człowieka ONZ, Assault on medical care in Syria, 13.09.2013, A/HRC/24/CRP.2
- OHCHR, Overview Report. Practices and policies affecting human rights in the Occupied Palestinian Territory, including East Jerusalem (7 October 2023 – 31 May 2025), 18.05.2026,
<https://www.ohchr.org/sites/default/files/documents/countries/opt/occupied-palestinian-territory-overview-report-east-jerusalem-practices-en.pdf> (dostęp: 24.05.2026)
- WHO, Effects of Nuclear War on Health and Health Services, Report of the WHO Management Group on Follow-up of Resolution WHA36.28, Geneva 1987,
<https://iris.who.int/server/api/core/bitstreams/ba2bd9fd-1d75-4672-a3e9-b66df956ec1f/content> (dostęp: 15.05.2026)
- WHO, Surveillance System for Attacks on Health Care (SSA). Methodology Version 1.0, Geneva 2018, WHO/WHE/EMO/2019.2/BRO,
<https://iris.who.int/server/api/core/bitstreams/6be521b9-cc94-4609-9c50-def0e470a5bb/content> (dostęp: 8.04.2026)
- MAEA, Nuclear Safety, Security and Safeguards in Ukraine. February 2022–February 2023,
<https://www.iaea.org/sites/default/files/documents/nuclear-safety-security-and-safeguards-in-ukraine-feb-2023.pdf> (dostęp: 8.04.2026)
- MTKJ, Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, The Hague, 8.06.2000, „International Legal Materials”, 2000, vol. 39, nr 5
- OBWE, Decision No. 6/07 Protecting Critical Energy Infrastructure from Terrorist Attack, 30.11.2007, MC.DEC/6/07

3. Akty prawa Unii Europejskiej

3.1. Rozporządzenia

- Rozporządzenie (WE) nr 725/2004 Parlamentu Europejskiego i Rady w sprawie podniesienia ochrony statków i obiektów portowych, 31.03.2004, Dz. Urz. L 129/6 z 29.04.2004
- Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 300/2008 w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002, 11.03.2008, Dz. Urz. L 97/72 z 9.04.2008

Rozporządzenia Rady (WE) NR 428/2009 ustanawiające wspólnotowy system kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania, 5.05.2009, Dz. Urz. UE L 134/1 z 29.05.2009

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013, 17.04.2019, Dz. Urz. L 151/15 z 7.06.2019

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/821 ustanawiające unijny system kontroli wywozu, pośrednictwa, pomocy technicznej, tranzytu i transferu produktów podwójnego zastosowania, 20.05.2021, Dz. Urz. UE L 206/1 z 11.06.2021

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2371 w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylenia decyzji nr 1082/2013/UE, 23.11.2022, Dz. Urz. L 314/26 z 6.12.2022

Rozporządzenie delegowane Komisji (UE) 2023/2450 uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2557 przez ustanowienie wykazu usług kluczowych, 25.07.2023, Dz. Urz. UE L 2023/2450 z 30.10.2023

3.2. Dyrektywy

Dyrektywa Rady 2008/114/WE w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, 8.12.2008, Dz. Urz. UE L 345/75 z 23.12.2008

Załącznik I do Dyrektywa Rady 2008/114/WE w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, 8.12.2008, Dz. Urz. UE L 345/75 z 23.12.2008

Załącznik III do Dyrektywa Rady 2008/114/WE w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, 8.12.2008, Dz. Urz. UE L 345/75 z 23.12.2008

Dyrektywa Rady 2009/7/EURATOM ustanawiająca wspólnotowe ramy bezpieczeństwa jądrowego obiektów jądrowych, 25.06.2009, Dz. Urz. UE L 172/18 z 2.7.2009

Dyrektywy Parlamentu Europejskiego i Rady 2014/65/UE w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE, 15.05.2014, Dz. Urz. UE L 173/349 z 12.6.2014

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148, 14.12.2022, Dz. Urz. L 333/80 z 27.12.2022

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE, 14.12.2022, Dz. Urz. UE L 333/164 z 27.12.2022

3.3. Pozostałe

Europejska Strategia Przeciwko Proliferacji Broni Masowego Rażenia, 10.03.2003, <https://data.consilium.europa.eu/doc/document/ST-15708-2003-INIT/en/pdf> (dostęp: 7.01.2026).

Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism, 20.10.2004, COM/2004/0702 final, <https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52004DC0702> (dostęp: 5.06.2024)

Wspólny Komunikat do Parlamentu Europejskiego i Rady „Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym odpowiedź Unii Europejskiej”, 6.04.2016, JOIN(2016) 18 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016JC0018> (dostęp: 2.06.2025)

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Plan działania na rzecz zwiększania gotowości na wypadek chemicznych, biologicznych, radiologicznych i jądrowych zagrożeń dla bezpieczeństwa”, 18.10.2017, COM(2017) 610 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52017DC0610> (dostęp: 2.06.2025)

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Zwalczanie dezinformacji w Internecie: podejście europejskie”, 26.04.2018, COM(2018) 236 final, <https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52018DC0236> (dostęp: 28.05.2025)

Wspólny Komunikat do Parlamentu Europejskiego, Rady Europejskiej i Rady „Zwiększenie odporności i wzmocnienie zdolności reagowania na zagrożenia hybrydowe”, 13.06.2018, JOIN(2018) 16 final, <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52018JC0016> (dostęp: 2.06.2025)

2018 Code of Practice on Disinformation, 28.06.2018 <https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation> (dostęp: 2.06.2025)

4. Akty prawa krajowego

4.1. Polska

Ustawa z dnia 10 kwietnia 1997 r. Prawo energetyczne, Dz. U. z 1997 r., nr 54, poz. 348

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny, Dz. U. z 1997 r., nr 88, poz. 553

Ustawa z dnia 22 stycznia 1999 r. o ratyfikacji Traktatu o całkowitym zakazie prób jądrowych, przyjętego przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 10 września 1996 r., 22.01.1999, Dz. U. z 1999 r., nr 15, poz. 136

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz. U. z 2002 r., nr 144, poz. 1204

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, Dz. U. z 2002 r., nr 156, poz. 1301

Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, Dz. U. z 2004 r., nr 171, poz. 1800

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz. U. z 2007 r., nr 89, poz. 590

Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej, Dz. U. z 2011 r., nr 112, poz. 654

4.2. Stany Zjednoczone

Instrukcje dla dowództw Armii Stanów Zjednoczonych w polu zatwierdzone przez prezydenta Stanów Zjednoczonych, 23.04.1863, w: P. K. Marszałek, Międzynarodowe prawo humanitarne konfliktów zbrojnych. Dokumenty, Wydawnictwo C.H. Beck, Warszawa 2019

Conduct of the Persian Gulf War, Final Report to Congress, 1.04.1992, <https://apps.dtic.mil/sti/pdfs/ADA249270.pdf> (dostęp: 21.12.2025)

Executive Order EO 13010 Critical Infrastructure Protection, 15.07.1996, <https://irp.fas.org/offdocs/eo13010.htm> (dostęp: 5.06.2024)

Military Commissions Act, 28.10.2009, <https://www.govinfo.gov/content/pkg/USCODE-2009-title10/html/USCODE-2009-title10-subtitleA-partII-chap47A-subchapVIII-sec950p.htm> (dostęp: 27.10.2024)

United States District Court Western District of Pennsylvania, Indictment, 15.10.2020, <https://www.justice.gov/usao-wdpa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware> (dostęp: 27.10.2024)

18 USC 2331: Definitions, 18-Crimes and Criminal Procedure, [https://uscode.house.gov/view.xhtml?req=\(title:18%20section:2331%20edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:18%20section:2331%20edition:prelim)) (dostęp: 2.06.2025)

4.3. Izrael

Israel's War with Hizbullah. Preserving Humanitarian Principles While Combating Terrorism, Diplomatic Notes No. 1, Ministry of Foreign Affairs of Israel, April 2007

Briefing to the Diplomatic Corps by the Vice Prime Minister and Minister of Foreign Affairs, 3.03.2008, <https://www.gov.il/en/pages/briefing-by-fm-livni-to-the-diplomatic-corps-3-mar-2008> (dostęp: 14.05.2026)

5. Orzeczenia oraz decyzje trybunałów i sądów międzynarodowych

5.1. Stały Trybunał Sprawiedliwości Międzynarodowej

Case of the S.S. "Wimbledon" (United Kingdom, France, Italy & Japan v. Germany), Judgment, 17.08.1923, Publications of the Permanent Court of International Justice, 1923, series A – no. 1

Case concerning factory at Chorzów (Germany v. Poland), Judgment, 13.09.1928, Publications of the Permanent Court of International Justice, 1928, series A – no. 13

5.2. Międzynarodowy Trybunał Sprawiedliwości

Corfu Channel (United Kingdom v. Albania), Judgment, 9.04.1949, ICJ Reports, 1949

North Sea Continental Shelf (Germany v. Denmark, Germany v. Netherlands), Dissenting Opinion of Judge Tanaka, 20.02.1969, ICJ Reports, 1969

Case concerning United States diplomatic and consular staff in Tehran (USA v. Iran), Judgment, 24.05.1980, ICJ Reports, 1980

Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. USA), Judgment, 27.06.1986, ICJ Reports, 1986

Legality of the threat or use of nuclear weapons, Advisory Opinion, 8.07.1996, ICJ Reports, 1996

LaGrand Case (Germany v. United States Of America), Request for the Indication of Provisional Measures, 3.03.1999, ICJ Reports, 1999

Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, 20.04.2010, ICJ Reports, 2010

Accordance with international law of the unilateral declaration of independence in respect of Kosovo, Advisory Opinion, 22.07.2010, ICJ Reports, 2010

5.3. Międzynarodowy Trybunał Karny dla byłej Jugosławii

Prosecutor v. Duško Tadić, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2.10.1995 r., IT-94-1

Prosecutor v. Duško Tadić, Appeals Chamber Judgement, 15.07.1999 r., IT-94-1

Prosecutor v. Stanislav Galić, Judgment, 5.12.2003, IT-98-29

Prosecutor v. Dario Kordić and Mario Čerkez, Judgment on Appeal, 17.12.2004, IT-95-14/2-A

Prosecutor v. Stanislav Galić, Judgment on Appeal, 30.11.2006, IT-98-29

Prosecutor v. Haradinaj et al., Trial Chamber Judgement, 3.04.2008 r., IT- 04-84-T

5.4. Międzynarodowy Trybunał Karny

Situation in the Democratic Republic of the Congo in the Case of the Prosecutor v. Germain Katanga, Judgment pursuant to article 74 of the Statute, 7.03.2014, ICC-01/04-01/07

Situation in the State of Palestine, Pre-Trial Chamber I, 21.11.2024

5.5. Trybunał Sprawiedliwości Unii Europejskiej

Wyrok w sprawie Oscar Bronner GmbH & Co. KG, C-7/97, 26.12.1998, ECLI:EU:C:1998:569

Opinia Rzecznika Generalnego – Google LLC, Alphabet, Inc., C-48/22 P, 11.01.2024, ECLI:EU:C:2024:14

5.6. Sądy krajowe

Wyrok Wojewódzkiego Sądu Administracyjnego we Wrocławiu, 2.02.2023, II SA/Wr 283/22

Postanowienie Wojewódzkiego Sądu Administracyjnego w Gliwicach, 7.06.2023, III SAB/Gl 99/23

Wyrok Wojewódzkiego Sądu Administracyjnego w Poznaniu, 21.09.2023, I SA/Po 440/23

5.7. Pozostałe

SCSL, Sesay case, Judgment, 2.03.2009, SCSL-04-15-T

6. Literatura

6.1. Monografie

Aleksandrowicz T., *Terroryzm międzynarodowy*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008

Aleksandrowicz T., *Świat w sieci. Państwa – społeczeństwa – ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Wydawnictwo Difin S.A., Warszawa 2014

Anzilotti D., *Cours de Droit International*, <https://archive.org/details/in.ernet.dli.2015.475454/page/n7/mode/1up> (dostęp: 9.04.2026)

Białek T., *Terroryzm. Manipulacja strachem*, Studio EMKA, Warszawa 2005

Boissier P., *History of the International Committee of the Red Cross, From Solferino to Tsushima*, Henry Dunant Institute, Geneva 1985

Bolechów B., *Terroryzm w świecie podwubiegunowym*, Wydawnictwo Adam Marszałek, Toruń 2002

Brownlie I., *Principles of Public International Law*, Clarendon Press, Oxford 1998

- Bothe M., Partsch K. J., Solf W. A., *New Rules for Victims of Armed Conflicts. Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949. Second Edition*, Brill, Nijhoff 2013
- Cała-Wacinkiewicz E., *Fragmentacja prawa międzynarodowego*, Wydawnictwo C.H. Beck, Warszawa 2018
- Czapliński W., Wyrozumska A., *Prawo międzynarodowe publiczne. Zagadnienia systemowe*, Wydawnictwo C.H. Beck, Warszawa 2014
- Grzebyk P., *Cele osobowe i rzeczowe w konfliktach zbrojnych w świetle prawa międzynarodowego*, Wydawnictwo Naukowe SCHOLAR, Warszawa 2018
- Drózd D., *Terroryzm i akt terroryzmu na świecie w świetle prawa*, Wydawnictwo My Book, Szczecin 2018
- Dunant H., *A Memory of Solferino*, International Committee of the Red Cross, Geneva, English version American Red Cross (1939, 1959)
- Fischer D., *History of the International Atomic Energy Agency. The First Forty Years*, Division of Publications International Atomic Energy Agency, Vienna 1998
- Graham T., LaVera D. J., *Cornerstones of Security: Arms Control Treaties in the Nuclear Era*, University of Washington Press, Washington DC 2002
- Henckaerts J.M., Doswald-Beck L., *Customary International Humanitarian Law Volume I: Rules*, Cambridge, 2005
- Hoffman F.G., *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, Arlington 2007
- Iwan-Sojka D., *Responsibility of war industry for lethal autonomous weapons systems*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2024
- Jarosz I., Jaroszewski P., Kijewski P., Kruk T. J., Silicki K., Grudziecki T., *System bezpieczeństwa cyberprzestrzeni RP*, Naukowa i Akademicka Sieć Komputerowa (NASK/ CERT Polska), Warszawa 2015
- Jasper S., *Russian Cyber Operations: Coding the Boundaries of Conflict*, Georgetown University Press 2020
- Jaśkiewicz-Kamińska S., *Prawo do bezpiecznej infrastruktury krytycznej*, Instytut Wydawniczy EuroPrawo, Warszawa 2016
- Kaldor M., *New and Old War. Organized Violence in a Global Era*, Stanford University Press, Cambridge 2012, 3. wydanie
- Kohler Ch., *An Ancient Practice with a New Face: The Use of Water as a Weapon in Times of Climate Change*, Peace Research Institute Frankfurt, Frankfurt 2020
- Kowalczevska K., *Sztuczna Inteligencja na wojnie. Perspektywa Międzynarodowego Prawa Humanitarnego Konfliktów Zbrojnych*, Wydawnictwo Naukowe Scholar Spółka z o.o., Warszawa 2021

- Koziej S., *Między piekłem a rajem. Szare bezpieczeństwo na progu XXI wieku*, Wydawnictwo Adam Marszałek, Toruń 2006
- Kulig K., *Teoria pracowniczej odpowiedzialności porządkowej*, Wydawnictwo C.H. Beck, Warszawa 2017
- Maciejewski R., *Ochrona infrastruktury krytycznej – narracje prawne i politologiczne*, FNCE Sp. z o.o., Poznań 2019
- Masło K., *Międzynarodowa odpowiedzialność karna jednostek za zbrodnie przeciwko ludzkości*, Wydawnictwo Instytutu Wymiaru Sprawiedliwości, Warszawa 2020
- Molendowska M., Ostrowska M., Górski P., *Infrastruktura krytyczna jako element bezpieczeństwa – wymiar europejski i krajowy*, Wydawnictwo Adam Marszałek, Toruń 2021
- Mustafovski R., *Military Communications Doctrine - A Systematic Guide to Command, Control, and Communications in Modern Armed Forces*, LAP LAMBERT Academic Publishing, London/Chisinau 2026
- Nemeth W. J., *Future War and Chechnya: A Case for Hybrid Warfare*, Naval Postgraduate School, Monterey 2002
- Nowakowska-Małusecka J., *Odpowiedzialność karna jednostek za zbrodnie popełnione w byłej Jugosławii i w Rwandzie*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2000
- Nowakowska-Małusecka J., *Sytuacja dziecka w konflikcie zbrojnym. Studium prawnomiędzynarodowe*, Oficyna Wydawnicza BRANTA, Bydgoszcz 2011
- Pictet J., *Le droit humanitaire et la protection des victimes de la guerre*, Institut Henry-Dunant, Geneve 1973
- Pięta J., *Broń Masowego Rażenia*, WSBIO, Warszawa 2006
- Płaczek J., *Filary bezpieczeństwa narodowego. Zarys teorii*, Wydawnictwo Lotniczej Akademii Wojskowej, Dęblin 2022, s. 10.
- Pszczółowski T., *Mała encyklopedia prakseologii i teorii organizacji*, Zakład Prakseologii Instytutu Filozofii i Socjologii PAN, Wrocław–Warszawa–Kraków–Gdańsk 1978
- Roscini M., *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford 2014
- Sandoz Y., Swinarski Ch., Zimmermann B., *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Genewa, 1987
- Schmitt M. N., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge 2017
- Sliedregt van E., *Individual Criminal Responsibility in International Law*, Oxford University Press, New York 2012
- Sun Tzu, *Sztuka Wojny*, Wydawnictwo Helion S.A., Gliwice 2008
- Szewko W., *Księga Dżihadu*, Alt.pl Sp. z o.o., Warszawa 2024

- Tomasiewicz J., *Terroryzm na tle przemocy politycznej*, Wydawnictwo APIS, Katowice 2000
- Żmigrodzki M. (red.), *Encyklopedia politologii. Tom 1 Teoria polityki*, Wydawnictwo Zakamycze, 1999
- Żuber M., *Broń Masowego Rażenia w Działalności Terrorystycznej*, Wydawnictwo Difin S.A., Warszawa 2015

6.2. Rozdziały w pracach zbiorowych

- Adamkiewicz J., *Militarny kontekst bezpieczeństwa infrastruktury energetycznej*, w: Kwiatkiewicz P., Szczerbowski R., Stańczyk K., Sobków R. (red.), *Energetyka w kręgu bezpieczeństwa i techniki*, FNCE Sp. z o.o., Poznań 2019
- Cieślarczyk M., *Problematyka bezpieczeństwa infrastruktury krytycznej postrzegana z różnych perspektyw badawczych*, w: Trybulska A. (red.), *Ochrona infrastruktury krytycznej*, Wydawnictwo Wyższej Szkoły Policji, Szczytno 2010
- Echevarria A. J., *The Civil War to the Boxer Rebellion*, w: Echevarria A. J., *Reconsidering the American way of war: US military practice from the revolution to Afghanistan*, Georgetown University Press, 2014
- Greenwood Ch., *International Humanitarian Law in Context*, w: Cheng Ch.-J. (ed.), *A New International Legal Order*, Brill | Nijhof, 2016
- Hemmings A. D., *The 1959 Antarctic Treaty and Subsequent Antarctic Treaty System*, w: Hemmings A. D., Offerdal K., Oral N., Conley H. A. (ed.), *History Lessons for the Arctic: What International Maritime Disputes Tell Us about a New Ocean*, Center for Strategic and International Studies (CSIS), Washington DC 2016
- Henderson D. A., *Bioterroryzm. Pierwsza linia naszego reagowania w ocenie gotowości amerykańskiej publicznej służby zdrowia i medycyny*, w: Alexander Y., Koenig M. (red.), *Superterroryzm biologiczny, chemiczny i nuklearny*, Wydawnictwo Bellona, Warszawa 2001
- Joshi A., *BTWC: The History of Early Negotiations*, w: Lele A. (ed.), *50 Years of the Biological Weapons Convention. Tracking the Journey*, Pentagon Press LLP, New Delhi 2025
- Łasa R., *Cyberbezpieczeństwo służby zdrowia podczas pandemii COVID-19. Aspekty prawa międzynarodowego*, w: Halushchenko M., Bartosik Ł. D., Urbańczyk M. (red.), *Pandemia COVID-19. Aspekty polityczne, społeczne, ekonomiczne i prawne*, Wydawnictwo Naukowe ArchaeGraph Diana Łukomiak, Poznań 2022
- Łasa R., *Międzynarodowe prawo humanitarne – bufor bezpieczeństwa pomiędzy infrastrukturą krytyczną a cyberatakiem*, w: Banasik M., Rogozińska A. (red.), *Teoria i praktyka bezpieczeństwa międzynarodowego: kontekst rosyjski*, Wydawnictwo Difin S.A., Warszawa 2021
- Marcinko M., *Międzynarodowy Ruch Czerwonego Krzyża i Czerwonego Półksiężyca*, w: Falkowski Z., Marcinko M. (red.), *Międzynarodowe prawo humanitarne konfliktów zbrojnych*, Wojskowe Centrum Edukacji Obywatelskiej, Warszawa 2014

- Marcinko M., *Podstawowe zasady międzynarodowego prawa humanitarnego konfliktów zbrojnych*, w: Falkowski Z., Marcinko M. (red.), *Międzynarodowe prawo humanitarne konfliktów zbrojnych*, Wojskowe Centrum Edukacji Obywatelskiej, Warszawa 2014
- Mattelaer A., *Nuclear Sharing and NATO as a 'Nuclear Alliance'* w: Frühling S., O'Neil A. (ed.), *Alliances, Nuclear Weapons and Escalation: Managing Deterrence in the 21st Century*, Australian National University Press, Acton 2021
- Mikos-Skuza E., *Pomoc humanitarna w świetle międzynarodowego prawa humanitarnego konfliktów zbrojnych*, w: Grzebyk P., Mikos-Skuza E. (red.), *Pomoc humanitarna w świetle prawa i praktyki*, Wydawnictwo Naukowe SCHOLAR, Warszawa 2016
- Pellet A., *The Definition of Responsibility in International Law*, w: Crawford J., Pellet A., Olleson S. (ed.), *The Law of International Responsibility*, Oxford University Press, New York 2010
- Stern B., *The Elements of an Internationally Wrongful Act*, w: Crawford J., Pellet A., Olleson S. (ed.), *The Law of International Responsibility*, Oxford University Press, New York 2010
- Tekielska P., Czekaj Ł., *Działanie służb w Unii Europejskiej realizujących zadania na rzecz bezpieczeństwa cybernetycznego*, w: Górka M. (red.) *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Wydawnictwo Difin S.A., Warszawa 2014
- Tomuschat Ch., *The Responsibility of the Other Entities*, w: Crawford J., Pellet A., Olleson S. (ed.), *The Law of International Responsibility*, Oxford University Press, New York 2010
- Trejnīs Z., *Infrastruktura Krytyczna – Koncepcje i Zarys*, w: A. Trybulska (red.), *Ochrona infrastruktury krytycznej*, Wydawnictwo Wyższej Szkoły Policji, Szczytno 2010
- Winterer E. L., *Nuclear Bomb Testing*, w: R. G. Gillespie, D. A. Clague (ed.) *Encyclopedia of Islands*, University of California Press, Berkley, Los Angeles and London 2009

6.3. Artykuły w czasopismach naukowych

- Abrashin R., *On Thin Ice: Qualification of Cyber-Attacks on Personal Data under International Humanitarian Law*, „Журнал ВШЭ по международному праву (HSE University Journal of International Law)”, 2024, vol. 2, no. 4
- Acharya A., Boutin J. D. K., *The Southeast Asia Nuclear Weapon-Free Zone Treaty*, „Security Dialogue”, 1998, vol. 29, no. 2
- Argyroudis S. A., Mitoulis S. A., Chatzi E., Baker J. W., Brilakis I., Gkoumas K., Vousdoukas M., Hynes W., Carluccio S., Keou O., Frangopol D. M., Linkov I., *Digital technologies can enhance climate resilience of critical infrastructure*, „Climate Risk Management”, 2022, vol. 35
- Barber R., *Uniting for Peace Not Aggression: Responding to Chemical Weapons in Syria Without Breaking the Law*, „Journal of Conflict and Security Law”, 2019, vol. 24, iss. 1

- Barcroft S., *The Hague Peace Conference of 1899*, „Irish Studies in International Affairs”, 1989, vol. 3, no. 1
- Barrett J. Q., *The Path from the 1907 Hague Conference to Nuremberg and Forward*, „Studies in Transnational Legal Policy”, 2008, vol. 39
- Bartels, *Timelines, borderlines and conflicts. The historical evolution of the legal divide between international and non-international armed conflicts*, „International Review of the Red Cross”, 2009, vol. 91, no. 873
- Bennett M., Gupta V., *Dealing in Security understanding vital services and how they keep you safe*, http://resiliencemaps.org/files/Dealing_in_Security.July2010.en.pdf (dostęp: 5.06.2024)
- Benvenuti P., *The ICTY Prosecutor and the Review of the NATO Bombing Campaign against the Federal Republic of Yugoslavia*, „European Journal of International Law”, 2001, vol. 12, no. 3
- Best G., *Peace Conferences and the Century of Total War: The 1899 Hague Conference and What Came After*, „International Affairs (Royal Institute of International Affairs 1944-)”, 1999, vol. 75, no. 3
- Blutman L., *In the trap of a legal metaphor: International soft law*, „The International and Comparative Law Quarterly”, 2010, vol. 59, no. 3
- Boczek J., Lewandowski M., *Wykorzystanie Owadów i Innych Organizmów w Akcjach Terroru i Konfliktach Zbrojnych*, „Zagadnienia Doradztwa Rolniczego”, 2015, 82(4)
- Bodansky D., *The Legal Character of the Paris Agreement*, „Review of European Community & International Environmental Law”, 2016, vol. 25, iss. 2
- Borrie J., *Banning cluster munitions*, „New Zealand International Review”, 2010, vol. 35, no. 5
- Breeze E. J., *Duty to act on knowledge: precautions, intelligence and the law of armed conflict*, „Journal of Conflict & Security Law”, 2024, vol. 29, iss. 3
- Brînzac M. G., Kuhlmann E., Dussault G., Ungureanu M. I., Chereches R. M., Baba C. O., *Defining medical deserts—an international consensus-building exercis*, „European Journal of Public Health”, 2023, vol. 33 (5)
- Buchan R., *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, „Journal of Conflict & Security Law”, 2012, vol. 17, iss. 2
- Bugnion F., *Birth of an idea: the founding of the International Committee of the Red Cross and of the International Red Cross and Red Crescent Movement: from Solferino to the original Geneva Convention (1859-1864)*, „International Review of the Red Cross”, 2012, vol. 94, nr. 888
- Burck K., S. Veini, *Attacks on chemical and nuclear facilities in Ukraine—legal frameworks and protections*, „Journal of Conflict & Security Law”, 2023, vol. 30
- Byron Ch., *Armed Conflicts: International or Non-International?*, „Journal of Conflict and Security Law”, 2001, vol. 6, iss. 1

- Capone F., *The Wave of Russian Attacks on Ukraine's Power Infrastructures: An Opportunity to Infuse Meaningfulness into the Notion of "Dual-use Objects"?*, „European Papers - A Journal on Law and Integration”, 2023, vol. 8, nr 2
- Carnahan B.M., *Lincoln, Lieber and the Laws of War: The Origins and Limits of the Principle of Military Necessity*, „The American Journal of International Law”, 1998, vol. 92, nr 2
- Carswel A. J., *Classifying the conflict: a soldier's dilemma*, „International Review of the Red Cross”, 2009, vol. 91, no. 873
- Cassese A., *The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia*, „European Journal of International Law”, 2007, vol. 18, nr 4
- Coupland R., *Humanity: What is it and how does it influence international law?*, „International Review of the Red Cross”, 2001, vol. 83, no. 844
- Courtland Moon van J. E., *Chemical Weapons and Deterrence: The World War II Experience*, „International Security”, 1984, vol. 8, no. 4
- Crawford J. W., *The Law of Noncombatant Immunity and the Targeting of National Electrical Power Systems*, „The Fletcher Forum of World Affairs”, 1997, vol. 21, no. 2
- Cronin B., *Reckless endangerment warfare: Civilian casualties and the collateral damage exception in international humanitarian law*, „Journal of Peace Research”, 2013, vol. 50, nr 2
- D'Alessandra F., Gillett M., *The War Crime of Starvation in Non-International Armed Conflict*, „Journal of International Criminal Justice”, 2019, vol. 17, iss. 4
- Dienelt A., *The Shadowy Existence of the Weapons Review and Its Impact on Disarmament*, „Sicherheit und Frieden (S+F)/Security and Peace”, 2018, vol. 36, no. 3
- Dinstein Y., *The Right to Humanitarian Assistance*, „Naval War College Review”, 2000, vol. 53, no. 4
- Docherty B., *Breaking New Ground: The Convention on Cluster Munitions and the Evolution of International Humanitarian Law*, „Human Rights Quarterly”, 2009, vol. 31, no. 4
- Dugard J., *Towards the Definition of International Terrorism*, „The American Journal of International Law”, 1973, vol. 67, nr 5, s. 95.
- Dupuis M.P., Heywood J.Q., Sarko M.Y.F., *The Sixth Annual American Red Cross-Washington College of Law Conference on International Humanitarian Law: A Workshop on Customary International Law and the 1977 Protocols Additional to the 1949 Geneva Conventions*, „American University Journal of International Law and Policy”, 1987, vol. 2, nr 2
- Durhin N., *Protecting civilians in urban areas: A military perspective on the application of international humanitarian law*, „International Review of the Red Cross”, 2016, vol. 98, iss. 901
- Fidler D. P., *Facing the global challenges posed by biological weapons*, „Microbes and Infection”, 1999, vol. 1, iss. 12

- Figueiredo B. M., *Strengthening the protection of civilian infrastructure in armed conflict: Practical measures to operationalize IHL and reduce civilian harm*, „International Review of the Red Cross”, 2026
- Fleming M., *Terroryzm polityczny w międzynarodowym prawodawstwie*, „Wojskowy Przegląd Prawniczy”, 1996, nr 1
- Gallais C., Filiol E., *Critical Infrastructure: Where Do We Stand Today? A Comprehensive and Comparative Study of the Definitions of a Critical Infrastructure*, „Journal of Information Warfare”, 2017, vol. 16, no. 1
- Gavrysh K., *Prosecuting Individuals for Environmental Harm in the Armed Conflict Between Russia and Ukraine: The Case of Destruction of the Kakhovka Dam*, „Polish Yearbook of International Law”, 2023, vol. XLIII
- Gellately R., College H., *Rethinking the Nazi Terror System: A Historiographical Analysis*, „German Studies Review”, 1991, vol. 14, no. 1
- Gierasimow W., *The Value of Science Is in the Foresight. New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations*, „Military Review”, January-February 2016, https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf (dostęp: 2.06.2025)
- Gisel L., Rodenhäuser T., Dörmann K., *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts*, „International Review of the Red Cross”, 2020, vol. 102, no. 913
- Goniewicz M., Goniewicz K., *Protection of medical personnel in armed conflicts—case study: Afghanistan*, „European Journal of Trauma and Emergency Surgery”, 2013, vol. 39 (2)
- Grębowski J., Skalski M., Bijak M., *The threat of weapons of mass destruction in the context of the conflict in Ukraine and its impact on battlefield medicine*, „Lekarz Wojskowy” 2025, vol. 103, no. 2
- Griffith B., *African Nuclear-Weapon-Free Zone Nears Realization*, „Arms Control Today”, 2008, vol. 38, no. 4
- Gross O., *Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-incidents*, „Cornell International Law Journal”, 2015, vol. 48, no. 3
- Gunawan Y., Pane M. E. R., *Responsibility for Excessive Infrastructure Damage in Attacks: Analyzing Russia's Attack in Ukraine*, „PETITA Jurnal Kajian Ilmu Hukum dan Syaria”, 2024, vol. 9, no. 1
- Gunderson G., *The Origin of the American Civil War*, „The Journal of Economic History”, 1974, vol. 34, nr 4
- Guź J., *Rola Agencji Bezpieczeństwa Wewnętrznego w zwalczaniu zagrożeń terrorystycznych na terytorium Rzeczypospolitej Polskiej*, „Studia nad Autorytaryzmem i Totalitaryzmem”, 2015, vol. 37, nr 3
- Hamourtziadou L., Jackson J., *Winning wars: the triumphs and myths of technology*, „Journal of Global Faultlines”, 2019, vol. 6, iss. 2

- Hansen J-E. S., *Concepts of offensive use of biological weapons*, „Militært Tidsskrift”, 2006, vol. 135
- Hathaway O. A., Crooto R., Levitz P., Nix H., Nowlan A., Perdue W., Spiegel J., *The Law of Cyber-Attack*, „California Law Review”, 2012, vol. 100, no. 4
- Hathaway O. A., Khan A., Revekin M. R., *The Dangerous Rise of “Dual-Use” Objects in War*, „The Yale Law Journal”, 2025, vol. 134
- Henckaerts J-M., *Study on customary international humanitarian law: A contribution to the understanding and respect for the rule of law in armed conflict*, „International Review of the Red Cross”, 2005, vol. 87, no. 857
- Hulme K., *Armed Conflict, Wanton Ecological Devastation and Scorched Earth Policies: How the 1990-91 Gulf Conflict Revealed the Inadequacies of the Current Laws to Ensure Effective Protection and Preservation of the Natural Environment*, „Journal of Armed Conflict Law”, 1997, vol. 2, no. 1
- Hutchins T. E., *Safeguarding civilian internet access during armed conflict: Protecting humanity’s most important resource in war*, „The Columbia Science & Technology Law Review”, 2020, vol. XXII, s. 179.
- Izak K., *Ataki terrorystyczne i sabotażowe na wybrane systemy infrastruktury krytycznej – perspektywa historyczna*, „Terroryzm – studia, analizy, prewencja”, 2025, wydanie specjalne
- Jevglevskaja N., *Weapons Review Obligation under Customary International Law*, „International Law Studies”, 2018, vol. 94
- Johannot-Gradis Ch., *Protecting the past for the future: How does law protect tangible and intangible cultural heritage in armed conflict?*, „International Review of the Red Cross”, 2015, vol. 97, no. 900
- Jorgensen N., *The Protection of Freshwater in Armed Conflict*, „Journal of International Law and International Relations”, 2007, vol. 3, nr 2
- Kacała-Szwarczyńska A., *Cyberatak w świetle międzynarodowego prawa humanitarnego konfliktów zbrojnych*, „Journal of Modern Science”, 2019, tom 2, nr 41
- Kanerva I., *Russia and the West: An Increasingly Difficult Relationship*, „Horizons: Journal of International Relations and Sustainable Development”, 2018, nr 12
- Kenig-Witkowska M. M., *Protection of the environment in times of non-international armed conflicts – a gap to be filled in*, „Studia Iuridica”, 2018, t. 78
- Kopeć R., *Zastosowanie broni biologicznej w konfliktach zbrojnych i atakach terrorystycznych*, „Annales Universitatis Paedagogicae Cracoviensis Studia de Securitate et Educatione Civili IV”, 2014
- Kopeć R., *Traktat o nierozprzestrzenianiu broni nuklearnej jako prawnomiędzynarodowy reżim zapobiegania proliferacji*, „Annales Universitatis Paedagogicae Cracoviensis Studia de Securitate et Educatione Civili V”, 2015

- Kosowski B., *Infrastruktura krytyczna w systemie bezpieczeństwa narodowego*, „Safety & Fire Technology”, 2019, vol. 54, iss. 2
- Kowalczevska K., *Computer network operations in the light of ius in bello*, „Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje”, 2014, nr 15, s. 140-141.
- Lallie H. S., Shepherd L. A., Nurse J. R. C., Erola A., Epiphaniou G., Maple C., Bellekens X., *Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic*, „Computers & Security”, 2021, vol. 105, no. 1
- Lasota-Jądrzak A., *Bezpieczeństwo infrastruktury krytycznej państwa*, „Rocznik Bezpieczeństwa Morskiego”, 2013, Rok VII
- Lazrak F., Nijkamp P., Rietveld P., Rouwendal J., *Cultural heritage and creative cities: an economic evaluation perspective*, Serie Research Memoranda 0036, VU University Amsterdam
- Łasa R., *Military review in the context of cyber-warfare. Article 36 of 1977 Additional Protocol I in practice*, „Acta Iuridica Resoviensia”, 2023, t. 43, nr 125
- Maclellan N., *The Nuclear Age in the Pacific Islands*, „The Contemporary Pacific”, 2005, vol. 17, no. 2
- Mačak K., *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law*, „Israel Law Review”, 2015, vol. 48, nr 1
- Małecka A., *Cyber-operations under international law*, „Colloquium: pedagogika, nauki o polityce i administracji”, 2022, t. 14, nr 3
- Marín A. P., Ben Ali R., *Guilt by association: Restricting humanitarian assistance in the name of counterterrorism*, „International Review of the Red Cross”, 2021, no. 916-917
- Maruf S., *Environmental Damage in Ukraine as Environmental War Crime under the Rome Statute*, „Journal of International Criminal Justice”, 2024, vol. 22, iss. 1
- Mendenhall E., *Nuclear-Weapon-Free Zones and Contemporary Arms Control*, „Strategic Studies Quarterly”, 2020, vol. 14, no. 4
- Mensa-Bonsu H. J. A. N., *The ICC, International Criminal Justice and International Politics*, „Africa Development”, 2015, vol. XL, no. 2
- Michailiuk B., *Broń biologiczna i bioterroryzm*, „Zeszyty Naukowe AON”, 2016, nr 1(102)
- Milewski J., *Identyfikacja infrastruktury krytycznej i jej zagrożeń*, „Zeszyty Naukowe AON” 2016, nr 4
- Mindrup A., *The Lieber Code: A Historical Analysis of the Context and Drafting of General Orders No. 100*, „The Cardinal Edge”, 2021, vol. 1 (27)
- Moir L., *Grave Breaches and Internal Armed Conflicts*, „Journal of International Criminal Justice”, 2009, vol. 7, no. 4
- Monagham S., Svendsen O., Darrah M., Arnold E., *NATO's Role in Protecting Critical Undersea Infrastructure*, Center for Strategic and International Studies, December 2023

- Newbill C.M., *Defining Critical Infrastructure for a Global Application*, „Global Legal Studies”, 2019, vol. 26, no. 2
- Niedźwiedzki D., *Kryzys humanitarny na granicy polsko-białoruskiej. Analiza zjawiska w perspektywie ładu społecznego*, „Politeja”, 2024, vol. 21, nr 1 (88/3)
- Ogunbanwo S., *The Treaty of Pelindaba: Africa Is Nuclear-Weapon-Free*, „Security Dialogue”, 1996, vol. 27, no. 2
- Pacek B., Pacek P., *Russia's devastating impact on critical infrastructure during the hybrid war in Ukraine*, „Bezpieczeństwo. Teoria i Praktyka”, 2023, nr 2 (LI)
- Piątkowski M., *Międzynarodowe prawo humanitarne wobec zastosowania broni zapalającej w konflikcie zbrojnym*, „Bezpieczeństwo – Teoria i Praktyka”, 2017, nr 2
- Pictet J., *The Medical Profession and International Humanitarian Law*, „International Review of the Red Cross”, 1985, vol. 25, no. 247, s. 198-199.
- Pursiainen C., *Russia's Critical Infrastructure Policy: What do we Know About it?*, „European Journal for Security Research”, 2021
- Ramadanovic P., *When Bombs Fall: Becoming American During the NATO Bombing of Yugoslavia*, „Discourse”, 2003, vol. 25, no. 1/2
- Redick J. R., *Regional Nuclear Arms Control in Latin America*, „International Organization”, 1975, vol. 29, no. 2
- Reed C., Anderson W., Kruczkiewicz A., Nakamura J., Gallo D., Seager R., McDermid S. S., *The impact of flooding on food security across Africa*, „Proceedings of the National Academy of Sciences of the United States of America”, 2022, vol. 119 (43)
- Reetz N. S., *Same Same but Different Why War-Sustaining Objects Can Be Destroyed but Not Targeted*, „Journal of Conflict & Security Law”, 2022, vol. 27, nr 3
- Robinson D. R., *The Treaty of Tlatelolco and the United States: A Latin American Nuclear Free Zone*, „The American Journal of International Law”, 1970, vol. 64, no. 2
- Rubenstein L., Haar R. J., Amon J. J., *Attacks on healthcare in war are being steadily normalized—we need to end impunity*, Opinion, BMJ, 2025, no. 390 (1964), <https://www.bmj.com/content/390/bmj.r1964> (dostęp: 24.05.2026)
- Rzeszuta M., *Sieć. Piąty Teatr Działań Wojennych: 2008 – Informatyczna Blokada Gruzji*, „Układ Sił”, 2020, nr 23
- Sandoz Y., *The History of the Grave Breaches Regime*, „Journal of International Criminal Justice”, 2009, vol. 7, no. 4
- Sassòli M., *State responsibility for violations of international humanitarian law*, „International Review of the Red Cross”, 2002, vol. 84, no. 846
- Schmitt M. N., *Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance*, „Virginia Journal of International Law”, 2010, vol. 50, nr 4

- Shakarian P., *The 2008 Russian Cyber Campaign Against Georgia*, „Military Review”, 2011, November-December
- Shue H., Wippman D., *Limiting Attacks on Dual-Use Facilities Performing Indispensable Civilian Functions*, „Cornell International Law Journal”, 2002, vol. 35, iss. 3
- Sidorkiewicz S., *Współczesne ujęcie funkcji państwa*, „Studia Elbląskie”, 2010, nr 11
- Smith D. C., *Military Medical History: The American Civil War*, „OAH Magazine of History”, 2005, vol. 19, nr 5
- Stohl M., *The Global War on Terror and State Terrorism*, „Perspectives on Terrorism”, 2008, vol. 2, nr 9, Special Issue: Under-investigated topics in terrorism research
- Subedi S. P., *Problems and Prospects for the Treaty on the Creation of a Nuclear-Weapon-Free Zone in Southeast Asia*, „International Journal of Peace Studies”, 1999, vol. 4, no. 1
- Sykulski L., *Rosyjska Koncepcja Wojen Buntowniczych Jewgienija Messnera*, „Przegląd Geopolityczny” 2015, tom 11
- Szpak A., *The Use of Water as a Weapon Under International Humanitarian Law with Special Emphasis on the Destruction of the Nova Kakhovka Dam*, „Studia Iuridica”, 2024, vol. 103
- Szumski A., *Status Prawny Donieckiej Republiki Ludowej i Ługańskiej Republiki Ludowej*, „Dyplomacja i Bezpieczeństwo”, 2015, nr 1 (3)
- Trumbull IV Ch.P., *Collateral damage and individual rights in armed conflict*, „Fordham Journal of International Law”, 2024, vol. 48, no. 2
- Tyczkowska-Kowerczyk A., *Zadania podejmowane na rzecz bezpieczeństwa publicznego wśród społeczności lokalnej jako przejaw działalności administracji publicznej*, „Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy”, 2020, nr 36 (3)
- Walek T., *Pojęcie, geneza i klasyfikacja zjawisk terrorystycznych*, „Securitologia” 2018, nr 2
- Wexler L., *International Humanitarian Law Transparency*, „Journal of Transnational Law & Policy”, 2014, vol. 23, iss. 1
- Wicks E., *The Meaning of ‘Life’: Dignity and the Right to Life in International Human Rights Treaties*, „Human Rights Law Review”, 2012, vol. 12, iss. 2, s. 219.
- Winter E., *Pillars not Principles: The Status of Humanity and Military Necessity in the Law of Armed Conflict*, „Journal of Conflict and Security Law”, 2020, vol. 25, iss. 1
- Wilt van der H., *War Crimes and the Requirement of a Nexus with an Armed Conflict*, „Journal of International Criminal Justice”, 2012, vol. 10, iss. 5
- Woudenberg van N., *The Long and Winding Road Towards an Instrument on Cluster Munitions*, „Journal of Conflict & Security Law”, 2008, vol. 12, no. 3
- Zarychta S., *Kontrola Zbrojeń i Traktaty Rozbrojeniowe Dotyczące Broni Jądrowej*, „Rocznik Bezpieczeństwa Morskiego”, 2015, rok IX, cz. IV

Zhukov Y. M., Talibova R., *Stalin's terror and the long-term political effects of mass repression*, „Journal of Peace Research”, 2018, vol. 55, no. 2

6.4. Pozostale

Amnesty International, *NATO/Federal Republic of Yugoslavia: „Collateral Damage” or Unlawful Killings? Violations of the Laws of War by NATO during Operation Allied Force*, London, 5.06.2000, <https://www.amnesty.org/en/documents/eur70/018/2000/en/> (dostęp: 21.12.2025)

CTC, *Physical protection of critical infrastructure against terrorist attacks, Counter-Terrorism Committee Executive Directorate Trends Report*, March 2017, <https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted-trends-report-march-2017-final.pdf> (dostęp: 5.06.2024)

Electricity Information Sharing and Analysis Center, *Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case*, Washington DC 2016, <https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf> (dostęp: 21.06.2024)

Federal Office for Information Security, *Third edition of the Franco-German common situational picture*, Bonn 2020, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DE-FR/de-fr_Lagebild_2020.pdf?__blob=publicationFile&v=1 (dostęp: 21.06.2024)

Human Rights Watch, *Civilian Deaths in the NATO Air Campaign*, New York, 7.02.2000, <https://www.hrw.org/reports/pdfs/g/general/natbm002.pdf> (dostęp: 21.12.2025)

Human Rights Watch, *Rain of Fire Israel's Unlawful Use of White Phosphorus in Gaza*, Report, March 2009, <https://www.hrw.org/reports/iopt0309webwcover.pdf> (dostęp: 1.03.2026)

Humanity in War, *Global Initiative to Galvanize Political Commitment to International Humanitarian Law. Progress Report*, October 2025, <https://www.upholdhumanityinwar.org/sites/default/files/2025-10/Global%20IHL%20Initiative%20Progress%20Report%20October%202025%20ENGLISH.pdf> (dostęp: 12.05.2026)

IHL in Focus: Spot Report Weaponizing Water and Humanitarian Collapse in Sudan: An International Humanitarian Law Assessment, The Geneva Academy of International Humanitarian Law and Human Rights, Geneva 2025, <https://geneva-academy.ch/wp-content/uploads/2025/09/IHL-Spot-Report-Weaponizing-Water-and-Humanitarian-Collapse-in-Sudan.pdf> (dostęp: 21.12.2025)

International Bank for Reconstruction and Development, *Joining Forces to Combat Protracted Crises. Humanitarian and Development Support for Water and Sanitation Providers in the Middle East and North Africa*, Washington D.C. 2021, https://www.icrc.org/sites/default/files/document_new/file_list/joining_forces_to_combat_protracted_crisis.pdf (dostęp: 8.04.2026)

- International Law Association, *Berlin Rules on Water Resources*, International Law Association Berlin Conference (2004), https://www.cawater-info.net/library/eng/l/berlin_rules.pdf (dostęp: 8.04.2026)
- International Law Institute, *Sixteenth Commission Humanitarian Assistance. Resolution of The International Law Institute*, 2.09.2003, <https://www.ifrc.org/Docs/idrl/I318EN.pdf> (dostęp: 8.04.2026)
- Izrael, *The Operation in Gaza 27 December 2008 – 18 January 2009. Factual and Legal Aspects*, 29.07.2009, <https://www.jewishvirtuallibrary.org/jsource/Peace/GazaOpReport0709.pdf> (dostęp: 27.10.2024)
- Jopling M., *The Protection of Critical Infrastructures. Special Report*, NATO Parliamentary Assembly, 24.08.2007, 162 CDS 07, https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/270/270907/270907jopling_en.pdf (dostęp: 5.06.2024)
- Komisja Nadzoru Finansowego, *Informacja na temat sytuacji sektora bankowego w 2022 roku*, Warszawa 2023, https://www.knf.gov.pl/?articleId=85173&p_id=18 (dostęp: 5.06.2024)
- Llinas M.M., *Hybrid Attacks on Critical Infrastructure* w: Bargués P., Bourekba M., Colomina C., *Hybrid threats, vulnerable order*, Barcelona Center for International Affairs, 2022, Report n°8
- OBWE, *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace*, Vienna 2013, <https://cdn.osce.org/sites/default/files/f/documents/4/b/103500.pdf> (dostęp: 5.06.2024)
- OECD, *Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security*, Investment Division, Directorate for Financial and Enterprise Affairs Organisation for Economic Co-operation and Development, May 2008
- OHCHR, *Attacks on Ukraine's Energy Infrastructure: Harm to the Civilian Population*, Bulletin, September 2024
- Organizacja Narodów Zjednoczonych ds. Wyżywienia i Rolnictwa, *Food Security. Policy Brief*, June 2006, Issue 2, https://www.fao.org/fileadmin/templates/faoitaly/documents/pdf/pdf_Food_Security_Cocept_Note.pdf (dostęp: 21.06.2024)
- Pillai H., *Protecting Europe's critical infrastructure from Russian hybrid threats*, Center for European Reform, 2023
- Polska, *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2020, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf (dostęp: 18.05.2026)
- RCB, *Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik 1. Charakterystyka systemów infrastruktury krytycznej*, Warszawa 2013

- RCB, *Narodowy Program Ochrony Infrastruktury Krytycznej*, Warszawa 2023
- Safeguarding Health in Conflict Coalition, *Epidemic of Violence: Attacks on Health Care in 2024*, Baltimore 2024, <https://insecurityinsight.org/wp-content/uploads/2025/04/2024-SHCC-Annual-Report.pdf> (dostęp: 8.04.2026)
- SIPRI, *Nuclear Security During Armed Conflict: Lessons from Ukraine*, Policy Paper, 2023
- Sova Ch., *Starvation Crimes and International Law: A New Era*, Center for Strategic and International Studies (CSIS), December 2024
- Starvation and Terror in Somalia*, Foreign Policy Bulletin, 1992, vol. 3, iss. 2
- Światowy Program Żywnościowy, *Global Report on Food Crises (GRFC) 2024*, <https://www.fsipplatform.org/report/global-report-food-crises-2024/> (dostęp: 21.06.2024)
- Thompson Ch. M., *The Bioterrorism Threat by Non-State Actors: Hype Or Horror?*, Naval Postgraduate School, Monterey, December 2006
- Thürer D., *Soft Law*, Encyclopedia entries, Max Planck Encyclopedias of International Law, 2009, <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1469> (dostęp: 21.05.2026)
- United Nations Environment Programme, *Rapid Environmental Assessment of Kakhovka Dam Breach*, Nairobi 2023, <https://wedocs.unep.org/rest/api/core/bitstreams/d16d8f8a-ee13-463e-b051-448ddb1577e/content> (dostęp: 8.04.2026)
- Urząd Komunikacji Elektronicznej, *Raport o stanie rynku telekomunikacyjnego w 2022 roku*, Warszawa 2023, <https://bip.uke.gov.pl/raporty/raport-o-stanie-ryнку-telekomunikacyjnego-za-2022-rok,78.html> (dostęp: 5.06.2024)
- USA, *Comments of the United States on the International Law Commission's draft principles on the protection of the environment in relation to armed conflicts*, 6.10.2021, https://legal.un.org/ilc/sessions/73/pdfs/english/poe_us.pdf (dostęp: 27.10.2024)
- USA, *Department of Defense Law of War Manual, June 2015 (Updated December 2016)*, <https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/USA-Law-of-War-Manual.pdf> (dostęp: 27.10.2024)
- USA, *Department of Defense Law of War Manual*, June 2015 (Updated July 2023), <https://media.defense.gov/2023/Jul/31/2003271432/-1/-1/0/DOD-LAW-OF-WAR-MANUAL-JUNE-2015-UPDATED-JULY%202023.PDF> (dostęp: 21.12.2025)
- USA, *DOD Dictionary of Military and Associated Terms*, Washington DC, The Joint Staff, November 2021, https://www.supremecourt.gov/opinions/URLs_Cited/OT2021/21A477/21A477-1.pdf (dostęp: 21.12.2025)
- USA, *Operations in Chemical, Biological, Radiological, and Nuclear Environments*, Joint Publication 3-11, 4 October 2013, https://edocs.nps.edu/2012/December/jp3_11.pdf, (dostęp: 4.01.2026)

- Víchová K., Hromada M., Paulus F., Valasek J., *CBRN Weapons as a Threat to Critical Infrastructure Elements*, 2022 6th International Conference on Medical and Health Informatics (ICMHI 2022), 13–15.05.2022, https://www.researchgate.net/publication/364557657_CBRN_Weapons_as_a_Threat_to_Critical_Infrastructure_Elements (dostęp: 15.05.2026)
- Wielka Brytania, *JSP 383 The Joint Service Manual of the Law of Armed Conflict*, Joint Service Publication 383, 2004 Edition, <https://assets.publishing.service.gov.uk/media/5a7952bfe5274a2acd18bda5/JSP3832004Edition.pdf>, (dostęp: 27.10.2024)
- World Health Organization, *The World Health Report 2000. Health systems: Improving Performance*, Geneva 2000
- Zanders J. P., *Preventing the Re-Emergence of Chemical Weapons. The evolution of chemical weapon use since 1990*, European Union Institute for Security Studies, Report 2019

7. Strony internetowe

Agencja Bezpieczeństwa Wewnętrznego	www.abw.gov.pl
Amnesty International	www.amnesty.org
Arms Control Association	www.armscontrol.org
Atlantic Council	www.atlanticcouncil.org
BBC	www.bbc.co.uk
Biuro Bezpieczeństwa Narodowego.	www.bbn.gov.pl
Bloomberg	www.bloomberg.com
Encyclopædia Britannica	www.britannica.com
CERT-EU	www.cert.europa.eu
Council on Foreign Relations	www.cfr.org
Komisja Europejska	www.commission.europa.eu
National Institute of Standards and Technology	www.csrc.nist.gov
CyberDefence24	www.cyberdefence24.pl
International cyber law: interactive toolkit	www.cyberlaw.ccdcoe.org
World Health Organization	www.data.who.int
Cambridge Dictionary	www.dictionary.cambridge.org
The Oxford Institute For Ethics, Law and Armed Conflict	www.elac.ox.ac.uk
European Medicines Agency	www.ema.europa.eu
Energetyka24	www.energetyka24.com

World Health Organization Extranet	www.extranet.who.int
Nextgov/FCW's	www.fcw.com
Serwis Rzeczypospolitej Polskiej	www.gov.pl
Global Firepower	www.globalfirepower.com
Health Policy Watch	www.healthpolicy-watch.news
Human Rights Watch	www.hrw.org
International Campaign to Abolish Nuclear Weapons	www.icanw.org
International Criminal Court	www.icc-cpi.int
InfoSecurity24	www.infosecurity24.pl
The Henry M. Jackson School of International Studies	www.jsis.washington.edu
The Lieber Institute for Law & Warfare	www.lieber.westpoint.edu
Library of Congress	www.loc.gov
Latham & Watkins	www.lw.com
UN News	www.news.un.org
The Nuclear Threat Initiative	www.nti.org
OECD Library	www.oecd-ilibrary.org
The Office of the High Commissioner for Human Rights	www.ohchr.org
Opinio Juris	www.opiniojuris.org
Ośrodek Studiów Wschodnich	www.osw.waw.pl
Oxford Learner's Dictionaries	www.oxfordlearnersdictionaries.com
Polska Agencja Prasowa	www.pap.pl
Polski Instytut Spraw Międzynarodowych	www.pism.pl
Fundacja im. Kazimierza Pułaskiego	www.pulaski.pl
Reuters	www.reuters.com
Rzeczpospolita	www.rp.pl
Słownik Języka Polskiego PAN	www.sjp.pwn.pl
NATO Strategic Communications Centre of Excellence	www.stratcomcoe.org
The Guardian	www.theguardian.com
Think Global Health	www.thinkglobalhealth.org
UNRWA	www.unrwa.org
Scientific Committee on the Effects of Atomic Radiation	www.unscear.org

World Food Programme

www.wfp.org

WP Wiadomości

www.wiadomosci.wp.pl

Vredespaleis

www.vredespaleis.nl

Wielki słownik języka polskiego

www.wsjp.pl

Spis tabel

Tabela 1. Systemy infrastruktury strategicznej.....	21
Tabela 2. Sektory, podsektory i kategorie podmiotów dla Dyrektywy 2022/2557.....	26
Tabela 3. Etapy identyfikacji infrastruktury krytycznej	30