

Mateusz Rakowski

Hybrydowość i asymetryczność przyszłych wojen w cyberprzestrzeni

Rozprawa doktorska
w dyscyplinie nauk o polityce i administracji
napisana pod kierunkiem naukowym
dr. hab. Andrzeja Dubickiego, prof. UŁ

Łódź, 2025

 **SZKOŁA DOKTORSKA
NAUK SPOŁECZNYCH**
Uniwersytet Łódzki

 **WYDZIAŁ STUDIÓW
MIĘDZYNARODOWYCH
I POLITOLOGICZNYCH**
Uniwersytet Łódzki

Spis treści

Wstęp.....	7
I. Podstawy teoretyczne podejmowanej problematyki.....	7
II. Przedmiot i cel badań.....	15
III. Pytania badawcze.....	16
IV. Hipoteza badawcza.....	16
V. Podejście i metody badawcze.....	17
VI. Układ pracy.....	20
 Rozdział I Pojęcie hybrydowości w teorii nowych wojen.....	23
1.1. Rys historyczny działań nieregularnych.....	26
1.1.1. Dziedzictwo starożytności dalekowschodniej.....	27
1.1.2. Dziedzictwo starożytnej Europy.....	28
1.1.3. Dziedzictwo średniowiecza w Europie.....	31
1.1.4. Nowożytność i rewolucje w Europie i świecie.....	35
1.1.5. Wielkie Wojny i era broni jądrowej.....	39
1.1.6. Konflikty okresu przejściowego.....	41
1.1.7. Współczesne przejawy „wojny hybrydowej”.....	42
1.2. Wykorzystanie i kształtowanie cyberprzestrzeni przez „hybrydowość”.....	45
1.2.1. Miejsce cyberprzestrzeni w działalności politycznej i wojskowej państwa.....	47
1.2.2. Znaczenie sektora prywatnego w cyberprzestrzeni.....	51
1.2.3. Systemowe ujęcie współpracy sektora prywatnego i publicznego w cyberprzestrzeni.....	55
Podsumowanie.....	64
 Rozdział II Asymetryczność w konfliktach dawnych, współczesnych i przyszłych.....	67
2.1. Rys historyczny działań asymetrycznych.....	69
2.1.1. Daleki Wschód w starożytności.....	70
2.1.2. Konflikty asymetryczne państw starożytnej Europy.....	71
2.1.3. Średniowiecze w Europie.....	72
2.1.4. Nowożytność w Europie i na Świecie.....	73
2.1.5. Świat po wielkich wojnach.....	77
2.1.6. Problemy USA i ZSRR z prowadzeniem wojny asymetrycznej.....	79
2.1.7. Asymetria w świecie pozimnowojennym.....	84
2.2. Wpływ i wykorzystanie asymetryczności w cyberprzestrzeni.....	85
2.2.1. Cyberprzestrzeń w koncepcjach zachodnich.....	87
2.2.2. Przestrzeń informacyjna w ujęciu rosyjskim.....	91
2.2.3. Chińskie koncepcje wykorzystania cyberprzestrzeni w konfliktach.....	96
2.2.4. Udział podmiotów pozapaństwowych w konfliktach w cyberprzestrzeni.....	101
Podsumowanie.....	108

Rozdział III Porównanie i krytyka koncepcji hybrydowości i asymetryczności.....	111
3.1. Analiza pojęcia hybrydowości i jej krytyka.....	112
3.1.1. Teoria strategiczna.....	113
3.1.2. Rewolucja w sprawach wojskowych — porównanie perspektywy zachodniej z chińską.....	117
3.1.3. Zachodnie spojrzenie na „wojnę hybrydową”.....	120
3.1.4. Rosyjskie spojrzenie na „wojnę nieliniarną” i konflikty „nowej generacji”.....	125
3.1.5. Wojna „hybrydowa”, czy „gibridnaja”? Krytyka pojęcia.....	130
3.2. Analiza pojęcia asymetryczności i jej krytyka.....	134
3.2.1. Rozwój koncepcji asymetryczności.....	135
3.2.2. Zachodnie spojrzenie na zagrożenia asymetryczne.....	141
3.2.3. Rosyjskie spojrzenie na zagrożenia asymetryczne.....	145
3.2.4. Chińskie spojrzenie na zagrożenia asymetryczne.....	148
3.2.5. Wojna asymetryczna, czy asymetria w wojnie — krytyka pojęcia.....	151
Podsumowanie.....	154
 Rozdział IV Analiza konfliktów czasów rewolucji cyfrowej.....	 157
4.1. Geneza konfliktów epoki cyfrowej: zmieniające się pole walki oraz postrzeganie konfliktów.....	160
4.1.1. Okres zarządzania informacją: dominacja wojska w przekazie.....	167
4.1.2. Okres rozpadu monopolu: zburzenie tradycyjnego modelu kontroli narracji.....	172
4.1.3. Okres tworzenia się nowego układu sił: wzrost znaczenia asymetrycznych aktorów w cyberprzestrzeni.....	176
4.2. Konsekwencje dla bezpieczeństwa międzynarodowego — konflikty w epoce cyfrowej.....	183
4.2.1. Wyzwania dla prawa międzynarodowego i NATO.....	184
4.2.2. Znaczenie sektora prywatnego w budowie bezpieczeństwa międzynarodowego.....	188
4.2.3. Rosnąca rola sztucznej inteligencji oraz automatyzacji w atakach.....	191
4.2.4. Wzrost znaczenia infrastruktury krytycznej jako celu.....	194
Podsumowanie.....	198
 Rozdział V Prognoza perspektyw i nowe ramy analizy wojen cyfrowych.....	 203
5.1. Prognozy rozwoju wojen cyfrowych: krytyka i perspektywy.....	205
5.1.1. Krytyka metafor i kategorii tradycyjnej wojny w odniesieniu do cyberprzestrzeni.....	208
5.1.2. Zagrożenia dla środowiska sieciocentrycznego: ryzyko destrukcji.....	211
5.1.3. Granice prognozowania: epistemiczne trudności i potrzeba nowych modeli.....	217
5.2. Probabilistyczne modelowanie ryzyka w konfliktach cyfrowych.....	223
5.2.1. Architektura proponowanego modelu oceny ryzyka.....	225
5.2.2. Moduł probabilistyczny — osadzenie analizy w kontekście sytuacji bieżącej.....	227
5.2.3. Zmienne, metryki i skalowanie ryzyka w proponowanym modelu.....	229
5.2.4. Dalsza kalibracja modelu i integracja z procesami decyzyjnymi.....	232
5.2.5. Przyszłe kierunki rozwoju proponowanego modelu na przykładzie praktycznych implementacji.....	235
Podsumowanie.....	239

Zakończenie.....	243
I. Usystematyzowanie kontekstu badań i podstaw teoretycznych podejmowanej problematyki.....	243
II. Odpowiedź na pytania badawcze.....	249
III. Weryfikacja hipotezy badawczej.....	253
IV. Wnioski.....	255
Wykaz rysunków i tabel.....	259
Wykaz skrótów.....	260
Bibliografia.....	264
Akty prawne, regulacyjne.....	264
Źródła publikowane.....	264
Monografie.....	270
Artykuły w czasopismach naukowych.....	281
Rozdziały w monografiach i publikacjach zbiorowych.....	302
Artykuły prasowe.....	308
Źródła internetowe.....	308

Wstęp

I. Podstawy teoretyczne podejmowanej problematyki

Wojna od zawsze się zmieniała, ewoluowała, wykorzystywała kolejne zdobycze nauki lub sama była zjawiskiem powodującym rozwój technologiczny ludzkości. Wiele z tych technologii powstałych zarówno w czasie wojny jak również pokoju, miało i nadal posiada podwójne zastosowanie. Rozwój techniki wojskowej szedł w parze ze zmianami w taktyce wojowania. Właściwie prawie każde wielkie starcie militarne przynosiło mniej lub więcej znaczące zmiany w obszarze wojskowości i wojen. Zatem postawienie pytania o naturę przyszłych wojen jest jak najbardziej zasadne — zwłaszcza, że XX wiek i kolejne dwie dekady następnego stulecia za sprawą postępu technologicznego (kolejnej rewolucji) przyniósł więcej niewiadomych niż gotowych rozwiązań. Jak będzie się prowadziło przyszłe wojny, jaki będą miały charakter, kto będzie aktorem starć militarnych w bliższej i dalszej perspektywie czasowej? Czy będą to nadal klasyczne wojny, czy będziemy mieć do czynienia z nową formą walki? Jaki wpływ na starcie będą miały klasyczne wymiary walki, a także te, które dopiero nimi się stają? I wreszcie jaki wpływ na przebieg przyszłych wojen będą mieć najnowsze zdobycze techniki, nowe koncepcje, doktryny oraz strategie działań militarnych? To tylko kilka podstawowych pytań, z którymi borykają się planiści, wojskowi, politycy, dziennikarze, jak również naukowcy.

Współcześnie nic nie jest jasne, nie mamy nawet podstawowego modelu przedstawiającego przyszłą wojnę. Istnieją co prawda mgliste, bliżej nieokreślone koncepcje i hipotetyczne możliwości co do tego jak to starcie może przebiegać, jednak nadal są to tylko próby nakreślenia czym może być przyszła wojna. Starania w wypracowaniu spójnej teorii prowadzone są od ponad trzydziestu lat. Jeszcze przed zakończeniem zimnej wojny, teoretycy wojskowości i część politologów byli zdania, iż zmiany jakie zachodzą w rozwoju technologicznym oraz stosunkach międzynarodowych wymuszą wręcz rewolucyjne zmiany w sposobie prowadzenia oraz rozwiązywania konfliktów. Jednak wówczas nikt się nie spodziewał zmian tak szybkich, że ludzkość stanie przed nie lada dylematem. Wymusił on konieczność znalezienia skutecznych rozwiązań w obszarze wojen i wojskowości dostosowanych do zupełnie nowej, cyfrowej i globalnej rzeczywistości. Jej specy-

ficzny charakter sprawił, iż zmianom uległy wszystkie sfery życia społecznego, stosunków gospodarczych oraz międzynarodowych.

Aż do tej pory badacze nie dokonali spójnego i kompleksowego przedstawienia cech hybrydowości oraz asymetryczności środowiska sieciocentrycznego, szczególnie w rozumieniu „Nowych Wojen”. Wynika to z faktu, iż cyberprzestrzeń stanowi stosunkowo nowy obszar asymetrycznych działań, który określić można jako nieograniczony w szerokim rozumieniu tego słowa. Na omawianą problematykę wpływ ma także tempo rozwoju metod walki cyfrowej, proporcjonalne do ekspansji sfery cyfrowej. Powoduje to, iż relacje między jej użytkownikami, wraz z używanymi przez nich narzędziami, osiągają współcześnie skomplikowane formy. Ich analiza, poprzez badania struktur oraz skutków użycia cyfrowego oręża, a także asymetrii starć, pozwoli lepiej zrozumieć przyszłe konflikty. Co więcej, istotnym dla badanego obszaru jest polemologiczne usystematyzowanie dwóch, jak się zdaje, najistotniejszych cech cyberprzestrzeni.

Nie ulega wątpliwości, iż wraz z gwałtownie postępującym rozwojem technologicznym, zagrożenia dla bezpieczeństwa wewnętrznego coraz częściej znajdują swe odpowiedniki w cyberprzestrzeni. I choć stanowi ona obszar nowy, to z punktu widzenia społeczeństwa informacyjnego jest solidnie ugruntowana. Podstaw omawianych przemian doszukiwać się można już w rozwoju radiotelekomunikacji, który miał miejsce podczas II Wojny Światowej. Zastosowane metody przetwarzania informacji, jej przechwytywania i ochrony, na stałe odmieniły sposób prowadzenia konfliktów. W związku z tym nadejście rewolucji cyfrowej nie było zaskoczeniem, a przewidywania co do jej kształtu wykraczały poza ówczesny stan rozwoju technologicznego. Przykładem może być wydana w 1960 roku praca *Man-Computer Symbiosis* autorstwa J. C. R. Licklidera. Poruszała ona koncept globalnej sieci komputerów oraz ich relacji z ludźmi (symbiozie). Samą ideę Internetu odnajdujemy w 12-tomowej publikacji Paula Barana, wydanej w 1962 roku. Traktowała ona o odpornych na ataki, rozproszonych sieciach cyfrowych transmisji danych, posiadających niegwieździstą strukturę.

Jednakże prawdziwym kamieniem milowym było stworzenie rozległej sieci ARPANET, którą 5 sierpnia 1968 roku zaprezentował Donald Davies. Był to początek istnienia ery Internetu — choć istnienia cyberprzestrzeni w sensie stricte można doszukiwać się w pierwszych urządzeniach cyfrowo przetwarzających dane. Co więcej, empiryczne obserwacje samej technologii pozwoliły Gordonowi Moore'owi zdefiniować w 1965 roku prawo mówiące, iż liczba tranzystorów podwaja się co około 18 miesięcy. Współcześnie

jednak liczbę tę skorygowano i jako *prawo Moore’a* przyjęto okres 24 miesięcy¹. Rozszerzono także tę regułę na pozostałe parametry sprzętu komputerowego. Jednakże takie tempo rozwoju technologicznego stanowi potencjalne zagrożenie dla obywateli, gdyż coraz więcej jego aspektów wychodzi poza ich horyzont rozumienia.

Podstaw problemu można doszukiwać się fakcie, że społeczeństwa ewoluują w sposób nienadążający za cyfrową rewolucją. Wcześniej osoby starsze rozumiały technologie młodych i odwrotnie. Wyjątku nie stanowiła nawet rewolucja przemysłowa, osadzona wyłącznie w rzeczywistym środowisku. Kiedy jednak wytworzono syntetyczną przestrzeń logiczną, w krótkim czasie doszło do rozwarstwienia społeczeństwa pod kątem umiejętności korzystania z cyberprzestrzeni. Powoduje to, iż osoby niepotrafiące przystosować się do zmian stają się bezbronne wobec zagrożeń, których nie potrafią nawet zidentyfikować. Jednocześnie wykładniczy charakter rozwoju technologicznego — zakładając utrzymanie takiego tempa — stawia wyzwanie każdemu obywatelowi współczesnego społeczeństwa informacyjnego. Co więcej, powszechne jest postrzeganie siebie przez użytkowników jako znajdujących się w szczycie rozwoju. Wysoko ponad czasem minionym, z pozornie bliskimi skokami technologicznymi, które mają nadejść. Łatwo można popaść w przekonanie o bezsprzecznej dominacji aktualnego pokolenia, bez zdania sobie sprawy, iż lada chwila stan rozwoju technologicznego — a tym samym liczby i skali zupełnie nowych zagrożeń — podwoi się. Jest to o tyle istotne, że omawiana problematyka przenika wszystkie aspekty życia ludzkiego. Jak zauważył Paul Forman, od lat 80. XX w. obserwujemy odejście od warunkowanej kulturowo tezy o prymacie nauki nad technologią na rzecz tezy o prymacie technologii nad nauką². W 1995 roku, na łamach książki *Being Digital*, Nicholas Negroponte ogłosił nawet, iż szeroko rozumianym składnikiem elementarnym przestał być atom, a stała się nim cyfra binarna³. Ukazuje to, jak mimo wczesnych przewidywań rewolucji cyfrowej, dopiero w XX wieku rozwinęła się dojrzała świadomość roli cyberprzestrzeni.

Powyższe ma szczególne znaczenie z punktu widzenia bezpieczeństwa państwa w co najmniej trzech głównych aspektach. Po pierwsze: środowisko sieciocentryczne,

¹ Szczególnie w mass-mediach wskazuje się, że prawo Moora staje się koncepcją przestarzałą, gdyż miniaturyzacja tranzystorów w procesorach dociera do fizycznych limitów. Jednakże nowoczesne technologie wielowarstwowej budowy półprzewodników (tranzystory 3D) wskazują na możliwość utrzymania rzeczzonego prawa w mocy; B.R. Jai, M.F. Shih, *Technology: Limited or Infinite?*, „Emerging Media” 2024, Vol. 2, Issue I., s. 60–61; X. Wang, C. Liu, Y. Wei, S. Feng, D. Sun, H. Cheng, *Three-dimensional transistors and integration based on low-dimensional materials for the post-Moore’s law era*, „Materials Today” 2023, Vol. 63, s. 179–185.

² Odwrócenie to traktowane jest także jako wskaźnik pozwalający na odróżnienie nowoczesności od postnowoczesności.

³ N. Negroponte, *Being Digital*, New York 1995, s. 4–12.

zwłaszcza w szerszym ujęciu technologii IT i OT, jest kluczowym komponentem całej infrastruktury krytycznej. Ponieważ aktualnie większość rozwiązań wdrażanych jest z zastosowaniem najnowocześniejszych rozwiązań, cyfrowa natura stała się immanentną cechą większości systemów. Sprawia to, iż skutki cyberataku w nie wymierzonego doprowadzić mogą nie tylko do strat w owej przestrzeni logicznej, lecz przede wszystkim w opartej na niej sferze rzeczywistej. W efekcie możliwe jest postawienie pod znakiem zapytania bezpieczeństwo całego kraju. Drugim problemem są omówione wcześniej sprawy społeczne. Nie jest bowiem nadużyciem stwierdzenie, iż ludzkość żyje w swoistej symbiozie z technologią, co szczególnie uwidacznia się na rynku konsumenckim. Powoduje to, że poszczególne jednostki oraz grupy są równie podatne na atak co infrastruktura krytyczna, tym samym stanowiąc oddolny wektor ataku na państwo. O wiele większym zagrożeniem pozostaje jednak możliwość wywierania bezpośredniego wpływu poprzez manipulację. Jak wskazuje raport *Zwalczanie analfabetyzmu funkcjonalnego (...)* Komitetu Regionów Unii Europejskiej z 2010 roku⁴, w krajach rozwiniętych od ok. 9 do nawet 15 % obywateli klasyfikowanych było jako analfabetów funkcjonalnych. Co bardziej niepokojące, według badania PIAAC⁵, aż 39% ankietowanych Polaków osiągało niższe wyniki w skali rozumienia tekstu, a w przypadku praktycznych umiejętności matematycznych: 38%. Z rozwiązywaniem problemów nie radziło sobie 48% Polaków. Zараzеm zaledwie 2,5% z nich osiągnęło wyniki wysokie, co jest wartością znacząco poniżej średniej OECD. Dla porównania: w Czechach najwyższe wyniki osiągało 14% ankietowanych, a w Niemczech 19%)⁶.

Dane te poddają w wątpliwość to, czy obywatele są w stanie sprawnie oraz trafnie oceniać rzetelność źródeł informacji, jak i sam przekaz. Bez tego nie sposób mówić o skutecznej obronie w środowisku narastającego szumu informacyjnego, gdzie zamiast wiedzy przekazywane są gotowe schematy myślowe, co wyjątkowo ułatwia cyberprzestrzeń, a szczególnie sieć Internet. Wskazane odgórne i oddolne aspekty bezpieczeństwa wewnętrznego, są bez wątpienia wyzwaniem stałym w czasie pokoju. Jednocześnie mogą jednak być przyczynkiem trzeciej kategorii omawianych zagrożeń. Trudno przecenić rolę technologii informatycznych w dowolnych sytuacjach konfliktowych, z którymi mierzą się współczesne państwa. Przy tym wpływa to na samą koncepcję prowadzenia dzia-

⁴ Komitet Regionów UE, *Zwalczanie analfabetyzmu funkcjonalnego – Opracowanie ambitnej europejskiej strategii przeciwdziałania wykluczeniu i wspierania rozwoju osobistego*, 1 lipca, [2010/C 175/07], 2010.

⁵ M. Sitek, A. Prokopek, P. Penszko, K. Chyl, J. Haman, *Główne wyniki międzynarodowego badania umiejętności dorosłych PIAAC 2023*, Warszawa 2024.

⁶ Tamże, s. 21–22, 34.

łań, bowiem cyberprzestrzeń zależna jest od sfery programowej oraz sprzętowej. Zniszczenie, uszkodzenie lub zmodyfikowanie jednego z komponentów powodować może zupełną zmianę topografii w prowadzonych operacjach. Oznacza to konieczność zachowania gotowości wobec zjawisk, których dotychczas (w takiej skali) nie napotymano. Co więcej, cyberprzestrzeń, pozbawiona geograficznych granic, nie tylko wymieniana jest obok pozostałych środowisk walki: lądu, morza, powietrza i kosmosu, lecz nierozzerwalnie je przenika.

Rozważanie kształtu przyszłych wojen nie może jednak opierać się wyłącznie na wnioskowaniu opartym o analizę cyberprzestrzeni. Jak wspomniano na początku, XX wiek był okresem kształtowania się współczesnego pola walki, w którym ostatnie trzydzieści lat w znaczącym stopniu przyczyniło się do rozwoju sposobów prowadzenia konfliktów zbrojnych na świecie. Wobec tego zasadnym jest, aby poza środowiskiem sieciocentrycznym pochylić się również nad ostatnimi formami ewolucji wojsk. Jeden z bardziej jaskrawych przykładów stanowi RMA (Revolution in Military Affairs) — doktryna i system rozwoju Sił Zbrojnych USA. Ta złożona i w efekcie niejednorodna koncepcja omawiana była przez wielu autorów, wypowiadających się zarówno w jej obronie (jako rewolucji oraz ewolucji), jak również zupełnie ją krytykujących.

Koncepcja przedstawiona przez Alvina Eugene Tofflera w pracy *Szok przyszłości*, opiera się na przełomach w historii prowadzenia konfliktów, a zatem ma wymiar rewolucyjny. Autor wyróżnia trzy fale działań wojennych. Pierwsza nierozzerwalnie wiąże się z rewolucją agrarną. Ówczesne walki, z wyjątkiem antycznej wojny peloponeskiej, były raczej jednodniowymi starciami, zgodnie z fundamentalną dla tego okresu *Sztuką wojenną* autorstwa Sun Tzu, unikano bezpośrednich starć. Powodowały one bowiem wysokie straty, dlatego należało wykorzystywać możliwości zwyciężenia bez walki. Drugą falę wyznaczyła rewolucja przemysłowa, a także towarzyszący jej nacjonalizm, biurokracja i znaczenie produkcji na wielką skalę. Umożliwiła ona prowadzenie masowych wojen przy wykorzystaniu mnogości ciężkiego uzbrojenia, tym samym w miejsce Sun Tzu za podstawę przyjmując *O wojnie* Carla von Clausewitza. Położył on nacisk na niszczeniu siły żywej przeciwnika oraz stwierdził, iż że wojna jest aktem przemocy posuniętym do ostatecznych granic. Było to zatem prowadzenie polityki innymi środkami. Trzecią falą jest rewolucja informacyjna po II Wojnie Światowej, w której zaczęto stosować broń nowego typu — precyzyjną oraz „inteligentną”. Czytelną granicę, od której można mówić o tej „erze”, według Tofflera (a także Erika Durschmieda i Johna A. Wardena III) wyznaczyła I wojna w Zatoce Perskiej. Wyróżnia się tutaj wykorzystanie nowoczesnych systemów dowodzenia i kontroli (C2), które rozwijane były przez C4 (dowodzenie, kontrola,

komunikacja, komputeryzacja i wywiad) aż po dzisiejszą formę C4ISR, do której włącza się jeszcze inwigilację oraz rozpoznanie (rekonesans). Całość składa się na lepszą świadomość pola walki oraz zwiększenie autonomii oddziałów frontowych.

Odmienne i bardziej pragmatyczne spojrzenie przedstawił Andrew F. Krepinevich, były oficer amerykańskiej armii. Negując podstawy powyższej koncepcji, zaproponował on spojrzenie ewolucyjne, tym samym wyróżniając aż dziesięć kolejnych etapów rozwoju pola walki. Ich charakteryzację zaczął od późnego średniowiecza. Wskazał zmiany poprzez małe rewolucje: piechoty i artylerii, żaglową na morzu, fortyfikacji, prochu strzelniczego, napoleońską, lądową w XIX wieku, marynarki w XIX wieku, międzywojenną (w mechanizacji, lotnictwie i informacji) oraz nuklearną. Krepinevich, podobnie jak Stephen D. Biddle, Michael E. O'Hanlon oraz Chris Hables Gray, postrzega graniczną u Tofflera I wojnę w Zatoce Perskiej jako jedynie zapowiedź przyszłych konfliktów. Zastosowanie na dużą skalę zaawansowanych technologii uważa za ewolucję wynikającą z poprzednich etapów i dostrzega przy tym liczne błędy, które odnotowano podczas konfliktu w Zatoce Perskiej.

W zupełnej opozycji do koncepcji RMA stoi Jeremy Black, brytyjski historyk. Na łamach wielu monografii twierdzi on, iż idea mechanizacji jest doktryną zawodną. Wskazuje także problem lekceważenia innych modeli prowadzenia wojny niż zachodnie. Technologie zastosowane podczas I i II wojny w Zatoce Perskiej okazały się zawodne do tego stopnia, iż w operacji Pustynna Burza 2/3 strat wojsk Stanów Zjednoczonych (w ludziach) wynikały z *friendly fire*. Co więcej, pomimo szybkiego zwycięstwa doktryny bitwy powietrzno-lądowej, tak jak inne pomysły, dostarczyła ona więcej trudności w praktyce, niż przewidywały to szkolenia — szczególnie jeżeli chodziło o synchronizację działań na dynamicznie zmieniającym się polu bitwy. Szczególnie istotnym było ukazanie przez Blacka wspomnianego już lekceważenia niezachodnich metod prowadzenia wojny, zwłaszcza wśród zwolenników RMA. Misja UNOSOM I w Somalii pokazała skutki takiego podejścia, jednocześnie zapowiadając nowe metody prowadzenia walki, nazwane przez autora nieregularnymi, a współcześnie znane jako hybrydowe.

Terminy „działania hybrydowe” oraz „wojna hybrydowa” pojawiły się już na przełomie mileniów. Jako istotną wskazuje się tu pracę Williama J. Nemetha z 2002 roku, zatytułowaną *Future war and Chechnya: A case for hybrid warfare*. Została ona poświęcona analizie konfliktu rosyjsko-czeczeńskiego. Autor zastosował wówczas pojęcie hybrydowości nie tylko w stosunku do działań prowadzonych przez czeczeńskich bojowników, lecz także do sposobu funkcjonowania tamtejszego społeczeństwa. Według autora, wojna hybrydowa charakteryzowała się:

- a) organizacją stron konfliktu odzwierciedlającą rozwój społeczno-ekonomiczny danej wspólnoty, wraz z obowiązującymi w niej normami,
- b) inną percepcją siły militarnej, która pozwalała postrzegać na równi potencjał partyzancki oraz wysoko zaawansowane technologicznie oddziały przeciwnika,
- c) wykorzystaniem nowoczesnych technologii zarówno w starciach, jak również działaniach pośrednich, np. propagandzie⁷.

Od momentu opublikowania pracy Williama J. Nemetha, wielu teoretyków podejmowało się rozwinięcia koncepcji wojen hybrydowych. W artykule autorstwa Franka G. Hoffmana *Conflict in the 21st century: Rise of the Hybrid Wars* poddano dokładnej analizie „wojny czwartej generacji”, szczególnie pod kątem zatarcia się klasycznych granic między uczestnikami, czy też stanem pokoju i konfliktu, a także utraty przez państwa monopolu na przemoc. Zbadano także „wojny złożone”, zawierające w sobie działania konwencjonalne i nieregularne, połączone na poziomie nie tylko operacyjnym, lecz przede wszystkim taktycznym oraz strategicznym. Jedną z najistotniejszych części stanowi jednak koncepcja „wojny bez ograniczeń”, która zakłada, że wszystkie sfery otaczającej nas rzeczywistości, będą stanowić jedno pole walki⁸.

Dokonawszy syntezy wskazanych elementów, zaproponowano uniwersalną definicję wojny hybrydowej jako zawierających w sobie zestaw różnych metod działań wojennych, wliczając w to działania konwencjonalne, nieregularne taktyki i ugrupowania zbrojne, akty terrorystyczne, w tym masową przemoc, oraz działania przestępcze. Co istotne, konflikty te prowadzone mogą być zarówno przez państwa, jak również podmioty pozapaństwowe.

Również rosyjscy teoretycy wojskowości zajęli się problematyką związaną ze zjawiskiem hybrydowości. Jednak pogląd rosyjski wydaje się być zgoła inny niż zachodnich ekspertów. Niezwykle istotnym w teoretycznym dyskursie był artykuł, *Ценность науки в предвидении (Znaczenie nauki w przewidywaniu)* Walerego Gierasimowa. Na jego łamach autor analizując wskazywane kierunki przyszłych wojen, stwierdza, zauważalna tendencja do zanikania granic między wojną i pokojem w XXI wieku. Z konieczności wynika więc, że nie będą one potrzebować formalnego aktu wypowiedzenia ich, tocząc się według nieznanych dotąd schematów. Autor wskazał, iż coraz istotniejsze stało się wykorzystanie instrumentów politycznych, ekonomicznych i humanitarnych, połączonych z manipulacją ludnością zamieszkującą teren konfliktu. Co więcej, nacisk położony zo-

⁷ W.J. Nemeth, *Future War and Chechnya: A Case for Hybrid Warfare*, Monterey 2002, s. 1–5, 18–20, 23–27, 49–54, 57–59, 76.

⁸ F. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington 2007, s. 18–25.

stał na asymetrię, rozumianą jednak jako wykorzystanie jednostek specjalnych oraz mobilnych, mieszanych oddziałów bojowych, niezaangażowanych we frontalne konflikty. Rosjanin również nie definiuje przyszłych wojen jako takich, nie używa też pojęć: wojna hybrydowa, starcie hybrydowe czy też konflikt hybrydowy. Chociaż wiele myśli zawartych w artykule nawiązuje do doświadczeń teoretycznych ekspertów z Europy Zachodniej i Stanów Zjednoczonych to rosyjski szef Sztabu Generalnego prezentuje punkt widzenia na zjawisko hybrydowości w oparciu o doświadczenie i rosyjską myśl wojskową⁹.

Biorąc pod uwagę powyższe zauważyć należy, iż przyszłe wojny (nazywane przez autorów nowymi, hybrydowymi lub nieregularnymi) mają charakter konglomeratu sił i środków, których synergia oraz konwergencja użycia pozwalają osiągać dotychczas niespotykane efekty we wszystkich przestrzeniach: na morzu, lądzie, w powietrzu, kosmosie, a także w przenikającej je oraz będącej istotną samą w sobie — cyberprzestrzeni. Dodatkowo problematyka ta będzie wiązać sobą też i inne obszary i zatem będzie badana oraz rozpatrywana w ujęciu politycznym, polemologicznym, społecznym oraz technologicznym. Tak szerokie ujęcie badanego przedmiotu i podmiotu zmusza do wyznaczenia kilku zasadniczych paradygmatów do, których należy zaliczyć przede wszystkim:

- przyszłe wojny będą się cechować licznymi zmiennymi, które będą miały znaczny wpływ na ich rozwój i zmiany w środowisku międzynarodowym;
- cyberprzestrzeń stanie się jednym z zasadniczych obszarów nowych form walki zwłaszcza bezkontaktowej i będzie ona miała istotny wpływ na relacje międzyludzkie oraz stosunków międzynarodowych;
- niemożliwe je stworzenie jednolitej koncepcji przyszłych wojen jako jednego zbioru zasad, bowiem zmienny charakter przyszłych działań uniemożliwia stworzenie ich teoretycznych podstaw, a zatem skutkuje stałą niepewnością.

U podstaw analizy powyższego legły dokumenty doktrynalne, strategiczne oraz źródła przedstawiające cele i interesy narodowe. Wśród nich wyróżnić należy *DoD Cyber Strategy*, *National Security Strategy* (Stany Zjednoczone), *Strategię bezpieczeństwa narodowego* [Стратегия национальной безопасности РФ], *Doktrynę wojskową* [Военная доктрина РФ], *Doktrynę bezpieczeństwa informacyjnego* [Доктрина информационной безопасности РФ] (Rosja) oraz *Oparte na prawie zarządzanie cyberprzestrzeni w Chinach w nowej erze* [新时代的中国网络法治建设], *Naukę o strategii wojskowej* [战略学] i Chińską strategię wojskową [中国的军事战略] (Chiny). Analizując działalność NATO wykorzystano zarówno formalnie zatwierdzone dokumenty i komuni-

⁹ В. Герасимов, *Ценность науки в предвидении*, „Военно-промышленный курьер” 2013, № 8(476), s. 2–3.

katy (w szczególności *Koncepcję Strategiczną*), jak również raporty, monografie oraz białe księgi, tworzone przez zespoły pracujące w strukturach Sojuszu.

W badaniu bieżącego stanu cyberprzestrzeni i operacji prowadzonych przez poszczególnych jej aktorów, kluczowymi okazały się publikacje agencji rządowych i służb specjalnych — UE, USA, Wielkiej Brytanii, jak również innych państw. Raporty, noty informacyjne oraz analizy techniczne dostarczyły cennego materiału źródłowego, umożliwiające lepsze zrozumienie bieżących działań w cyberprzestrzeni oraz przyszłych ich kierunków. Uzupełniając wykorzystano materiały uznanych firm sektora cyberbezpieczeństwa, prowadzących własne zespoły analityczne, a także organizacji non-profit. W efekcie uzyskano pełniejszy obraz środowiska sieciocentrycznego, który stał się podstawą do dalszego wnioskowania.

Ze względu na licznosc i szeroki przekrój źródeł naukowych, wyselekcjonowanie najważniejszych pozycji przy zachowaniu ich reprezentatywności nie jest możliwe. W ich doborze skupiono się natomiast na pokryciu poszczególnych obszarów przedmiotu badań. Wykorzystane monografie i artykuły dotyczyły m.in. działalności państwa, jego administracji i instytucji, wojskowości (zwłaszcza na szczeblu strategicznym) oraz relacji międzynarodowych. Dopełnieniem była analiza roli sektora prywatnego, jak również badania nad podatnościami technicznymi, architekturą systemów i samą cyberprzestrzenią. Istotnym okazały się także prace dotyczące wpływu informacji na człowieka (jednostkę i grupy), pozwalające lepiej zrozumieć zachodzące zmiany społeczne. Źródła tych kategorii dobrano ze zwróceniem uwagi na afiliacje autorów, a przez to potencjalny wpływ kulturowo-polityczny. Wiązało się to zarówno z wykorzystaniem wielojęzycznych materiałów, jak również tekstów w języku angielskim, lecz publikowanych przez autorów spoza kręgu zachodniego. Odzworowano to w strukturze poszczególnych części rozdziałów, dzieląc analizę na trzy perspektywy (zachodnią, rosyjską oraz chińską).

II. Przedmiot i cel badań

Przedmiotem badań są podstawy teoretyczne i ewolucja zjawiska wojny, konfliktu, środowiska i zmiennych odnoszących się do tej problematyki jak również wykorzystanie nowoczesnych technologii oraz użycie cyberprzestrzeni we współczesnych i przyszłych konfliktach o naturze asymetrycznej, nieregularnej oraz hybrydowej.

Celem badań stało się dokonanie analizy i usystematyzowania dotychczasowej wiedzy odnoszącej się do różnych form i zjawisk związanych ze współczesnymi konfliktami, a zwłaszcza nieregularnymi, hybrydowymi, asymetrycznymi. Ponadto starano się

także określić zmiany w sposobie prowadzenia wojen by sformułować dane wyjściowych jako podstawy do przyszłych badań nad paradygmatem związanym z nieprzewidywalnością ewolucji w rozwoju zjawiska wojny (w ujęciu wykorzystania środowiska sieciocentrycznego). Pozwoliło to na zaproponowanie ram teoretycznych opartych na probabilistycznym modelu ryzyka, uwzględniającym możliwość jego zastosowania na poziomie strategicznym, operacyjnym i taktycznym. Uwzględnia on wstępne prognozy przyszłych form prowadzenia działań w cyberprzestrzeni, wraz z rozwojem jej roli wykorzystania, jak również zagrożeń dla samego środowiska cyfrowego.

III. Pytania badawcze

Pytanie główne (zasadnicze):

- a) W jakim stopniu oraz w jaki sposób cyberprzestrzeń wpłynęła i będzie miała wpływ na współczesne konflikty oraz jaką rolę odgrywać będzie ona w przyszłych wojnach?

Pytania szczegółowe:

- b) Jak należy definiować i rozumieć cyberprzestrzeń oraz co jest jej przedmiotem i jakie są jej podmioty?
- c) Jak należy definiować i rozumieć hybrydowość, asymetryczność oraz nieregularność w wojnach i konfliktach zbrojnych w dziejach ludzkości?
- d) W jakim stopniu można będzie łączyć różne formy prowadzenia działań zarówno w przestrzeniach klasycznych jak i przestrzeni informatycznej oraz w jakim kierunku będzie ewoluowały działania w szeroko rozumianej cyberprzestrzeni?
- e) W jakim stopniu dojdzie do odczłowieczenia (odhumanizowania) walki w cyberprzestrzeni?
- f) Czy rola cyberprzestrzeni będzie w przyszłych konfliktach zagrożona oraz czy skupiać się one będą na ograniczaniu wpływu środowiska sieciocentrycznego na działania wojenne?

IV. Hipoteza badawcza

Rewolucja cyfrowa towarzyszyła zmianom w metodach prowadzenia walki, które nastąpiły po II Wojnie Światowej. Skala wpływu środowiska sieciocentrycznego na współczesny świat doprowadziła do nierozzerwalnego scalenia go z techniką wojskową, co zmieniło postrzeganie cyberprzestrzeni jako obszaru działań konfliktowych, zaraz obok lądu, morza, powietrza oraz kosmosu. Środowisko sieciocentryczne przenika jednak

wszystkie te przestrzenie zarówno w czasie wojny, jak przede wszystkim pokoju, w efekcie część konfliktów przenosząc w sferę cybernetyczną. Powoduje to silny wzrost znaczenia nieregularności, hybrydowości i asymetryczności działań, odmieniając dotychczasowe metody prowadzenia wojen. Wobec tego ich przyszłość będzie szybko ewoluować w stronę prowadzenia walk informacyjnych i manipulacji. Efektem tego będą dwa wektory: wymierzone bezpośrednio w państwa i ich infrastrukturę krytyczną oraz wojskową (dowodzenia), a także społeczeństwa. Wobec powyższego kraje będą ograniczać zależność krytycznych sfer od cyberprzestrzeni przez stosowanie zastępczych rozwiązań technologicznych, dążących do uodpornienia na skutki wyłączania sieci cyfrowych.

V. Podejście i metody badawcze

Problematyka badań nad przedmiotem pracy jest interesująca z wielu powodów. Mimo stosunkowo niewielkich ram czasowych rewolucji cyfrowej — zwłaszcza wobec całości rozwoju prowadzenia walki zbrojnej — skala skoku technologicznego jest znacząca. Co więcej, tempo przenikania kolejnych obszarów przez cyberprzestrzeń sprawia, iż trudne staje się merytoryczne oraz zdystansowane śledzenie zachodzących zmian. Samo wskazanie przedmiotu procesu badawczego nie pozwoli jednak osiągnąć niczego ponad stworzenie zbioru danych, co w kontekście pracy naukowej miałoby charakter pozorowany i odtwórczy. Dlatego u podstaw wykorzystania opisanych poniżej metod legło sformułowanie problemu, polegającego na wykazaniu obiektywnego stanu niewiedzy na gruncie dotychczasowych osiągnięć nauki w tym obszarze. Co więcej, nie wszystkim badanym zjawiskom oraz przedmiotom przyporządkować można skonkretyzowane wskaźniki. Wobec tego istotnym stało się zdefiniowanie podstawowych zmiennych w oparciu o znane już definicje sprawozdawcze. Natomiast jeżeli pojęcie objaśniane jest w rozbieżny sposób, na drodze analizy lub syntezy ustalano jedno brzmienie, do którego porównywano wyniki podczas całego procesu. Pozwoliło to uniknąć zatarcia się granic między wskaźnikiem i zmienną, a także wykazać relacje między nimi (korelację, przyczynowość lub zaprzeczyć im mimo pozornego powiązania). Co więcej, przez wzgląd na złożoność zagadnienia „Nowych Wojen” oraz trudność w przewidywaniu rozwoju technologicznego, kluczowe stało się poświęcenie szczególnej uwagi rozumowaniu indukcyjnemu, aby prognozy nie były zbyt ogólne i nieokreślone. Jeżeli nawet niemożliwym stanie się przewidzenie pewnych zjawisk, to wykazanie konkretnych braków w ogólnym i mało określonym obszarze niewiedzy stanowi wartość dodaną, dbając o dostarczenie właściwych wskaźników pozwalających na zweryfikowanie efektów badań w niniejszej dysertacji.

Jedną z trzech metod jakie przyjęto przy tworzeniu niniejszej pracy jest analiza systemowa, którą to wybrano ze względu na jej szerokie zastosowanie w naukach politycznych podczas badania zmian zachodzących w stosunkach międzynarodowych oraz znaczenie dla zrozumienia zjawisk społecznych. Badanie systemowe jest ze swej natury interdyscyplinarne, co konweniuje z poruszaną w dysertacji tematyką, dotyczącą spraw społecznych, politologicznych, polemologicznych oraz technologicznych. Metoda ta okazała się być przydatną w poznawaniu złożonej problematyki w odniesieniu do szybko zmieniającego się otoczenia. Istotnym jest jednak przyznanie, że należy wystrzegać się uczynienia z niej jakkolwiek rozumianego celu, co mogłoby prowadzić do jednostronnego ujęcia tematu. A to z kolei stanowi podstawę krytyki omawianych w pracy problemów, jako postrzegania konfliktów wyłącznie z perspektywy zachodniej. Wobec tego koniecznym było wykorzystanie z punktu widzenia metodologicznego paradygmatu interpretatywnego. Zakłada on, że do zrozumienia danego społeczeństwa lub kultury, a w przypadku niniejszej pracy sposobu postrzegania oraz prowadzenia konfliktów zbrojnych, wymagane jest wniknięcie w daną społeczność. Zatem zamiast oceniania poszczególnych spojrzeń na współczesne wojny przez wcześniej przygotowany model teoretyczny, należy sporządzać merytoryczny opis różniących się od siebie podmiotów międzynarodowych (reprezentatywnych dla różnych podejść do problematyki dysertacji). Szczególną uwagę zwrócono na kwestie społeczne (relatywizm kulturowy), o których często się zapomina lub wręcz lekceważy podczas badań nad zjawiskami wojen, a których wpływ i znaczenie z pewnością będzie wzrastało. Niezaprzeczalny jest fakt, że społeczeństwo odgrywa jedną z najistotniejszych ról we współczesnych wojnach i konfliktach.

Komplementarną wobec powyższej metody jest analiza porównawcza, wybrana ze względu na założenie występowania różnic między badanymi podmiotami oraz postrzeganiem przedmiotu pracy, możliwości wyznaczenia konkretnych cech celem ich porównania, jak również sposobność do dostrzegania prawidłowości. Co więcej, interpretacja najistotniejszych pojęć oraz kategorii problematyki poruszanej w dysertacji pozostaje porównywalna w skali globalnej, z zastrzeżeniem jednak konieczności dostrzegania regionalnych oraz globalnych uwarunkowań. Jednak co należy podkreślić trudno — zwłaszcza w przypadku analizy transgranicznej cyberprzestrzeni — ustalić jasne granice terytorialne. Z kolei za zasadnicze granice czasowe przyjęto jednak okres rewolucji cyfrowej, choć badania byłyby niepełne, gdyby nie wziąć pod uwagi zdarzeń przeszłych z historii wojskowości.

Z tego powodu nierozzerwalnie z poprzednim wyborem, dla pełniejszego zrozumienia poruszanych problemów, łączy się analiza historyczna, pozwalająca na rzetelne

badanie linii rozwojowej konfliktów na świecie. Szczególnie uwzględniono w niej zdarzenia relatywnie niedawne, bynajmniej nie traktowane z tego powodu jako pewne. Mając na uwadze powszechną dla tematyki dysertacji manipulację w przekazie, niezwykle istotną w ocenie prawdopodobieństwa prawdziwości informacji jest metoda historyczna. Co więcej, wzbogaciła ona badania o możliwość przyrównania określonych zjawisk do ich odpowiedników w przyszłości, aby pełniej dostrzec dotychczasowe zmiany celem prognozowania przyszłych trendów.

Ponadto w procesie badawczym skorzystano z pomocniczych metod uzupełniających. Wśród nich wyróżnić należy przede wszystkim syntezę, która stosowana głównie po wyżej wymienionej analizie, uzupełniana była za pomocą generalizacji sprawozdawczej i historycznej. Całość wzbogacono metodą porównawczą — w oparciu o indukcję i dedukcję. Przy zastosowaniu paradygmatu interpretatywnego oraz analizy różnych spojrzeń na konflikty zbrojne, istotna dla wyciągania wniosków okazała się być umiejętność syntezy zebranej wiedzy. Dopiero w ten sposób obrobione dane posłużyć mogły do opracowania modeli teoretycznych lub prognoz dotyczących przedmiotu dysertacji. Dla lepszego poznania punktu widzenia reprezentatywnego podmiotu międzynarodowego, a co z tym związane zrozumienia jego zachowań i decyzji, ważne okazało się abstrahowanie izolujące. Metoda ta może w szczególnych przypadkach poprzedzać wszystkie pozostałe i umożliwiać ich zastosowanie wśród jasno wyznaczonych granic (izolacji). Bez nich bowiem mogłoby zachodzić ryzyko poddania analizie lub syntezie części innego podmiotu, bądź spraw z nich związanych, co z kolei doprowadziłoby do nieprawidłowego wnioskowania. Przy tym należy podkreślić, iż przez badanie podmiotów cechujących się relatywizmem kulturowym, w wielu przypadkach niemożliwe jest ogólne dowodzenie z użyciem reguł logiki formalnej. To co w jednych warunkach postrzegane byłoby jako w sposób przeciwny niż w innych, niekoniecznie oznaczać będzie sprzeczność i błąd racji jednej ze stron konfliktu. Pozorna niezgodność byłaby raczej wynikiem próby porównania innych układów odniesienia, co stanowiłoby błąd. Dlatego tak ważne stało się uzupełnienie złożonych metod analizy o abstrahowanie izolacyjne oraz syntezę.

Wybór powyższych metod badawczych uwarunkowany jest złożonością oraz interdyscyplinarnością poruszanej tematyki, co stanowi argument przemawiający za zastosowaniem komplementarnych wobec siebie analiz. Rzetelne ich przeprowadzenie winno ograniczyć ryzyko subiektywnej oceny zjawisk. Winno to także pozwolić na stałą kontrolę wstępnych założeń badawczych celem wprowadzenia konceptualnych zmian lub ograniczeń, które nie mogły zostać dostrzeżone przed podjęciem badań.

Istotnym jest podkreślenie, że podczas tworzenia niniejszej dysertacji wykorzystywano zaawansowane algorytmy uczenia maszynowego. Przy ich pomocy tłumaczono teksty w językach nieznanych autorowi, które następnie weryfikowano z językoznawcami, zwracając szczególną uwagę na słowa niemające właściwych odpowiedników w języku polskim i angielskim. Wśród tak użytych modeli wyróżnić należy: *Alphabet GNMT* oraz *DeepL CLM*, które okazjonalnie wspierane były przez tłumaczenia z użyciem *GPT-3.5*, *GPT-4*, *GPT-4o* oraz *GPT-5*. Modele *GPT* we wskazanych wersjach zostały również wykorzystane do wsparcia redakcji i korekty tekstu.

VI. Układ pracy

Praca składa się z pięciu rozdziałów, wstępu, zakończenia oraz wykazów.

Przedmiotem rozdziału pierwszego jest pojęcie hybrydowości w teorii nowych wojen. Za cel obrano próbę jej zdefiniowania na podstawie dotychczasowych definicji, jak również krytyki sensu stosowania terminologii wojen hybrydowych, zamiast których proponuje się pojęcie konfliktów nieregularnych. Co więcej, istotnym jest określenie roli cyberprzestrzeni w hybrydowości oraz tego, jak w ogóle środowisko sieciocentryczne jest przez nią wykorzystywane oraz kształtowane.

Przedmiotem rozdziału drugiego jest asymetryczność, zarówno w konfliktach dawnych, jak również współczesnych. Cel stanowi porównanie skali asymetrii między starciami historycznymi i nowoczesnymi, wraz z ustaleniem jej znaczenia dla aktualnych konfliktów oraz przyszłych wojen. Ponadto ważnym jest określenie roli cyberprzestrzeni w tym aspekcie, której to podmioty z immanentnych cech środowiska pozostają asymetryczne. Istotnym stało się też wskazanie wpływu tego imperatywu na pozostałe przestrzenie zarówno w ujęciu bezpieczeństwa (znaczenie dla zachowania pokoju), lecz także wpływu na prowadzenie konfliktów.

Przedmiotem rozdziału trzeciego są braki w aktualnej wiedzy dotyczącej asymetrycznych, hybrydowych wojen, jak również krytyka dotychczasowych systemów pojęciowych. Celem jest porównanie spojrzenia zachodniego (amerykańskiego), wschodniego (rosyjskiego) oraz dalekowschodniego (chińskiego) na omawianą tematykę. Istotnym jest także przedstawienie roli cyberprzestrzeni w sporze o słuszność konceptualną wojen hybrydowych oraz ustalenie jej wpływu na dotychczasowe ustalenia.

Przedmiotem rozdziału czwartego jest przedstawienie oblicza współcześnie rozgrywanych nowych wojen, poprzez analizę konfliktów bieżących oraz sięgających do początków rewolucji cyfrowej. Celem stała się potrzeba skonfrontowania teoretycznych

koncepcji z realnymi działaniami, szczególnie tymi które podejmowano w cyberprzestrzeni. Przytoczenie konkretnych przykładów, z dbałością o ich reprezentatywność oraz istotę dla omawianej problematyki, pozwoliło skonkludować i ocenić teoretyczną część badań oraz stało się podstawą do stworzenia prognoz.

Przedmiotem rozdziału piątego jest prognoza perspektyw w celu ustalenia możliwych form przyszłych wojen. Istotnym stało się nie tylko wyprowadzenie wniosków z ustaleń poprzednich rozdziałów, lecz także skonfrontowanie ich z trendami technologicznymi. Podjęto krytykę przenoszenia teorii, pojęć i prób rozumienia rzeczywistości domeny kinetycznej na środowisko sieciocentryczne. Wzięto też pod uwagę próby ograniczenia roli środowiska sieciocentrycznego przez uszkodzanie lub niszczenie infrastruktury, a szczególnie wykorzystanie impulsów elektromagnetycznych o dużym natężeniu (EMP/HEMP). Konkluzją takiego obrazu stał się paradygmat niepewności, wobec którego zaproponowano teoretyczne ramy odpowiedzi: probabilistyczny model oceny ryzyka.

Zakończenie stanowi syntetyczne przedstawienie wniosków z pracy, przedstawiające zjawisko „Nowych Wojen” w czasie od rewolucji cyfrowej, przez aktualne konflikty, po ich przyszłe formy.

* * *

Pragnę podziękować mojej Ani, za wyjątkowe wsparcie, motywację i wiarę w ukończenie niniejszej rozprawy. Rodzicom — za to, że w ogóle mogłem się znaleźć w tym miejscu, dzięki ich trosce oraz zapewnieniu możliwości rozwoju. Ponadto dziękuję Promotorowi, prof. Andrzejowi Dubickiemu, za cierpliwość, poświęcony czas, jak również wszystkie uwagi, które stanowiły cenną pomoc w przygotowaniu dysertacji. Dziękuję też prof. Andrzejowi Krzakowi — za lata inspirowania do pracy i naukowego wsparcia.

Rozdział I

Pojęcie hybrydowości w teorii nowych wojen

Koncepcja wojny hybrydowej, choć zaproponowana w 1998 roku przez Roberta G. Walkera¹ i we współcześnie znanej formie redefiniowana w 2007 roku przez Franka Hoffmana², początkowo nie wychodziła poza sferę niszowych teorii wojskowych³. Jednakże wraz z aneksją Krymu w 2014 roku nastąpił nagły zwrot, który wyniósł hybrydowość do głównego nurtu — tak badań w dyscyplinie bezpieczeństwa, jak również mediów. Powstałe w ten sposób nowe pojęcia (lub też adaptacja starych, jak wskazują ich krytycy) posłużyły do opisu wyzwań stawianych przez bardzo szerokie spektrum zagrożeń. Co więcej, kiedy stosowano i rozwijano koncepcję wojny hybrydowej, często czyniono to przez dedukowanie ze studiów konkretnych przypadków, analizy porównawcze i podobne⁴. Tak ściśle skupienie się na przedmiocie badań prowadziło do pominięcia zmiennych zewnętrznych — a szczególnie tych, które wynikają np. z różnic kulturo-

¹ Wielu autorów uważa, że jako pierwszy (w 2002 roku) o hybrydowości pisał William J. Nemeth. Jednakże terminu „wojna hybrydowa” użył w 1998 roku Robert G. Walker i zdefiniował ją jako „leżącą w intersekcji między wojną specjalną a konwencjonalną”. Zauważył on, że w koncepcji hybrydowości, tak jak w jej użyteczności dla konfliktu, nie ma niczego nowego. Podkreślał, że jest to tylko szczególna kombinacja istniejących form wojny; R.G. Walker, *Spec Fi: The U.S. Marine Corps and Special Operations*, Monterey 1998, s. 4–5, W.J. Nemeth, *Future War and Chechnya: A Case for Hybrid Warfare*, Monterey 2002, s. 29, 71–78.

² Rozumieć to należy przez współczesne pojmowanie definicji. W podobny sposób przedstawiono ją w 2006 roku przez autorów raportu *Quadrennial Defense Review* (QDR), lecz została potraktowana jako ogólny koncept — rozwinięcie pracy Williama J. Nemetha. Por. *Quadrennial Defense Review Report*, D. Rumsfeld (ed.), Washington D.C. 2006, s. 1–5, 10–11, 19–20, 35–39, 42–51, F. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington 2007, s. 14–33, 43–44, 58–59.

³ Nie jest też bynajmniej koncepcją wyłącznie zachodnią (czy rosyjską). Podczas wojny chińsko-indyjskiej (1962) Mao Zédōng z powodzeniem łączył działania konwencjonalne z nieregularnymi, stosując także podejście niesymetryczne. W efekcie Chińska Armia Ludowo-Wyzwoleńcza początkowo stosowała wyłącznie taktykę partyzancką, dzięki niej powoli zwiększając liczebność, co w efekcie pozwoliło przejść do prowadzenia walki konwencjonalnej; P.R. Mansoor, *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, [w:] *Hybrid Warfare in History*, W. Murray, P.R. Mansoor (eds.), New York 2012, s. 5–14.

⁴ E. Reichborn-Kjennerud, P. Cullen, *What is Hybrid Warfare?*, „Policy Brief” 2016, No. 1, s. 1.

wych, społecznych czy mentalności. Zbyt szerokie pojmowanie badanego zjawiska sprawiło też, że hybrydowość nie ma jednej, uniwersalnej definicji⁵.

W efekcie stała się ona swoistym słowem-wytrychem, bardzo ogólnym i przez to tracącym na wartości dla celów analizy środowiska bezpieczeństwa⁶. Opracowywane teorie winny pomagać w rozumieniu złożonej natury współczesnych konfliktów — przez rozpoznanie wyzwań oraz wsparcie rozwoju decyzyjności tak na szczeblu politycznym, jak również wojskowym (strategicznym, operacyjnym i taktycznym)⁷. Co więcej, rzeczowe rozszerzenie używanych pojęć sprawiło, iż w źródłach zaciera się różnica między działaniami hybrydowymi oraz nadrzędnymi strategiami (doktrynami). To dodatkowo umniejszało przydatność omawianego konceptu.

Przeszkodą w zrozumieniu zagrożenia hybrydowego wydaje się być niemożność sklasyfikowania, czym jest de facto przedmiotowe zjawisko. Sprzeczne definicje tego odwiecznego konstruktów ograniczają zdolność teoretyków i planistów wojskowych do właściwego wyobrażenia sobie wspólnego zestawu hybrydowych motywacji zagrożenia oraz potencjalnych działań. Żadna definicja nie może być adekwatna do wielu kontekstów, które różnią się: czasem, przestrzenią i logiką. Wskazuje to na potrzebę skonstruowania teorii sugerującej zasady, które rzucają światło na naturę i przejawy organizacji hybrydowych w konfliktach hybrydowych.

W wojnie hybrydowej agresor nie sięga po klasyczną inwazję, lecz realizuje cele z wykorzystaniem niejawnych operacji, sabotażu, cyberprzestrzeni czy bojówek powstańczych na terytorium potencjalnego przeciwnika. Nie wymaga ona nawet podjęcia klasycznych operacji wojskowych, ani też oficjalnego wypowiedzenia wojny⁸. Przy tym zagrożenie hybrydowe w wyjątkowy sposób koncentruje się na zdolnościach organizacyjnych i generalnie zmierza do uzyskania asymetrycznej przewagi nad konwencjonalnymi przeciwnikami(-ami) w określonym środowisku. Ta przewaga nie tylko utwierdza się w sferze siły militarnej, ale także w bardziej holistyczny sposób we wszystkich elementach systemu pozamilitarnego sfery funkcjonowania państwa, w obszarach: dyplomacji, informacji, wojskowości, gospodarki, finansów, wywiadu, egzekwowaniu prawa i innych.

⁵ P. Cullen, N. Wegge, *Warning of hybrid threats*, [w:] *Intelligence Analysis in the Digital Age*, S. Stenslie, L. Haugom, B.H. Vaage (eds.), New York 2021, s. 85–87.

⁶ G.P. Gentile, *The imperative for an American general purpose army that can fight*, „Orbis” 2009, No. 3, s. 460–462.

⁷ F.G. Hoffman, *Hybrid Warfare and Challenges*, „Joint Force Quarterly” 2009, Issue 52 (1st quarter), s. 36–37.

⁸ Е.Н. Бугорская, О.В. Емельянова, *"Гибридная война" как новый тип войны в 21 веке*, [w:] *Актуальные проблемы международных отношений в условиях формирования мультиполярного мира*, К.В. Михайловна (ред.), Курск 2019, s. 88.

Omawiana przewaga generuje efekt przejścia reguł pola bitwy z walki konwencjonalnej do tych sfer zdominowanych przez hybrydę. Rozumieć przez to należy zupełną zmianę tempa oraz intensywności prowadzenia działań, czy możliwość oddziaływania w głębi terytorium danego państwa⁹.

Nie jest to bynajmniej zjawisko nowe. Starcia znaczących sił niemal zawsze uzupełniane były nieregularnymi modelami wsparcia militarnego walczących wojsk: czy to w sposób satelicki względem zasadniczych przedsięwzięciach wojennych, czy w symbiozie z nimi. Wcześniej istniał jednak konsensus co do prowadzenia działań, w którym mowa była o kontaktowych starciach przy relatywnej symetrii, jako podstawie wszystkich operacji wojskowych (o czym mówiły np. systemologia wojskowa Eduarda Szewielewa¹⁰, czy Carl von Clausewitz w „O wojnie”)¹¹.

Odwołując się do tekstów Clausewitza, klasyczne działania militarne należałoby raczej określić jako główny trzon wywierania wpływu przez jedno państwo na inne, jak również osiągania celu. Szczególnie, iż mówił on o braku umiarkowania w stosowaniu wszystkich dostępnych metod, co w ogóle odróżniało wojnę od polityki¹². Zatem to co miało być charakterystycznym elementem działań hybrydowych, tak naprawdę obecne było zawsze, jako jedna z cech prowadzenia konfliktów. Dlatego współcześnie, 200 lat po Clausewitzu, wojny tylko w pełni potwierdziły jego teorię. Stąd też istotnym będzie rozważanie hybrydowości jako silnie osadzonej w klasycznych teoriach wojennych, a nie stojącej w opozycji do nich. Niezależnie od tego, czy rozpatruje się ją jako tylko poszerzoną funkcję klasycznych konfliktów, czy odrębny system integrujący jego elementy na rzecz jednego celu, osiąganego poprzez konwergencję i synergę działań. A wartym jest podkreślenia, że przeciwnie do pierwotnych koncepcji zachodnich, które wyróżniały hybrydowość, w źródłach rosyjskich przedstawiano raczej symbiozę regularnych i nieregularnych działań wojennych¹³.

⁹ T. McCulloh, *The Inadequacy of Definition and the Utility of a Theory of Hybrid Conflict: Is the “Hybrid Threat” New?* [w:] *Hybrid Warfare. JSOU Report 13-4*, eds. T. McCulloh, R. Johnson, Florida 2013, s. 2.

¹⁰ Eduard Gennadijewicz Szewielew (ros. Эдуард Геннадьевич Шевелев), ur. 17 czerwca 1935 roku, brak informacji o śmierci, profesor, konsultant przy ówczesnej Rosyjskiej Akademii Administracji Publicznej przy Prezydencie Federacji Rosyjskiej (Российская академия государственной службы при Президенте Российской Федерации), publikujący pod jej afiliacją; Э.Г. Шевелев, *Системология национальной безопасности на рубеже веков: состояние и перспективы развития*, „Вестник Самарского государственного аэрокосмического университета” 2004, № 2, s. 47; Шевелев Эдуард Геннадьевич, „Центр военно-политических исследований”, <http://eurasian-defence.ru/?q=node/22749> [odczyt: 23 listopada 2022].

¹¹ Э.Г. Шевелев, *Введение в военную системологию*. Москва 1993, s. 80–85; C. von Clausewitz, *O wojnie*, Warszawa 2010, s. 24–25.

¹² Tamże, s. 29–31, 37–43.

¹³ Н.А. Комлева, *Гибридная война: сущность и специфика*, „Известия Уральского →26

Pozornie trudnym do zrozumienia wydaje się skala rozpowszechnienia współcześnie rozumianego pojęcia hybrydowości, mimo wszystkich jego braków. Źródeł doszukiwać się można w fakcie, iż dowódca wojskowy winien przygotować się do prowadzenia działań wojennych przez jasne zrozumienie charakteru przyszłych wojen. Zawsze było błędem, że minione konflikty, zwłaszcza te wygrane przez dany podmiot międzynarodowy, wykorzystywano jako wzorzec szkoleniowy dla przyszłego pokolenia. Trudność wprowadzania nowoczesnych idei naukowych, czy to na etapie wdrażania, czy jeszcze opracowywania, nie przynosiła jednak aż tak istotnych reperkusji dla samych działań wojennych¹⁴. Jednakże szybki rozwój technologiczny sprawił, iż braki we właściwym prognozowaniu konfliktów już nie tylko utrudniały branie w nich udziału, lecz mogły doprowadzić do zupełnego braku możliwości przygotowania własnych sił. Stąd też należy określić jaką rolę pełni cyberprzestrzeń w szeroko pojmowanej hybrydowości, a także jak środowisko sieciocentryczne jest przez nią kształtowane.

Rozważania na temat wojny hybrydowej skupiać się winny nie tyle na ponownym definiowaniu tego terminu, ile na wyjaśnianiu całości koncepcji, by ta stała się użyteczna. Wynika to z faktu, iż koncepcje wpływają nie tylko na treść naszej komunikacji (szczególnie przez strategie), lecz także sposób, w który je wykorzystujemy. Wobec szerokiej, politycznej adaptacji terminu hybrydowości pojawiła się silna — choć wciąż niezaspokojona — potrzeba jasności definicyjnej. W źródłach dostrzec można polemikę nad tym, czy omawiana problematyka jest nowa, albo czy ma użyteczność analityczną. Omawiane potrzeby wcale jednak nie oznaczają, że termin wojny hybrydowej zostanie zsyntetyzowany, gdyż zasadnym wydaje się jego zanegowanie celem przedstawienia spójniejszych podstaw modelu „Nowych Wojen”.

1.1. Rys historyczny działań nieregularnych

Jak zauważono we wprowadzeniu, oraz jak wynika ze źródeł pierwotnych, które definiują wojnę hybrydową: nie jest ona niczym nowym. Przeciwnie, wywarła wpływ na wynik wielu starć w historii. Dlatego celem lepszego zrozumienia współczesnego jej pojmowania, czy też zasadności stosowania obecnie rozpowszechnionych definicji, należałoby dokonać analizy przedmiotowego zjawiska w wybranych konfliktach na przestrzeni dziejów.

федерального университета. Серия 3: Общественные науки” 2017, т. 12, № 3 (167), s. 129.

¹⁴ В.И. Слипченко, *Войны шестого поколения. Оружие и военное искусство будущего*, Москва 2002, s. 6.

Aby analizowanie elementów hybrydowości było w ogóle możliwe poczyniono założenie, że wojna hybrydowa to rodzaj połączenia działań konwencjonalnych i nieregularnych (partyzanckich, powstańczych czy terrorystycznych), które mogą być podejmowane przez podmioty państwowe i pozapaństwowe, zmierzające do osiągnięcia celów politycznych (w rozumieniu Clausewitza). Przy tym siły nieregularne powinny być centralnie dowodzone. Tu należy podkreślić, iż historycznie niejednokrotnie nie jest to możliwe, ale przedsięwzięcia takich aktorów wciąż pozostają koherentne względem jednej strategii, skierowanej przeciwko siłom najeźdźczym, a przez to spełniające jej założenia¹⁵. Jednocześnie hybrydowość będzie analizowana na wszystkich poziomach wojny — od taktycznego, przez operacyjny, po wspomniany strategiczny. Co istotne, strukturę działań nieregularnych winna determinować polityka.

1.1.1. Dziedzictwo starożytności dalekowschodniej

Jednym z najstarszych źródeł, istotnych dla badanej problematyki, jest *Sztuka wojny*. W swym dziele z V wieku p.n.e. Sun Tzu pisał, że „osiągnąć sto zwycięstw w stu bitwach nie jest szczytem osiągnięć. Najwyższym osiągnięciem jest pokonać wroga bez walki. Dlatego sprawą najwyższej wagi w wojnie jest rozbicie strategii wroga”¹⁶. Mimo, iż kontekst tego fragmentu dotyczy doprowadzenia potencjału przeciwnika do stanu braku zdolności do dalszej walki, to w dalszej części czytamy: „użyj w bitwie *konwencjonalnej* siły do nawiązania akcji bojowej, zaś *niezwykłej* (chi)¹⁷ siły do zdobycia zwycięstwa. Dlatego możliwości tych, biegłych w użyciu „niezwykłej” siły chi są nieskończone”¹⁸.

W chińskiej literaturze odnaleźć można interpretację, że Sun Tzu zatem pozbawia walkę „choreografii” bezpośrednich starć i proponuje raczej nieregularne, asyme-

¹⁵ Część źródeł odróżnia od siebie wojnę *złożoną* i *hybrydową*. Autorzy podają, że w przypadku tej pierwszej mówimy o wykorzystaniu sił regularnych i nieregularnych w zasadniczo spójnym kierunku, czyli z zachowaniem konwergencji, ale bez szczególnej synergii. Hybrydowość ma się tu wyróżniać ścisłą współpracą poszczególnych komponentów, tym samym będąc podkategorią wojny złożonej. Jest to jednak rozróżnienie współczesne i nieprzydatne do celów analizy historycznej, gdyż zasadniczo wszystkie wojny są złożone. Dlatego w dalszej części założenia definicji *wojny złożonej* będą zrównane z *wojną hybrydową*. J. Regina-Zacharski pojęcie „wojny złożonej” tłumaczy też jako „kompozytową” — uważając, że lepiej oddaje to jej istotę; T.M. Huber, *Compound Warfare: A Conceptual Framework* [w:] *Compound Warfare. That Fatal Knot*, T.M. Huber (ed.), Fort Leavenworth 2002, s. 1–3, 21, S. Minasyan, „Hybrid” vs. “Compound” War: Lessons From The Ukraine Conflict, „PONARS Eurasia Policy Memo” 2015, No. 401, s. 2, 4–5, por. J. Regina-Zacharski, *Wojna w świecie współczesnym. Uczestnicy — cele — Modele — Teorie*, Łódź 2014, s. 330.

¹⁶ Sun Tzu, *Sztuka wojny*, Warszawa 1994, s. 35.

¹⁷ Angielski przekład autorstwa L. Gilesa tłumaczy ten fragment jako *działania pośrednie* (indirect), odróżniając je od bezpośrednich starć w rozumieniu podobnym do nieregularnego, por. Sun Tzu, *Sun Tzu on the Art of War: The Oldest Military Treatise in the World*, Leicester 2000, s. 15, Sun Tzu, *The Art of War*, S.B. Griffith (ed. & trans.), Oxford 1971, s. 91.

¹⁸ Sun Tzu, *Sztuka...*, s. 56

tryczne podejście, odrzucające stałość w wojnie¹⁹. Myśl ta jest wykorzystywana przez Chińską Armię Ludowo-Wyzwoleńczą podczas szkolenia dowódców w sposób, który przez Zachód może nie być do końca rozumiany. Bariera kulturowo-językowa niejednokrotnie pomija wysoki kontekst języka chińskiego²⁰, utrudniający nie tylko jego tłumaczenie na języki niskiego kontekstu, lecz przede wszystkim rozumienie. Dlatego słowa z pozoru dość jednoznaczne. Chińscy wojskowi interpretują jako inherentną zmienność wojny, wymagającą szczególnie ostrożnego i metodycznego podejścia²¹. Zarazem dodają serię reguł, które winny być stosowane dynamicznie, celem uzyskania przewagi w różnych warunkach — w dużej mierze przez zmylenie przeciwnika. To z kolei rozumieją jako supremację walki niekonwencjonalnej, wartość fortelu oraz imperatyw utrzymywania przewagi i właściwego jej wykorzystania²². I choć historycznie tego rodzaju metody walki były uważane przez część dowódców za niemoralne (niehonorowe), to z czasem opisane powyżej wprowadzanie przeciwnika w błąd, wpisujące się w ramy wojny hybrydowej, uznano za akceptowane w chińskim rozumieniu wojny²³.

1.1.2. Dziedzictwo starożytnej Europy

Na podstawie poczynionych wcześniej założeń, początków hybrydowości na kontynencie europejskim odszukać możemy już w V wieku p.n.e.: podczas Wojny Peloponeńskiej między Atenami oraz Spartą. Wówczas Spartanie zdali sobie sprawę, że muszą utrzymać znaczne siły w Lakonii i Mesenii, aby zapobiec powstaniu helotów, na których opierała się nie tylko ich wojskowość, lecz także rolnictwo. Działania Ateńczyków, takie jak budowa bazy w Pylos, zakładały tworzenie podstępem warunków dla powstania heladzkiego, które nadałoby konwencjonalnemu konfliktowi coś, co współcześnie nazwalibyśmy wymiarem nieregularnym. Szczególnie, że działania te były ściśle podporządkowane polityce.

Po tym, jak siły ateńskie ufortyfikowały Pylos na południowo-zachodnim wybrzeżu Peloponezu w 425 roku p.n.e., zajmując pozycje wraz z Messeńczykami z Naupaktos, których przodkowie zostali wygnani z tego terytorium przez Spartan, po wielkim powstaniu helotów w 464 roku p.n.e. Messeńczycy podjęli serię najazdów na Lakonię, w czym pomagała im umiejętność posługiwania się lokalnym dialektem. Heloci zaczęli wkrótce dezertować do Pylos, doprowadzając do powstania nadzwyczajnej sytuacji

¹⁹ Ren Li, *Lectures on Sunzi's Art of War*, Beijing 2013, 32.

²⁰ E.T. Hall, *Beyond culture*, New York 1989, s. 85–105.

²¹ Ma Jun, *Ma Jun Explains Sunzi's Art of War*, Beijing 2008, s. 170–171.

²² R. Tingguang, L. Weiguo, *Sun Tzu's Art of War: Collected Expositions*, Beijing 2013, 27–28.

²³ Fu Chao, *Sunzi's Art of War: A Structural Analysis*, Beijing 2010, 211.

w całej Sparcie. Jej destabilizacja wynikała m.in. z faktu, iż Spartanie przygotowali się do regularnej wojny, posiadając dobrze wyszkolone falangi, jednak zupełnie nieprzygotowane na formę konfliktu nieregularnego Tukidydes opisał to w następujących słowach:

Lacedemończycy [Spartanie] nie byli przyzwyczajeni dotąd do tego rodzaju rabunkowej wojny, a wobec tego, że heloci przechodzili na stronę Messeńczyków, zaczęli się obawiać, żeby ruch ten nie zatoczył jeszcze większych kręgów w kraju. Mimo że nie chcieli przed Ateńczykami wyjawić swych kłopotów, zdecydowali się jednak wysłać poselstwo i starać się, o ile to będzie możliwe, o odzyskanie Pílos i o zwrot jeńców. Lecz Ateńczycy stawiali już większe wymagania i liczne poselstwa lacedemońskie odprawiali z niczym. Taki był przebieg wypadków pod Pílos²⁴.

Sama groźba wojny dziś zwanej hybrydową sprawiła, że Spartanie podjęli próbę zakończenia konfliktu w sposób pokojowy²⁵. Ateny jednak na to nie przystały, wobec czego doszło do wybuchu regularnej wojny²⁶. Należy przy tym zauważyć, iż choć elementy hybrydowe nie były tylko nieznaczącym elementem wszystkich działań, lecz realnie wpłynęły na decyzje Spartan, które finalnie doprowadziły do eskalacji konfliktu²⁷.

Innym przykładem wykorzystania nieregularnych działań w ujęciu hybrydowym są wojny punickie. Były to konflikty między Republiką Rzymską oraz Kartaginą, toczące się w III i II wieku p.n.e. i skupione wokół sporów o wpływy polityczne i gospodarcze w zachodniej części basenu Morza Śródziemnego. Szczególną uwagę zwrócić można na drugą wojnę punicką (218–201 rok p.n.e.), w której zastosowano metody walki nieregularnej celem przewyciężenia przewagi liczebnej przeciwnika.

W 217 roku p.n.e. Kartagińczycy bez oporu przebyli Alpy dzięki wybraniu trudnej, lecz niestrzeżonej trasy. Hannibal próbował wciągnąć główną armię rzymską do zaciętej bitwy, niszcząc obszar, który mieli chronić. Sprowokowało to ją do pospiesznego pościgu, wprost w zasadzkę Hannibala. W bitwie nad Jeziorem Trazymeńskim zupełnie zwyciężył nad armią rzymską²⁸. W wyniku paniki w Rzymie i wyboru Kwintusa Fabiusza Maksimusa na dyktatora, przyjęto strategię unikania zasadniczych starć na rzecz osłabiania najeźdźcy. Czyniono to przez wyczerpywanie jego żołnierzy i zasobów — dopóki Rzym nie odbuduje sił (później nazwaną Strategią Fabiusza). Efektem było jednak wy-

²⁴ Tukidydes, *Wojna peloponeska*, K. Kumaniecki (tłum. i red.), Warszawa 1957, s. 220.

²⁵ Tukidydes, *Wojna peloponeska...*, Warszawa 1957, s. 139, Plutarch, *Żywoty sławnych mężów (Perykles)*, M. Brożek (tłum. i red.), Wrocław 1956, s. 29.

²⁶ Tamże, s. 143.

²⁷ R. Kulesza, *Wojna peloponeska*, Warszawa 2006, s. 76–77.

²⁸ A. Goldsworthy, *The Fall of Carthage: The Punic Wars 265–146 BC*, London 2006, s. 184–190.

łącznie opóźnienie właściwych działań wojennych i nie osiągnięto przy tym istotnych sukcesów w rozumieniu likwidowania jednostek przeciwnika²⁹.

Wyraźniejszy przykład użycia przez Rzymian sił nieregularnych pochodzi jednak z 210 roku p.n.e., Operacje na Sycylii były zakończone, inwazja Kartaginy na wyspę nie powiodła się, przegrali sprzymierzeńcy punicy, a Syrakuzy i Agrigento zdobyli Rzymianie. Sytuację w Agathyrnie komplikowała dodatkowo duża liczba mężczyzn, pochodzących z rozbitych oddziałów, dezterterów, uchodźców, czy niewypłacalnych dłużników. Próbuąc przetrwać, parali się m.in. działalnością przestępczą, przez co stanowili zagrożenie dla przywrócenia pokoju w republice rzymskiej. Co istotniejsze, utrudniali także wznowienia rolnictwa. Było to szczególnym problemem, gdyż wojna z Hannibalem doprowadziła do znaczących braków w dostawach zboża, a handel zagraniczny Rzymu praktycznie nie istniał³⁰. Jednocześnie ludność Regium (dziś Reggio di Calabria) potrzebowała doświadczonych ludzi, zdolnych do walki najemnej, aby pomóc spłądrować Brutium i w ten sposób przejąć strategiczne zapasy. Sytuację tę wykorzystał Marcus Valerius Laevinus, konsul rzymski na Sycylii, który zebrał 4000 spośród wspomnianych, „rozbitych” bandytów i dezterterów, a następnie przesiedlił ich do Regium, gdzie mogli zostać użyci w walce z Brutium³¹. Co więcej, Rzymianie wykorzystali także przestępców bruttyjskich, mieszkających wcześniej na plądrowanych terenach, przeciwko ich własnemu państwu³².

Omawiana sytuacja Rzymu pokazuje, że zdesperowani i uzbrojeni „wolni strzelcy”, którzy prowadzą głównie działalność przestępczą, to nie tylko wyzwanie dla bezpieczeństwa państwa. Stawszy się najemnikami³³ służącymi Regium, wzmocnili siły Republiki. Z kolei ci zrekrutowani bezpośrednio spośród Bruttów, dodatkowo osłabili sojusznika Hannibala. Była to zatem konwergencja działań klasycznych i nieregularnych, która służyła jednej polityce rzymskiej.

²⁹ Tamże, 198–199.

³⁰ A. Pikulska-Radomska, *Fiscus non erubescit. O niektórych italskich podatkach rzymskiego pryncypatu*, Łódź 2003, s. 24.

³¹ T. Livius, *Books XXVI-XXVII With An English Translation*, W. Heinemann (ed.), Cambridge 1943, księga 26, roz. 24, wer. 7–18, księga 27, roz. 12, wer. 3–6, s. 63–66; Polibius, *The Histories, volume IV*, W.R. Paton (ed.), Cambridge 1925, księga 9, roz. 27, wer. 10–11; Plutarch, *Lives, volume III, Pericles and Fabius Maximus. Nicias and Crassus*, B. Perrin (ed.), Cambridge 1916, roz. 22, wer. 1–4, s. 183–185.

³² Właściwie Brutium było konfederacją miast ze stolicą w Cosentii. W czasie II wojny punickiej Bruttowie opowiedzieli się po stronie Hannibala; T. Livius, *Books XXVI-XXVII*, księga 26, roz. 40, wer. 2–10, s. 153–157.

³³ Pojawiające się w źródłach *latro*, w ujęciu z III i II w. p.n.e., może oznaczać płatnika lub najemnika w bardziej współczesnym rozumieniu; M.P. Fronda, *Between Rome and Carthage. Southern Italy during the Second Punic War*, Cambridge 2010, s. 373.

Nie są to jedyne przykłady prowadzenia działań nieregularnych podczas wojen punickich, z których dowódcy czerpali wartość praktyczną w ujęciu strategicznym oraz taktycznym. Tym samym zyskiwali reputację przez wykazanie się sprytem oraz manipulowanie wrogiem. Jednakże użycie tego rodzaju form walki miało także znacznie bardziej przyziemne powody. Pozwalały zabijać, niszczyć i wzbogacać się bez ryzyka, jakie niesły klasyczne starcia — to jest poniesienia strat w regularnej armii. W końcu strata istotnej liczby żołnierzy mogła przeważać o przegraniu całej wojny, co tym bardziej uzasadniało podejmowanie walki nieregularnej. Miało to także znaczenie wizerunkowe: omawiane działania demonstrowały „umiejętności, siłę i odwagę”³⁴. Doceniano wówczas, że nie odrzucano żadnej z form prowadzenia wojny: ani tradycyjnych taktyk, „ani tych uderzeń, które zależą od odważnej i silnej inicjatywy”³⁵ — za jaką uważano działania nieregularne.

Należy także podkreślić, że omawiane metody nieczęsto miały decydujący wpływ, a przytoczone przykłady są raczej najjaskrawszymi, a nie próbką reprezentatywną. Dlatego źródła historyczne często uznawały je za mało istotne przez ograniczony wpływ na końcowy wynik wojny, tym samym jedynie wspominając o formach nieregularnych. Jednak zauważyć można, że kumulacja działań dziś zwanych „hybrydowymi” może wpłynąć na przebieg całej kampanii, tak jak w przypadku wojen punickich.

1.1.3. Dziedzictwo średniowiecza w Europie

Powyższe działania w wiekach średnich zostały przeniesione przede wszystkim w partycypację pośrednią. Użycie najemników, choć znane wcześniej, zaczęło być szerzej stosowane i zyskiwać na znaczeniu. We wczesnych latach omawianej epoki walka za pieniądze zdominowana była przez Wikingów³⁶, a nieco nieco później Normanów³⁷.

Wraz z rozwojem chrześcijaństwa i uzyskiwanymi przez nie wpływami, europejskie doktryny wojenne nie tylko naznaczone były dziedzictwem rzymskim, lecz także zostały osadzone w teologii chrześcijańskiej. Opierały się one na trzech conceptach: słuszności przyczyny, właściwego autorytetu i sprawiedliwej intencji. Pierwsza z nich obejmowała samoobronę (w ujęciu religijnym i patriotycznym) oraz karanie złoczyńców. Druga mówiła, że aby wypowiedzieć sprawiedliwą wojnę, konieczna jest władza publiczna. Ostatnia z kolei postulowała, że sprawiedliwy żołnierz nie może kierować się zyskiem,

³⁴ Polibius, *The Histories, volume I*, W.R. Paton (ed. & trans.), Cambridge 1922, księga 1, roz. 57, wer. 2, s. 158.

³⁵ Tamże, księga 1, roz. 57, wer. 5, s. 158–159.

³⁶ Т.О. Васильевич, Теория и практика «гибридного» противоборства: обзор конфликтов с XV века до наших дней, „Конфликтология” 2021, № 2, s. 2–4.

³⁷ N.S. Price, *The Vikings in Brittany*. „Saga Book” 1986–1989, Vol. 22, s. 329–330, 371.

nienawiścią lub zemstą, lecz chrześcijańską miłością do sprawiedliwości³⁸. Ma to szczególne znaczenie, gdyż ściśle powiązanie polityki i religii chrześcijańskiej sprawiło, że niemoralna i przez to oficjalnie „nielegalna” była chęć zdobycia zysków (choćby przez grabieże) czy walki z szeroko rozumianą ludnością (gdyż nie czyniono wówczas rozróżnienia na cywilów i biorących udział w walce)³⁹. Ponieważ wciąż były to realne cele polityki, państwa uciekały się do metod przenoszących odpowiedzialność na inne grupy.

Średniowieczni żołnierze najemni, zwłaszcza od początku XIV wieku, wykorzystywani byli tak w klasycznych starciach, jak również w nieoficjalnej, zasadniczo przestępczej działalności („niegodnej” rycerstwa). Czasami organizowali się też na wzór współczesnych armii prywatnych czy jednostek separatystycznych. Przykładem jest działalność routierów⁴⁰ podczas wojny stuletniej — na całym obszarze północnej i południowo-zachodniej Francji. Wojska obu stron brały udział nie tylko w głównej kampanii wojennej, lecz również przedłużającej się okupacji. Do tej wykorzystywano właśnie najemników⁴¹, służących samemu królowi i realizujących jego cele polityczne oraz strategiczne⁴². W przypadku routierów nie były to bynajmniej niewielkie grupy, lecz duże jednostki, składające się z dobrze wyszkolonych i zorganizowanych żołnierzy, często z całą strukturą dowodzenia, czy systemem zarządzania zdobytymi łupami⁴³. Mimo to np. Kenneth Fowler sugeruje, iż routierzy nie mieli wielkiego znaczenia militarnego⁴⁴.

³⁸ F. H. Russel, *The Just War in the Middle Ages*, Cambridge 1975, s. 6, 18–25, I. Stouraitis, ‘Just War’ and ‘Holy War’ in the Middle Ages, „Jahrbuch der Österreichischen Byzantinistik” 2012, T. 62, s. 230–232.

³⁹ Rozróżnienie cywilów od walczących, a szczególnie ich ochrona, rozwijały się powoli. Początkowo dotyczyła ona zasadniczo duchownych, lecz synod z Charroux w 989 roku wstępnie objął także słabych i bezbronnych, co później kontynuowano. W dokumentach z synodu w Toluges z 1027 roku czytamy: *nikt nie zaatakowałby w żaden sposób mnicha lub duchownego podróżującego bez broni, ani żadnego mężczyzny idącego do kościoła lub wracającego z jego rodziną, ani żadnego mężczyzny towarzyszącego kobietom*; Mansi, *Sacrorum Conciliorum Nova, et Amplissima Collectio*, T. Head (trans.), [w:] *The Peace of God: Social Violence and Religious Response in France around the Year 1000*, T. Head, R. Landes (eds.), Ithaca-London 1992, s. 327–328, 334.

⁴⁰ Routier/-rzy, wyjątkowo liczne kompanie najemników, w skład których wchodziła w dużej mierze jazda, dobrze wyszkoleni żołnierze (man-at-arms), czasem także wspierana przez rozmaitych grabieżców. We Francji często nazywano ich „Englishmen”, choć tak naprawdę składali się z Gaskończyków, Germanów, Hiszpanów i Anglików. Co więcej, niektórzy z nich działali pod własnym, jednym symbolem, co zastępowało późniejsze mundury i wskazywało na skalę barbaryzacji pola walki; W. Urban, J. Terry, *Medieval Mercenaries. The Business of War*, London 2006, s. 95, 106; J.F. Verbruggen, *The Art of Warfare...*, s. 127–144.

⁴¹ R. Cox, *Asymmetric warfare and military conduct in the Middle Ages*, „Journal of Medieval History” 2012, Vol. 38, No. 1, s. 122.

⁴² C. Oman, *A History of the Art of War in the Middle Ages. Volume I*, London 1991, s. 471–477, J.F. Verbruggen, *The Art of Warfare in Western Europe during the Middle Ages*, Woodbridge 1997, s. 138.

⁴³ Tamże, s. 9.

⁴⁴ K. Flower, *Medieval Mercenaries volume I. The Great Companies*, Oxford 2000, s. 106.

Dostrzec tu można pewną analogię do operacji związanych z aneksją Krymu i konfliktem w Donbasie w 2014 roku, w związku z użyciem grup i pododdziałów tzw. „zielonych ludzików”, którzy stanowili wsparcie dla prorosyjskich separatystów. Niewątpliwie byli oni żołnierzami sił specjalnych Federacji Rosyjskiej, którzy prowadząc działania nieregularne, wpisywali się definicyjnie w teoretyczny model wojny hybrydowej⁴⁵. „Zielone ludziki” były dobrze wyszkolonymi żołnierzami, którym postawiono precyzyjne cele i udzielono odpowiedniego wsparcia bojowego oraz logistycznego. Ich zasadniczym zadaniem było zabezpieczyć interesy państwa rosyjskiego. Natomiast brak oznaczeń na mundurach był niewątpliwie elementem mającym wprowadzić błąd nie tylko siły zbrojne i policyjne przeciwnika, lecz przede wszystkim stanowił istotny składnik wojny informacyjnej toczonej przez Moskwę z Zachodem. Podobny opis można zastosować do sposobu wykorzystania routierów i innych grup najemnych, walczących pod dowództwem Henryka III⁴⁶. Przy czym inna pozostaje skala wykorzystania metod „hybrydowych”, zupełnie różna od tej z 2014 roku.

Średniowiecze charakteryzowało się epoką wojny rycerskiej, gdzie reguły toczonych walki były jasno określone do zamiaru celu. Jednak konflikty militarne oraz wojny przedmiotowej epoki niosą nam szereg przykładów łączenia klasycznych form wojowania z wykorzystaniem nieregularnych form. Zarazem musimy zdać sobie sprawę z faktu, że te archaiczne modele hybrydowości z reguły nie miały praktycznie wpływu na przebieg i zakończenie średniowiecznych konfliktów militarnych. Na uwagę zasługuje natomiast użycie przez strony konfliktu ludności cywilnej mieszczaństwa oraz chłopstwa. Przykładem może być rozprawienie się angielskich partii chłopskich z francuskim rycerstwem wycofującym się po bitwie pod Lincoln w 1217 roku⁴⁷. Nieregularne i doraźnie organizowane oddziały zostały powołane do życia dekretemi królewskimi, które zezwalały na przeciwstawienie się najeźdźcom i zezwalały na prowadzenie działań zbrojnych głównie w samoobronie. Królewskie edykty w tym konkretnym przypadku były niezbędnym i uzasadnionym krokiem mającym na celu nie tylko poszerzenie bazy oporu przeciw agresorom i włączeniu poddanych do walki, lecz przede wszystkim uzyskaniu czasu na odtworzenie potencjału bojowego, dlatego też klasyczna wojna i reguły musiały ustąpić doraźnym formom walki toczonej przez nieregularne siły. Mimo, że takie siły nie miały znaczącego wpływu na przebieg wojny, to stały się jednym z jej elementów. Ich działania

⁴⁵ A. Szpak, *Status „małych zielonych ludzików” w konflikcie zbrojnym na Ukrainie*, „Stosunki Międzynarodowe” 2016, Tom 52, Nr 1, s. 133–135.

⁴⁶ J.F. Verbruggen, *The Art of Warfare...*, s. 138.

⁴⁷ J.A. Giles, *Roger of Wendover's Flowers of History: Comprising the History of England from the Descent of the Saxons to A.D. 1235. Volume II*, London 1849, s. 397.

objęły zatem nie do końca zdefiniowany obszar, mieszczący się pomiędzy przemocą polityczną, prywatną oraz zwykłą samoobroną, co także zdradza pewne elementy tego, co współcześnie kwalifikowalibyśmy pod pojęciem hybrydowości⁴⁸.

Innym przejawem przedmiotowych działań może być wojna partyzancka toczona przez Helwetów walczących z dominacją habsburską w XIV wieku⁴⁹, która jest przykładem wykorzystania nieregularnych form działań militarnych w celu uzyskania niepodległości przez Szwajcarów. Mimo iż w walce z rycerstwem Szwajcarzy podejmowali klasyczne działania⁵⁰, to zastosowali także szereg elementów właściwych dla prowadzenia zarówno działań partyzanckich (czy parapartyzanckich), jak również wprowadzania w błąd z równoczesnym przygotowaniem obrony w ujęciu właściwym dla przedmiotowej epoki⁵¹.

Kolejnym niezwykle interesującym przykładem prowadzenia działań hybrydowych było wykorzystanie przez Wielkie Księstwo Litewskie, jak również i Koronę Polską, powstania na Żmudzi z roku 1409⁵². Działania partyzanckie inicjowane i wspierane mili-

⁴⁸ R. Cox, *Asymmetric warfare...*, s. 116.

⁴⁹ Wojna austriacko-szwajcarska, toczyła się od stycznia do września 1499 roku między Starą Konfederacją Szwajcarską i rodem Habsburgów (sprzymierzonym ze Związkiem Szwabskim). Ostatecznie zakończyła walki Szwajcarów o ich niepodległość, które najintensywniej toczono w XIV wieku. W omawianym konflikcie nigdy nie uczestniczyły całe armie żadnej ze stron. W dużej mierze chaotyczne, źle zaplanowane działania, skupiały się na najazdach granicznych, niszczeniu wiosek, czy okrucieństwach na ludności cywilnej, łupieniu itd. Często pozbawioną celu, destrukcyjną naturę tych starć, Hans Kurz ocenił jako „wojnę dla wojny”. W końcowej fazie Habsburgowie ze Związkiem Szwabskim odnieśli porażkę pod Schwaderloh, Frastanz, Calven oraz Dornbach (gdzie Szwajcarzy stracili tylko 500 ludzi, a pokonali 3000 rycerzy przeciwnika). Wojna zakończyła się 22 września 1499 roku, przez podpisanie porozumienia pokojowego w Bazylei — za pośrednictwem Ludovico Maria Sforzy, który nakłaniał obie strony do zakończenia walki; A. Winkler, *The Swabian War of 1499: 500 Years Since Switzerland's Last War of Independence*, „Swiss American Historical Society Review” 1999, Vol. 35, No. 3, s. 10; H.R. Kurz, *Schweizerschlachten*, Bern 1962, s. 141.

⁵⁰ W dużych starciach Szwajcarzy wykorzystywali, np. charakterystyczne formacje pikinierów (niem. *Haufen* — tłum, sterta), czyli zbite szeregi, podobne w formie do macedońskich falang, w skład których wchodziły związki taktyczne liczące od 50 do 300 żołnierzy. Formacje te były zdolne odpierać ataki ze wszystkich stron, a sposób ich funkcjonowania wymagał od Szwajcarów zachowania żelaznej dyscypliny — co się udawało; A. Winkler, *The Swiss in the Swabian War of 1499: An Analysis of the Swiss Military at the End of the Fifteenth Century. Military at the End of the Fifteenth Century*, „Swiss American Historical Society Review” 2020, Vol. 56, No 3, s. 75.

⁵¹ W czasie wojny habsbursko-szwajcarskiej Szwajcarzy wykazali się wysoką mobilnością swoich wojsk. Gwałtowne zmiany pozycji, długie marsze po zmroku, czy nocne ataki z zaskoczenia na ufortyfikowane pozycje spowodowały, że przeciwnik często nie stawiał wielkiego oporu. Natomiast w brutalnych najazdach łączonych z plądrowaniem, Wykorzystywano także pozamilitarne grupy bojowe, pozbawione prawnego usankcjonowania, które zbiorczo zwano „siłami niezależnymi” (niem. *Freiharste*). Szwajcarzy posiadali też efektywną, rozproszoną milicję (niem. *Landsturm*), która zdolna była odpierać ataki przeciwnika w niemalże dowolnym miejscu; A. Winkler, *The Swiss in the Swabian War of 1499*, s. 75–77; A. Winkler, *The Swabian War of 1499*, s. 11–13.

⁵² Powstanie na Żmudzi wybuchło 31 maja 1409 roku — wszczęte przez miejscową ludność, uciskaną przez Krzyżaków, zaczęło się spaleniem zamku Christmemel. Zostało ono wsparte przez litewskiego księcia Witolda Kiejstutowicza, a przez zobowiązania wynikające z unii obu narodów także przez polskiego króla Władysława Jagiełłę. Było to bezpośrednią przyczyną wybuchu wielkiej wojny

tarnie przez Litwinów i Polaków były preludium do tzw. Wielkiej wojny polsko-krzyżackiej 1410–1411. Miało one wpłynąć na przygotowania Zakonu do starcia z sąsiadem, wywołać chaos i spowodować na zaangażowanie przynajmniej części potencjału państwa zakonnego w tej prowincji. Trudno współcześnie określić w jakim stopniu zaangażowanie Polaków i Litwinów w rebelię żmudzką osłabiło potencjał Zakonu, jednak z pewnością było uciążliwe dla Malborka, bowiem dyplomacja krzyżacka często podnosiła na arenie międzynarodowej kwestię zaangażowania Korony w rewoltę żmudzką⁵³.

1.1.4. Nowożytność i rewolucje w Europie i świecie

W czasach nowożytnych również spotykamy się z użyciem różnych form działań hybrydowych podczas prowadzonych wojen. Klasyczna wojna epoki nowożytnej skupiała się na dążeniu jednej ze stron konfliktu do rozstrzygnięcia wojny poprzez stoczenie decydującej bitwy, która zaważała na losach wojny. Elementy hybrydowości na znaczną skalę w konfliktach pojawiły się w drugiej połowie XV wieku, w związku z wykorzystaniem przez podmioty państwowe wojsk najemniczych. Jednak należy podkreślić, że ich działania nie miały charakteru stricte nieregularnego. Taktyka walki była dostosowana do wymogów epoki, a służyły one temu z władców, którego było stać na usługi najemników. Z pewnością ciekawym elementem złotego wieku najemnictwa było powstanie pierwszych paramilitarnych organizacji zrzeszających najemników — kompanii⁵⁴. Interesują-

z zakonem krzyżackim, która wybuchła 6 sierpnia 1409 roku; Z. Nowak, *Akt rozpoczynający „Wielką Wojnę”. List wypowiedni wielkiego mistrza Ulryka von Jungingen z 6 sierpnia 1409 roku*, „Komunikaty Mazursko-Warmińskie” 1976, nr 1, s. 81; K. Militzer, *Historia zakonu krzyżackiego*, Kraków 2007, s. 207.

⁵³ Powstanie, nazywane przez Krzyżaków „zdradą Żmudzinów” (niem. *den Sam ayten des vorethnisses*), było przedmiotem wielu działań dyplomatycznych ze strony zakonu. Szczególnie, że mimo zapewnień Witolda Kiejstutowicza w korespondencji, jakoby nie popierał powstania, wywiad krzyżacki donosił coś innego. Wielki mistrz zakonu często pisał tak do księcia litewskiego, jak i króla polskiego — szczególnie, że nie otrzymywał odpowiedzi, czy Polska poprze Żmudzinów. Zdaniem Zenona Nowaka, polemizującego z Kurtem Forstreuterem, list wypowiedni (akt rozpoczynający wojnę) wielkiego mistrza, który to przywoływał poprzednie próby dyplomatycznego rozwiązania sporu, był także wyrazem lekceważenia. Kancelaria polska wykorzystywała w międzynarodowej korespondencji głównie łacinę, co czynili też Krzyżacy. Jednakże wspomniany list sporządzono w języku niemieckim; Z. Nowak, *Akt rozpoczynający „Wielką Wojnę”*..., s. 81, K. Forstreuter, *Die deutsche Sprache im auswärtigen Schriftverkehr des Ordenslandes und Herzogtums Preußen*, Königsberg 1933, s. 12.

⁵⁴ Kryzys systemu feudalnego w XIV wieku, wynikający z fal głodu, wojen i epidemii spowodował, że często młodszy synowie rycerzy nie dziedziczyli majątków, czy w inny sposób zmuszeni byli do działania na własną rękę. Szukali więc okazji do zbudowania majątku przez łupy wojenne, a swoją walką — za opłatą — starali się zwracać na siebie uwagę władców, by podnieść swoją pozycję. Stopniowe spotęgowanie tego zjawiska sprawiło, że ci najemnicy zaczęli gromadzić się w formie pierwszych kompanii — już w XIV wieku. Miało to szczególne znaczenie, gdyż z racji dużej nieprzewidywalności pojedynczych „płatnych rycerzy”, zlecniodawcy poszukiwali raczej całych oddziałów najemnych, a nie pojedynczych wojowników o wątpliwym pochodzeniu. Z czasem kompanie te stały się wojskiem lepszym od osiadłego rycerstwa, które głównie mnożyło majątki, niechętnie podchodząc do obowiązków militarnych. Zarazem ciągła profesjonalizacja kompanii sprawiła, że na przełomie XV i XVI wieku można mówić o wyższości najemników nad →36

cym przykładem mogą być kondotierzy, którzy działali głównie w Włoszech od XIV do XVI wieku, zawierając kontrakty (*condotte*)⁵⁵ z miastami-państwami i książętami. Tworzyli własne kompanie złożone z zawodowych żołnierzy, które funkcjonowały jak paramilitarne organizacje, oferujące usługi wojskowe na zasadach komercyjnych⁵⁶. Ich działalność miała ogromny wpływ na przebieg wojen włoskich, a jednocześnie ukazuje wczesną formę zjawiska, które dziś porównujemy do prywatnych firm wojskowych, znanych nam z wojen końca XX i początku XXI wieku.

Cechą charakterystyczną dla działań hybrydowych okresu nowożytnego i kolejnych dekad aż po wiek XIX z pewnością jest użycie doraźnie organizowanych pododdziałów (najczęściej) kawalerii, świetnie wyszkolonych, tylko nominalnie (z reguły) poddanych dowódcom sił regularnych, które wykonywały zadanie rozpoznawcze, rajdowe, zmuszające przeciwnika do określonych działań. Na tym etapie należałoby uznać, iż tego rodzaju poczynania są właściwe dla prowadzenia kampanii czy operacji wojskowej opisywanej epoki, jednak ich aktywność ukierunkowana była na szeroko rozumianą dywersję na tyłach wroga, wprowadzanie chaosu i dezorganizacji na zapleczu, sianiu paniki i terroryzowaniu ludności cywilnej. Przy tym stosowane metody postępowania zwłaszcza z ludnością cywilną, a następnie po przez przekaz ustny upublicznianiu faktu popełnianych okrucieństw (*de facto* zbrodni wojennych na szeroką skalę) powodowało, że morale oraz zbudowanie jakichkolwiek form oporu ze strony społeczeństwa jednej ze stron konfliktu (zaatakowanej) okazywało się niemożliwe. W tym wypadku, przykładem niech będą działania polskich lisowczyków⁵⁷ (również występujący pod określeniem straceńcy lub chorągwie elearskie⁵⁸) podczas walk na wschodnich kresach Rzeczypospolitej na począt-

rycerstwem tracącym zdolności bojowe; K. Gryglewski, *Przyczyny rozwoju wojsk najemnych i zaciężnych w Europie od XIV do XVI wieku*, „Kurier Instytutu Historii” 2017, nr 5–6 (102–103), R. XII, s. 5–6; W. Urban, *Średniowieczni Najemnicy*, Warszawa 2008, s. 8.

⁵⁵ N. Ferguson, *The Ascent of Money: A Financial History of the World*, New York 2008, s. 41.

⁵⁶ J. Malarczyk, *Myśliciele włoskiego Renesansu o potrzebie rewolucyjnego przewrotu w Italii*, „Czasopismo prawno-historyczne” 1985, t. XXXVII, z. 1, s. 34.

⁵⁷ Lisowczycy (lisowczyki) — formacja najemna, złożona głównie z Polaków, Rusinów, Litwinów i Tatarów, powołana w 1607 roku ze względu na chęć odciążenia skarbu Rzeczypospolitej od wypłat żołdu. Zapewniano im swobodę grabieży łupów wojennych jako wynagrodzenia za służbę. Przemieszczali się szybko, pokonując dziennie do 150 km — nie ciągnęli wozów, lecz zaopatrywali się przez ciągłe rabunki. Pozwalało to na stosowanie zagonów, foteli, czy taktyki podstępów. Jako świetnie wyszkoleni jeźdźcy, walczyli zazwyczaj z dużym okrucieństwem, które było powodem uchwalenia kolejnych ustaw w 1623, 1624 i 1625 roku (i wielokrotnie później). Zawarto w nich nakaz podjęcia skrajnych środków przeciw żołnierzom zawiązującym konfederacje. W efekcie Lisowczyków rozwiązano około 1635 roku; *Volumina legum. Tom III*, Petersburg 1859, f. 449, 463–466, 522, s. 216, 223, 251; R. Sikora, *Wojskowość polska w dobie wojny polsko-szwedzkiej 1626–1629. Kryzys mocarstwa*, Poznań 2005, s. 83–91.

⁵⁸ Chorągwie elearskie — nazwa wywodząca się od węgierskiego *elu iaro*, oznaczającego „wpród idący”. Przekształcenie w *elea* wynikać mogło z zastosowania wymowy łacińskiej, lub dodatkowo skojarzenia z *electus armiger*, znaczącego „wybrany, wpród oręż noszący”. Formacja, o

ku XVII wieku, czy też wykorzystanie ich umiejętności w trakcie wojny trzydziestoletniej (1618-1648).

Stosowane przez nich formy działań bojowych z pewnością mogą być zaliczane do modeli właściwych dla walki hybrydowej, realizowanej zarówno w fazie wojny, jak i przed konfliktem militarnym. Działania prowadzone przez grupy i oddziały lisowczyków niszczące infrastrukturę logistyczną, nie były jedynymi skutkami mającymi negatywny wpływ na stronę przeciwną. Wydaje się, że dużo istotniejsze miało oddziaływanie psychologiczne — sianie postrachu pozostawiającego długotrwały efekt w społeczeństwie⁵⁹. Wpisuje się to jako część składowa w zjawisko, które współcześnie definiujemy jako wojna informacyjna.

Dostrzegamy też w tej działalności elementy dezinformacji wojskowej⁶⁰ w fazie pierwotnej. Rzecz jasna pojęcie to zostanie dopiero wprowadzone do obiegu i teorii prowadzenia polityki i wojen dopiero w drugiej dekadzie XX wieku, jednak różne elementy zjawiska dezinformacji (w szerszym lub węższym ujęciu) pojawiają się praktycznie już w starożytności i z pewnością wpisują się w teorię hybrydowości.

Jeszcze innym przykładem występowania elementów działań hybrydowych były wojny toczone przez Koronę brytyjską w XVIII wieku w Indiach. Brytyjczycy w utrzymaniu swoich posiadłości kolonialnych, zwłaszcza w opisywanym rejonie świata, wykorzystywali przede wszystkim siły jakimi dysponowały Kompanie czyli wielkie towarzystwa gospodarcze, zajmujące się zasadniczo eksploatacją podbitych ziem. Jest to jednak eufemizm, bowiem Kompania Wschodnioindyjska⁶¹ nie tylko zajmowała się handlem, lecz

której mowa, była czasem nazywana od swych dowódców — Lisowczykami od Lisowskiego, Rusinowczykami od Rusinowskiego, Strojonowczykami od Strojonowskiego itd.; W. Dembołęcki, *Pamiętniki o Lisowczykach, czyli przewagi elearów polskich. 1619–1623*, Kraków 1859, s. 15–16.

⁵⁹ T. Srogosz, *Między mitem sublimacji a mitem apokalipsy wojennej w badaniu historii wojskowości XVII wieku*, „Acta Universitatis Lodzensis. Folia Historica” 2024, nr 117, s. 13–14.

⁶⁰ Dezinformacja wojskowa — jest podkategorią ogółu działań prowadzonych w sposób systematyczny, fachowy i mających na celu mylenie co do faktycznych zamierzeń i przedsięwzięć, z użyciem szerokiego przekroju metod. W przypadku tej kategorii dezinformacji jej obiektem są: przeciwnik, własne wojska oraz otoczenie. Stawia ona silny nacisk nie tylko na mylenie rekonesansu oponenta, lecz także utwierdzanie go o słuszności wyciąganych wniosków. Można tu wyróżnić działania ofensywne, pozwalające na uzyskanie inicjatywy i zaskoczenia, a także defensywne — zmierzające do poprawienia bezpieczeństwa oraz stwarzania warunków ku temu; T. Grabowski, *Metody walki informacyjnej w mediach elektronicznych na przykładzie konfliktu rosyjsko ukraińskiego (2014–2016)*, „Horyzonty Polityki” 2016, Nr 7 (20), s. 41–42; M.J. Wachowicz, *Ujęcie teoretyczne pojęcia dezinformacji*, „Wiedza Obronna” 2019, nr 1–2, s. 230–232.

⁶¹ Kompania Wschodnioindyjska (ang. *East India Company*) — została założona w 1600 roku celem prowadzenia handlu w Indiach wschodnich. Funkcjonowała w oparciu o nowoczesny model dyrektorów i akcjonariuszy, mających udział w firmie. Miała przy tym zdecentralizowaną strukturę zarządzania, która skutecznie funkcjonowała w sytuacji posiadania monopolu. Zasadnicze zmiany nastąpiły w 1784 roku, kiedy brytyjski Parlament powołał Radę Komisarzy, która przejęła kontrolę nad sprawami wojskowymi i cywilnymi Kompanii. W roku 1834, spółka straciła komercyjny charakter oraz handlowy monopol, zyskując charakter organu administracyjnego,

uprawiała politykę i była strażnikiem interesów Korony, funkcjonując obok (raczej współdziałając) administracji politycznej oraz Wojskowej Królestwa.

Utrzymaniem porządku w koloniach i poszerzaniem wpływów zajmowały się głównie siły najemnicze, dowodzone przez zawodowych podoficerów i oficerów brytyjskich, które werbowano wśród plemion sprzyjających Koronie (np. sipaje⁶²). Jednostki te w procesie szkolenia osiągały (a nawet przewyższały) regularne jednostki brytyjskie, jednocześnie stanowiąc realną siłę przeciwko siłom zbrojnym księstw i królestw niepodbitych przez Brytyjczyków⁶³. Intensywna eksploracja subkontynentu Indii w XVIII wieku doprowadziła do licznych konfliktów i wojen z niepodległymi państwami. Władcy hinduscy w bezpośrednich starciach z armią brytyjską okazali się bezsilni, dlatego pod koniec XVIII zmienili taktykę działań. Jej część przystosowała się jednak do walk z Wielką Brytanią, czego dokonano za sprawą walki hybrydowej, np. w południowych Indiach.

W latach 1767–1799 Królestwo Majsuru stoczyło łącznie cztery wojny przeciwko Brytyjczykom. Siły królewskie były w stanie w klasycznym starciu pokonać niewielkie oddziały brytyjskie, jednak w starciu z siłami głównymi poniosły klęskę, dodatkowo tracąc część swoich wojsk.

W związku z tak niekorzystną sytuacją operacyjną zmieniono taktykę działania, którą należy scharakteryzować jako hybrydową. Skupiono się na unikaniu starć z głównymi siłami Brytyjczyków i obronie ważnych ośrodków swojego państwa, przy jednoczesnym nękanii administracji okupacyjnej i niszczeniu infrastruktury logistycznej armii brytyjskiej. Operacjami dywersyjnymi i wznicianiem buntów i rebelii zajmowały się oddziały prawie 18 tysięcznej nieregularnej kawalerii, działającej na brytyjskim zapleczu. Organizowali oni rajdy na zajęte terytoria, niszczyli magazyny i likwidowali ośrodki administracji oraz mniejsze oddziały wojsk brytyjskich, jednocześnie podsycając ducha oporu wśród ludności⁶⁴.

podległego Parlamentowi. Jednak już w międzyczasie Kompania funkcjonowała jak twór pararządowy, w konsekwencji wprowadzając reformy społeczne i edukacyjne, które doprowadziły do odrodzenia kulturowego Indii, ale też wzrostu nacjonalizmu religijnego. Kompanii zarzucano obskurantyzm, reakcjonizm czy negatywnie oceniano monopol. Ale np. Bankey B. Misra wskazuje, że spółka wypracowała i dała Indiom nowoczesny system rządowy, który był reprezentatywnym przykładem ery reform w Anglii; G.M. Anderson, R.E. McCormick, R.D. Tollison, *The economic organization of the English East India Company*, „Journal of Economic Behavior & Organization” 1983, No. 4 (2–3), s. 222–223, 227, 237–238; B.B. Misra, *The Central Administration of the East India Company, 1773–1834*, Manchester 1959, s. V, 1–5.

⁶² C. Wickremesekera, *Best Black Troops in the World': British Perceptions and the Making of the Sepoy 1746–1805*, New Delhi–Manohar 2002, s. 181–183.

⁶³ R.G.S. Cooper, *Culture, Combat, and Colonialism in Eighteenth-and Nineteenth-Century India*, „The International History Review” 2005, Vol. 27, No. 3, s. 534–549.

⁶⁴ L. Gilady, J. MacKay, *Bringing the Insurgents Back In: Early Wars in British India*, „Terrorism and Political Violence” 2015, Vol. 25, Issue 5, s. 802; N.H.M. Chancellor, *Mysore: The Making and*

Wykorzystując te formy działań nieregularnych, władcy Królestwa Majsuru nie tylko utrzymali niezawisłość, lecz zmusili Brytyjczyków do zawarcia niekorzystnych dla nich porozumień pokojowych. Ostatecznie Majsur został wchłonięty przez Wielką Brytanię. Podbój jednak zakończył się powodzeniem tylko dlatego, że Korona Brytyjska zaangażowała w działania militarne znaczne siły, skoncentrowała wszystkie zasoby, jak również wykorzystwała kawalerię Marahtów⁶⁵.

1.1.5. Wielkie Wojny i era broni jądrowej

W obu wojnach światowych, w których ścierały się armie o podobnych potencjałach, można właściwie doszukiwać się źródeł symetrycznego postrzegania sztuki wojennej⁶⁶. Niemniej, także w tym okresie doszukiwać się można działań nieregularnych, choć należy przy tym zauważyć, iż w źródłach można spotkać błędną identyfikację zjawiska hybrydowości. Np. Hall Gardner przyrównał aneksję czeskich Sudetów przez faszystowskie Niemcy w październiku 1938 roku do zajęcia Krymu przez Federację Rosyjską⁶⁷. W rzeczywistości rzeczona aneksja była skutkiem porozumień monachijskich, a zatem doszukiwanie się jej źródeł w działaniach nieregularnych jest nietrafione.

Możemy natomiast zauważyć, jak podczas drugiej wojny chińsko-japońskiej (1937–1945) Mao Zedong wraz z jego dowódcami sprawnie łączyli różne formy walki, w tym nieregularnej, prowadząc zarówno działania symetryczne i asymetryczne. Co istotne, postrzegali je jako równie ważne oraz istniejące w tym samym kontinuum walki. Elementy hybrydowe nie stanowiły jedynie wsparcia klasycznych metod. Później doświadczenia te zostały użyte podczas kampanii pod koniec chińskiej wojny domowej (1948–1949), doprowadzając do wycofania się sił Chińskiej Partii Narodowej (z Czang Kai-szekiem na czele) na Tajwan⁶⁸.

Unmaking of a Model State, „South Asian Studies” 2010, No. 13, s. 112; M. Vartavarian, *An Open Military Economy: The British Conquest of South India Reconsidered, 1780-1799*, „Journal of the Economic and Social History of the Orient” 2014, No. 57 (4), s. 489–491.

⁶⁵ J. Ferris, *Small Wars and Great Games: The British Empire and Hybrid Warfare, 1700–1970* [w:] *Hybrid Warfare Fighting Complex Opponents from the Ancient World to the Present*, eds. W. Murray, P.R. Mansoor, Cambridge 2012, s. 204.

⁶⁶ Q. Wright, *A Study of War*, Chicago 1965, s. 8.

⁶⁷ H. Gardner, *Crimea, Global Rivalry, and the Vengeance of History*, New York 2015, s. 151–152.

⁶⁸ A.D.W. Forbes, *Warlords and Muslims in Chinese Central Asia: a political history of Republican Sinkiang 1911–1949*, Cambridge 1986, s. 215–225; G.J. Bjorge, *Compound Warfare in the Military Thought and Practice of Mao Zedong and the Chinese People's Liberation Army's Huai Hai Campaign (November 1948 — January 1949)* [w:] *Compound Warfare: The Fatal Knot*, ed. T.M. Huber, Fort Leavenworth 2002, s. 170–213.

Wśród aspektów obszaru badań okresu przejściowego między wojnami klasycznymi i „nowymi”, należy wspomnieć także o pojęciu ery wojen przedjądrowych oraz jądrowych⁶⁹.

Taka koncepcja opierająca się o podział na dwie „epoki” jest często przedstawiana przez rosyjskich teoretyków wojskowości, choć w obu przypadkach wyróżniają oni generacje. W przypadku konfliktów przednuklearnych, pierwsza generacja to okres broni białej i walki w skali taktycznej, druga — użycie prochu, działania operacyjno-taktyczne, trzecia — broń gwintowana, działania operacyjno-strategiczne i czwarta — uzbrojenie samopowtarzalne, armie masowe, wojna w skali strategicznej⁷⁰. Druga era dzieli się z kolei na generację broni jądrowej (okres zimnej wojny) oraz wojnę bezkontaktową — w której celem jest niszczenie podstawowych funkcji państwa, jego systemów dowodzenia, najważniejszych obiektów wojskowych, jak również gospodarki⁷¹.

„Era” wojen jądrowych pokrywa się także z powołaniem Organizacji Narodów Zjednoczonych, co miało istotny wpływ na kształtowanie się konfliktów w następnych dekadach. Podpisana 26 czerwca 1945 roku Karta Narodów Zjednoczonych już w preambule potępiła wojnę, usuwając ją z katalogu akceptowalnych narzędzi polityki państw⁷². Nie przyniosło to kresu wojnom, ani nawet konfliktom ogólnie. Przeciwnie: wiele napięć zostało przesuniętych do tzw. wojen zastępczych (proxy wars), które zdefiniowały drugą połowę XX wieku. W dużej części zmotywowane lękiem przed reperkusjami hipotetycznej otwartej wojny między Związkiem Socjalistycznych Republik Radzieckich i Stanami Zjednoczonymi⁷³, doprowadziły do realizowania strategicznych celów mocarstw przez konflikty na terytoriach państw trzecich. W ten sposób próbowano zmieniać lub zachowywać równowagę sił, z zapewnieniem pokoju w samej Europie⁷⁴.

⁶⁹ В.И. Слипенченко, *Войны шестого поколения. Оружие и военное искусство будущего*, Москва 2002, s. 4–15.

⁷⁰ Sam koncept czterech generacji wojen jest przedmiotem krytyki. Wskazuje się m.in. nieliniowy, a raczej równoległy rozwój sztuki wojennej, brak możliwości wyznaczenia jasnych granic. Żadna pojedyncza strategia lub linearna interpretacja historii nie może objąć złożoności ludzkich doświadczeń konfliktów zbrojnych. Natomiast próby rysowania wyraźnych granic wymagają dużych uproszczeń, co z kolei podważa analityczną przydatność takiej propozycji. Zob. S. Purhonen, *Generations on paper: Bourdieu and the critique of 'generationalism'*, „Social Science Information” 2016, Vol. 55 (I), s. 105–110; M. Evans, *Elegant Irrelevance Revisited: A Critique of Fourth-Generation Warfare*, „Contemporary Security Policy” 2005, Vol. 26, Issue 2, s. 244–248; R. Johnson, *Hybrid War and Its Countermeasures: A Critique of the Literature*, „Small Wars & Insurgencies” 2018, Vol. 29, Issue 1, s. 148.

⁷¹ A. Krzak, *Wojny przyszłości po rosyjsku — wojna hybrydowa, informacyjna i psychologiczna na tle konfliktu ukraińskiego*, „Przegląd Bezpieczeństwa Wewnętrznego” 2018, Nr 18 (10), s. 23.

⁷² *Charter of The United Nations and Statute of the International Court of Justice*, San Francisco 1945, s. 2.

⁷³ J.L. Gaddis, *Zimna Wojna. Historia podzielonego świata*, Kraków 2007, s. 98–99.

⁷⁴ S.A. Hashemi, M. Sahrapeyma, *Proxy Wars and US's Smart-Power Strategy (the Case of Syria)*,

Ta bipolarna organizacja światowego systemu, choć opisywana niebezpiecznym poziomem napięcia, okazała się być wysoce stabilną — choć tylko z punktu widzenia państw półkuli północnej, zasadniczo Zachodu. Układ ten był postrzegany inaczej choćby w Azji — ze względu na wojnę koreańską w latach 1950–1953, lub wietnamską (1955–1975), czy na Bliskim Wschodzie, podczas radzieckiej interwencji w Afganistanie (1979–1989). Niepomijalne są także regionalne konflikty interesów, np. o Kaszmir, który stanowi przedmiot sporu między Pakistanem, Indiami oraz Chinami. Tłąc się przez dekady, był on przyczynkiem do licznych walk z użyciem sił partyzanckich i milicyjnych⁷⁵. Ponadto w omawianiu problematyki drugiej połowy XX wieku należy wymienić zjawiska tzw. wojen rewolucyjnych z lat 60. i 70⁷⁶. Dotyczą one obszarów, które do II Wojny Światowej znajdowały się pod władzą europejskich potęg kolonialnych. Wojny te rozciągały się od Azji Południowo-Wschodniej po Afrykę — od Indonezji, przez Somalię, po Gwineę czy Sierra Leone. Starcia te wynikały nie tyle z pokolonialnych sporów granicznych, ile z wewnętrznych sporów o władzę i politykę społeczno-gospodarczą. Poza konfliktami etnicznymi, często sięgającymi daleko w historię, znaczącym problemem były także różnice religijne oraz kulturowe, stanowiące punkt zapalny na całe dekady⁷⁷.

1.1.6. Konflikty okresu przejściowego

Do podobnych sporów dochodziło także w miejscach, gdzie przez wiele dziesięcioleci funkcjonowały społeczności wieloetniczne i wieloreligijne — jak w Bośni. Eskalacja otwartej przemocy sprawiła, że wymienione różnice w społeczeństwie zostały zmienione w błędy definiowania „przyjaciela” i „wroga”. Jest to o tyle istotne, iż właśnie rozpad byłej Jugosławii uważa się za przyczynek do poważnej, współczesnej debaty na temat konfliktów, której punktami kulminacyjnymi były wzajemnie konkurencyjne interpretacje „zderzenia cywilizacji” oraz „ekonomi wojennej”⁷⁸. Co więcej, między innymi tego rodzaju wojny były postrzegane jako etap przejściowy między konfliktami klasycznymi i hybrydowymi (nie tylko przez wykorzystanie elementów współcześnie rozumianej hybrydowości, lecz choćby jej natężenie). Był to też czas szczególnego dehumanizowania konfliktu zbrojnego i niszczenia przeciwnika z dystansu pozostającego poza jego możli-

2011-2016), „The Quarterly Journal of Political Studies of Islamic World” 2018, Vol. 6, No. 24, s. 84–86.

⁷⁵ K.M. Arif, *Khaki Shadows: Pakistan 1947–1997*, Oxford 2001, s. 88; B. Stein, *A History of India*, Oxford 2010, s. 358.

⁷⁶ K. Finlayson, *The 1960s: A Decade of Revolution*, „Veritas” 2008, Vol. 4, No. 4, s. 14–21.

⁷⁷ H. Münkler, *The New Wars*, Cambridge–Malden 2005, s. 7–8.

⁷⁸ S.P. Huntington, *Zderzenie cywilizacji i nowy kształt ładu światowego*, Warszawa 2011, s. 8–11, 370–376; K.C. Matuszek, *Systemy wojenne: współczesne wojny w perspektywie teorii Niklasa Luhmanna*, Kraków 2010, s. 7.

wościami — np. podczas wojny powietrznej w byłej Jugosławii w 1999 roku⁷⁹. Podobny przebieg miała także pierwsza wojna w Zatoce Perskiej. Z kolei druga potwierdziła obrany w ten sposób kierunek rozwoju technologii walki, zmierzającej do eliminowania drugiej strony bez dawania szansy na odpowiedź⁸⁰.

Ukazuje to także, że pozimnowojenne konflikty przeprowadziły system światowy ze wspomnianej paradoksalnej stabilności formuły bipolarnej do okresu długotrwałej turbulencji. To oznaczać by miało, że przyszłość oparta będzie na chaosie, przerywanym krótkotrwałymi, niestabilnymi okresami uporządkowania. Mimo, że taki opis zdaje się być przesadzonym pesymizmem, to współcześnie możemy mówić, iż żyjemy w świecie „międzyepoki”⁸¹.

1.1.7. Współczesne przejawy „wojny hybrydowej”

Jugosławia i Czeczenia, o których pisał Nemeth (także bardziej w charakterze etapu przejściowego)⁸² wprowadziły świat w okres wojen hybrydowych. Poza wspomnianymi wojnami w Zatoce Perskiej, należy tu wymienić także drugą wojnę libańską z 2006, gdzie Hezbollah skutecznie zastosował przeciwko Izraelowi konglomerat metod konwencjonalnych, nieregularnych i elementów walki informacyjnej⁸³.

Z kolei w 2008 roku, podczas wojny w Osetii Południowej, zastosowano właściwie wszystkie metody, które dziś przypisujemy konfliktom hybrydowym. Wykorzystano nie tylko konwencjonalną interwencję, lecz przede wszystkim siły separatystyczne, operacje informacyjne, czy choćby działania w środowisku teleinformatycznym. Blokada gruzińskiej sieci Internet i paraliż systemów dowodzenia, okazały się skutecznymi środkami prowadzenia walki⁸⁴.

Innym przykładem było wykorzystanie elementów hybrydowości przez Irak przeciwko Daesh, zwanemu „Państwem Islamskim” (choć nie powinno się tego rozpatrywać

⁷⁹ N.J. Wheeler, *Dying for 'Enduring Freedom': Accepting responsibility for civilian casualties in the war against terrorism*, „International Relations” 2002, Vol. 16, No. 2, s. 206.

⁸⁰ J. Regina Zacharski, *Wojna w świecie współczesnym...*, s. 162–163.

⁸¹ Tamże, s. 22.

⁸² W.J. Nemeth, *Future war and Chechenya...*, s. 63–72.

⁸³ Przez lata zagrożenia ze strony Organizacji Wyzwolenia Palestyny i Hamasu, Izrael zbytnio skupił się na walce przeciwpartyzanckiej. W takich momentach Hezbollah wykorzystywał metody konwencjonalne. Umiejętność szybkiego adaptowania do sytuacji i wykorzystywania różnych form walki doprowadziła do strategicznego zwycięstwa Hezbollah; W.M. Arkin, *Divining Victory Airpower in the 2006 Israel-Hezbollah War*, Maxwell AFB 2007, s. XVIII–XIX; D.T. Lasica, *Strategic Implications of Hybrid War: A Theory of Victory*, Fort Leavenworth 2009, s. 5–6, 17.

⁸⁴ D. Dejneka, *Siły Zbrojne Federacji Rosyjskiej w operacjach XXI wieku*, [w:] *Rosyjska wizja prowadzenia operacji militarnych*, S. Markiewicz (red.), Warszawa 2018, s. 101–102; S. Gvineria, *Information Warfare as Russia's Hybrid Warfare Tool*, [w:] *Information Warfare — New Security Challenge for Europe*, T. Čížik (ed.), Bratislava 2017, s. 76–91.

jako starcia z podmiotem państwowym). Podczas konfliktu w 2014 roku można było zaobserwować konwergencję sił konwencjonalnych (w tym amerykańskich), kurdyjskich partyzantów (peszmergów), czy różnego rodzaju milicji⁸⁵.

Ostatecznie uwagę należy zwrócić na konflikt ukraiński z 2014 roku, gdyż to on rozpowszechnił amerykańską definicję wojny hybrydowej, zarówno w publicystyce i świadomości społecznej, jak również dyskursie politycznym oraz naukowym — także w Rosji. Jednocześnie szybko zaczęto nadużywać tego pojęcia, które często stosowano jako skrót myślowy, niewymagający dalszego zgłębienia, mimo że tak naprawdę nie wyjaśniało ono współczesnych konfliktów. Szczególnie, że wiele aspektów hybrydowości, które wymienia Hoffman, zostało pominiętych⁸⁶. Co ważniejsze, konflikt ukraiński nie dowiódł nawet wyjątkowej skuteczności „hybrydowej” wojny.

O ile postrzegano go jako pewne novum, to szybkie postępy gwarantowała — przede wszystkim — zasadnicza przewaga Federacji Rosyjskiej. Służbę Bezpieczeństwa Ukrainy trawiła korupcja, brak profesjonalizmu, lecz również obecność oficerów nie tylko pozostających pod wpływem rosyjskim, lecz także wprost antyukraińskich⁸⁷. Sytuacja nie była lepsza w strukturze dowodzenia armią, jak również w samym jej stanie — zarówno pod kątem przygotowania strategicznego, wyszkolenia i uzbrojenia. A warto jest także podkreślenie dominacji rosyjskiej artylerii i sił powietrznych, które często były nieśluszenie pomijane w kontekście mówienia o działaniach hybrydowych⁸⁸.

Zdaje się zatem, że bezrefleksyjne użycie określenia „wojna hybrydowa” względem konfliktu w Ukrainie jest uproszczeniem i wyolbrzymieniem czynników tak wewnętrznych, jak również zewnętrznych. Byłoby to jednak nadużyciem, gdyż omawiany konflikt nosi wiele cech wojny hybrydowej sensu largo. Wśród nich wymienić można asymetryczność stron (zarówno pod kątem militarnym, lecz także potencjału ekonomicznego) korzystających z nieregularnych metod walki, poniżej progu wojny. Sam przebieg konfliktu charakteryzował się niską intensywnością, lecz zarazem szerokim wykorzystaniem elementów wojny informacyjnej i psychologicznej. Najistotniejszym jest jed-

⁸⁵ V.I. Batyuk, *The US Concept and Practice of Hybrid Warfare*, „Strategic Analysis” 2017, Vol. 41, Issue 5, s. 471–473; J. Schroefl, S.J. Kaufman, *Hybrid Actors, Tactical Variety: Rethinking Asymmetric and Hybrid War*, „Studies in Conflict & Terrorism” 2014, Vol. 37, Issue 10, s. 869–875.

⁸⁶ A. Krzak, *Wojny przyszłości po rosyjsku...*, s. 18–21, 28.

⁸⁷ Tamże, s. 31–32.

⁸⁸ M. Galeotti, *‘Hybrid War’ and ‘Little Green Men’: How It Works, and How It Doesn’t*, [w:] *Ukraine and Russia: People, Politics, Propaganda and Perspectives*, A. Pikulicka-Wilczewska, R. Sakwa (ed.), Bristol 2015, s. 162–163.

nak konwergencja powyższych działań, która przyczyniła się do powstania efektu synerгии, pozwalającej na skuteczne i wielotorowe realizowanie założonych celów⁸⁹.

Mimo ogólnego spopularyzowania terminu hybrydowości, zdecydowanie nie jest on jedynym sposobem definiowania współczesnych wojen. Przeciwnie, elementy wchodzące w zbiór pojęć hybrydowych dostrzegamy już w starożytności⁹⁰. Przytoczone konflikty historyczne nie są bynajmniej staranną selekcją zdarzeń potwierdzających hipotezę, lecz stanowią ogólny ich przegląd. Należy przy tym uwzględnić trudność wynikającą z faktu, iż nierzadko pomijano choćby sprawy walki partyzanckiej. Uważano ją za niegodną, barbarzyńską lub niewartą wspomnienia przez wzgląd na niewielki na starcia — np. jak w przypadku wojen peloponeskich czy punickich. Trudno też mówić o rozróżnieniu na cywilów i walczących, a przez to hybrydowym obraniu za cel tych pierwszych. Na przestrzeni wieków obie te kategorie rozmywały się w jedno⁹¹ i faktyczne zmiany przyniósł dopiero XIX wiek⁹². Wcześniejsze próby kodyfikowania wojen także nie interesowały się sprawami cywilów, albo podejmowały je dość lakonicznie, np. jak Lieber w swoim „Kodzie”⁹³. Wcześniej, w traktacie o wojnie partyzanckiej, wyrażał on typową dla wojskowych i teoretyków pogardę dla formacji nieregularnych⁹⁴.

W perspektywie takiego dyskursu w dziejach trudno zakładać, iż ekspozycja elementów nieregularnych zawsze była proporcjonalna do ich faktycznego użycia. Dlatego też pozorny wzrost wykorzystania elementów walki hybrydowej wynikać może nie tyle z faktycznych zmian w sposobie prowadzenia wojny, lecz samego jej postrzegania lub sposobu definiowania — przynajmniej częściowo.

⁸⁹ A. Gorzkowicz, *Wojna hybrydowa na Ukrainie jako przykład współczesnych konfliktów zbrojnych*, „Roczniki Studenckie Akademii Wojsk Lądowych” 2017, nr 1, s. 153–154; J. Regina-Zacharski, *Ukraina 2014–2015: wojna (nie)hybrydowa*, „Zeszyty Naukowe AON” 2015, nr 3(100), s. 41–43; M. Tarnawski, *Rosyjska koncepcja konfliktu nieliniowego*, [w:] *Czynnik wojskowy w środowisku międzynarodowym na przełomie XX i XXI wieku*, Ł. Jureńczyk, S. Sadowski, M. Jastrzębski, J. Waskan (red.), Bydgoszcz 2016, s. 59–61.

⁹⁰ J. Flis, *Wojna hybrydowa — zjawisko nowe czy ewolucja starego?*, „Ante Portas — Studia nad Bezpieczeństwem” 2018, Nr 2 (11), s. 17; A. Krzak, *Wojny przyszłości po rosyjsku...*, s. 11; P.H. Пухов, *Муф о „гибридной войне”...*, [odczyt: 30 lipca 2022]; B. Renz, *Russia and ‘hybrid warfare’*, „Contemporary Politics” 2016, Vol. 22, No. 3, s. 284, 286.

⁹¹ F. Freedman, *Przyszła Wojna*, tłum. W. Jeżewski, Ożarów Mazowiecki 2019, s. 62–63.

⁹² Wówczas władze Szwajcarii, m.in. pod wpływem „A Memory of Solferino” Henrego Dunanta, podjęły decyzję o powołaniu Międzynarodowego Komitetu Czerwonego Krzyża, który dokładnie sprecyzował w Konwencji Genewskiej pozycję cywila; *Protokół dodatkowy do konwencji genewskich z 12 sierpnia 1949 r., dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych*, (Dz. U. z 1992 r., nr 41, poz. 175, załącznik), art. 50, s. 21.

⁹³ F. Lieber, *Instructions for the Government of Armies of The United States in the Field*, Washington 1898, art. 20–22, s. 9.

⁹⁴ F. Lieber, *Guerrilla parties: considered with reference to the laws and usages of war*, New York 1862, s. 7–22.

Należy też zadać pytanie, czy konflikty oparte wyłącznie na pośrednich metodach wywarcia wpływu politycznego w ogóle mogłyby być przyszłością? W końcu celem wojny nie jest tylko osłabienie przeciwnika, czy też przymuszenie do go konkretnych działań, a często po prostu zajęcie terytorium. Wymaga to przynajmniej częściowego użycia klasycznej siły, także łączonej z nieregularnymi przedsięwzięciami⁹⁵, co bynajmniej nie jest koncepcją nowoczesną.

W ten sposób tezy o rzekomej innowacyjności wojny hybrydowej falsyfikuje analiza historyczna. Brakuje w niej zupełnie nowej strategii i taktyki, czy też jakiegokolwiek innej rewolucji. Jest to ewolucja rozwiązań stosowanych od wieków, w tym: działań partyzanckich, dywersyjnych i sabotażowych, wprowadzania przeciwnika w błąd tak na polu walki, jak również przed aktem wojny. Wspierano to irredentą polityczną oraz militarną, wykorzystując np. działania psychologiczne wobec mniejszości etnicznych, celem ich wykorzystania do działań odśrodkowych — choćby separatystycznych na tle dążeń narodowych. Nowy jest natomiast arsenał sił i środków, w który włącza się nie tylko zaawansowane technologicznie uzbrojenie (w rozumieniu ewolucji znanego już sprzętu wojskowego), lecz także cyberprzestrzeń. Ta umożliwia prowadzenie wcześniej nieznanych działań, np. ataków hackerskich (w tym na infrastrukturę krytyczną), czy zupełnie odmienia istniejące (dezinformacja, fake news, operacje wpływu)⁹⁶. Zdaje się także, że kolejnym narzędziem o podobnej skali niewiadomych i szerokiego wachlarzu możliwości użycia będzie sztuczna inteligencja.

1.2. Wykorzystanie i kształtowanie cyberprzestrzeni przez „hybrydowość”

W ujęciu historii wojskowości, cyberprzestrzeń jest stosunkowo nowym obszarem interakcji, w tym także politycznej aktywności państw. Mimo to, odgrywa jedną z najistotniejszych ról w kształtowaniu współczesnych teorii wojskowych i strategii.

Początków wirtualnej przestrzeni, a przynajmniej jej funkcji, można dopatrywać się w rozwoju oraz użyciu radiotelekomunikacji, obserwowanego już od II Wojny Światowej.

⁹⁵ F. Freedman, *Przyszła Wojna...*, s. 304–305.

⁹⁶ Należy zauważyć, że tempo ewolucji konfliktów i użycia w nich nowoczesnych technologii jest także wyzwaniem dla prawa międzynarodowego, czego przykładem była reakcja świata wobec konfliktu w Ukrainie w 2014 roku. Strona prawna nie jest jednak przedmiotem niniejszej dysertacji. Zob. P. Ochmann, J. Wojas, *Wojna hybrydowa jako przykład umiędzynarodowionego konfliktu wewnętrznego*, „Studia Prawa Publicznego” 2018, nr 2 (22), s. 119–120; M. Kowalski, *Prawo do samoobrony jako środek zwalczania terroryzmu międzynarodowego*, Warszawa 2013, s. 82; T. Gazzini, *The Changing Rules on the Use of Force in International Law*, Manchester 2005, s. 138.

wej⁹⁷. Wtedy też rozpoczęto prace nad pierwszymi komputerami, w latach 1943–1945 opracowując Elektroniczny, numeryczny integrator i komputer (Electronic numerical integrator and computer — ENIAC)⁹⁸. Zasadniczym celem stworzenia tej maszyny miało być tworzenie tablic artyleryjskich dla Laboratorium Badań Balistycznych Armii USA. Jego pierwszy program służył jednak do zbadania wykonalności budowy broni termojądrowej⁹⁹. Mimo, że początkowo uważano go za projekt pionierski, to po 1975 roku (odtajnieniu części dokumentów dotyczących okresu okoliczno wojennego) dostrzeżono jeszcze inne projekty: niemieckie „maszyny Zusego”¹⁰⁰ oraz Colossus¹⁰¹, czy amerykański ABC¹⁰². Stało się to przyczynkiem nie tylko do rozwoju technologicznego, lecz także myśli artystów, pisarzy i naukowców.

W 1960 roku Joseph Carl Robnett Licklider spisał swoje wyobrażenia o przyszłości interaktywnej kooperatywy między człowiekiem i maszyną, w której fantazjował o globalnej sieci komputerów¹⁰³. Już dwa lata później Paul Baran zaproponował protoplastę Internetu przez cyfrowe sieci o niegwieździstej, rozproszonej strukturze — zaprojektowanej tak, aby oprzeć się atakom. Między innymi to jego starania przyczyniły się do wynalezienia komutacji pakietów¹⁰⁴, a wskazać tu należy także Donalda Daviesa¹⁰⁵. Ten

⁹⁷ S.P. Górka, *Wpływ kolejnych rewolucji w sprawach wojskowych na przyszłe wojny*, „Kultura i polityka” 2014, Nr 16, s. 81–82.

⁹⁸ J.P. Eckert, J.W. Mauchly, *Electronic numerical integrator and computer*, (Patent US3120606A), filled 26.06.1947, issued 04.02.1964.

⁹⁹ R. Rhodes, *Dark Sun: The Making of the Hydrogen Bomb*, New York 1995, s. 251; S. McCartney, *ENIAC, the triumphs and tragedies of the world's first computer*, New York 1999, s. 103.

¹⁰⁰ Konstrukcje Kondrada Zuse, Z1, Z2 i Z3 (zapoczątkowane jako V1 od „model eksperymentalny”, niem. VersuchsModell, zmienione dla odróżnienia od niemieckich pocisków), były zasilanymi elektrycznie, mechanicznymi kalkulatorami binarnymi; K. Zuse, *Frühe Gedanken zur Auswirkung des Computers auf die Gesellschaft*, [w:] *Geschichten der Informatik. Visionen, Paradigmen, Leit motive*, H.D. Hellige (hg.), Berlin 2004, s. 31–42.

¹⁰¹ Wersję pierwszą zbudowano w roku 1943, a drugą w 1944. Uważany jest za pierwszy na świecie programowalny komputer elektroniczny, choć wówczas służyły do tego fizyczne przełączniki oraz wtyczki, a nie znane nam dziś cyfrowe programy; T. Sale, *The Colossus of Bletchley Park — The German Cipher System*, [w:] *The First Computers: History and Architecture*, R. Rojas, U. Hashagen (eds.), Cambridge 2000, s. 351–364.

¹⁰² Atanasoff–Berry Computer — opracowany w 1942 roku przez Johna V. Atanasoffa z pomocą Clifforda Bettego, uważany był za pierwszy prototyp zautomatyzowanego komputera elektronicznego, jednak nieprogramowalnego; M. Campbell-Kelly, W. Aspray, *Computer: A History of the Information Machine*, New York 1996, s. 84.

¹⁰³ J.C.R. Licklider, *Man-Computer Symbiosis*, Cambridge 1960, s. 4.

¹⁰⁴ Komutacja pakietów — zasada fragmentacji przesyłanej informacji na małe pakiety danych, które mogą być wysyłane niezależnymi od siebie drogami, by następnie zostać złożonymi w całość u adresata. Paul Baran przedstawił ten koncept Siłom Powietrznym USA w 1961 roku, a w 1962 wydał publikację podsumowującą jego badania. Istotnym był także cykl jedenastu publikacji pod wspólnym tytułem *On Distributed Communications*; P. Baran, *On Distributed Communications Networks*, Santa Monica 1962, s. 1–9, 19–21, 26–40; C.S. Yoo, P. Baran, *Network Theory, and the Past, Present, and Future of Internet*, „Penn Law: Legal Scholarship Repository” 2018, pos. 2040, s. 1–4.

¹⁰⁵ D.W. Davies, *An Historical Study of the Beginnings of Packet Switching*, „British Computer —→47

dodatkowo w 1968 roku zaprezentował stworzenie rozległej Sieci Agencji Zaawansowanych Projektów Badawczych (Advanced Research Projects Agency Network — ARPANET), będącej przodkiem współczesnego internetu¹⁰⁶.

Od tego momentu rozwój technologii tylko przyspieszał, a obecne tempo jej progresji wydaje się być imperatywem porównywalnym z postępem biologicznym¹⁰⁷, czy też nawet go wyprzedzającym¹⁰⁸. Co więcej, powstanie licznych sieci, z Internetem na czele, zmieniło cyberprzestrzeń w rozległy, pozbawiony granic ośrodek przechowywania i przepływu informacji, który przede wszystkim cechuje się ogromną entropią. Całość stawia zatem zupełnie nowe wyzwania dla systemów bezpieczeństwa, czy samego prowadzenia wojen. Jest to szczególnie problematyczne dla demokracji, aby zachować różnorodność przy globalnym ujęciu sprawiedliwości czy przeciwdziałania zagrożeniom¹⁰⁹.

1.2.1. Miejsce cyberprzestrzeni w działalności politycznej i wojskowej państwa

Środowisko sieciocentryczne stanowi współcześnie istotną przestrzeń dla sfer politycznej i wojskowej, choć niewyłączną — ani teraz, ani potencjalnie w przyszłości. Wbrew powszechniejącej gloryfikacji cyberprzestrzeni, z racji swych cech nie może ona zastąpić rzeczywistości w stopniu, w jakim przedstawiają to technokratyczne wizje¹¹⁰. Jednakże fakt, iż współcześnie środowisko sieciocentryczne nie jest wyłącznym forum decyzyjności, ani przestrzenią walki, nie umniejsza skali wykorzystania go w charakterze narzędzia. Z jednej strony to „tylko” komponent wywierania nacisku, lecz z drugiej: posiada on własną, wyjątkową charakterystykę, która dotychczas nie była spotykana w takiej skali. Jest ona wyzwaniem nie tylko w ontologicznym podejściu do definiowania cyberprzestrzeni, lecz przede wszystkim osadzeniu w niej racji stanu państw. Problematyka ta należy do elementów jakościowej zmiany cywilizacyjnej¹¹¹.

Aby w ogóle mówić o użyciu środowiska sieciocentrycznego przez państwa, lub jego miejscu w teorii wojen, należy odpowiedzieć na pytanie: jaką jurysdykcję mają nad

Society Journal” 2001, Vol. 44, No. 3, s. 151–162.

¹⁰⁶ J. Hofmokl, *Rozwój pola organizacyjnego Internetu — dominacja sieciowej formy porządku społecznego*, „Studia Socjologiczne” 2002, Nr 4 (167), s. 99–100.

¹⁰⁷ J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego”, 2013, nr 9, s. 225.

¹⁰⁸ K. Demir, G.E. Güraksin, *Determining middle school students' perceptions of the concept of artificial intelligence: A metaphor analysis*, „Participatory Educational Research”, Vol. 9, No. 2, s. 298–309.

¹⁰⁹ D. Harvey, *Justice, Nature and the Geography of Difference*, Cambridge 1996, s. 438.

¹¹⁰ M. Graham, S. Khosravi, *Reordering Public and Private in Iranian Cyberspace: Identity, Politics, and Mobilization*, „Global Studies in Culture and Power”, Vol. 9, No. 2, s. 242.

¹¹¹ P. Lewandowski, Ł. Orgmasz, *Racja stanu Polski w cyberprzestrzeni i cyberbezpieczeństwie*, „De Securitate Et Defensione. O Bezpieczeństwie I Obronności” 2022, Nr 8 (1), s. 128.

nim podmioty międzynarodowe? Stwierdzenie, że jakaś część cyfrowej przestrzeni jest suwerenna, bo utrzymywana pozostaje przez infrastrukturę teleinformatyczną na terytorium określonego państwa, nie rozwiązuje problemu. Przykłady płynące z praktyki, np. stosowanie Rozporządzenia ogólnego o ochronie danych osobowych, opierają się na poszanowaniu prawa i ustalonych w nim norm. Stąd arbitralne dzielenie cyberprzestrzeni na strefę Unii Europejskiej (w tym jej użytkowników), pozwala stosować wspomniane prawo, jak w przypadku kary dla spółki Meta z 2023 roku¹¹². Jednak w przypadku działań wykorzystujących środowisko sieciocentryczne jako przestrzeń walki (między aktorami państwowymi i pozapaństwowymi), immanentnie wykracza się poza granice prawa. Zatem tak postrzegana „terytorialność” cyberprzestrzeni staje się nieznaczącym, strategicznym konceptem, który i tak nie będzie poszanowany przez strony konfliktu.

Dlatego uznanie suwerenności konkretnych „fragmentów” cyberprzestrzeni nie może być strategią defensywną, ani nawet odstraszącą, gdyż tym środowisku nie ma to zastosowania¹¹³. Brak motywacji przeciwnika do zachowania posłuszeństwa wobec takich proklamacji powoduje, że w ukryciu prowadzi on operacje pod osłoną problemu atrybucji¹¹⁴ i w efekcie unikania odpowiedzialności¹¹⁵. Można to zaobserwować choćby w powszechnych działaniach podmiotów środowiska sieciocentrycznego, przejawiających się w co prawda mniej brutalnych w skutkach, lecz zarazem częstszych atakach¹¹⁶.

¹¹² Komisja ds. Ochrony Danych zarzuciła spółce Meta Platforms Ireland Limited naruszenie art. 46 (1) RODO przez niewłaściwe przysyłanie danych użytkowników Unii Europejskiej na serwery poza jej obszarem — ulokowane w Stanach Zjednoczonych. Zdaniem Komisji, informacje te mogły być odczytane na żądanie tamtejszych urzędów, co naruszało prywatność obywateli UE; *Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation*, 12 May, [DPC ref. IN-20-8-1] 2023, s. 1–5, 200–214

¹¹³ Warto jednak przyznać, że o ile kwestie suwerenności logicznej przestrzeni cyfrowej zwykle są niemożliwe do obronienia, to indukowały istotne debaty, przekładające się na lepsze wypracowanie strategii i przez to wpływające na bezpieczeństwo państw; N. Schmidt, *Neither Conventional War, nor a Cyber War, but a Long-Lasting and Silent Hybrid War*, „Obrona a strategie” 2014, Vol. 14 No. 2, s. 80; M.N. Schmitt, *States and cyberspace*, [w:] *Tallinn Manual on the International Law Applicable to Cyber Warfare*, M.N. Schmitt (ed.), Cambridge 2013, s. 16–39.

¹¹⁴ Problem atrybucji dotyczy częstej niemożliwości w określeniu agresora w cyberprzestrzeni, bądź faktycznego podmiotu stojącego za nim. Złośliwy kod — jeżeli akurat taki wektor ataku został użyty — może być napisany przez osoby zupełnie nieznane, czy w ogóle zakupiony. W większości przypadków nie da się zatem jednoznacznie określić „producenta broni”, a tym bardziej anonimowej osoby, grupy lub całego podmiotu, w tym międzynarodowego. I o ile możliwości określenia prawdopodobieństwa co do tożsamości agresora poprawiają się, to jak uważa Betts — problem atrybucji wciąż znacząco upośledza skuteczność odstraszenia w środowisku sieciocentrycznym; J.S. Nye, *Deterrence and Dissuasion in Cyberspace*, „International Security” 2017, Vol. 41, No. 3, s. 49–50; R.K. Betts, *The Soft Underbelly of American Primacy: Tactical Advantages of Terror*, „Political Science Quarterly” 2002, Vol. 117, No. 1, s. 31; L. Chircop, *A due diligence standard of attribution in cyberspace*, „International & Comparative Law Quarterly” 2018, Vol. 67, No. 3, s. 662–668.

¹¹⁵ N. Choucri, *Cyberpolitics in International Relations*, Cambridge 2012, s. 4.

¹¹⁶ T. Rid, *More Attacks, Less Violence*, „Journal of Strategic Studies” 2013, Vol. 36, No. 1, s. 139–142.

Problem ten wynika z powszechnie rozpoznanych cech cyberprzestrzeni. Jako pierwszą należy wymienić transformację czasu potrzebnego na prowadzenie faktycznego ataku do niemalże natychmiastowości. Faza przygotowawcza ataku bywa relatywnie łatwa do ukrycia, a samo podjęcie wrogich działań niejednokrotnie nie pozostawia wiele miejsca na obronę — o ile agresor odpowiednio wykorzystał luki bezpieczeństwa. Kolejną sprawą jest wspomniana łatwość przekraczanie fizycznych granic jurysdykcji, czy jej odrzucanie z samej istoty tego, czym jest środowisko sieciocentryczne. Nie pomagają także płynność reguł i szeroko rozumianych konfiguracji (elementów, podmiotów, przestrzeni), bądź powszechna dostępność. To wszystko prowadzi do dekonstrukcji konwencjonalnego myślenia o „terytorium”, a tym samym granicach obronności państw, musząc odnajdywać precyzyjne odzwierciedlenie w strategiach¹¹⁷. Zwłaszcza, że konwencjonalne modele w nich przedstawiane z reguły nie mogą być aplikowane do cyberprzestrzeni. Nie można oczekiwać eskalowania klasycznego konfliktu, rozumianego jako regularnej wojny, wyłącznie na jej obszarze¹¹⁸.

Wszystko to ma istotne implikacje dla postrzegania hybrydowości. Jednym z jej większych problemów jest bowiem brak jasności definicji. Definiując łącznie dwanaście konkretnych zagrożeń hybrydowych, NATO tylko w dwóch przypadkach wymieniło użycie siły w klasycznym rozumieniu¹¹⁹. Pozostałe poruszają m.in. takie działania jak nacisk dyplomatyczny, wpływ na przestępczość zorganizowaną i korupcję, czy wykorzystanie surowców i ekonomii do wywierania nacisku na inne państwa¹²⁰. Zasadnym jest więc postawienie pytania o granicę między zwykłą konkurencją oraz faktycznymi działaniami hybrydowymi. Cyberprzestrzeń zdaje się tutaj tworzyć jaskrawszy podział: przedsięwzięcia jakkolwiek objęte możliwością stosowania prawa, jak to określono powyżej, mogą znaleźć się w kategorii konkurencji. Z kolei wykraczające poza — być postrzegane jako hybrydowe. Ta metoda rozróżnienia mogłaby być kluczowa ze względu na drugi z istotnych problemów działań hybrydowych.

Zwięzłe ich zdefiniowanie, czy też przynajmniej nakreślenie jasnych granic, samo w sobie nie podnosiłoby wartości takiego pojęcia (ze strategicznego punktu widzenia). Często kiedy pojawia się propozycja nowej definicji, jak np. „wojny hybrydowej”, w pierwszym etapie ocenia się czy odnosi się ona do czegoś nowego. To jednak nie „nowość” po-

¹¹⁷ N. Schmidt, *Neither Conventional War...*, s. 78.

¹¹⁸ E. Gartzke, *The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth*, „International Security” 2013, Vol. 38, No. 2, s. 41–73.

¹¹⁹ B. Heap, P. Hansen, M. Gill, *Strategic Communications Hybrid Threats Toolkit*, Strategic Communications Hybrid Threats Toolkit, Riga 2021, s. 10–11.

¹²⁰ Tamże.

winna być przyczynkiem do tworzenia nowych koncepcji, lecz jak „istota” propozycji odnosi się do rzeczywistości: czy jest znacząca i przydatna dla naszych celów¹²¹. Bez możliwości praktycznego stosowania — precyzyjnego i zoperacjonalizowanego, pojęcie takie jak „wojna hybrydowa” może stać się jedynie teoretyczną modą. Niezwykle rozbudowaną akademicko, lecz pustą i nieprzydatną praktycznie. Wspomniana możliwość jasnego rozgraniczenia na konkurencję międzypaństwową (lub między państwami i podmiotami prywatnymi, albo tylko nimi) oraz działania hybrydowe, może więc pomóc przypisać konkretne znaczenie i zastosowanie „hybrydowości”.

Co oczywiste, niemożliwym jest też prowadzenie wyłącznej cyberwojny, gdyż nie pozwalałoby to na realne zwiększanie zasięgu terytorium, władzy, czy przejmowanie surowców. Słowem: zwiększanie wpływów i umacnianie strategicznej pozycji. Mimo wszystko cyberprzestrzeń jest już obszarem prowadzenia działań wojennych i jej znaczenie będzie rosnąć, a przez to zwiększać się będzie skala oddziaływania powyżej opisanych wyzwań. Takiego wzrostu oczekiwać można m.in. na polu dążenia przewagi strategicznej, uzyskiwanej przez możliwości wykorzystywania luk w systemach teleinformatycznych przeciwnika: w rozumieniu zakłócenia zdolności cywilnych, wojskowych, czy uzyskania dostępu do informacji niejawnych, czy prowadzenia walki informacyjnej (dezinformacji, propagandy, stosowania socjotechnik), jak również ekonomicznym. Istotnym jest także fakt, że tego rodzaju działania, szczególnie przez elastyczność, jaką oferuje cyberprzestrzeń, mogą być prowadzone w dowolnej fazie konfliktu, a także poza nim. Jednakże nie tylko w fazie przygotowawczej, do wstępnego osłabienia przeciwnika, lecz również po konflikcie. Wówczas wykorzystywanie metod hybrydowych w cyberprzestrzeni może skutecznie utrudniać odzyskanie stabilności ekonomicznej, politycznej, czy instytucjonalnej.

Istotną dla poruszanej problematyki jest także perspektywa¹²². Z punktu widzenia prawa, czy też bezpieczeństwa publicznego, nieakceptowalne są jakiegokolwiek działania w cyberprzestrzeni, wymierzone w dostawy usług. Należy przez to rozumieć cyberataki na infrastrukturę krytyczną, np. energetyczną czy wodną. Wymaga to jednak niezwykle wysokich standardów bezpieczeństwa, które mogą wykraczać poza praktyczne możliwości państwa — ze względu na wyżej wymienione powody. Jednakże z punktu widzenia strategiczno-militarnego, cyberatak może się wiązać z reperkusjami podobnymi do zupełnie

¹²¹ C. Libiseller, *'Hybrid warfare' as an academic fashion*, „Journal of Strategic Studies” 2023, 21 Feb [wydane poza numerem], s. 17–19.

¹²² J.A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Washington 2002, s. 3.

zwyczajnych przerw w dostawach usług — związanych z wypadkami, awariami i podobnymi. Jeżeli tylko częstotliwość ich występowania sama w sobie nie będzie problemem, to wówczas te same ataki mogą być uznane za mało znaczące dla ogólnego bezpieczeństwa¹²³.

Stąd działania hybrydowe w cyberprzestrzeni nie tylko niosą za sobą wyjątkowe wyzwania, lecz stanowią takowe same w sobie. Zbytne skupienie się na zapobieganiu cyberataków może wymagać ponoszenia zbyt wielkich kosztów, tym samym nie pozwalając na zapewnienie odpowiedniej ochrony najbardziej krytycznym sektorom państwa. Z kolei „poświęcenie” części infrastruktury przez przyjęcie poziomów akceptowalnego ryzyka, może wpłynąć odbiorców danych usług, bezpośrednio zmieniając relacje między obywatelami i państwem — szczególnie w obszarze zaufania.

Odpowiedzią na ten problem zdaje się być ścisła współpraca sektora publicznego i prywatnego, szczególnie w przypadku chęci skutecznego przeciwdziałania cyberzagrożeniom. W takim wypadku podmioty sektora prywatnego muszą odgrywać aktywną rolę w zabezpieczaniu środowiska cyfrowego. Nie wystarcza bowiem, aby firmy „stały obok” organów państwowych i czekały na egzekwowanie przepisów dotyczących szeroko rozumianej cyberprzestępczości, czy nawet cyberataków w militarnym znaczeniu. Zachowanie odpowiedniej czujności i pro-aktywności pozostaje w interesie sektora prywatnego¹²⁴. Kluczowym problemem są natomiast osiągnięcie konwergencji wysiłków publicznych oraz prywatnych w zapewnieniu cyberbezpieczeństwa, a przez to odpowiedniego balansu między dwoma sektorami i końcowego efektu synergii.

1.2.2. Znaczenie sektora prywatnego w cyberprzestrzeni

U podstaw rzeczowej współpracy między państwem i aktorami prywatnymi należy najpierw ustalić: w jaki sposób ma ta kooperacja przebiegać? Jest to zasadniczy problem, który do dziś nie został właściwie rozwiązany. Od lat sektor prywatny wspierał państwo na zasadach dobrowolnej samoregulacji i stosowania procedur bezpieczeństwa — ze względu na wcześniej opisaną zbieżność interesów¹²⁵. Również współcześnie jest to model zasadniczy, choć w ciągu ostatniej dekady coraz więcej państw wdrażało model nakazanej samoregulacji. Podmioty sektora prywatnego musiały wówczas spełniać określone kryteria, lecz te miały raczej ramowy charakter i pozostawiały dużą dowolność we

¹²³ Tamże.

¹²⁴ J.S. Hiller, R.S. Russell, *The challenge and imperative of private sector cybersecurity: An international comparison*, „Computer Law & Security Review” 2013, No. 29, s. 245.

¹²⁵ F.B. Hare, *Private Sector Contributions to National Cyber Security: A Preliminary Analysis*, „Journal of Homeland Security and Emergency Management” 2009, Vol. 6, No. 1, s. 5.

wdrażaniu¹²⁶. Z tak obranym kierunkiem polemizuje m.in. James P. Farwell. Uważa on, że aby wzmocnić cyberbezpieczeństwo, należy usuwać przeszkody legislacyjne i funkcjonować w oparciu o partnerstwo między interesami publicznymi oraz prywatnymi. Jego zdaniem to sektor prywatny może być źródłem zachęty do ochrony interesów narodu¹²⁷.

Z punktu widzenia państwa, które naturalnie nie chce tracić kontroli nad elementami systemu bezpieczeństwa, takie podejście może być uznane za niewłaściwe. Sugeruje się także, że w warunkach samoregulacji, do ponoszenia (przez podmioty prywatne) oczekiwanych wydatków na cyberbezpieczeństwo, potrzebna jest odpowiedź prawna lub rynkowa¹²⁸. Szczególnie w przypadku tej drugiej, reakcja i zasadnicze „uregulowanie” mogą być procesem długim, zdecydowanie nieprzystającym cyberzagrożeniom. Te, jak wskazano wcześniej, mogą być wydarzeniami nagłymi oraz krótkotrwałymi. Ponadto wskazuje się, że obowiązki wynikające z przepisów prawa sprzyjają ogólnej poprawie bezpieczeństwa — także poza obszarem, którego bezpośrednio dotyczą¹²⁹. Przykładem może być wspomniane już rozporządzenie ogólne o ochronie danych osobowych, przyjęte i wdrożone przez Unię Europejską wobec swoich obywateli. Zastrzeżenie, iż zewnętrzni operatorzy muszą dostosować się do tego prawa, ilekroć chcą dokonywać interakcji z obywatelami UE, wprost doprowadziło do globalnego polepszenia praktyk związanych z poszanowaniem prywatności i przetwarzania danych osobowych. Nie bez znaczenia był także ramowy charakter rzeczoności rozporządzenia, który ułatwił jego wdrażanie i adaptowanie przez inne państwa, dla których rozwiązania UE stały się wzorcem¹³⁰.

Analizy funkcjonowania systemów komputerowych dowodzą jednak, że mechanizmy samoregulacji mogą być skuteczną odpowiedzią na zagrożenia w cyberprzestrzeni. Wskazuje się m.in. zalety autonomizowania, czyli przenoszenia wiedzy i możliwości na możliwie zindywidualizowane podmioty środowiska sieciocentrycznego, umożliwiając im szybkie i właściwe reagowanie na incydenty¹³¹. Potwierdzenie słuszności takiego

¹²⁶ K.S. Min, S.W. Chai, M. Han, *An International Comparative Study on Cyber Security Strategy*, „International Journal of Security and Its Applications” 2015, Vol. 9, No. 2, s. 12, 16–19.

¹²⁷ J.P. Farwell, *Industry’s Vital Role in National Cyber Security*, „Strategic Studies Quarterly” 2012, Vol. 6, No. 4, s. 34–35.

¹²⁸ B.H. Kobayashi, *An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and other Public Security Goods*, „Supreme Court Economic Review” 2006, Vol. 14, s. 263–264.

¹²⁹ J.S. Hiller, R.S. Russell, *The challenge and imperative...*, s. 245.

¹³⁰ P.M. Schwartz, *Global Data Privacy: The EU Way*, „New York University Law Review” 2019, Vol. 94, Rev. 771, s. 134–137, 145–146.

¹³¹ E. Alqurashi, G. Wills, L. Gilbert, *A Viable System Model for Information Security Governance: Establishing a Baseline of the Current Information Security Operations System*, [w:] *Security and Privacy Protection in Information Processing Systems*, L.J. Janczewski, H.B. Wolfe, S. Sheno (eds.), Auckland 2013, s. 249.

podejścia można odnaleźć w modelowaniu matematycznym z użyciem teorii gier¹³². Przy tym podkreśla się, że kluczowe jest systemowe podejście do zarządzania takimi podmiotami przez zachowanie skutecznych form sprzężenia zwrotnego. Po pierwsze, system agreguje dzięki temu informacje na temat zagrożeń, mogąc użyć ich w celach prewencyjnych¹³³. Po drugie, umożliwia to skorelowanie częstotliwości wykorzystywania działań samoregulacyjnych z częstotliwością występowania ataków, aby ocenić ogólną ewolucję procesów danego systemu. Jeśli ten relatywny wskaźnik nie pogorszy się (proporcja incydentów bezpieczeństwa ogółem nie wzrośnie względem przypadków aktywnego przeciwdziałania), to ewolucję tę należy uznać za pozytywną¹³⁴.

Całość ukazuje pełniejszy obraz subtelного balansu w środowisku bezpieczeństwa cyberprzestrzeni: między samoregulacją licznych podmiotów sektora prywatnego oraz interwencjonizmem podmiotów państwowych i ponadpaństwowych. Jednak czy taki podział ma sens w przypadku środowiska sieciocentrycznego? O ile jest on znaczący z punktu widzenia prawnych granic oraz funkcjonowania instytucji państwowych, to przeciwnik takiego rozgraniczenia uznawać nie musi. Dla niego liczy się jedynie osiągnięty cel, a nie to kto zarządza związaną z nią infrastrukturą, oprogramowaniem, dostarcza rozwiązania technologiczne, lub je wykorzystuje. Usunięcie z rozważań podziału na podmioty prywatne i państwowe, w tym przypadku niczego nie zmienia — atakujący w cyberprzestrzeni przeprowadzi czynności zasadniczo tak samo. Mimo to, państwa wciąż zachowują pewną przewagę oddziaływania w środowisku, związaną z rozwiązaniami prawnymi oraz możliwością wywierania nacisku na sektor prywatny.

Wspomniane modele matematyczne teorii gier oparte są o samoregulację przez opłacalność działań¹³⁵. To z kolei może być skutecznym narzędziem wspomnianego nacisku. Zamiast wprowadzać normy nakazujące określone działania, państwo lub inny, uprawniony podmiot prawa międzynarodowego, może penalizować niektóre zachowania ogólnie, lub tylko o ile doprowadziły do jakichś reperkusji. Wówczas samoregulacja sektora prywatnego jest ukierunkowywana na określony cel, lecz zarazem wdrożenie konkretnych metod jego osiągnięcia wciąż pozostaje w sferze wolnego wyboru. Co więcej, ka-

¹³² R. Solovey, *Game-Theoretic Approach to Self-Regulation of Dynamic Network Infrastructure to Protect Against Cyber Attacks*, [w:] *2020 International Scientific and Technical Conference Modern Computer Network Technologies*, R. Smeliński (ed.), Moscow 2020, s. 5–6; M. A. Poltavtseva, *Formation of Data Structures in the Problems of Active Security Monitoring*, „Automatic Control and Computer Sciences” 2021, Vol. 57, Issue 2, s. 1204, 1206–1207.

¹³³ E. Alqurashi, G. Wills, L. Gilbert, *A Viable System Model...*, s. 250–251.

¹³⁴ D. Zegzhda, D. Lavrova, E. Pavlenko, A. Shtyrkina, *Cyber Attack Prevention Based on Evolutionary Cybernetics Approach*, „Symmetry” 2020, Vol. 12, Issue 11, s. 17

¹³⁵ R. Solovey, *Game-Theoretic Approach to Self-Regulation of...*, s. 5–6.

ralność jedynie za incydenty prowadzące do określonych skutków może mieć dodatkowy, pozytywny wpływ na bezpieczeństwo środowiska sieciocentrycznego. Ponownie przytoczyć tu można rozwiązania rozporządzenia ogólnego o ochronie danych osobowych. Podmiot, w którym dojdzie do naruszenia przepisów o przetwarzaniu danych osobowych, może uniknąć konsekwencji finansowych (lub ograniczyć je), o ile sam, na określonych warunkach, zgłosi fakt zaistnienia wycieku¹³⁶. Takie sformułowanie przepisów motywuje do proaktywnego działania na rzecz poprawy bezpieczeństwa, a jednocześnie wzmacnia ewentualną współpracę między podmiotami prywatnymi i wykonawczymi dla danego prawa, zachęcając do rozwoju dobrych praktyk na rzecz bezpieczeństwa¹³⁷. Jednakże sama skala interwencjonizmu oraz ramowego podejścia do przepisów wykonawczych, czy też strategii bezpieczeństwa, winna stanowić istotny czynnik balansowania w systemie. Omawiane rozporządzenie jest bowiem krytykowane m.in. za to, że wciąż wiele podmiotów prywatnych (szczególnie małych) nie dostosowało się do przepisów. Ponadto szyfrowanie informacji przetwarzanych elektronicznie wciąż nie jest szeroko zaadaptowane¹³⁸. Mimo to, rzeczne rozporządzenie wciąż pozostaje krokiem w dobrą stronę oraz praktycznym przykładem sposobu tworzenia prawa, które może skutecznie oddziaływać na środowisko sieciocentryczne.

Istotnym jest, że wykorzystanie sektora prywatnego pozostaje kluczowe dla zapewnienia bezpieczeństwa państwa w przestrzeni cyfrowej. Odpowiednio ustrukturyzowana współpraca może stać się istotnym czynnikiem odstrasającym tak przeciwnika wewnętrznego, jak również zewnętrznego. Szczególnie, że nie mamy rozwiązań skutecznej obrony sieci pod kątem świadczenia usług własnych użytkowników (obywateli) oraz obsługi infrastruktury, a zarazem utrzymania globalnych połączeń¹³⁹. Nie można także uznać, że nieregularne i hybrydowe działania będą odgrywać tu wyłącznie niekorzystną rolę, przez wzmacnianie pozycji przeciwnika, lub wręcz odwrotnie: stymulować obronność zdywersyfikowaną na podmioty prywatne, gdyż leży to w ich interesie. Działania te dają podobne możliwości obu stronom, lecz zarazem znacząco przyspieszają

¹³⁶ Zgodnie z art. 83, ust. 4, niezgłoszenie naruszenia jest podstawą do nałożenia kary administracyjnej. Z kolei dokonanie zgłoszenia w przewidzianym przepisami trybie, współpraca z właściwym dla administratora organem zajmującym się ochroną danych osobowych, jak również wykazanie stosowania zabezpieczeń, mogą skutkować nienalożeniem kary lub znaczącym jej zmniejszeniem.

¹³⁷ G. Buckley, T. Caulfield, I. Becker, *“It May Be a Pain in the Backside but...” Insights into the Resilience of Business after GDPR*, [referat konferencyjny] *New Security Paradigms Workshop*, North Conway, 2022, s. 12; M. Mollaeefar, S. Ranise, *Identifying and quantifying trade-offs in multi-stakeholder risk evaluation with applications to the data protection impact assessment of the GDPR*, „Computers & Security” 2023, Vol. 129, s. 3–5.

¹³⁸ G. Buckley, T. Caulfield, I. Becker, *“It May Be a Pain...”*, s. 3.

¹³⁹ H.G. Rice, *Unconventional Cyber Warfare: Creating a Cyber Resistance in the Private Sector*, Quantico 2019, s. 12.

ewolucję metod i form cyfrowej walki. To przenosi odpowiedzialność za ewentualną dysproporcję w możliwościach atakującego oraz obrońcy na pozostałe elementy środowiska bezpieczeństwa.

1.2.3. Systemowe ujęcie współpracy sektora prywatnego i publicznego w cyberprzestrzeni

Analiza sektora prywatnego i publicznego, jego celów, potrzeb oraz możliwości, a szczególnie mechanizmów samoregulacji i sprzężenia zwrotnego, sugeruje możliwość zastosowania modelu systemu politycznego Davida Eastona. Czerpiąc z cybernetyki, założył on stworzenie wysoce abstrakcyjnych ram metateoretycznych, stosując logiczne związki między aksjomatami, w które możliwe byłoby wpisanie całej dyscypliny nauk o polityce¹⁴⁰. Jednakże rzeczywisty holizm i uniwersalność do dziś pozostają przedmiotem dyskusji¹⁴¹. Jednakże dotychczas cyberprzestrzeń przedstawiano raczej jako zjawisko samo w sobie (głównie społeczne)¹⁴², definicyjnie syntetyczne. Autorzy dostrzegali w niej także ewolucyjną siłę napędową procesów politycznych¹⁴³, lub narzędzie służące tak rozwiązywaniu problemów państw, jaki je generujące¹⁴⁴. Innymi słowy, środowisko sieciocentryczne jest badane jako odzwierciedlenie realnych procesów politycznych, lub powód tworzenia nowych. Jednak analizy skupiające się na cyberprzestrzeni w przedmiotowym jej ujęciu pozostają nieliczne.

Samo środowisko sieciocentryczne rozpatrywane może być jako zawierające podmiot — użytkowników sieci, a także przedmiot — szeroko rozumianą informację cyfrową. Jednocześnie oba te pojęcia należy rozumieć jako ogólne, modelowe kategorie, w skład których mogą wchodzić inne, liczne definicje¹⁴⁵. Istotne są także zależności między użytkownikami sfery cyfrowej, którzy czynią z niej przestrzeń interakcji społecznych,

¹⁴⁰ D. Easton, *The Political System. An Inquiry into the State of Political Science*, New York 1966, s. 52–63.

¹⁴¹ P. Leslie, *General Theory in Political Science: A Critique of Easton's Systems Analysis*, „British Journal of Political Science” 1972, Vol. 2, Issue 2, s. 159–163, 168–169, 171–172; C.W. Barrow, *There are Better Alternatives than Easton: A Critical Rejoinder to William J. Kelleher*, „New Political Science” 2018, Vol. 40, Issue 1, s. 191–193, 196–197.

¹⁴² R. Gibson, W. Lusoli, S. Ward, *The Australian public and politics on-line: Reinforcing or reinventing representation?*, „Australian Journal of Political Science” 2008, Vol. 43, Issue 1, s. 112–113, 118–121, 128–129.

¹⁴³ N.H. Nie, D.W. Miller III, S. Golde, D.M. Butler, K. Winneg. *The World Wide Web and the U.S. Political News Market*, „American Journal of Political Science” 2010, Vol. 54, No. 2, 429–433.

¹⁴⁴ J.N. Druckman, M.J. Kifer, M. Parkin, *Timeless Strategy Meets New Medium: Going Negative on Congressional Campaign Web Sites, 2002–2006*, „Political Communication” 2010, Vol. 27, Issue 1, s. 88–91, 95, 98.

¹⁴⁵ Kategorie te nie zawsze są tak nazywane, lecz zasadniczo rozumiane i wykorzystywane w podany sposób, zob. M. Heim, *The Erotic Ontology of Cyberspace*, [w:] *The Metaphysics of Virtual Reality*, M. Heim (ed.), Oxford 1993; C. Chesher, *The Ontology of Digital Domains*, [w:] *Virtual Politics: Identity and Community in Cyberspace*, D. Holmes (ed.), London–Thousand Oaks–New Delhi 1997.

a przez to pozwalają aplikować dotychczasowe teorie polityczne w środowisku sieciocentrycznym¹⁴⁶. Dodatkowo motywuje to możliwość stosowania modelu Eastona, szczególnie w jego behawioralnym aspekcie.

Należy jednak podkreślić, że wspomniana dychotomia kategorii, choć zrozumiała i szeroko stosowana, to współcześnie napotykała problem. Sztuczna inteligencja może pełnić funkcje użytkownika, a także być rozumiana sama w sobie jako złożony rodzaj informacji (gdyż nie sposób nadawać jej cech osobowości i autonomicznego podejmowania decyzji). Ontologiczne rozważania o naturę sztucznej inteligencji nie mają jednak wpływu na sedno badań systemowych, lecz wydaje się, iż przydatność kategorii pośredniej winna być oceniona.

Jednocześnie przyjęte zostało, że sama idea „przestrzenności” rzeczywistości cyfrowej nie ma znaczenia dla rozumienia systemu. Należy bowiem pamiętać, że o ile cyberprzestrzeń jest wymieniana jako piąta przestrzeń walki, obok lądu, powietrza, wody i kosmosu¹⁴⁷, to nie sposób pominąć krytyki takiego jej postrzegania. Podejście to jest oparte w postmodernizmie i przekonaniu, że przestrzenność rzeczywistości cyfrowej jest konstruowana społecznie — jako wynik sieci połączeń¹⁴⁸. To z kolei miałoby skłaniać ku pojęciu środowiska sieciocentrycznego¹⁴⁹. Dla przedmiotu niniejszej pracy, „cyberprzestrzeń” oraz „środowisko sieciocentryczne” używane są w sposób tożsamy.

Aby w ogóle zacząć rozważania nad zastosowaniem teorii systemów według Eastona, należy najpierw odpowiedzieć na pytanie, jak on sam postrzegał system polityczny. A ten określał jako mechanizm formowania oraz sprawowania władzy w społeczeństwie celem alokacji dóbr i zasobów¹⁵⁰.

Władza, w rozumieniu Eastona, była już oceniana pod kątem systemu. Jedną z publikacji rozróżnia dobra w środowisku sieciocentrycznym na informację i uwagę użytkowników, tej drugiej przypisując wyższą wartość. Jednocześnie autorzy twierdzą, że tutaj nie ma mowy o jakimkolwiek ośrodku władzy, który regulowałby ją¹⁵¹. W zamian odwołują się do konceptów miękkiego wpływu, np. przez wielkoskalowe agregatory me-

¹⁴⁶ J.E. Cohen, *Cyberspace as/and Space*, „Georgetown Law Faculty Publications and Other Works” 2007, 107 Colum. L. Rev. 210-256, s. 218, 221-224, 235-238.

¹⁴⁷ J.A. Warden, *The Enemy as a System*, „Airpower Journal” 1995, Vol. 9, No. 1, s. 44-55.

¹⁴⁸ J.E. Cohen, *Cyberspace as/and Space...*, s. 226.

¹⁴⁹ O ile przyznać należy, że to zależności między elementami systemu winny być przedmiotem badań w rozumieniu politycznym, a nie sama „przestrzeń”, to podejście takie byłoby bezzasadnym dla rozważań nad bezpieczeństwem.

¹⁵⁰ Zob. D. Easton, *An Approach to the Analysis of Political Systems*, „World Politics” 1957, Vol. 9, No. 3.

¹⁵¹ S.S. Shirin, N.M. Bogolubova, J.V. Nikolaeva, *Application of David Easton's Model of Political System to the World Wide Web*, „World Applied Sciences Journal” 2014, Vol. 30, No. 8, s. 1084.

diów, czy do ściśle technicznych aspektów cyberprzestrzeni. Za rodzaj systemowej władzy uważają np. instytucje zajmujące się dystrybucją adresów IP czy rejestracją domen¹⁵². W innym źródle możemy odnaleźć, że władza (dążenie do niej) to po prostu siła napędowa szeroko rozumianych, agresywnych działań w cyberprzestrzeni. Podmioty dlatego dopuszczają się ataków, że chcą uzależniać od siebie innych aktorów lub infrastrukturę, rozszerzać swój wpływ, a w efekcie pomnażać zyski¹⁵³. Jeszcze inna analiza wyszczególnia trzy odsłony władzy, z których każda może być sprawowana środkami miękkimi lub twardymi. Są to: indukcja — wywieranie wpływu na inny podmiot, by ten podjął działania, których w innym wypadku by nie czynił, kontrola agendy — uniemożliwienie drugiemu aktorowi podejmowania decyzji przez wykluczenie jego strategii, a także warunkowanie — czyli wpływ na preferencje przeciwnika tak, że ten nawet nie bierze pod uwagę pewnych strategii¹⁵⁴. Istotnym jest jednak poszerzenie tego o koncept dyfuzji władzy w domenie cybernetycznej, czyli rozłożenie jej na wielką liczbę użytkowników w cyberprzestrzeni, przy jednoczesnej redukcji różnic sprawowania władzy między nimi¹⁵⁵. Autor argumentuje, że tak nastoletni haker, jak i rząd, mogą na równi wyrządzać szkody w cyberprzestrzeni — a zatem w „dyfuzji” widzi zjawisko asymetryczności. To z kolei wprost sprzeciwia się dawnemu pojmowaniu cyberprzestrzeni jako narzędzia hegemonicznego sprawowania władzy¹⁵⁶. Jeżeli rozważyć klasyczne koncepty współpracy i konkurencji między państwami, to dwoma kluczowymi czynnikami pojawienia się hegemonii są niska współpraca oraz wyższy próg zdobywania władzy¹⁵⁷. Jak wcześniej wskazano, środowisko sieciocentryczne nie tylko sprzyja współpracy (mimo zachowania pewnej konkurencyjności), lecz dodatkowo ją premiuje, stanowiąc podstawę zachowania bezpieczeństwa. Zarazem dyfuzja władzy, która zdaje się być zbieżna z konceptem asymetryczności, znacząco obniża próg. I choć nie można pomijać głosów sugerujących, że cyberprzestrzeń może służyć za pewne narzędzie implementacji hegemonii osiągananej w inny sposób¹⁵⁸, to nie sposób traktować ją jako znaczącej w tym aspekcie. Rysuje to zatem obraz władzy rozproszonej, lecz cechującej się tym samym większą nieprzewidywalnością.

¹⁵² Tamże, s. 1085.

¹⁵³ N. Choucri, *Emerging Trends in Cyberspace: Dimensions and Dilemmas*, [w:] *Cyberspace: Malevolent Actors, Criminal Opportunities and Strategic Competition*, P. Williams, D. Fiddner (eds.), [AD1014198] 2016, s. 65–70.

¹⁵⁴ J.S. Nye Jr., *Cyber Power*, Cambridge 2010, s. 7

¹⁵⁵ Tamże, s. 9–17.

¹⁵⁶ J.E. Cohen, *Cyberspace as/and Space...*, s. 226.

¹⁵⁷ D. Brizhinev, N. Ryan, R. Bradbury, *Modelling Hegemonic Power Transition in Cyberspace*, „Complexity” 2018, Vol 2018, Art. ID: 9306128, s 1–2, 10.

¹⁵⁸ Zob. S. Lobastova, *Geopolitics of Cyberspace and Virtual Power*, „Journal of Liberal Arts and Humanities” 2020, Vol. 1, No. 3.

Rozważając istotę cyberprzestrzeni pod kątem zastosowania modelu Eastona, należy rozważyć kwestię dóbr i zasobów, które należy w pierwszej kolejności rozróżnić. W klasycznym rozumieniu, dobra to materialne towary lub produkty fizyczne, które posiadają wartość i zaspokajają ludzkie pragnienia lub potrzeby. Mogą one być produkowane, konsumowane oraz sprzedawane w ramach systemów ekonomicznych. Później w definicję włączono również dobra niematerialne¹⁵⁹. Zasoby są natomiast szeroko rozumianym potencjałem i czynnikiem produkcji, czyli procesu przetwarzającego zasoby na dobra (oraz usługi). Jednocześnie należy podkreślić, że to jak zasoby zostaną wykorzystane, a zatem jak mogą być interpretowane, silnie zależy od procesów społecznych, tworzących kontekst. Jest to zatem pojęcie silnie relacyjne i heterogeniczne — zawsze może być postrzegane przez pryzmat wielu kategorii, które silnie na siebie wpływają¹⁶⁰. Istotnym rozróżnieniem omawianych pojęć, wynikających z ich roli w ekonomii, jest charakter wejściowy zasobów i wyjściowy w przypadku dóbr. Takie rozumienie pozwala na osadzenie ich w konkretnych miejscach systemu.

Podobne definiować można powyższe pojęcia w samym środowisku sieciocentrycznym. Cyfrowa informacja jest w tym wypadku jedynym dobrem pierwotnym. O ile może być interpretowana wtórnie jako jej zawartość (np. wiedza), to sama w sobie stanowi konkretny koncept — czy to rozumiany zupełnie abstrakcyjnie, czy jako konkretny stan logiczny właściwej jej infrastruktury teleinformatycznej, która wspomniane dane przechowuje¹⁶¹.

Zasoby cyfrowe stanowią jednak dużo szerszy koncept. Przede wszystkim może odwoływać się do zbioru samych informacji cyfrowych (dóbr w cyberprzestrzeni). Tak rozumiane zasoby (danych) implikują też interesujący koncept. Ze względu na syntetyczną naturę środowiska sieciocentrycznego — fakt że jest to przestrzeń stworzona i utrzymywana, a nie zastana, to zasoby cyfrowe nie mogą być niczyje¹⁶². Co najwyżej za takie, z pragmatycznych przyczyn, uznać można zasoby wspólne w przestrzeni cyfrowej, czyli

¹⁵⁹ P. Hill, *Intangibles and Services: A New Taxonomy for the Classification of Output*, „The Canadian Journal of Economics” 1999, Vol. 32, No. 2, s. 426–427; J. Bowen, *Managing Service Organizations: Does Having a “Thing” Make a Difference?*, „Journal of Management” 2002, Vol. 28, No. 3, s. 448–449; L. Araujo, M. Spring, *Services, products, and the institutional structure of production*, „Industrial Marketing Management” 2006, Vol. 35, No. 7, s. 798–799.

¹⁶⁰ H. Bathelt, J. Glückler, *Resources in Economic Geography: From Substantive Concepts towards a Relational Perspective*, „Environment and Planning A: Economy and Space” 2005, Vol. 37, Issue 9, s. 1546–1547, 1557–1559.

¹⁶¹ Informacja definiowana jest wielowymiarowo, nie tylko z perspektywy organizacyjno-technicznej, lecz także semiotycznej, społecznej lub ściśle ekonomicznej, por. J. Oleński, *Ekonomika informacji*, Warszawa 2001, s. 286–291.

¹⁶² S. Czetwertyński, *Tragedia zasobów niczych a gospodarka internetowa*, „Rynek Społeczeństwo Kultura”, nr 3(7), s. 35.

pozostające poza ścisłą regulacją prawną i przez to wykorzystywane w dowolny sposób przez podmioty. Ich istnienie jednak zawsze zapewnia infrastruktura (urządzenia) będące czyjąś własnością. Innym rodzajem zasobów w środowisku sieciocentrycznym są cyfrowe odpowiedniki klasycznie rozumianych zasobów ekonomicznych — wraz z kapitałem potencjału ludzkiego, wiedzy i podobnych.

David Easton argumentuje, że *wejście* systemu składa się z żądań i wsparcia, co nadaje całości dynamicznego charakteru — system nie jest statyczny, lecz opisują go stałe procesy¹⁶³. Żądania rozumiane są tu jako zbiór potrzeb, pragnień i roszczeń ogółu społeczeństwa wobec władzy, dotyczących alokacji dóbr, regulacji zachowań, partycypacji w systemie oraz komunikacji¹⁶⁴. Z kolei wsparcie to podtrzymywanie systemu przez podporządkowanie się jego regułom przez posłuszeństwo, wspólny system przekonań, pracę na jego rzecz itd¹⁶⁵.

W ten sposób definiować możemy również zasoby cyfrowe, w skład których wchodzi przede wszystkim szeroko rozumiane potrzeby podmiotów cyberprzestrzeni, pokrywające się z żądaniami rozumianymi przez Eastona. Jedyną różnicą jest tutaj ośrodek władzy, wobec którego są wystosowywane. Literatura wymienia tutaj właścicieli wielkich portali i dostawców usług, których działania wpływają na sieć, np. Google (Alphabet), Facebook (Meta) i podobnych¹⁶⁶. Jest to jednak wyłącznie powierzchowne podejście do pojęcia władzy. Należy raczej twierdzić, że podmioty środowiska sieciocentrycznego wysuwają swoje żądania nie wobec konkretnego aktora(ów), lecz bardziej abstrakcyjnego konceptu władzy rozproszonej. Ich oczekiwania, dotyczące zachowań pozostałych podmiotów, komunikowania, ciągłości i sposobu przetwarzania informacji cyfrowych oraz wielu innych, są potrzebami uniwersalnymi, za które wszyscy użytkownicy sieci w pewnym stopniu ponoszą odpowiedzialność. To zarazem daje wyraz wsparcia dla istoty systemu. Partycypacja w nim oznacza akceptację takiego stanu rzeczy i przyjęcie konceptu dyfuzji władzy, nawet jeśli nie odbywa się to z pełną świadomością znaczenia tegoż rozproszenia. Źródeł takiego stanu rzeczy można doszukiwać się tak w kwestii umowy społecznej, jak również syntetycznego, wspólnie wytworzonego stanu środowiska sieciocentrycznego (gdyż do powiększania przestrzeni logicznej przyczynia się ogół infrastruktury, włączając w to personalne komputery i podobne).

¹⁶³ D. Easton, *An Approach to the Analysis of Political Systems...*, s. 387.

¹⁶⁴ Tamże, s. 388–390.

¹⁶⁵ Tamże, s. 390–391.

¹⁶⁶ S.S. Shirin, N.M. Bogolubova, J.V. Nikolaeva, *Application of David Easton's...*, s. 1086.

Wyjściem z tegoż systemu są natomiast informacje — rozumiane jako cyfrowe stany logiczne (dane), jak i to co niosą za sobą. Są zarówno przedmiotem sieci sensu stricto, jak również reprezentują decyzje i polityki (w szerokim rozumieniu tego słowa). To na podstawie tych przetwarzanych informacji, zmieniają się żądania i wsparcie, a zatem następuje sprzężenie zwrotne.

Co więcej, to właśnie na podstawie takiego wyjścia jesteśmy w stanie analizować ewaluować wewnętrzne procesy, które nie zaszyby bez tego, co zostało wyżej określone jako wejście. Jasno wyznaczone są także granice takiego systemu, gdyż tożsame są z granicami cyberprzestrzeni samej w sobie. Pozwala to zdecydowanie identyfikować środowisko sieciocentryczne jako system polityczny sam w sobie, gdyż spełnia ono przesłanki wskazywane przez Eastona¹⁶⁷. Ma to jednak istotne implikacje dla klasycznie rozumianego systemu politycznego: ogranicza bowiem jego wpływ w środowisku sieciocentrycznym. Nie jest ono jedynie przestrzenią, taką jak ląd, woda, powietrze czy kosmos, w którym państwo może proklamować przynależność jakiegoś obszaru oraz podejmować co do niego decyzje. Stanowi raczej przestrzeń, która z samej swej natury jest pewnego rodzaju systemem.

Zatem zdaje się, że państwa i inne podmioty prawa międzynarodowego mogą być jedynie jednym z podmiotów, które konkurują wraz z innymi w sferze cyfrowej — z wpływem zwykle o wiele większym od innych, ze względu na wcześniej wymienione powody, jednak nigdy wyłącznym. Byłoby to jednak niedopowiedzeniem, gdyż system nie może istnieć w próżni, lecz w konkretnym środowisku. Easton sam wskazuje, że składają się na nie m.in. inne systemy w których przedmiotowy system funkcjonuje¹⁶⁸. Dynamicznie adaptuje się on do zmian w swym otoczeniu, tak aby utrzymać zmienne kluczowe dla jego funkcjonowania w akceptowalnym zakresie¹⁶⁹. Nie jest w tym jednak pasywny, bo jeżeli ze strony środowiska pojawiają się jakieś „zakłócenia”, to system próbuje też je korygować — na tyle, na ile ma do tego środki i możliwość wpływu¹⁷⁰.

Skoro cyberprzestrzeń jest środowiskiem sztucznie wytworzonym, to koniecznie musi być systemem funkcjonującym w ścisłej relacji do innych, m.in. tego, co rozumiemy przez klasyczne systemy polityczne. Jest to jednak relacja podrzędna, za czym przemawiają obserwacje empiryczne: to w jaki sposób klasycznie rozumiana władza państwowa może kształtować cyberprzestrzeń nie jako jeden z aktorów wewnątrz niej, lecz tworząc

¹⁶⁷ D. Easton, *An Approach to the Analysis of Political Systems...*, s. 384–386.

¹⁶⁸ Tamże, s. 388.

¹⁶⁹ P. Leslie, *General Theory in Political Science...*, s. 157.

¹⁷⁰ D. Easton, *A framework for political analysis*, New York 1965, s. 132.

odpowiednie „zakłócenia”. Systemowo rozumiane środowisko cyfrowe reaguje więc na zmiany w otoczeniu, korygując swoje działanie tak, aby osiągnąć równowagę pozwalającą na dalsze funkcjonowanie. Wskazany przez Eastona brak pasywności wskazuje jednak, że wywarcie zbytniego nacisku może spowodować reakcję podsystemu cyberprzestrzeni względem systemu politycznego.

Wnioski wysuwające się z analizy systemowej mają szczególne implikacje dla postrzegania działań hybrydowych w cyberprzestrzeni. Należy bowiem podkreślić, że po pierwsze: dopóki państwo nie przeniesie wszystkich swoich krytycznych aktywów i wymiarów funkcjonowania do środowiska sieciocentrycznego, to niemożliwe będzie prowadzenie „prawdziwej”, wyłącznej walki w tej przestrzeni. Nieosiągalne jest też skuteczne realizowanie celów klasycznych konfliktów, gdyż zasoby naturalne lub terytorium są poza zasięgiem takich przedsięwzięć. Co jednak istotne: cyberprzestrzeń, wraz z jej systemem — niezależnie od tego jak złożonym — będzie pozostawać bytem podrzędnym względem systemu politycznego.

Często pomijanym aspektem jest też koszt działania w środowisku sieciocentrycznym. Przede wszystkim: ze względu na jego złożoność, obie strony (atakujący oraz obrońca) decydują się na kompromisy w zakresie ataku i bezpieczeństwa cybernetycznego. Wszystkie podejmowane decyzje obejmują przez to uogólnioną analizę kosztów oraz korzyści. Jednak to coś więcej niż pieniądze: czas, elastyczność, wygoda (wykorzystywania systemów)¹⁷¹ i prywatność (danych oraz obywateli) muszą być wzięte pod uwagę dla każdej ze stron. Skutki kompromisów ze strony obrońcy są szeroko omawiane i zrozumiałe. Jednak istotne pozostają tu możliwości agresora: jak wiele czasu i środków może on przeznaczyć na cyberataki i co przez nie może osiągnąć, a jakie efekty przyniosłaby podobna inwestycja wysiłków w klasyczne metody walki.

Jeżeli celem przeciwnika jest działanie w ukryciu, unikając bezpośredniej agresji, to wówczas nawet wysokie koszty (szeroko rozumiane) są uzasadnione. Przykładem może być wykorzystanie Stuxnet¹⁷² w sabotażu przeciwko irańskiemu programowi atomowe-

¹⁷¹ B. Scheiner, *The Psychology of Security*, [w:] *Progress in Cryptology — AfricaCrypt*, S. Vaudenay (ed.), Casablanca 2008, s. 51.

¹⁷² *Stuxnet* — złożone, samo-replikujące się złośliwe oprogramowanie (rodzaj robaka), wpływało na sposób pracy wirówek atomowych do wzbogacania uranu przez okresowe zaburzanie parametrów pracy. Przez ten termin rozumiany jest jednak ogół całego cyberataku, który przeprowadzono w 2010 roku. Wówczas okrzyknięto go pierwszym na świecie użyciem cyberbroni. Był to raczej prototyp takiego oprogramowania, ewolucyjnie początek rozwoju cyberoręża — choć nie można go w związku z tym bagatelizować; J.P. Kesan, C.M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, „Harvard Journal of Law & Technology” 2012, Vol. 25, No. 2, s. 423; A. Nourian, S. Madnick, *A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet*, „IEEE Transactions on Dependable and Secure Computing” 2018, Vol. 15, Issue 1, s. 1–2, 16–18.

mu. Skutecznie go opóźniono (choć nie aż tak, jak zakładali atakujący) przez zaatakowanie infrastruktury ośrodka atomowego w Natanz wyłącznie z użyciem środków cybernetycznych w 2010 roku. Co ważne, brakowało twardych dowodów na tożsamość agresora dzięki wyrafinowaniu operacji¹⁷³.

Jednakże w przypadku konfliktu, takiego jak na Ukrainie w 2022 roku, zalety cyberataku — np. problem atrybucji — tracą na znaczeniu, przez co wysokie koszty stają się nieuzasadnione. Co więcej, przeprowadzane przez Rosję mobilizacje i tempo postępów walki sugerują niedoszacowanie potencjalnych strat oraz możliwości obronnych Ukrainy. W takiej sytuacji inwestowanie zbyt wielu środków w cyberwalkę może być strategicznie nieuzasadnione, jeżeli broń kinetyczna mogłaby wyrządzić większe szkody przy tych samych nakładach sił i środków. Potencjalnie wyjaśnia to, dlaczego w ukraińskiej infrastrukturze teleinformatycznej odkryto liczne ślady wpływu rosyjskiego (złośliwego oprogramowania). Zarazem nie odnotowano cyberataków o wielkim znaczeniu, lecz wiele pomniejszych — prowadzonych wprawdzie na dużą skalę, ale bez spowodowania znaczącego zagrożenia dla bezpieczeństwa Ukrainy¹⁷⁴.

Należy jednak podkreślić, że są to wnioski wstępne, gdyż w czasie wojny władze skupiają się na wojnie, a nie prowadzeniu śledztw ws. każdego cyberzagrożenia. Co więcej, być może jedną z przyczyn takiego stanu rzeczy jest zbytne zdywersyfikowanie wektorów ataków na podmioty prywatne (zarówno prawnie regulowane, jak i np. grupy hakerskie), które w obliczu wojny mogły wycofać się z działalnością za granicę. Dlatego tak istotnymi stają się i będą stawać cyberwojska — akumulujące potencjał prowadzenia walki cybernetycznej w sposób przewidywalny, lojalny, synergiczny oraz koherentny wobec pozostałych rodzajów sił zbrojnych.

Zdawałoby się, że wobec powyższego, przynajmniej do czasu rozwinięcia technologii oręża cybernetycznego, takie metody walki będą szczególnie użyteczne w przypadku działań hybrydowych. Jednakże i tu nie można zapomnieć, że jest to broń obosieczna, przypominająca bumerang. Ilekroć złośliwe oprogramowanie jest wykorzystywane przeciwko jednej ze stron, to koniecznie musi ono zostać dostarczone do infrastruktury przeciwnika. Ten z kolei może je przechwycić, a następnie dokonać analiz kodu źródłowego, tym samym zwiększając własny potencjał obronny i ofensywny. Rozumiejąc funkcjonowanie lub sposób tworzenia cyberbroni przez agresora, można dokonać adekwatnej re-

¹⁷³ T. Rid, B. Buchanan, *Attributing Cyber Attacks*, „Journal of Strategic Studies” 2015, Vol. 38, No. 1–2, s. 21.

¹⁷⁴ A.D. Givens, M. Gorbachevsky, A.C. Biernat, *How Putin's Cyberwar Failed in Ukraine*, „Journal of Strategic Security” 2023, Vol. 16, No. 2, s. 102–109.

wizji własnych systemów obronnych. Możliwe jest jednak użycie tak odkrytych mechanizmów przeciw samemu atakującemu.

Zatem prowadzenie działań hybrydowych z użyciem takich środków, może prowadzić do trudnych w przewidzeniu skutków związanych z kontratakiem — choć nie tylko. Broń cybernetyczna bywa ze swej natury masowa¹⁷⁵, a zaprojektowanie skutecznych mechanizmów jej proliferacji w czasie ataku może doprowadzić do omyłkowego zaszkodzenia własnej infrastruktury. Z kolei ataki precyzyjne wymagają wcześniejszego, bardzo szczegółowego rozpoznania celu, co podnosi koszty i wpływa na czas opracowania cyberbroni. Te wątpliwości są jednak istotne głównie dla państw oraz jego instytucji. Nie-wielkie podmioty, jak np. grupy hakerskie, nie mają zwykle „wiele do stracenia” w kwestii własnej infrastruktury, a przez to ich ataki mogą być potencjalnie bardziej brutalne lub nieprzewidywalne w skutkach.

W świetle poprzednich podrozdziałów, powyższe zdaje się wysuwać interesujące implikacje. Owszem: wojna hybrydowa nie jest niczym nowym, a różnego rodzaju działania nieregularne, zbieżne z jej definicją, były wykorzystywane we właściwie każdym większym konflikcie, gdyż przynosiły większą korzyść (strategiczną, polityczną lub społeczną) niż wykorzystanie środków klasycznych. Co więcej początkowy „zachwyt” pojęciem hybrydowości przy okazji agresji na Ukrainę w 2014 roku nie wniósł wiele nowego w metody prowadzenia wojen, co ukazuje choćby rozwój tego konfliktu i rozpoczęcie przez Rosję wielkoskalowej agresji w 2022 roku.

Wszystko to jednak odnosi się do ewolucji kinetycznego pola walki, poszerzane-go o środki wspierające go z zachowaniem konwergencji celów. Samo środowisko sieciocentryczne traktowano jako po prostu kolejną przestrzeń — o znaczeniu być może mniejszym, niż początkowo zakładano. Jednakże rozważając je jako odrębny system, o własnej „polityce” i aktorach (podmiotach), być może potrzeba zmiany postrzegania sposobu prowadzenia walki. To nie między państwami będą się rozgrywać cyberwojny, a przynajmniej nie wyłącznie — gdyż ani niczego w ten sposób nie podbiją, ani też nie wywrą odpowiednio znaczącego wpływu. Nawiązując do treści drugiego podrozdziału nie będzie nadużyciem stwierdzenie, że cyberwojna nie jest prawdziwą wojną — w rozumieniu strategii (niezależnie czy rozbitych na wielkie i zwyczajne, czy też nie)¹⁷⁶.

¹⁷⁵ W.H. Boothby, *Methods and Means of Cyber Warfare*, „International Law Studies” 2013, Vol. 83, s. 391–394; C.D. Wallace, *Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis*, Tallin 2018, s.19–20.

¹⁷⁶ E. Gartzke, *The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth*, „International Security” 2013, Vol. 38, No. 2 s. 73.

Realnym zagrożeniem w cyberprzestrzeni są natomiast prywatne podmioty, którym sprzyja atrybucja i sposób funkcjonowania tego środowiska. Co więcej, im bardziej postępować będzie integracja państwa oraz jego instytucji ze sferą cybernetyczną, tym bardziej tego rodzaju działania zyskają na znaczeniu. To z kolei stanowić będzie ogromne wyzwanie, gdyż tempo rozwoju technologii bezpośrednio narzuci tempo procesów w budowaniu cyberbezpieczeństwa, muszącego nadążać za nowymi zagrożeniami.

Podsumowanie

Koncepcja hybrydowości w działaniach wojennych odzwierciedla ewoluującą naturę konfliktów w XXI wieku. Wojna hybrydowa, charakteryzująca się integracją taktyki konwencjonalnej i niekonwencjonalnej, stanowi złożone i wielowymiarowe wyzwanie dla bezpieczeństwa narodowego. Aby skutecznie przeciwdziałać zagrożeniom hybrydowym, państwa muszą wzmocnić swoją cyberobronę, ulepszyć wywiad i świadomość sytuacyjną, wspierać współpracę międzynarodową oraz opracować kompleksowe strategie obronne. Koncepcja ta stała się także kluczowym tematem w dyskursie na temat współczesnych działań wojennych, szczególnie w ramach teorii nowych wojen. Na tę zmianę paradygmatu — w rozumieniu dynamiki konfliktu — znaczący wpływ ma ewoluujący charakter zagrożeń i zmieniający się krajobraz globalnego bezpieczeństwa. Hybrydowość w działaniach wojennych obejmuje szeroki wachlarz strategii łączących taktykę konwencjonalną i niekonwencjonalną, co nabiera coraz większego znaczenia od czasu aneksji Krymu przez Rosję w 2014 r. Konflikty te często wymykają się tradycyjnym kategorizacjom, co wymaga bardziej inkluzywnego terminu opisującego niezliczone stosowane taktyki. Wojna hybrydowa integruje różne wymiary walki, w tym konwencjonalne operacje wojskowe, taktykę nieregularną, terroryzm i wojnę cybernetyczną, tworząc w ten sposób wyrafinowane i wielowarstwowe podejście do osiągania celów strategicznych.

Historyczny rozwój koncepcji hybrydowości w działaniach wojennych można przypisać różnym formom nieregularnych konfliktów i wojny partyzanckiej, które zawsze wykazywały elementy taktyki hybrydowej. Jednak formalne uznanie i konceptualizacja wojny hybrydowej jako odrębnego podejścia pojawiło się bardziej wyraźnie pod koniec XX i na początku XXI wieku. Konflikty w Libanie w 2006 r., podczas których Hezbollah skutecznie połączył taktykę partyzancką z konwencjonalną wojną przeciwko Izraelowi, posłużyły jako prekursor dla pełniejszego zrozumienia wojny hybrydowej. Aneksja Krymu w 2014 r. stanowiła istotny punkt zwrotny w uznawaniu i stosowaniu wojny hybrydowej. Połączono wówczas operacje cybernetyczne, walkę informacyjną i użycie

żołnierzy walczących bez oznakowania przynależności państwowej. Choć wartym podkreślenia jest także, iż całość poprzedziła uprzednia destabilizacja państwa, m.in. przez indukowanie korupcji czy budowanie nastrojów w społeczeństwie. Osiągnięto wówczas założone cele bez wywoływania konwencjonalnej reakcji wojskowej na pełną skalę ze strony Zachodu.

Operacja ta podkreśliła skuteczność taktyki hybrydowej w osiąganiu celów strategicznych przy jednoczesnym uniknięciu bezpośredniej konfrontacji i związanych z nią kosztów politycznych i gospodarczych. Jednakże sama w sobie nie była celem, a jedynie środkiem przejściowym w drodze do konfliktu rosyjsko-ukraińskiego z 2022 roku.

Koncepcja wojny hybrydowej opiera się na kilku kluczowych elementach, które odróżniają ją od tradycyjnych form konfliktu. Jednym z ciekawszych elementów jest wykorzystanie cyberprzestrzeni jako pola bitwy. Operacje cybernetyczne mogą być wymierzone w infrastrukturę krytyczną, taką jak sieci energetyczne, sieci komunikacyjne i systemy finansowe, powodując znaczne zakłócenia i szkody gospodarcze bez konieczności fizycznej obecności. Całość obejmuje szereg działań, w tym hakowanie, szerzenie dezinformacji i manipulowanie mediami społecznościowymi w celu wpływania na opinię publiczną i procesy polityczne. Towarzyszy im odpowiednia synergia oraz celowa konwergencja, co odróżnia je od po prostu użycia szerokiego wachlarza środków.

Wskazane w niniejszym rozdziale wojna informacyjna i operacje psychologiczne wydają się być istotnymi elementami walki hybrydowej, których celem jest kształtowanie percepcji, wpływanie na zachowanie oraz podważanie morale i spójności przeciwnika. Wiąże się to z wykorzystaniem propagandy, fałszywych wiadomości czy kampanii dezinformacyjnych w celu nie tylko wywoływania zamieszania, lecz przede wszystkim podważania zaufania do instytucji państwowych i przywództwa.

W konfliktach hybrydowych wojna informacyjna wykorzystywana jest jako uzupełnienie operacji wojskowych i cybernetycznych, tworząc kompleksowe podejście do osiągnięcia celów strategicznych. Kontrolując środowisko informacyjne, aktorzy hybrydowi mogą kształtować krajobraz strategiczny.

Cechą charakterystyczną walk hybrydowych jest także wykorzystywanie podmiotów niepaństwowych i sił zastępczych. Podmioty te, do których mogą należeć grupy powstańcze, bojówki i prywatne kompanie wojskowe, zapewniają państwom środki do prowadzenia operacji w sposób pośredni i możliwy do wiarygodnego zaprzeczenia. Podmioty niepaństwowe są często wykorzystywane do prowadzenia działań, które byłyby problematyczne politycznie lub prawnie dla sił państwowych, co dostrzegamy nawet w najstarszych kornikach historycznych. Takie podejście zmniejsza ryzyko eskalacji oraz ograni-

cza koszty polityczne i ekonomiczne związane z konwencjonalnymi operacjami wojskowymi.

Postępująca integracja zdolności cybernetycznych ze strategiami hybrydowymi zmieniła charakter konfliktów, umożliwiając aktorom atakowanie infrastruktury krytycznej, prowadzenie szpiegostwa i zdalne wpływanie na procesy polityczne. Cyberataki na infrastrukturę krytyczną mogą mieć niszczycielskie skutki, powodując powszechne zakłócenia i szkody gospodarcze. Z kolei możliwość przeprowadzania takich operacji na odległość i z możliwością wiarygodnego zaprzeczenia (problem atrybucji) czyni z nich atrakcyjną opcję dla podmiotów hybrydowych.

Choć sama walka nieregularna nie jest nowa, to zagrożenia wynikające z użycia cyberprzestrzeni stanowią poważne wyzwanie dla bezpieczeństwa narodowego i wymaga ponownego przemyślenia tradycyjnych strategii obronnych. Wymaga to przede wszystkim kompleksowego podejścia dążącego do integracji zdolności wojskowych, wywiadowczych, policyjnych, a także informacyjnych i cybernetycznych. Tak jak środowisko sieciocentryczne płynnie przenika wszystkie aspekty działalności państwa, tak jego odpowiedź powinna być równie spójna oraz scalona. Wiąże się to z inwestowaniem w infrastrukturę cyberbezpieczeństwa, rozwijaniem solidnych zdolności reagowania na incydenty oraz wspieraniem współpracy między sektorem publicznym i prywatnym. Skuteczna cyberobrona wymaga ciągłego monitorowania, dzielenia się informacjami o zagrożeniach i umiejętności szybkiego reagowania na incydenty cybernetyczne, szczególnie przez skuteczną wymianę między systemami. Należy jednak pamiętać, że ich integracja może stanowić kolejne zagrożenie samo w sobie — przeciwnik może bowiem skuteczniej uzyskiwać dostęp do zasobów. Dlatego potrzebna jest zwiększona świadomość sytuacyjna, pozwalająca na identyfikowanie pojawiających się zagrożeń oraz proaktywne reagowanie.

Wydaje się, że wspólne wysiłki państw, organizacji międzynarodowych i podmiotów sektora prywatnego mogą zwiększyć zbiorową zdolność wykrywania, powstrzymywania i reagowania na działania hybrydowe, szczególnie w środowisku sieciocentrycznym. Przyjmując podejście holistyczne, państwa mogą stworzyć bardziej odporną i adaptacyjną postawę obronną, zdolną przeciwstawić się wieloaspektowemu charakterowi wojny hybrydowej.

Rozdział II

Asymetryczność w konfliktach dawnych, współczesnych i przyszłych

Zjawisko asymetrii w wojnach i konfliktach stało się jednym z kierunków studiów w dziedzinie historii wojskowości, polemologii oraz stosunków międzynarodowych. Omawiane w poprzednim rozdziale złożone, wielowymiarowe i nieregularne formy konfliktów z ich definicji wymagały użycia nie tylko kombinacji środków lub sposobów prowadzenia walki, lecz także zróżnicowania potencjału aktorów.

Wśród nowych sposobów opisywania wojny, „asymetria” należy do jednych z najszerszych, choć zdecydowanie nie nowych w swej naturze. Już w 1962 roku, prezydent John F. Kennedy zwrócił się do absolwentów Akademii Wojskowej Stanów Zjednoczonych w słowach:

jest to inny rodzaj wojny, nowy w swojej intensywności, starożytny w swoim pochodzeniu — wojna partyzantów, wywrotowców, powstańców, zabójców, wojna z zasadzki zamiast walki; poprzez infiltrację, zamiast agresji, dążenie do zwycięstwa poprzez erozję i wyczerpanie wroga zamiast angażowania go¹.

Już w latach 90. XX wieku, termin „wojny asymetrycznej” zaczął pojawiać się w dokumentach rządowych USA, wówczas będąc jeszcze pojęciem niemal tożsamym z wojną hybrydową. Włączano w niego terroryzm (atak na World Trade Center z 2001 roku), użycie improwizowanych bomb przydrożnych (wojna w Zatoce Perskiej) lub wirusów komputerowych, czy proliferację broni masowego rażenia². I o ile część z tych zjawisk weszła później w system pojęciowy „asymetrii”, to np. włączanie arsenału atomowe-

¹ Oryg. *This is another type of war; new in its intensity, ancient in its origin--war by guerrillas, subversives, insurgents, assassins, war by ambush instead of by combat; by infiltration, instead of aggression, seeking victory by eroding and exhausting the enemy instead of engaging him*; Department of Defense. Defense Communications Agency, White House Audio Recordings 1961–1963, Access No. WH-103-001, ID JFKWHA-103-001, J.F. Kennedy, *Remarks to the Graduating Class of the U.S. Military Academy*, West Point-New York 1962, 8:22–8:48 [audio].

² D.F. Buffaloe, *Defining Asymmetric Warfare*, „The Land Warfare Papers” 2006, No. 58, s. 2.

go było niepotrzebnym „rozwodnieniem” terminu. Owszem, wzmacniało to potencjał pewnych państw, jednakże dysproporcja na tym poziomie istniała zawsze. Rozważanie jej w charakterze „asymetryczności” pozbawiałoby jej sensu stricto.

Ten jednak sam może być kwestionowany. Wskazywano bowiem, że „asymetria” nie może być jasno określona, gdyż sam akt jej zdefiniowania przeczy jej naturze, znaczeniu, celowi oraz wadze³. To jednak zaprzeczałoby sensowi dyskusji nad tym zjawiskiem i choćby próbie określenia jego ram lub interpretowania, np. przez pryzmaty: dystrybucji władzy, statusu organizacyjnego aktorów, metod walki oraz norm⁴. Takie ujęcie stawia od razu pytanie: czy elementy „wojny hybrydowej” nie wchodzą w skład tych kategorii, jednocześnie jako całość („asymetryczność”) definiując pewne aspekty samej „hybrydowości”.

Niepomijalne jest także zróżnicowanie podejść, które zawęża postrzeganie lub badanie asymetrii. Dlatego dostrzec można podejście skupiające się ściśle na konfliktach zbrojnych i przeciwdziałaniu aktywności podmiotów niepaństwowych, które przez działania niekonwencjonalne wykorzystują szczególne przypadki przewagi taktycznej. Niektórzy badacze skupiają się jednak wyłącznie na terroryzmie i zagrożeniach w czasie pokoju. Inni jeszcze, jak w przypadku Chin — rozwojowi możliwości A2/AD⁵ przez tworzenie asymetrycznej przewagi w określonych obszarach geograficznych⁶.

To skrzyżowanie pojęć stanowi wyzwanie nie tylko dla samych badań, lecz także dla paradygmatów bezpieczeństwa — międzynarodowego, wewnątrzpaństwowego, a także cyberprzestrzeni. Zrozumienie płynnej, dynamicznej natury współczesnych konfliktów jest niezbędne do sformułowania skutecznych strategii, które odnoszą się do współczesnych zagrożeń, które wykraczają poza konwencjonalne doktryny wojskowe. Ma to szczególne znaczenie przez wzgląd na fakt, jak często działania w środowisku sieciocentrycznym nie dotyczą bezpośrednio spraw militarnych, lecz mają pośredni wpływ tak na nie, jak również na obiekty ich zainteresowania. Wzajemne powiązania hybrydowości i asymetrii wymagają wszechstronnej analizy, aby odkryć ich wpływ na stabilność mię-

³ J.G. Chace, *Defining Asymmetric Warfare: A Losing Proposition*, „Joint Force Quarterly” 2011, No. 61, s. 124.

⁴ J. Ångström, *Evaluating Rivalling Interpretations of Asymmetric War and Warfare*, [w:] *Conceptualising Modern War*, K.E. Haug, O.J. Maaø (eds.), London 2011, s. 31.

⁵ Anti-access/area denial (A2/AD) — strategia kontrolowania dostępu oraz zastrzegania obszarów.

⁶ D.E. Johnson, *Hard Fighting: Israel in Lebanon and Gaza*, Santa Monica-Arlington-Pittsburgh 2011, s. 148–161, 170–180; O.S. Mastro, *China’s Anti-access-Area Denial (A2/AD) Capabilities: Is American Rebalancing Enough?*, [w:] *American Strategy and Purpose: Reflections on Foreign Policy and National Security in an Era of Change*, W.H. Natter III, J. Brooks (eds.), Lexington 2014, s. 118–125; M. Kaldor, *New and Old Wars. Organized violence in a Global Era*, Cambridge 2012, s. 132–143, 189–194.

dzynarodową, wysiłki pokojowe i bezpieczeństwo regionalne. Co więcej, tak jak paradygmaty bezpieczeństwa (szeroko rozumiane) nie są jednolite dla wszystkich właściwych im podmiotów, tak stosowanie koncepcji nieregularności oraz asymetryczności napotyka problemy z uniwersalnością. Zdaje się, że jedynym wspólnym mianownikiem jest tutaj niepewność.

Niniejszy rozdział ma na celu ustanowienie jasnych ram pojęciowych do analizy i oceny asymetrii w historycznych, współczesnych i przyszłych konfliktach. Badając rzeczywiste zjawisko w różnych okresach, jak również porównując ze współczesnym kontekstem, istotnym stanie się rzucenie światła na ewolucyjny charakter dynamiki konfliktów oraz znaczenia asymetrii.

2.1. Rys historyczny działań asymetrycznych

Podobnie jak hybrydowość (nieregularność) działań obserwowana była na przestrzeni wieków, tak i asymetryczność w konfliktach nie jest niczym nowym. Konflikty które nawet postrzegać można jako starcie dwóch porównywalnych podmiotów, zawsze albo dążyły do pogłębiania asymetrii i tym samym osiągania przewagi, albo też wykorzystywały asymetrię na szczeblu operacyjnym oraz taktycznym, by wspierać zasadniczą strategię działań wojennych. Zatem można postrzegać ją jako zjawisko powszechne oraz zawsze oczekiwane, a przez to nieprzydatne badawczo.

Jednak współczesne rozumienie „asymetryczności” wydaje się skupiać na stanie wejściowym — asymetrii między stronami konfliktu przed jego rozpoczęciem i późniejszych implikacjach. Takie podmiotowe ujęcie asymetrii, zamiast przedmiotowego traktowania jej jako narzędzia prowadzenia walki, może legnąć u podstaw rozpoznawania zmian asymetryczności w konfliktach na przestrzeni dziejów.

Co więcej, istotnym pozostaje też wzięcie pod uwagę państwowości i pozapaoństwa aktorów. Różne bowiem są ich cele, możliwości oraz implikacje teoretyczne. Podnoszony jest argument, że współcześnie większość przemocy ma sprywatyzowany charakter⁷. W kontekście „nowych wojen” postrzeganych jako połączenie wojny (agresji w celach politycznych), przestępczości (agresji w celach prywatnych) i naruszenia praw człowieka (agresji przeciwko cywilom)⁸, takie podejście zyskuje na znaczeniu dla rozróżnienia tego, co jest konfliktem „nowej generacji”, a co reprezentuje „minioną erę”. Szczególnie, że nie należy spodziewać się rewolucji, a raczej zmian ewolucyjnych.

⁷ J. Mueller, *The Remnants of War*, Ithaca 2004, s. 2.

⁸ M. Kaldor, *New and Old Wars...*, s. 207.

Dlatego w analizie rozwoju „asymetryczności” poszukiwać należy nie tylko dysproporcji potencjału między stronami konfliktu, lecz także progresywnej erozji państwowego monopolu na użycie agresji w celach realizowania swojej strategii. A skoro definicyjnie jest to przesunięcie w kierunku przestępczości, to oczekiwać można też wzrostu barbarzyństwa w prowadzeniu wojen⁹.

2.1.1 Daleki Wschód w starożytności

Potrzebę wykorzystania asymetrii, czy nawet celowego prowokowania sytuacji taktycznych wykorzystujących ją, opisywał w V w. p.n.e. Sun Tzu:

Strategia wojny polega na przebiegłości i stwarzaniu złudzeń. Dlatego, jeśli jesteś do czegoś zdolny, udawaj niezręcznego, jeśli jesteś aktywny, stwarzaj pozory bierności. Jeśli jesteś blisko, stwórz pozory dużej odległości, jeśli uwierz, że jesteś daleko, znajdź się niespodziewanie blisko. Staraj się wprowadzić wroga w błąd, stwórz dezorganizację w jego armii i dopiero wtedy uderzaj. (...) Kiedy wróg koncentruje się, przygotuj się do odparcia ataku, kiedy jest mocny, unikaj go. Próbnij rozszkościć wrogiego generała i wprowadzić go w błąd. (...) Zaatakuj, kiedy nie będzie przygotowany, zrób wypad, kiedy się tego nie spodziewa¹⁰.

Choć autor pisze w kontekście konfliktów dawnych, przedstawiając liczne przykłady użycia regularnej siły militarnej, to wykorzystanie asymetrii zajmuje centralne miejsce w jego myśli. Istotna jest także trwałość tych idei. Szczególnie w przypadku chińskich badaczy teorii wojen, ta leżąca u podstaw asymetryczność stanowi jeden z kluczowych elementów prowadzenia walki¹¹.

Zarazem jednym z jaskrawszych przykładów wykorzystywania myśli Sun Tzu w praktyce była wojna koreańskiego królestwa Koguryŏ (37 p.n.e. — 668 n.e.) z Chinami dynastii Sui (581–618). Mimo ogromnej dysproporcji zasobów materialnych i siły militarnej (nawet do 13:1 na korzyść Chin), Koguryŏ unikało bezpośrednich starć militarnych, sprawnie wykorzystując taktyki obronne i celowo przeciągając wojnę. Walcząc o przetrwanie, królestwo to nie zwracało uwagi na koszty działań, a te z kolei stały się znaczącym problemem dla Chin Sui. Co więcej, sprawne wykorzystanie dyplomacji, nieregular-

⁹ M. Heupel, B. Zangl, *Von 'alten' und 'neuen' Kriegen. Zum Gestaltwandel kriegerischer Gewalt*, „Politische Vierteljahresschrift” 2004, No. 45, s. 355.

¹⁰ Sun Tzu, *Sztuka...*, s. 11–13.

¹¹ W.H. Tsai, *An Analysis of China's Information Technology Strategies and their Implication for US National Security*, Monterey 2006, 63–69, 81–82; G.W. Jinn, *China's Development of Asymmetric Warfare Capabilities and the Security of Taiwan*, Monterey 2004, s. 53, 60–62; T. Yoshihara, *Chinese Information Warfare: A Phantom Menace Or Emerging Threat?*, Carlisle 2001, s. 15–28; U. Ojiako, Y. Liu, J. Johnson, *Eastern promises: a philosophical exploration of decision making under 'unconventional' and asymmetric competition*, „International Journal of Business Environment”, Vol. 5, No. 1, s. 77–82, 84–85.

nych starć, morale i determinacji broniących się mieszkańców Koguryŏ, synergicznie pozwoliły osiągnąć zwycięstwo, który zdawało się być niemożliwym¹².

2.1.2. Konflikty asymetryczne państw starożytnej Europy

Dalekowschodnie podejście do taktyki walki nie było jednak jedynym, tak wczesnym opisem nieregularnych i asymetrycznych działań. *Epitoma Re Militaris* Wegecjusza¹³ należy wskazać jako jedno z najbardziej znaczących dzieł z zakresu teorii wojskowej sprzed *O wojnie* Clausewitza¹⁴. Oferuje ono więcej więcej niż zwykły opis rzymskich działań wojennych, zawierając liczne wskazówki, dające wgląd w ówczesne prowadzenie wojsk. Autor radzi unikać bezpośrednich konfrontacji i faworyzować podstęp oraz finezję, aby stopniowo pokonać wroga, podkreślając znaczenie mobilności, szybkości i zwożenia¹⁵. Podkreśla elastyczność planowania strategicznego i taktycznego oraz potrzebę zrozumienia charakteru i możliwości wroga, podobnie jak w myśl Sun Tzu „poznaj swojego wroga i poznaj siebie”.

II Wojna Punicka, którą omówiono w rozdziale pierwszym, również przedstawiana jest jako jeden z przykładów konfliktu asymetrycznego¹⁶, szczególnie w kontekście wykorzystania *latro* (najemników, banitów)¹⁷. Podobnie postrzega się Wojnę Peloponeńską między Atenami i Spartą. Podkreślając nierównomierność sił, wskazywana jest nierównomierność walki, wykorzystującej grabieżę, stosowanie przemocy i współcześnie rozumianego terroru, zwłaszcza na peryferiach¹⁸.

Interesującym przykładem są także wojny toczone w latach 534–551 n.e. między Rzymem Justyniana oraz Wandalami w Afryce Północnej (tzw. wojna Cesarstwa Bizantyjskiego z Wandalami). Asymetryczność tych konfliktów dotyczy poziomów strategiczno-taktycznych, zasobów ekonomiczno-militarnych, czy etniczno-religijnych¹⁹. Rzymianie mieli wówczas przewagę liczebności armii, jej świetnego uzbrojenia oraz wyszkolenia.

¹² J. Kim, S.C. Tucker, G.H. Kim, *How did the Weaker Actor Defeat the Stronger Actor? Koguryŏ's War with Sui (612–614) Revisited*, „Sungkyun Journal of East Asian Studies” 2018, Vol. 18, No. 2, s. 225–242; A.C. Nahm, *A panorama of 5000 years: Korean history*, Seoul. 1989, s. 18.

¹³ Wegecjusz (Publius Flavius Vegetius Renatus), rzymski historyk żyjący w II połowie IV w. n.e.

¹⁴ G. R. Watson, *The Roman Soldier*, Ithaca 1969, s. 25–26.

¹⁵ Vegetius, *Epitome of Military Science*, N.P. Milner (ed. & trans.), Liverpool 1996, Book 3, s. 68–69, 116, 118.

¹⁶ A. Lele, *Asymmetric Warfare: A State vs Non-State Conflict*, „OASIS” 2014, No. 20, s. 103.

¹⁷ P. Porter, *Shadow Wars: Asymmetric Warfare in the Past and Future*, „Security Dialogue” 2006, Vol. 37, No. 4, s. 559.

¹⁸ Zob. V.D. Hanson, *A War Like No Other: How the Athenians and Spartans Fought the Peloponnesian War*, New York 2006.

¹⁹ G.W. Shea, *Justinian's North African Strategy in the Johannis of Corippus*, „Byzantine Studies” 1983, t. 10, s. 29–38.

Stosowali szybkie natarcia przez szerokie wykorzystanie kawalerii, jak również braku doświadczenia Maurów w np. walce obronnej. Nie brakowało też ataków na ludność cywilną, małe garnizony, unikania otwartej walki (choć nie zawsze), czy wykorzystywania przewagi terenu. Wprawdzie żadne z tych działań nie było przełomowym, lecz pokazało możliwości wykorzystania asymetrii do tego stopnia, że ostatecznie konflikt wygaśł nie przez zwycięstwo jednej ze stron, lecz powolną budowę powiązań i sojuszy, a w efekcie wykreowanie nowej rzeczywistości²⁰.

2.1.3. Średniowiecze w Europie

W średniowieczu asymetria zaczęła stawać się zjawiskiem interesującym, gdyż w kontekście takich starć na znaczeniu zyskiwały różnice religijne oraz etniczne, a także wynikające z nich implikacje²¹. Dyplomacja, wiara, propaganda, czy inne działania opisane w poprzednim rozdziale, wprawdzie były wykorzystywane od początków państwowości. We wskazanym okresie zyskały jako narzędzie realizowania lub przeciwdziałania asymetrii.

Przykładem może być podbój Europy Wschodniej (Rusi) przez Mongołów w latach 1240–1242. Ze względu na różnice kulturowo-religijne, chrześcijańska narracja przypisała Tatarom wyjątkowe okrucieństwo wraz z popełnianiem wielu zbrodni: niszczenia całych miast i mordowania ludności cywilnej, kanibalizmu, czy np. zabijania jednostek, które uciekały z pól bitew bez zamiaru dalszej walki (oraz możliwości skutecznej obrony)²². To wszystko posłużyło za podstawę do dalszego prowadzenia polityki, a tym samym pogłębiania podziałów i wykorzystywania asymetrii na tle etniczno-religijnym. W budowaniu historycznej supremacji (wpływów) Kościoła w Europie miały też udział krucjaty²³. Wojny albigeńskie (1209–1229) przeciwko katarskim heretykom z Langwedocji są tu przykładem wyjątkowo przesyconym okrucieństwami popełnianymi przez każdą ze stron konfliktu, w którym Kościół i jego pozycja same w sobie wyznaczały już oś asyme-

²⁰ M. Stachura, *Żołnierze Justyniana w Afryce — okupanci czy wyzwoliciele?*, „Przegląd Historyczno-Wojсковy” 2022, nr 4, s. 78–92; M. Stachura, *Wojna Justyniana z Maurami — przykład konfliktu asymetrycznego?*, „Prace Historyczne” 2016, nr 4, s. 633–642; M. Wilczyński, *Wojna bizantyńsko-wandalaska 533–53*, „Rocznik Naukowo Dydaktyczny/Prace Historyczne XII” 1987, nr 109, s. 30–35.

²¹ M. Prestwich, *Transcultural Warfare — the Later Middle Ages*, [w:] *Transcultural Wars. From the Middle Ages to the 21st Century*, H.H. Kortüm (ed.), Berlin 2006, s. 43–56.

²² V. Barysenka, *The presentation of the Tatars and the Turks in the legends related to miraculous images/icons of Our Lady in the 17–18th centuries in the Eastern Territories of the Polish-Lithuanian Commonwealth*, „Eikón Imago” 2022, Vol. 11, s. 172–179, 182; A. Ayton, *From Muhi to Mohács. Armies and Combatants in Later Medieval European Transcultural Wars*, [w:] *Transcultural Wars. From the Middle Ages to the 21st Century*, H.H. Kortüm (ed.), Berlin 2006, s. 220–223.

²³ R. Cox, *Asymmetric warfare and military conduct in the Middle Ages*, „Journal of Medieval History” 2012, Vol. 38, No. 1, 119–121.

trii. Wagę takiej przewagi podkreśla też określenie tychże krucjat jako pierwszego ideologicznego ludobójstwa²⁴.

W ujęciu polityczno-wojskowym, na uwagę zasługują wojny bałtyckie, toczące się w od XII do XIV wieku na terenie Prus, Inflant i Litwy. Niemieccy oraz zachodnioeuropejscy krzyżowcy dysponowali wówczas lepszą technologią wojskową i fortyfikacjami, tworząc asymetrię gospodarczo-wojskową. To skłoniło pogańskich Bałtów do unikania klasycznych bitew i uciekania się do taktyki partyzanckiej²⁵. Kiedy pod koniec XIII wieku Litwini osiągnęli parytet organizacji gospodarczej i politycznej, losy wojny zmieniły się na ich korzyść. Krzyżacy przeszli do najazdów wyniszczających, czyli „Reise”²⁶. Nie inaczej wyglądały choćby spory graniczne między Anglią i Walią w XIII wieku. Walijczycy, uznając swoją niższość militarną w stosunku do Anglo-Normanów, stosowali taktykę partyzancką. Jednakże tu istotną rolę odegrał także kontekst kulturowo-etniczny, który nadal temu konfliktowi wyjątkowo okrutnego przebieg²⁷.

Średniowieczna asymetria polityczno-wojskowa, czy też związana z czynnikami kulturowo-etniczno-religijnymi, zdaje się mieć wyraźny związek z brutalizacją działań wojennych²⁸. Poddaje to w wątpliwość, że rycerskość miała jakkolwiek znaczący wpływ na postępowanie wojskowe, a raczej podkreśla wielowymiarowość ówczesnych konfliktów, której nie należy pomijać²⁹.

2.1.4. Nowożytność w Europie i na Świecie

Kontynuując wątek Tatarów, warto zwrócić uwagę na działania Imperium Osmańskiego w XVII wieku w Europie Wschodniej. Wykorzystało ono szczególne warunki geopolityczne, historyczne, społeczno-ekonomiczne czy religijne, jak również słabo bronioną granicę Rzeczypospolitej Obojga Narodów. W ten sposób Tatarzy opanowali sztukę wojny asymetrycznej, która posłużyła za demonstrację zdolności do agresywnej projekcji siły militarnej i politycznej. Szczególną rolę odgrywało wykorzystanie oddolnego nacisku na inne państwa — przez demografię, gospodarkę, nastroje społeczne czy sto-

²⁴ R. Lemkin, *Lemkin on Genocide*, Plymouth 2012, s. 71–73; F.R. Chalk, K. Jonassohn, *The History and Sociology of Genocide: Analyses and Case Studies*, New Haven 1990, s. 114–138; M.G. Pegg, *A Most Holy War. The Albigensian Crusade and the Battle for Christendom*, New York 2008, s. 188–191.

²⁵ G. Leighton, *Ideology and Holy Landscape in the Baltic Crusades*, Leeds 2022, s. 5.

²⁶ R. Cox, *Asymmetric warfare...*, s. 108–109.

²⁷ J.E. Morris, *The Welsh Wars of Edward I*, Oxford 1901, s. 8–16.

²⁸ Należy podkreślić, że czasami silniejsza pozycja jednego z adwersarzy narzucała pewne zobowiązania etyczne, jak np. immunitet dla duchowieństwa, który stał się przyczynkiem do dalszego rozróżniania między walczącymi i cywilami.

²⁹ R. Cox, *Asymmetric warfare...*, s. 125.

sunki polityczne pośród szlachty. Dzięki temu możliwa stawała się pewna destabilizacja i osiąganie celów politycznych, bez prowadzenia konwencjonalnej wojny.³⁰

Hordy tatarskie w operacjach asymetrycznych charakteryzowały się dużą nieprzewidywalnością, zachowaniem dyskrecji do momentu ataku i wyjątkową mobilnością — szczególnie jednostek nieliniowych. Działały na różnych obszarach, obierając za cel środowiska cywilne, w szczególności infrastrukturę gospodarczą i zasoby demograficzne docelowego obszaru³¹. Tak szerokie zastosowanie elementu zaskoczenia utrudniało skuteczną obronę, stanowiąc podstęp wojskowy. Na przykład podczas przemarszu Hordy Krymskiej w 1594 roku i przemarszu kawalerii Krymsko-Bujakowskiej w 1624 roku, ciągle wiadomości o napadach Tatarów nie tylko wyczerpywały dowództwo, ale doprowadziły do zubożenia ludności (przez liczne, fałszywe alarmy). Wojownicy tatarscy wykazali się nieprzewidywalnymi manewrami, co widać podczas najazdu w 1629 roku, kiedy to wielokrotnie zmieniali trasy, aby wprowadzić w błąd polskich dowódców. Należy podkreślić, że wojna informacyjna i wywiadowcza była przez Tatarów wykorzystywana bardzo szeroko³².

Zdawałoby się, że Imperium Osmańskie należałoby uznać za przeciwnika symetrycznego i porównywalnego, gdyż dysponowało siłami zdolnymi do prowadzenia konwencjonalnych starć. Jednakże strony najazdy Tatarów nigdy nie stanowiły dla państwa polsko-litewskiego zagrożenia natury egzystencjalnej — choć takim były już dla regionów południowo-wschodnich. Zatem celowo wykorzystywano elementy walki asymetrycznej, indukując ją, a tym samym osiągając rezultaty z mniejszymi stratami własnymi — szczególnie przez unikanie wielkich starć, a wciąż wywieranie skutecznego wpływu polityczno-społeczno-gospodarczego.

Interesującego przykładu asymetrii można też się doszukiwać w działaniach pirackich na Karaibach w XVII wieku, skierowanych głównie przeciwko europejskim kolonialistom. Agresorzy maksymalizowali korzyści m.in. przez obieranie za cel słabo chronionych statków kupieckich. Piraci szukali dogodnych lokalizacji geograficznych, takich jak wąskie drogi wodne i wejścia do portów, wykorzystując jednocześnie ogólną nieprze-

³⁰ V. Ostapchuk, *Crimean Tatar long-range campaigns: The view from Remmal Khoja's History of Sahib Gerek Khan*, [w:] *Warfare in the Eastern Europe, 1500–1800*, B.J. Davies (ed.), Leiden 2012, s. 163–171.

³¹ A. Gliwa, *Doświadczenie inwazji tatarskich w narracjach ludowych i pamięci zbiorowej jako niematerialne dziedzictwo kulturowe Polski południowo-wschodniej*, „Ochrona Zabytków” 2014, nr 1, s. 64–67.

³² A. Böldyrew, K. Łopatecki, *Polish Way: The Light Cossack Cavalry in the Era of Military Revolution*, „Вестник СПбГУ. История” 2020, T. 65. Вып. 3, s. 685–689; A. Gliwa, *The Tatar Military Art of War in the Early Modern Period: An Example of Asymmetric Warfare*, „Acta Poloniae Historica” 2016, nr 114, s. 209–213; S. Sarnicki, *Księgi hetmańskie*, Kraków 2015, s. 436–440.

widywalność działań oraz element zaskoczenia³³. Przy tym bywali świetnie zdyscyplinowani w swych działaniach i sprawnie unikali starć z okrętami wojennymi³⁴. W ten sposób zdolni byli przejmować nawet setki jednostek kupieckich w relatywnie krótkim czasie³⁵. Kpt. Bartholomew Roberts, pirat pochodzenia walijskiego, miał zająć nawet ok. 470 statków, choć informacje bywają rozbieżne (szczególnie w kwestii pierwszych lat jego działalności)³⁶. Stało się to zatem wyjątkowym wyzwaniem dla państw kolonialnych — które pomimo dysponowania ogromnymi flotami wojennymi, długo jeszcze musiały szukać skutecznych dróg do zniwelowania problemu piractwa.

Rozważając problematykę asymetrii, poza badaniem nierówności potencjałów stron, należy też zwrócić uwagę na przewidywanie strategii każdej ze stron, co stanowić może wyzwanie ze względu na odmienną kulturę wojskową, struktury i wyposażenie. Zdolność adaptacji i szybkość przystosowania się do nowych sytuacji odgrywają kluczową rolę w określeniu wyniku. Taka asymetria jest z natury niestabilna, ponieważ obie strony ostatecznie przyjmą lepsze metodologie lub broń, choć niekoniecznie szybko. Bariery społeczne, polityczne oraz instytucjonalne mogą utrudniać słabszej stronie przyjęcie radykalnych zmian, podczas gdy strona silniejsza może utrudniać dostęp do jej lepszych praktyk wojskowych i broni.

Z takim właśnie wyzwaniem mierzyła się Brytyjska Kompania Wschodnioindyjska (omówiona już w rozdziale pierwszym). Zabezpieczenie jej interesów na terenie Indii wymagało odpowiedniego porozumienia się z lokalnymi książętami. Sojusze oznaczały jednak dzielenie się technologią wojskową z siłami indyjskimi, która trafić mogła jednak do sił wrogich Brytyjczykom. Co więcej, europejscy najemnicy w Indiach również zaferowali wiedzę specjalistyczną w zakresie zachodniej technologii wojskowej, pogłębiając ten problem³⁷. Kompania miała jednak nadzieję, że konserwatywne interesy oraz wpływy w Indiach będą w stanie zahamować istotne zmiany społeczno-polityczne, które były

³³ K. Lane, *Punishing the sea wolf: corsairs and cannibals in the early modern Caribbean*, „Nieuwe West-Indische Gids” 2003, No. 3(4), s. 202.

³⁴ E. Street, S.S. Chen, *Teamwork from the Golden-Age Pirates: Could this Strategy Work in Today's Contemporary Sports Setting?*, „Missouri Journal HPERD” 2018, vol. 28, s. 7–10.

³⁵ D.J. Puchala, *Of Pirates and Terrorists: What Experience and History Teach*, „Contemporary Security Policy” 2005, Vol. 26, No. 1, s. 10.

³⁶ P.B. Nutting, *The Madagascar Connection: Parliament and Piracy, 1690-1701*, „The American Journal of Legal History” 1978, Vol. 22, No. 3, s. 205; D. Conlin, *Pirates of the Atlantic: robbery, murder and mayhem off the Canadian East Coast*, Halifax 2009, s. 32; A. Bialuschewski, *Between Newfoundland and the Malacca Strait: a Survey of the Golden Age of Piracy, 1695-1725*, „The Mariner's Mirror” 2004, Vol. 90, Issue 2, s. 177–178.

³⁷ G.J. Bryant, *Asymmetric Warfare: The British Experience in Eighteenth-Century India*, „The Journal of Military History” 2004, Vol. 68, No. 2, s. 431–434.

wymogiem rzeczywistej modernizacji tamtejszych sił³⁸. To dałoby Brytyjczykom czas na dostosowanie europejskiego modelu wojskowego do lokalnego kontekstu³⁹. Jednakże z militarnego punktu widzenia asymetria nie sprzyjała wyłącznie Kompanii, ponieważ jej armia stawiała czoła niewystarczającej jakości kawalerii i problemom logistycznym. Rekompensowali to dyscypliną i siłą ognia w defensywie, czy wykorzystaniem do celów wojskowych koni gospodarskich⁴⁰. Natomiast armie indyjskie czerpały korzyści z obfitości lekkiej kawalerii i koczowniczych handlarzy zbożem (celem zapewnienia środków). Jednak „rewolucja wojskowa” faworyzowała piechotę i artylerię nad kawalerią, co doprowadziło do asymetrii, która zmusiła Hindusów do dostosowania organizacji wojsk — aby po roku 1750 przeciwstawić się lepszym jednostkom brytyjskim⁴¹.

Imperium Brytyjskie musiało się zmierzyć z asymetrycznością jeszcze nie raz — także na przełomie XIX i XX wieku. Wskazać tu należy drugą wojnę burską, toczoną w latach 1899–1902 pomiędzy z dwiema republikami burskimi: Republiką Południowoafrykańską (Transwalem) i Wolnym Państwem Orańskim, jest godnym uwagi przykładem asymetrycznego konfliktu. Potencjał bojowy obu stron był zupełnie nierówny — świetnie uzbrojone i dobrze wyszkolone siły Imperium Brytyjskiego bez trudu mogły niszczyć jednostki przeciwnika w konwencjonalnych walkach, które to zresztą starali się prowadzić. Republiki burskie za wszelką cenę nie dawały się wciągać w wielkoskalowe bitwy, wykorzystując raczej taktyki partyzanckie, nieregularne oraz szybkie najazdy⁴². Co więcej, Burowie posiadali dogłębną wiedzę na temat krajobrazu Republiki Południowoafrykańskiej, którą wykorzystywali na swoją korzyść. Mogli z łatwością poruszać się po trudnym terenie, wykorzystując go także do ukrywania się, co utrudniało Brytyjczykom skuteczne ściganie ich. W połączeniu z technikami najazdu-uderzenia-szybkiego odwrotu, pozwoliło to osiągnąć początkową przewagę nad siłami Korony — szczególnie, że lo-

³⁸ C.C. Davies, *Warren Hastings, and Oudh*, Oxford 1939, 236–237.

³⁹ C. Markovits, *The Political Economy of Opium Smuggling in Early Nineteenth Century India: Leakage or Resistance?*, „Modern Asian Studies” 2009, Vol. 43, No. 1, s. 108–110; L. Subramanian, *Banias and the British: The Role of Indigenous Credit in the Process of Imperial Expansion in Western India in the Second Half of the Eighteenth Century*, „Modern Asian Studies” 1987, Vol. 21, No. 3, s. 509–510.

⁴⁰ A. Orme, *A History of the Military Transactions of the British Nation in Indostan: from the Year 1745*. Vol. 2, Norderstedt 2020, s. 217

⁴¹ G.J. Bryant, *Asymmetric Warfare...*, s. 468–469.

⁴² D. Steele, *Sailsbury and the Soldiers*, [w:] *The Boer War. Distraction, Experience and Image*, J. Gooch (ed.), London-New York 2013, s. 10, 13–18; A. Wessels, *The Anglo-Boer War (1899–1902) and its traumatic consequences*, [w:] *Breaking Intergenerational Cycles of Repetition A Global Dialogue on Historical Trauma and Memory*, P. Gobodo-Madikizela (ed.), Opladen-Berlin-Toronto 2016, s. 163.

kalne ludy afrykańskie sympatyzowały z Burami, zapewniając im schronienie, zasoby oraz istotne informacje.

Dlatego siły brytyjskie same podjęły działania niekonwencjonalne, uderzając w Burów dwojako. Po pierwsze: zastosowali taktykę spalonej ziemi, niszcząc pola uprawne, zapasy żywności, co znacząco utrudniło skuteczne prowadzenie walki przez afrykańskie republiki⁴³. Jeszcze większe oddziaływanie miały natomiast obozy koncentracyjne, w których internowali cywilów (kobiety i dzieci) z obszarów walk, wywierając na Burach dodatkowy nacisk⁴⁴. W obozach zginęło bowiem ok. 27 tysięcy ludzi, a w walce tylko 7 tysięcy⁴⁵. Choć odzew prasy europejskiej i amerykańskiej był bardzo negatywny, to Imperium Brytyjskie osiągnęło sukces i zajęło obie republiki burskie⁴⁶. Dla Imperium Brytyjskiego była to jednak kosztowna oraz przedłużająca się wojna, która wywołała też skutki wewnętrzne — sprzeciw Brytyjczyków, głównie zamieszkujących większe metropolie⁴⁷.

2.1.5. Świat po wielkich wojnach

Okres wojen światowych stanowi raczej sztandarowy przykład konfliktów regularnych i starcia porównywalnych adversarzy — w myśl pruskiego podejścia Clausewitza. Odnaleźć można stwierdzenia przeciwne, np. o ile Norwegia broniła się stosunkowo zaciekle w 1940 roku (korzystając z przewagi pogody, znajomości terenu i fortyfikacji), to Dania została zajęta przez III Rzeszę praktycznie bez walki⁴⁸. Polemizować jednak należy z tezą o asymetrii sensu stricto. W tym przypadku wciąż mamy prawnie równe podmioty międzynarodowe, podobnie rozwinięte, z relatywnie bliskiego kręgu kulturowego. Z kolei rzeczona różnica potencjałów jest sama w sobie powodem warunkującym racjonalność decyzji o agresji. W historii państwa napadały na inne zasadniczo w momencie,

⁴³ K.O. Morgan, *The Boer War and the Media (1899–1902)*, „Twentieth Century British History” 2002, Vol. 13, No. 1, s. 11.

⁴⁴ Tamże, s. 1, 3, 9.

⁴⁵ Szczególnie widoczna jest dysproporcja w ofiarach. Walczącymi byli właściwie sami mężczyźni, a w obozach ginęły kobiety i dzieci. O ile początkowe źródła podawały ok. 14 tysięcy ofiar obozów, to późniejsze badania wskazały na liczbę sięgającą 27 tysięcy; K. Moruzi, *Feminine Bravery: The Girl's Realm (1898–1915) and the Second Boer War*, „Children's Literature Association Quarterly” 2009, Vol. 34, No. 3, s. 246–247.

⁴⁶ E.V. Heyningen, *The Concentration Camps of the South African (Anglo-Boer) War, 1900–1902*, „History Compass” 2009, Vol. 7, No. 1, s. 32–33; J.R. Jewell, *Using barbaric methods in South Africa: The British concentration camp policy during the Anglo-Boer War*, „Scientia Militaria — South African Journal of Military Studies” 2012, Vol. 31, No. 1, s. 15–18.

⁴⁷ A. Mack, *Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict*, World Politics 1975, Vol. 27, No. 2, s. 176.

⁴⁸ M. Pazdej, *Recepcja wojny zaprezentowana w traktatach Sun Tzu i Carla von Clausewitza oraz możliwość ich wykorzystania do metodologicznego określenia nowoczesnych konfliktów asymetrycznych*, „Świat Idei i Polityki” 2014, t. 13(14), s. 164–165.

w którym miały określoną przewagę (i oczywiście cel). Dlatego wydaje się, że odnajdywanie *asymetryczności* w takich przykładach tylko rozwadnia badany termin.

Z kolei ruchy partyzanckie — o ile asymetryczne z samej swej definicji, to były tylko elementem składowym większego konfliktu, a nie wojną samą w sobie. Nie były też dla niej wystarczająco znaczące, aby wynosić je do rangi zupełnie odmieniającej przebieg walk. Miały wpływ lokalny, a ponadto dla wielu narodowości stanowią istotny element historii, przez co bywają gloryfikowane i bardziej eksponowane w źródłach oraz kulturze⁴⁹. Jednakże oceniając je z punktu widzenia przedmiotu niniejszej pracy, w tym kontekście nie wydają się być one przykładem rzeczywistych konfliktów asymetrycznych. Pozostaje to jednak istotnym dla późniejszych rozważań nad asymetrią.

Po II wojnie światowej rosło jednak znaczenie wojen asymetrycznych, a ich udział w ogólnej liczbie konfliktów zaczął wzrastać. Co więcej, podmioty prawa międzynarodowego musiały zacząć liczyć się z realnym zagrożeniem ze strony pozornie słabszych przeciwników⁵⁰.

Na początku XX wieku w Algierii funkcjonowała purytańska sekta islamska znana jako *Amis du Manifeste et de la Liberté*⁵¹, która opowiadała się za całkowitym odrzuceniem kultury europejskiej i dążyła do fizycznej izolacji od Francuzów. To przygotowało grunt pod późniejszą rewolucję w latach 1954–1962, wszczętą przez Front Wyzwolenia Narodowego⁵² (franc. Front de Libération Nationale, dalej: FLN). Początkowe ataki z użyciem technik partyzanckich przekształciły się w pełnowymiarowy konflikt. FLN dążyła

⁴⁹ S.P. Ramet, *The denial syndrome and its consequences: Serbian political culture since 2000*, „Communist and Post-Communist Studies” 2007, No. 40, s. 45; A. Waldron, *China's New Remembering of World War II: The Case of Zhang Zizhong*, „Modern Asian Studies” 1996, Vol. 30, No. 4, s. 948; J-H Lim, *Victimhood Nationalism in Contested Memories: National Mourning and Global Accountability*, [w:] *Memory in a Global Age. Discourses, Practices and Trajectories*, A. Assmann, S. Conrad (eds.), New York 2010, s. 138–141; zob. C. Schmitt, *Theorie des Partisanen: Zwischenbemerkung zum Begriff des Politischen*, Berlin, 1975; M. Gross, *Rewriting the nation: World War II narratives in Polish history textbooks*, [w:] *Post-Socialism is not Dead: (Re)Reading the Global in Comparative Education*, I. Silova (ed.), Bingley 2010.

⁵⁰ M.P. Fischerkeller, *David versus Goliath: Cultural judgments in asymmetric wars*, „Security Studies” 1998, Vol. 7 No. 4, s. 1–3.

⁵¹ Przyjaciele Manifestu i Wolności (franc. Amis du Manifeste et de la Liberté, AML) — ruch założony przez nacjonalistę Ferhata Abbasa w ramach sprzeciwu francuskiej kolonizacji Algierii. Zradyzalizował się w okresie II wojny światowej, tracąc nadzieję na „równość w ramach Republiki Francuskiej” i dostrzegając w tym „rasowe przedsięwzięcie dominacji i wyzysku.. *Autor Manifestu Narodu Algierskiego* (franc. Le Manifeste du peuple Algérien), opublikowanego w 1943 roku; J.F. Lane, *Ferhat Abbas, Vichy's National Revolution, and the Memory of the Royaume arabe*, „L'Esprit créateur” 2007, Vol. 47, s. 19, 22.

⁵² Front Wyzwolenia Narodowego (franc. Front de Libération Nationale, trl. arab. Dżabhat at-Tahrīr al-Waṭani) — założona 1 listopada 1954 roku opozycja polityczna, w 1962 roku przekształcona w nacjonalistyczną partię polityczną o panarabskim, antyimperialistycznym i socjalistycznym charakterze; J. Foran, *Taking Power: On the Origins of Third World Revolutions*, New York 2005, s. 97–98.

do utworzenia islamskiego państwa algierskiego, podczas gdy Francja początkowo opierała się zmianom. Punktem zwrotnym była bitwa o Algier w 1956 roku. Konflikt przekształcił się w brutalną wojnę kolonialną, w której FLN przejmował kontrolę w niektórych regionach, ale mierzył się z wewnętrznymi konfliktami⁵³. Należy podkreślić, że dla Algierii był to okres charakteryzujący się oporem zorganizowanym przez małą grupę intelektualistów i polityków z klasy średniej, który nie odzwierciedlał pragnień i obaw ideologicznych narodu algierskiego⁵⁴. Całe przedsięwzięcie udało się jednak przez zachowanie synergii oraz konwergencji wielu wysiłków z pogranicza polityki, dyplomacji, propagandy, psychologii, czy spraw socjalnych, wojskowych oraz para-wojskowych. Kluczowy był także element religijny⁵⁵. Całość zakończyła się negocjacjami i porozumieniem z Évian, zawartym 19 marca 1992 roku. Algieria uzyskała niepodległość 5 lipca.

Wojna algierska oferuje kluczowy wgląd we współczesne konflikty i asymetryczne wojny, kładąc nacisk na *przetrwanie* jako najważniejszy cel. Podejścia niekinetyczne często przeważają nad podejściami kinetycznymi, podkreślając potrzebę zintegrowanej strategii, jedności wysiłków i wiedzy specjalistycznej w zakresie rozważań polityczno-psychologicznych⁵⁶. Współczesna sztuka rządzenia obejmuje dyplomację publiczną, wywiad, operacje informacyjne i sojusze, co wymaga połączenia działań wojskowych i pozamilitarnych. To ukazuje, że chociaż siła zachowuje użyteczność, to charakter wojny ewoluje i element społeczno-międzynarodowy może stanowić istotny wektor działań. Dlatego podkreślić należy znaczenie strategii holistycznych i zrozumienia polityczno-psychologicznych wymiarów działań wojennych. Dostosowanie się do tej rzeczywistości jest kluczowe dla powodzenia współczesnych konfliktów.

2.1.6. Problemy USA i ZSRR z prowadzeniem wojny asymetrycznej

Równie istotną jest tocząca się w latach 1955–1975 wojna wietnamska, która była najdłuższym, XX-wiecznym konfliktem przeciwpartyzanckim w jakim brały udział Stany Zjednoczone. Co więcej, był to pierwszy raz kiedy siły amerykańskie, charakteryzujące się znaczącą przewagą technologiczną i potencjałem militarnym, przegrały. W strate-

⁵³ M. Alexander, J.F.V. Keiger, *France and the Algerian War: strategy, operations and diplomacy*, „Journal of Strategic Studies” 2002, Vol. 25, No. 2, s. 20.

⁵⁴ M.G. Manwaring, *The Complexity of Modern Asymmetric Warfare*, Oklahoma 2012, s. 12; H. Roberts, *North African Islamism in the Blinding Light of 9-11*, „Crisis States Programme” 2003, No. 34, s. 21.

⁵⁵ R. Fantasia, E.L. Hirsch, *Culture in rebellion: The appropriation and transformation of the veil in the Algerian revolution*, [w]: *Social Movements and Culture. Volume 4*, H. Johnston, B. Klandermans (eds.), Minneapolis 1995, s. 148–150.

⁵⁶ M. Connelly, *Rethinking the Cold War and Decolonization: The Grand Strategy of the Algerian War for Independence*, „International Journal of Middle East Studies” 2001, Vol. 33, No. 2, s. 238–239.

gicznym rozumieniu poruszanej problematyki, porażka wynikała z czynników asymetrycznych⁵⁷.

Co ważne, jeszcze przed rozpoczęciem działań wiadomo było, jakiego oporu USA mogły się spodziewać. 6 marca 1946 roku w Paryżu podpisano porozumienie pomiędzy Demokratyczną Republiką Wietnamu (Việt Minh) oraz Francją, gdzie uznano Wietnam Północny za autonomiczne państwo w ramach Unii Francuskiej, posiadające własny rząd i wojsko. Wietnam przystał na ograniczenie swojej niepodległości w zamian za francuską pomoc w walce z wtargnięciem Chin. Jednak napięcie wzrosło, co doprowadziło do francuskiej okupacji Hajfongu w listopadzie 1946 roku i obalenia rządu Hồ Chí Minha. To właśnie on ostrzegł zachodniego agresora w słowach: „zabijcie dziesięciu naszych ludzi, a my zabijemy jednego z waszych. To wy pierwsi będziecie mieli dosyć”⁵⁸. Szybko okazało się, że była to zapowiedź stosowania nieregularnej, partyzanckiej taktyki sił komunistycznych, stanowiącej dla Francuzów duże wyzwanie. Dlatego Stany Zjednoczone udzieliły wsparcia lotniczego (z użyciem bombowców), ale nie zapobiegło to wycofaniu się Francji z Wietnamu Północnego w 1954 roku, po porażce pod Điện Biên Phủ⁵⁹.

Kiedy siły amerykańskie przystąpiły do walki rok później, okazały się one zupełnie nieprzygotowane do starć z partyzantami, którzy dodatkowo świetnie wykorzystywali przewagę znajomości terenu. Co więcej, Amerykanie nie zaadaptowali znaczących zmian w technice walki. Za to Wietnamczycy stosowali podejście trójfazowe, oparte na myśli wojny rewolucyjnej Mao Zedonga. Początkowo skupili się oni na *mobilizacji politycznej*, tworząc spójną organizację, rekrutując oddanych członków i budując zaplecze — lokalne wsparcie oraz podstawy ideologiczne, cementujące wypracowany potencjał. W dalszej fazie (najdłuższej) przeszli do *wojny partyzanckiej*, skupiając się na rozszerzeniu wsparcia do odległych miejsc, tak by móc atakować na dużym obszarze, tym samym budując pro-partyzanckie morale (przez wzgląd na skalę działań). Wykorzystywano w tym celu ukrywanie bojowników wśród cywilów (właściwie: nie-kombatantów), agresję z zaskoczenia przez uderzenie i ucieczkę, a także kontrolę populacji. Znaczącą rolę odegrały sieci tuneli czy stworzenie siatek informatorów, co pozwoliło zniwelować przewagę technologiczną Amerykanów, na której starali się oni polegać⁶⁰. Ostatnia faza to *wielkoskalowa walka z przeciwnikiem*, którą wykorzystując wcześniej zbudowane wspar-

⁵⁷ F.B. Miles, *Asymmetric Warfare: an Historical Perspective*, Carlisle 1999, s. 18.

⁵⁸ A. Dmochowski, *Wietnam: wojna bez zwycięzców*, Kraków 1991, s. 134.

⁵⁹ J. Macdonald, J.W. Hackett, M. Malczyk, *Wielkie Bitwy Historii*, Warszawa 1994, s. 196; B.B. Fall, *Street Without Joy: The French Debacle in Indochina*, Mechanicsburg 1994, s. 34–38.

⁶⁰ M. Sturken, *Tangled Memories: The Vietnam War, the AIDS Epidemic, and the Politics of Remembering*, Berkeley-Los Angeles-London 1994, s. 16, 45.

cie społeczne, a zarazem powszechny sprzeciw okupantowi, używa wszystkich sił i środków do walki — celem zupełnego wyparcia agresora⁶¹. Niezrozumienie głębi oraz skali działań, było jednym ze znaczących czynników dających Wietnamowi Północnemu przewagę⁶². Szczególną rolę odegrały też morale — systematyczne budowanie w społeczeństwie poczucia jedności i potrzeby przetrwania⁶³, które kontrastowały z licznymi problemami Amerykanów, przeciągającą się wojną oraz brakiem sukcesów.

Przez wzgląd na powyższe, wojna wietnamska stanowi doskonały przykład konfliktu asymetrycznego, w którym niezwykle istotną jest nie tylko jego wielowymiarowość, szczególnie ze strony słabszego aktora, lecz potrzeba w ogóle zrozumienia tak szerokiego spektrum aspektów walki, polityki i spraw społecznych. Inaczej nawet ogromna przewaga technologiczna, militarna oraz ekonomiczna może kompletnie zawieść, co dobitnie pokazały Stany Zjednoczone. Co więcej, przegrały one nie tyle militarnie, co politycznie — a to ukazuje jak daleki zasięg mogą mieć reperkusje wywoływane zjawiskiem *asymetryczności*. Odrębną kwestią pozostaje pytanie, czy Wietnam Północny tak naprawdę wygrał (czy bilans strat i zysków był pozytywny?), lub czy w ogóle ma to znaczenie. Zdaje się bowiem, szczególnie na powyższym przykładzie, że w wojnie asymetrycznej słabsza strona musi wyłącznie nie przegrać, a przeciągający się konflikt w końcu wykończy agresora i zmusi go do wycofania się.

Nie tylko Zachód zmagał się z opisanymi powyżej problemami. Interwencja wojskowa Związku Radzieckiego w Afganistanie, prowadzona w latach 1979–1989, pozwala na zbadanie dynamiki, wyzwań i konsekwencji asymetrii we współczesnych działaniach wojennych. Podczas gdy Związek Radziecki szczycił się przytłaczającą przewagą militarną i zaawansowaną technologią, afgański ruch oporu, składający się głównie z luźno zorganizowanych mudżahedinów, zastosował niekonwencjonalną taktykę opartą na dogłębnej znajomości terenu, skomplikowanych sieciach lokalnych i walce partyzanckiej. Wynikająca z tego nierównowaga sił oraz asymetryczny charakter konfliktu miały głębokie konsekwencje nie tylko dla najbliższego regionu, ale także dla globalnej geopolityki, będąc jedną z przyczyn upadku Związku Radzieckiego⁶⁴. Niepomijalnym jest także czynnik

⁶¹ D.W. Craig, *Asymmetrical Warfare and the Transnational Threat: Relearning the Lessons from Vietnam*, North York 1998, s. 7–8.

⁶² Amerykanie zaczęli badać taktykę opartą o myśl dalekowschodnią jeszcze w czasie wojny wietnamskiej (np. w *The New Face of War*), jednakże bardziej pogłębione analizy pojawiły się dopiero retrospektywnie, wymieniając fazy: początkowej, ukrytej działalności wywrotowej, zorganizowanej walki partyzanckiej i wojnę ruchu (zapożyczoną dosłownie od Mao Zedonga); R.A. Mountel, *Indo-China in retrospect: The Communist Insurgency*, Carlisle 1973, s. 12.; zob. M.W. Browne, *The New Face of War*, New York 1965.

⁶³ A. Lele, *Asymmetric Warfare...*, s. 106–107.

⁶⁴ A. Brown, *The Gorbachev Factor*, Oxford 1997, 306.

wpływu Stanów Zjednoczonych, które poprzez Centralną Agencję Wywiadowczą (CIA) wspierały mudżahedinów w walce — co zresztą było pokłosiem wojny w Wietnamie⁶⁵.

Na mocy memorandum Breżniewa z grudnia 1979 roku (*O sytuacji w „A”*) podjęto decyzję o interwencji w Afganistanie. W porozumieniu z tamtejszym sztabem generalnym sił zbrojnych, ustalono rozmieszczenie 75 tysięcy żołnierzy radzieckich w Demokratycznej Republice Afganistanu⁶⁶. Inwazję w rozpoczęto od operacji Sztorm-333 (ros. *Шторм-333*), której celem było odsunięcie od władzy ówczesnego prezydenta Afganistanu, Hafizullaha Amina. Dokonano przejęcia kilku czołowych budynków wojskowych i administracyjnych w Kabulu⁶⁷. Co istotne z punktu widzenia pracy, dokonali tego żołnierze przebrani w mundury armii afgańskiej, dowodzeni przez byłego radzieckiego łącznika wojskowego w Kabulu, gen. Witalija Primakowa, który sam podszywał się pod tureckiego oficera⁶⁸. Chociaż całość zakończyła się sukcesem, to samo zabicie głowy państwa nie mogło dać legitymizacji nowo powołanej władzy Babraka Karmala, zgodnej z interesem ZSRR i opierającej się o współpracę z nim⁶⁹. Władze radzieckie początkowo spodziewały się, że ich interwencja będzie krótkotrwała, co okazało się założeniem błędnym.

W czasie trwającej dziewięć lat wojny/operacji można wyróżnić trzy główne fazy. Pierwsza, rozpoczęta w 1979 roku, skupiała się na zajęciu Afganistanu przez regularne jednostki Armii Radzieckiej. W kolejnych miesiącach następowała rotacja oddziałów, w których służyli poborowi z różnych republik ZSRR, w tym także z republik środkowo-azjatyckich. Ponadto już wtedy zaczęto toczyć pierwsze, istotne walki z siłami partyzantkimi⁷⁰. Druga faza, trwająca od 1982 do 1986 roku, była okresem intensywnych walk, w czasie których okupant stopniowo tracił kontrolę nad krajem, częściowo z powodu wsparcia CIA dla mudżahedinów. Wyróżnić tu należy wyposażenie ich w systemy FIM-92 Stinger⁷¹, wykorzystujące naprowadzane podczerwienią pociski ziemia-powietrze, które

⁶⁵ Po wojnie w Wietnamie siły zbrojne i służby specjalne USA zaangażowały się w konflikty asymetryczne (powstania) państw rozwijających się. Wymienić tu można interwencję piechoty morskiej w Bejrucie (1982–1984), będące zaangażowaniem bezpośrednim. Natomiast wykorzystanie doradców wojskowych celem pomocy armii Salwadoru w walce z komunistycznymi powstańcami Frontu Wyzwolenia Narodowego im. Farabunda Martíego (1981–1992), jest przykładem interwencji pośredniej; F.B. Miles, *Asymmetric Warfare...*, s. 19.

⁶⁶ G. Hughes, *The Soviet–Afghan War, 1978–1989: An Overview*, „Defence Studies” 2008, Vol. 8, No. 3, s. 332.

⁶⁷ Н.И. Шилов, *Афганистан 30 лет спустя: последствия ввода советских войск в ДРА для страны и региона*, „Вестник МГИМО” 2010, №2, s. 1–3.

⁶⁸ R. Braithwaite, *Afgantsy: The Russians in Afghanistan 1979–89*, New York 2011, s. 29.

⁶⁹ Tamże, s. 103.

⁷⁰ J.B. Amstutz, *Afghanistan: The First Five Years of Soviet Occupation*, Washington 1994, s. 127.

⁷¹ G. Crile, *Charlie Wilson's War: The Extraordinary Story of the Largest Covert Operation in History*, New York 2003, s. 302, 519.

okazały się wyjątkowo skutecznymi przeciw radzieckim śmigłowcom⁷². Doprowadziło to do powolnego wycofywania się sił zbrojnych ZSRR, od 1986 do 1989 roku, będącego trzecią fazą. Nie było to jednak proste, gdyż wojska radzieckie zostały niejako uwięzione w centrum kraju po zajęciu przez mudżahedinów szlaków wiodących na północ⁷³.

Samych przyczyn wycofania się ZSRR należy szukać właśnie w wojnie asymetrycznej, podczas której ponosili „śmierć od tysiąca cięć”⁷⁴ z rąk przeciwnika, który walczył nie tyle z nadzieją na konkretne zwycięstwo, co o *przetrwanie*. Dlatego o ile straty po stronie konwencjonalnych sił (armii radzieckiej i afgańskiej) były wprost proporcjonalne do liczby żołnierzy przeciwnika, to straty po stronie partyzantów już nie. Bo owszem, im bardziej zintensyfikowane były działania przeciw nim, tym większe ponosili straty, choć nie w stałej zależności. Dokładne położenie mudżahedinów często nie było znane. Kiedy partyzanci atakowali zawsze w konkretne cele, wyrządzając szkodę, konwencjonalne armie strzelały czasem na ślepo⁷⁵, czemu sprzyjało ukształtowanie terenu.

Interesujący był także przekrój taktyk stosowanych przez mudżahedinów. Na szeroką skalę wykorzystywali zasadzki — poprzedzane zbieraniem informacji wywiadowczych, dobrze planowane i przeprowadzane z zachowaniem dużej dyscypliny. Wykorzystywali też już wcześniej umocnione pozycje (w ramach innych działań), aby znacząco obniżyć koszty (głównie czasu). Przykładem może być zasadzka z września 1983 roku, pod górą Kohe Duranay, w której mudżahedini zaatakowali jadący z Kabulu konwój wojsk radzieckich, niszcząc 33 pojazdy opancerzone i 27 ciężarówek. Całość okazała się na tyle skutecznie zorganizowana, że impas wynikający z przewagi partyzantów przełamało dopiero użycie artylerii⁷⁶. Z podobną skutecznością przeciwdziałali zasadzkom na nich samych. Ponadto organizowali najazdy (oraz obronę przed nimi, np. podczas ataku wojsk ZSRR na pozycje Saigania), blokowali łączność okupanta i sprawnie prowadzili walki w terenie zurbanizowanym, czy przeciwko lotnictwu ZSRR⁷⁷. Wykorzystywali też niewybuchy (o masie 0,25–0,5 t), które transportowali pod osłoną nocy celem podłożenia

⁷² A. Rashid, *Taliban: Militant Islam, Oil and Fundamentalism in Central Asia*, New Haven 2000, s. 129.

⁷³ S. Haroon, *The Rise of Deobandi Islam in the North-West Frontier Province and Its Implications in Colonial India and Pakistan 1914–1996*, „Journal of the Royal Asiatic Society” 2008, No. 18 (1), s. 66–67.

⁷⁴ A.A. Jalali, L.W. Grau, *The Other Side of the Mountain: Mujahideen Tactics in the Soviet-Afghan War*, Quantico 2002, s. ix.

⁷⁵ Co interesujące, była to obserwacja naukowców zachodnich, badających toczący się wówczas konflikt w Afganistanie — co dodatkowo pokazuje, jak zmieniło się podejście Zachodu po konflikcie w Wietnamie; P. Allan, A.A. Stahel, *Tribal Guerrilla Warfare against a Colonial Power: Analyzing the War in Afghanistan*, „The Journal of Conflict Resolution” 1983, Vol. 27, No. 4, s. 600.

⁷⁶ A.A. Jalali, L.W. Grau, *The Other Side of the Mountain...*, s. 39–41.

⁷⁷ C.J. Dick, *Mujahideen Tactics in the Soviet-Afghan War*, Camberley 2002, s. 7–13.

na szlakach komunikacyjnych, szczególnie na mostach, wiaduktach i innych przeprawach. Odpalane zdalnie, skutecznie unieruchamiały konwoje i niszczyły pojazdy przeciwnika⁷⁸.

Strategia mudżahedinów w wojnie partyzanckiej przeciwko żołnierzom ZSRR kładła nacisk na wytrzymałość i wolę narodową, które umożliwiły *przetrwanie*, bez silnego dążenia do zwycięstwa na polu bitwy. Ponosząc straty, ale też utrzymując ogólną siłę, finalnie doprowadzili do wycofania się wojsk radzieckich. Należy też podkreślić, że popełniali liczne błędy, m.in. często obierając te same cele lub nie zapewniając odpowiedniej ochrony kontrolowanych przez siebie terytoriów. ZSRR nie wykorzystał jednak tych słabości — a to doszukiwanie się takowych mogłoby stanowić skuteczny wyłom w przewadze zyskiwanej przez działania asymetryczne.

2.1.7. Asymetria w świecie pozimnowojennym

Przejście z zimnej wojny do epoki globalizacji oznaczało dla świata, a w szczególności dla Europy, okres transformacji politycznych, gospodarczych i militarnych. Dekompozycja dotychczasowych układów sił oraz władzy przebiegała różnie. Część państw przekształcała się pokojowo w Polsce czy Węgrzech. Z kolei w byłej Jugosławii napięcia rosły, nacjonalizm przeżywał renesans, a ogólna niestabilność Bałkanów wywołała konflikt na wielką skalę, w którym to zaczęły pojawiać się nowe elementy prowadzenia walki (omówione w rozdziale I). Rozpad świata dwubiegunowego nie przyczynił się jednak do ustalenia nowej *równowagi* sił, lecz wprowadził asymetrię⁷⁹. Co więcej, równocześnie wzrosła liczba zagrożeń ze strony mniejszych podmiotów, umacnianych przez podziały narodowościowe, etniczne, religijne czy ideologiczne. Wzrastały też związki z przestępczością zorganizowaną. Stworzyło to zatem grunt pod rozwój wojen asymetrycznych, często wynikających z konfliktów wewnętrznych, które wówczas nie były jeszcze odpowiednio badane. Jedne źródła wskazywały na to, że pluralizm etniczny lub reformy demokratyczne są tak naprawdę zapalnikiem, inne — iż wręcz przeciwnie⁸⁰. Dlatego przygotowanie się do skutecznej walki i wyciąganie trafnych wniosków były utrudnione⁸¹.

Do szerokiego spektrum problematyki asymetrii dołączyły też wyzwania terroryzmu, choć początkowo niewpływające na światowe bezpieczeństwo w sposób istotny. Zamach na World Trade Center z 1993 roku pochłonął niewiele ofiar, przez co nie wywarł

⁷⁸ T. Horváth, J.Z. Szatai, *History of detection of explosive devices 2.(1951 to the present)*, „Land Forces Academy Review” 2020, Vol. XXV, No. 4(100), s. 292–295.

⁷⁹ D. Gibas-Krzak, *Asymetryczne Bałkany*, Częstochowa 2015, s. 13–15.

⁸⁰ E. Newman, *Conflict Research and the ‘Decline’ of Civil War*, „Civil Wars” 2009, Vol. 11, No. 3, s. 260–261, 275.

⁸¹ F. Freedman, *Przyszła Wojna...*, Ożarów Mazowiecki 2019, s. 202.

wielkiego wrażenia. Zaczęło się to zmieniać podczas zamachów na ambasady amerykańskie w Kenii i Tanzanii⁸², lecz punktem zwrotnym był atak na World Trade Center z 11 września 2001 roku.

Zamach ten miał ówczesnie niewyobrażalną skalę. Liczba ofiar oraz medialność zdarzenia sprawiły, że oddziaływał on na cały świat. Wywołał przy tym wstrząs psychologiczny i lęk związany z zachwianiem systemu bezpieczeństwa. Ataku dokonano bowiem w samym sercu Stanów Zjednoczonych, odpowiadających wówczas za niecałe 40% światowych wydatków na zbrojenia⁸³. Co więcej, ciosu nie zadało inne państwo, czy może ich koalicja — lecz grupa terrorystyczna. Nie miała stricte własnego terytorium, głowy „państwa”, regularnych wojsk. Wymagała nie tylko walki, lecz najpierw rozpoznania z kim walczyć i kto może być zagrożeniem. Zrodziło się zatem nowe wyzwanie, wymagające wielkoskalowego, synergicznego połączenia wysiłków wywiadowczych, militarnych oraz politycznych.

Dobrze ugruntowane podmioty niepaństwowe osiągają przy tym zdolności zagrażające państwowości. Wynika to z możliwości wykorzystania broni masowego rażenia, ataków wymierzonych w środowisko, gospodarkę, społeczeństwo (w ujęciu społeczno-psychologicznym), infrastrukturę i instytucje obywatelskie, a także podmioty prywatne. Działalność ta przenika zatem wszystkie istotne aspekty codziennego życia, podobnie jak cyberprzestrzeń, będąca katalizatorem wielu przejawów walki asymetrycznej⁸⁴. Dlatego koniecznym staje się holistyczne spojrzenie na to zjawisko, a nie próby wyłącznie wąskiego definiowania i analizowania selektywnie wybranych studiów przypadków. O ile pomagają one zrozumieć konkretne przykłady zastosowania walki asymetrycznej, jej przejawy i możliwe różnice — religijne, kulturowe lub społeczne — to nie można ich ekstrapolować na całość działań asymetrycznych.

2.2. Wpływ i wykorzystanie asymetryczności w cyberprzestrzeni

Cyberprzestrzeń postrzegana jest głównie przez pryzmat wolności przepływu informacji, otwartości infrastruktury oraz technicznego wymiaru bezpieczeństwa. Takie podejście, głęboko zakorzenione w liberalnej tradycji myślenia o porządku międzynarodowym, pomija jednak coraz bardziej widoczny proces rekonfiguracji tej przestrzeni

⁸² Tamże, s. 248.

⁸³ E. Sköns, E. Loose-Weintraub, W. Omitoogun, P. Stålenheim, R. Weidacher, *Military expenditure and arms production*, [w:] *Sipri Yearbook 2001*, Stockholm 2001, s. 236–242.

⁸⁴ A. Lele, *Asymmetric Warfare...*, s. 105–106.

przez państwa dążące do cyfrowej suwerenności⁸⁵. Środowisko sieciocentryczne nie jest już bowiem wyłącznie techniczną infrastrukturą komunikacyjną, lecz dynamicznie kształtowaną przestrzenią o charakterze strategicznym⁸⁶. Należy zauważyć, że w konsekwencji zmienia się także podejście do samej władzy. W tym ujęciu definiowana jest jako zdolność aktora do wywierania wpływu na pozostałe podmioty poprzez działania w cyberprzestrzeni oraz zdolność do kształtowania tego środowiska zgodnie z własnymi preferencjami⁸⁷. To odchodzenie od rozumienia siły jako czysto militarnej ku zintegrowanemu modelowi, gdzie technologiczne, informacyjne i normatywne czynniki decydują o przewadze, jest kluczowe dla zrozumienia asymetrii. Otwiera to bowiem dostęp do tak zdefiniowanej władzy szerokiemu spektrum podmiotów.

Co więcej, struktura cyberprzestrzeni nie jest sztywna. Umożliwia więc nie tylko poruszanie się w niej, lecz aktywne jej kształtowanie — poprzez normy, regulacje, technologie oraz praktyki kulturowe, co zostało poruszone w poprzednim rozdziale. To może prowadzić zarówno do powstawania cyberdomeny zróżnicowanej, lecz także pofragmentowanej, rodząc nowe formy asymetrii w samej przestrzeni, a nie tylko pomiędzy jej podmiotami. Skrajnym tego przykładem są próby wydzielania izolowanych przestrzeni cybernetycznych, takich jak projekt RuNet — zamkniętej, narodowej sieci⁸⁸. Są to działania zmierzające do osiągnięcia przewagi poprzez modyfikowanie reguł dostępu do informacji i kontroli infrastruktury. Powyższe pozwala uzyskać strategiczną przestrzeń operacyjną o ograniczonym wpływie zewnętrznych zagrożeń, bez angażowania się w konflikt między państwami. Z jednej strony chroni to część własnej domeny wpływu, a zarazem nie uniemożliwia skutecznego prowadzenia ataków wymierzonych w przeciwnika. Zatem wprost prowadzi do asymetrii samej przestrzeni, która w tym wypadku nie jest celem samym w sobie. Jest raczej punktem wyjścia do dalszej zdolności eskalacji.

⁸⁵ Cyfrowa suwerenność rozumiana jako zdolność państwa lub grupy podmiotów międzynarodowych do sprawowania legitymowanej kontroli nad zasobami, procesami oraz infrastrukturą cyfrową — obejmującą dane, oprogramowanie, algorytmy, standardy komunikacyjne, sprzęt, usługi i systemy informatyczne. Oznacza to zarówno możliwość wpływania na ich funkcjonowanie oraz rozwój, jak również korekty ewentualnych odchyłeń od założonych celów społecznych, ekonomicznych czy politycznych. W rezultacie, cyfrowa suwerenność to nie tylko kwestia technologii i polityki, lecz przede wszystkim legitymizacji władzy w warunkach asymetrycznej zależności od podmiotów komercyjnych; L. Floridi, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, „Philosophy & Technology” 2020, No. 33, s. 371–376; s. J. Phole, T. Thiel, *Digital sovereignty*, „Internet Policy Review” 2020, Vol. 9, Issue 4, s. 8–13.

⁸⁶ H.I. Langø, *Slaying Cyber Dragons: Competing Academic Approaches to Cyber Security*, [NUIP-WP 820], Oslo 2013, s. 10–13.

⁸⁷ N. Choucri, *Cyberpolitics in International Relations*, Cambridge 2012, s. 4–9.

⁸⁸ G. Asmolov, P. Kolozaridi, *The imaginaries of RuNet: the change of the elites and the construction of online space*, „Russian Politics” 2017, Vol. 2, No. 1, s. 61–70.

Juha Kukkola⁸⁹ proponuje nazwę strukturalnej asymetrii [cyberprzestrzeni] i jej osadzenie w ramach neoklasycznego realizmu oraz kultury strategicznej. Zarazem rozumie ją jako przewagę wynikającą nie z chwilowej różnicy potencjałów, lecz z trwałego przekształcenia reguł gry w cyberprzestrzeni. Cel ten osiągnąć może być na trzech poziomach: fizycznym (np. infrastruktury sieciowej), syntaktycznym (np. protokołów komunikacyjnych) oraz semantycznym (samej informacji)⁹⁰. W efekcie pojawia się asymetria nie tylko operacyjna, lecz także konceptualna, prowadząca do trudności w przewidywaniu działań i skutecznym reagowaniu na zagrożenia. Co istotne, wyzwaniem stanowi także budowanie odstraszania w cyberprzestrzeni, rozumianego w kontekście zniechęcania potencjalnego przeciwnika do podjęcia określonych działań poprzez zagrożenie użyciem siły lub innych środków represji⁹¹. W teorii odstraszania, wywodzącej się z okresu zimnej wojny⁹², kluczowe są trzy elementy: zdolność (posiadanie środków do reakcji), wiarygodność (przekonanie przeciwnika, że zostaną użyte) oraz komunikacja (jasne przekazanie warunków reakcji). W kontekście środowiska sieciocentrycznego, tak rozumiane skuteczne odstraszanie jest utrudnione z uwagi na trudności w atrybucji ataków, brak przejrzystości co do zdolności stron, jak również dynamicznie zmieniających się reguły gry.

2.2.1. Cyberprzestrzeń w koncepcjach zachodnich

Pomimo rozwiniętych teorii i hipotez związanych z cyberwojnami, Zachodnie podejście dość długo pozostawało bierne na uwzględnienie możliwości przed-konfliktowego kształtowania środowiska operacyjnego w cyberprzestrzeni. Podobnie, problematyczna była integracja analiz technicznych lub wojskowych z politycznym i kulturowymi⁹³. Zrozumienie strukturalnych problemów domeny cybernetycznej nadal jednak zdaje się pozostawać spojrzeniem niszowym.

⁸⁹ Juha Kukkola — kapitan fińskich sił obronnych (Puolustusvoimat — Försvarsmakten), badacz i wykładowca Departamentu Wojny w Fińskim Uniwersytecie Obrony Narodowej w Helsinkach. Nota biograficzna w: V. Siukonen, M. Ristolainen, J.P. Nikkarila, J. Kukkola, *Are We There Yet?: Monitoring the Technical Deployment of the National Segments of the Internet*, [referat konferencyjny] *MILCOM 2019–2019 IEEE Military Communications Conference (MILCOM)*, Norfolk 2020, s. 1.

⁹⁰ J. Kukkola, *Cyber asymmetry — Towards new strategic thinking?*, [w:] *Game Changer: Structural transformation of cyberspace*, J. Kukkola, M. Ristolainen, J.P. Nikkarila (eds), Riihimäki 2017, s. 166–171.

⁹¹ Zob. J.S. Nye Jr., *Soft Power — the Means to Success in World Politics*, New York 2004; R.K. Betts, *The Lost Logic of Deterrence. What the Strategy That Won the Cold War Can—and Can't—Do Now*, „Foreign Affairs” 2013, Vol. 92, No. 2.

⁹² R.K. Betts, *The Concept of Deterrence in the Postwar Era*. „Security Studies” 1991, Vol. 1, No. 1, s. 25–36.

⁹³ Zob. R.A. Clarke, R. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, [b.m.w.] 2010; M.C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge 2007.

W 2011 roku amerykański Departament Obrony opublikował *Strategię operowania w cyberprzestrzeni*. Zawierała ona pogląd, iż „(...) aby zachować skuteczność operacyjną [w cyberprzestrzeni], należy izolować i neutralizować wpływ, wykorzystując redundantną przepustowość lub przenosząc operacje z jednego systemu do drugiego. Wiele sieci może zwiększyć różnorodność, odporność i pewność misji w operacjach cyberprzestrzeni. Departament Obrony inwestuje w badania mające na celu zidentyfikowanie możliwości przeniesienia operacji do bezpiecznych sieci na dużą skalę i w całym spektrum operacji”⁹⁴.

Centrum Doskonałości Cyberobrony NATO (NATO Cooperative Cyber Defence Centre of Excellence — CCDCOE) wydało w 2020 roku publikację *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*⁹⁵. Na łamach jednego z jej rozdziałów, J. Kukkola badał rosyjskie postrzeganie asymetrii strukturalnej, w którym wyrażał poglądy z wyżej opisanymi. Jego kluczowa teza głosi, że państwo, które izoluje swoją infrastrukturę, zyskuje przewagę nad tymi, które pozostają otwarte i bardziej podatne na operacje informacyjne i destrukcyjne. Rosyjski projekt ukazany jest jako forma modelowania środowiska operacyjnego (ang. *shaping the domain*), a nie tylko reakcji na zagrożenia. Autor wskazał, że różnice w swobodzie działania, odporności, zdolności dowodzenia oraz zrozumieniu wspólnego obrazu operacyjnego między zamkniętym a otwartym systemem państwowym mogą przełożyć się na znaczącą przewagę w konflikcie międzypaństwowym⁹⁶. W podobny sposób temat został ujęty jeszcze w dalszej części publikacji, podkreślając jak strukturalną niekorzyść środowiska sieciocentrycznego, która faworyzuje agresora i stawia w gorszej pozycji broniącego się⁹⁷. Należy jednak podkreślić, iż publikacja ta nie ma charakteru wiążącego. Jest raczej zbiorem analiz, a samo strukturalne ujęcie asymetrii zdaje się być pomijane w istotnych dokumentach NATO. Pomimo skoncentrowania się na relacjach między aktorami, Sojusz zaproponował jednak koncepcję autonomicznego agenta obrony cybernetycznej (ang. *Autonomous Intelligent Cyber Defence Agent — AICA*). Zakłada ona możliwość stopniowego wycofywania się z otwartej

⁹⁴ Oryg. (...) be able to remain operationally effective by isolating and neutralizing the impact, using redundant capacity, or shifting its operations from one system to another. Multiple networks can add diversity, resiliency, and mission assurance to cyberspace operations. DoD is investing in research to identify options for shifting its operations to secure networks at scale and across the full spectrum of operations; *Department of Defense Strategy for Operating in Cyberpace*, Arlington 2011, s. 6.

⁹⁵ *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, A. Ertan, K. Floyd, P. Pernik, T. Stevens (eds.), Tallinn 2020.

⁹⁶ J. Kukkola, *The Russian National Segment of the Internet as a Source of Structural Cyber Asymmetry*, [w:] tamże, s. 9–13, 16–18, 23–26.

⁹⁷ J. Bellasio, E. Silfversten, *The Impact of New and Emerging Technologies on the Cyber Threat Landscape and Their Implications for NATO*, [w:] tamże, s. 89–90.

i rozproszonej architektury cyberprzestrzeni na rzecz inteligentnie kontrolowanej i ściśle nadzorowanej infrastruktury obronnej. Podkreśla się konieczność budowy wewnętrznych systemów autonomicznych zdolnych do działania niezależnie od zewnętrznych źródeł informacji oraz podejmowania decyzji bez udziału człowieka⁹⁸. Tak ujęty kierunek, choć niewpisujący się wprost w powyższą definicję strukturalnej asymetrii, wskazuje na możliwość kształtowania warunków operacyjnych przez państwo poprzez systemową izolację lub różnicowanie dostępu, co może prowadzić do powstania strukturalnej przewagi nad mniej odpornym przeciwnikiem.

W *Narodowej cyber-strategii* z 2022 roku, brytyjski rząd wskazuje na cyberprzestrzeń jako domenę, w której państwo może — i musi — kształtować własną architekturę infrastruktury fizycznej i logicznej⁹⁹. Chociaż dokument nie posługuje się terminem strukturalnej asymetrii, to wyraźnie zakładają możliwość budowy osłon sieciowych, które ograniczają zewnętrzny dostęp oraz wzmacniają odporność systemową¹⁰⁰. To z kolei dawać ma państwu przewagę operacyjną, nawet jeśli podmiot zewnętrzny miałby nadal dostęp do globalnych systemów. Co więcej, w osiągnięciu tych celów należy ściśle uwzględniać współpracę z sektorem prywatnym czy środowiskiem asymetrycznym¹⁰¹.

Podobne podejście wyraża Unia Europejska. Dyrektywa NIS¹⁰² oraz Europejskiej Agencji ds. Cyberbezpieczeństwa (ENISA) koncentrują się na budowie spójnej, odpornej infrastruktury cyfrowej w państwach członkowskich. W wielu aspektach wpisuje się to w koncepcję strukturalnej asymetrii. Choć dokumenty unijne nie używają tego terminu, dążenie do harmonizacji wymogów bezpieczeństwa w sektorach krytycznych, tworzenie wspólnych norm zarządzania ryzykiem i obowiązek wymiany informacji sprzyjają kształtowaniu architektury odpornej systemowo. Budowa przewagi przez różnicowanie poziomu odporności między UE a aktorami zewnętrznymi — zwłaszcza niedemokratycznymi — to element asymetrii strukturalnej, choć realizowany bardziej defensywnie niż ofensywnie.

Wnioski płynące z powyższego przeglądu pokazują, że asymetria cybernetyczna nie jest zjawiskiem tymczasowym ani ograniczonym do niepaństwowych aktorów. Prze-

⁹⁸ P.T. Thales i inni, *Towards an Active, Autonomous and Intelligent Cyber Defense of Military Systems: the NATO AICA Reference Architecture*, [IST-152-RTG], 2018, s. 2–8.

⁹⁹ HM GOV, *National Cyber Strategy 2022. Pioneering a cyber future with the whole of the UK*, London 2022, s. 71–72, 80, 86–87, 104, 106.

¹⁰⁰ Tamże, s. 64–76.

¹⁰¹ Tamże, 35–36.

¹⁰² Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148, Eur-lex L 333/80, (dalej: NIS2).

ciwnie — w ujęciu strukturalnym stanowi trwały komponent kształtowania przewagi strategicznej przez rekonstruowanie cyberdomeny. Asymetria w cyberprzestrzeni to bowiem nie tylko różnica w potencjale operacyjnym, lecz przede wszystkim zdolność do zmiany środowiska, w którym ten potencjał ma zostać wykorzystany. Wobec tego, zachodnie koncepcje cyberbezpieczeństwa muszą zyskać większą zdolność adaptacyjną — nie tylko na poziomie technologii, lecz również w zakresie rozumienia politycznych konsekwencji cyfrowej suwerenności. Przede wszystkim jednak przejść muszą z pozycji reaktywnej (obronnej) na proaktywną (agresywną), tak aby możliwym stało się wykorzystanie potencjału odstraszania. Koreluje to z dyskusjami prowadzonymi w kręgu Zachodu, które ukazują konflikty w cyberprzestrzeni jako starcie strategii ofensywnych i defensywnych, często czytane przez pryzmat analogii zimnowojennych (np. „cyber Pearl Harbor”¹⁰³) oraz dylematów związanych z odstraszaniem nuklearnym¹⁰⁴. Takie ujęcie prowadzi do uproszczeń, zarazem utrudniając uchwycenie szarości pomiędzy atakiem oraz obroną. Szczególnym problemem staje się wówczas ujęcie aktywnej obrony („active cyber defense”)¹⁰⁵, którą jedni utożsamiają z czystym atakiem, a inni z legalnym monitorowaniem i kontrśrodkami przeciwko agresorom¹⁰⁶.

Wartym wskazania jest także amerykańskie podejście do przyszłych konfliktów w ramach „defending forward” i „persistent engagement”¹⁰⁷. Jest to projekcja władzy poza granicami własnego kraju, wynikająca z przekonania o wyjątkowej roli Stanów Zjednoczonych jako światowego lidera w cyberprzestrzeni. Rodzi to jednak napięcia między ofensywą a skuteczną obroną, zwłaszcza w obliczu technicznej złożoności systemów cyfrowych i trudności w wiarygodnym przypisywaniu ataków.

W obliczu powyższych wyzwań zachodni eksperci coraz częściej postulują podejście interdyscyplinarne, łączące perspektywy z zakresu nauk o bezpieczeństwie międzynarodowym, psychologii politycznej, prawa międzynarodowego oraz informatyki. Tylko

¹⁰³ Zob. J.J. Wirtz, *The Cyber Pearl Harbor*, „Intelligence and National Security” 2017, Vol. 32, No. 6; R.K. Palmer, *Critical Infrastructure: Legislative Factors for Preventing a Cyber-Pearl Harbor*, „Virginia Journal of Law & Technology” 2014, Vol. 18, No. 3.

¹⁰⁴ U. Tor, *‘Cumulative Deterrence’ as a New Paradigm for Cyber Deterrence*, „Journal of Strategic Studies” 2017, Vol. 40, No. 1–2, s. 102–103; J.S. Nye Jr., *Nuclear Lessons for Cyber Security?*, „Strategic Studies Quarterly” 2011, Vol. 5, No. 4, s. 21–23; P. Pijpers, K. Arnold, *Rethinking Cyber Deterrence*, „Journal of Strategic Security” 2025, Vol. 18, No. 1, s. 61, 66–68.

¹⁰⁵ R.S.S. Dewar, *The “Triptych of Cyber Security”: A Classification of Active Cyber Defence*, [w:] *2014 6th International Conference on Cyber Conflict*, P. Brangetto, M. Maybaum, J. Stinissen (eds.), Tallin 2014, s. 9–13.

¹⁰⁶ J. Burton, *The Future of Cyber Conflict Studies*, „The Cyber Defense Review” 2022, Vol. 7, No. 3, s. 104.

¹⁰⁷ S.B. Seagroatt, *Persistent Engagement and Defend Forward: the United States' Critical Role in Cyberspace*, [OMB 0704-0188] 2021, s. 1–4; Department of Defense, *Cyber Strategy*, 2018, s. 1–5, 7.

w ten sposób można uwzględnić zarówno uwarunkowania strategiczne, jak i poznawcze, regulacyjne czy techniczne, które będą kształtować charakter przyszłych konfliktów w cyberprzestrzeni¹⁰⁸. Jest to istotny krok naprzód względem dotychczasowego skupienia się na selektywnych obszarach, czy dominacji ujęcia technicznego. Często koncentrowano się na podatnościach, systemach informatycznych czy narzędziach obronnych jest istotne. Tymczasem cyberprzestrzeń to nie tylko infrastruktura, ale także przestrzeń rywalizacji poznawczej, prawnej i politycznej.

Z jednej strony, decyzje strategiczne podejmowane są w warunkach niepewności i dezinformacji, co wymaga uwzględnienia psychologii poznawczej, teorii decyzji i badań nad manipulacją informacją. Z drugiej — coraz częściej cyberdziałania balansują na granicy prawa międzynarodowego, czego nie sposób rozstrzygnąć bez analizy reżimów normatywnych i luk prawnych, np. w zakresie przypisywania odpowiedzialności czy proporcjonalności reakcji. Ponadto rozwój narzędzi opartych na sztucznej inteligencji i automatyzacji generuje nowe wyzwania etyczne i regulacyjne. Jednakże dopiero takie kompleksowe podejście pozwala wyjść poza paradygmat „cyberwojny” jako domeny wyłącz- nie ekspertów IT. Umożliwia ono analizę konfliktów jako złożonych zjawisk systemo- wych, w których splatają się cele strategiczne państw, możliwości technologiczne, struk- tury społeczne oraz mechanizmy percepcji i oddziaływania psychologicznego. Tylko in- tegrując te wszystkie wymiary — techniczny, normatywny, poznawczy i polityczny — można skutecznie modelować, przewidywać i przeciwdziałać przyszłym zagrożeniom w środowisku cyfrowym.

2.2.2. Przestrzeń informacyjna w ujęciu rosyjskim

W ujęciu rosyjskim, przestrzeń informacyjna — i w konsekwencji cyberprze- strzeń — jest uznawana za kluczową domenę dla operacji wojskowych nowej generacji¹⁰⁹. Stwierdzenie to opiera się na idei, że głównym polem bitwy jest umysł. Wojny nowej ge- neracji są zdominowane przez wojnę informacyjną i psychologiczną, mającą na celu mi- nimalizację użycia twardej siły militarnej. Obejmuje to skoordynowaną manipulację całą domeną informacyjną w celu stworzenia wirtualnej rzeczywistości¹¹⁰.

Koncepcja Rosyjska różni się zasadniczo od dominującej na Zachodzie wizji cy- berprzestrzeni. W doktrynie NATO i państw UE, cyberprzestrzeń rozumiana jest przede

¹⁰⁸ J. Burton, *The Future of Cyber Conflict...*, s. 114–115.

¹⁰⁹ В.Л. Черноперов, У.И. Сулейманова, *Гибридная война: предпосылки появления, концепции, сущность, цели, инструментарий, правовые вопросы, риски*, „Ноосферные исследования” 2021, Вып. 3, s. 39–42.

¹¹⁰ C.K. Bartles, *Getting Gerasimov Right*, „Military Review” 2016, No. Jan-Feb, s. 30–35.

wszystkim jako infrastruktura sieciowa i logiczna, będąca dodatkową domeną operacyjną obok lądu, morza, powietrza i przestrzeni kosmicznej. Zakłada się względną neutralność tej przestrzeni i stosunkowo czytelne kryteria naruszenia suwerenności lub dokonania aktu agresji (np. zniszczenie infrastruktury krytycznej)¹¹¹.

Rosja natomiast traktuje cyberprzestrzeń jako jeden z wymiarów znacznie szerszej przestrzeni informacyjnej, która obejmuje nie tylko systemy techniczne, ale również procesy poznawcze, media, kulturę i wartości społeczne. Celem działań w tej przestrzeni nie jest jedynie kontrola danych, lecz modyfikacja środowiska poznawczego przeciwnika, jego intencji i decyzji politycznych. Pozwala to traktować przestrzeń informacyjną jako strategicznie uprzywilejowane pola działania, umożliwiające realizację wielu celów państwowych bez konieczności konwencjonalnej konfrontacji zbrojnej.

Rosja wykorzystuje ofensywne operacje cybernetyczne i walkę elektroniczną jako narzędzia asymetryczne. Jednostki GRU (np. Fancy Bear¹¹²) i SWR (np. Nobelium¹¹³) prowadzą szeroki zakres cyberataków, które mogą mieć fizyczne skutki, takie jak zakłócanie infrastruktury krytycznej. Dlatego Gierasimow i inni teoretycy mówią o „długodystansowych, bezkontaktowych działaniach” jako głównym środku osiągnięcia celów. Cyberprzestrzeń, ze swoją zdolnością do atakowania krytycznych obiektów i systemów dowodzenia i kontroli (C2) przeciwnika na odległość, idealnie wpisuje się w tę koncepcję. Ta dominacja cyberprzestrzeni w asymetrycznej wojnie bezkontaktowej oznacza, że Rosja postrzega ją jako kluczowy obszar, w którym może zneutralizować przewagę technologiczną Zachodu, unikając jednocześnie bezpośredniej konfrontacji kinetycznej, która byłaby dla niej kosztowna¹¹⁴.

¹¹¹ N. Kushwaha, P. Roguski, B.W. Watson, *Up in the Air: Ensuring Government Data Sovereignty in the Cloud*, [w:] *12th International Conference on Cyber Conflict. 20/20 Vision: The Next Decade. Proceedings 2020*, T. Jančárková, L. Lindström, M. Signoretti, I. Tolga, G. Visky (eds.), Tallin 2020, s. 57–61.

¹¹² Grupa APT28 (znaną też jako Fancy Bear lub UAC-0001). Jej działalność przypisuje się rosyjskiej Jednostce 26165 z 85. Głównego Centrum Służb Specjalnych, działającego w ramach GRU (Głównego Zarządu Wywiadowczego). Odpowiedzialna jest m.in. za liczne operacje w Ukrainie; NSA, CISA, FBI, NCSC, *Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments*, [U/OO/158036-21, PP-21-0782] 2021, s. 1–5; NSA, FBI, *Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware*, [U/OO/160679-20, PP-20-0714], 2020, s. iii, 1–5.

¹¹³ Grupa APT29 (znaną też jako Nobeium, UNC3524). Jej działalność przypisywana jest rosyjskiej SWR (Służbie Wywiadu Zagranicznego Federacji Rosyjskiej); NSA, CISA, FBI, *Russian SVR Targets U.S. and Allied Networks*, [U/OO/132340-21, PP-21-0292], 2021, s. 1–3; NCSC, CISA, FBI, NSA, *Advisory. Further TTPs associated with SVR cyber actors*, [1.0] 2021, s. 2, 11; CERT NASK, NCSC, FBI, CISA, NSA, SKW, *Russian Foreign Intelligence Service (SVR) Cyber Actors Use JetBrains TeamCity CVE in Global Targeting*, [1.0] 2023, s. 3.

¹¹⁴ M. Kofman i inni, *Russian Military Strategy: Core Tenets and Operational Concepts*, [DRM-2021-U-029755], 2021, s. 72–77.

Powyższe podnosi znaczenie cyberbezpieczeństwa dla państw zachodnich, ponieważ atak na infrastrukturę informacyjną może mieć równie destabilizujące skutki jak tradycyjny atak wojskowy. Przykładami mogą być cyberataki na Estonię z 2007 roku¹¹⁵, czy kampanie dezinformacyjne w kontekście wyborów 2014-2016 (USA, Brexit, Francja, Czarnogóra, Czechy, UK, Hiszpania)¹¹⁶.

Federacja Rosyjska prezentuje zatem podejście „cybernetyczno-psychologiczne”, integrujące operacje w cyberprzestrzeni z działaniami wpływu i dezinformacją. Celem nie jest wyłącznie zakłócenie infrastruktury, lecz trwałe oddziaływanie na procesy decyzyjne i percepcję zagrożeń u przeciwnika, co wpisuje się w rosyjskie rozumienie „informacyjnego środowiska walki” (ang. information confrontation)¹¹⁷. Co istotne, w podejściu tym nie spotyka się wyraźnego rozróżnienia między czasem pokoju a wojny — działania informacyjne i cybernetyczne są prowadzone w sposób ciągły, co z perspektywy Zachodu utrudnia klasyfikację aktów agresji i reakcję w ramach prawa międzynarodowego¹¹⁸. Przykładem jest *Koncepcja działalności Sił Zbrojnych Federacji Rosyjskiej w przestrzeni informacyjnej* z 2011 roku¹¹⁹, która wskazuje, że wojna informacyjna to konfrontacja państw w celu zakłócenia systemów informacyjnych, destabilizacji struktur politycznych i społecznych, manipulacji psychologicznej oraz wymuszania korzystnych decyzji u przeciwnika¹²⁰. W tym ujęciu cyberprzestrzeń i przestrzeń informacyjna są tożsame z polem walki, w którym prowadzi się działania zakrojone na szeroką skalę — często skrycie i bez formalnego wypowiedzenia wojny.

Zarazem informacja sama w sobie staje się bronią. Już *Koncepcja bezpieczeństwa narodowego FR* z 2000 roku¹²¹ — i w sposób bardziej szczegółowy Doktryna bezpieczeń-

¹¹⁵ S. Haataja, *The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach*, „Law, Innovation and Technology” 2017, No. 9(2), s. 150–163.

¹¹⁶ V. Narayanan, P.N. Howard, B. Kollanyi, M. Elswah, *Russian Involvement and Junk News during Brexit*, [COMPROP D.M.2017.10, 2017, s. 1–4; V.C. Keating, O. Schmitt, *Ideology and influence in the debate over Russian election interference*, „International Politics” 2021, Vol. 58, No. 5, s. 3–10. E. Anderson, *State-Specific Vulnerabilities to Russian Influence: A Case Study of Montenegro*, Brno 2019, s. 28–29, 38–39.

¹¹⁷ E. Zinovyeva, *U.S. Digital Diplomacy: Impact on International Security and Opportunities for Russia*, „Security Index: A Russian Journal on International Security” 2013, Vol. 19, No. 2, s. 38; В. Герасимов, *Ценность науки в предвидении*, „Военно-промышленный курьер” 2013, № 8(476), s. 2–3.

¹¹⁸ I.N. Dylevsky, S.A. Komov, S.V. Korotkov, A.N. Petruinn, *Operations in Cyberspace: Theory, Politics, Law*, „Military Thought” 2011, Vol. 20, No. 3, s. 158–60.

¹¹⁹ Министерство Обороны Российской Федерации, *Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве*, Москва 2011.

¹²⁰ Tamże, s. 5.

¹²¹ *Концепция национальной безопасности Российской Федерации*, [в редакции Указа Президента Российской Федерации от 10 января 2000], Москва 2000.

stwa informacyjnego FR z 2016 roku¹²²) — definiowały zagrożenia dla Rosji właśnie z tej perspektywy. Dokumenty te zawierają rozbudowane katalogi zagrożeń technicznych (np. zakłócanie łączności, przechwytywanie danych), ale też zagrożeń moralno-społecznych, jak erozja duchowości, osłabianie potencjału kreatywnego społeczeństwa czy dekonstrukcja systemu wartości. Co istotne, strategia rosyjska oficjalnie przedstawiana jest jako defensywna i kooperacyjna — zakłada wzmocnienie regulacji wewnętrznych, ochronę infrastruktury krytycznej i współpracę międzynarodową w zwalczaniu „cyberterrorizmu”. Jednocześnie rosyjskie działania operacyjne (w tym dezinformacja, kampanie wpływu czy ataki cybernetyczne) wskazują na doktrynalne cele destabilizacji przeciwnika oraz poszerzania własnej swobody operacyjnej. Choć oficjalnie działania te są prowadzone tylko obronnie, to mogą być odpowiedzią na wpływ Zachodu na kulturę rosyjską (okcydentalizację). Tak szerokie ujęcie przesłanki sprawia jednak, że Rosja rości sobie prawo do stałego „przeciwdziałania” temu zagrożeniu, nie wykazując przy tym konkretnej metodologii. Podejście to jest kontynuowane w *Strategii bezpieczeństwa narodowego* FR z 2021 roku¹²³.

W zaktualizowanej w 2021 roku *Polityce międzynarodowego bezpieczeństwa informacyjnego*, Federacja Rosyjska utrzymała ciągłość celów i narzędzi znanych z wcześniejszych dokumentów strategicznych. Podkreślono znaczenie społeczno-politycznego wymiaru konfrontacji w przestrzeni cyfrowej, interpretowanej jako element trwającej wojny informacyjnej, rzekomo prowadzonej przez państwa Zachodu. W związku z tym uzasadniono potrzebę kontroli dostępu obywateli do niezależnych treści w przypadku zagrożenia destabilizacją wewnętrzną¹²⁴. Dokument wskazuje także na strategiczne znaczenie fragmentaryzacji globalnej sieci oraz aktywnego wpływu Rosji na międzynarodowe procesy regulacyjne. Prawa człowieka, w tym wolność informacji, nie są traktowane jako priorytet, co odróżnia tę politykę od standardów zachodnich¹²⁵. Wpisuje się to zatem we wcześniej omówioną koncepcję asymetrii strukturalnej.

Rosyjskie podejście do przyszłych konfliktów w cyberprzestrzeni opiera się na pojęciu *cyber grey zone* — szarej strefy, w której państwa realizują swoje cele strategiczne,

¹²² Доктрина информационной безопасности Российской Федерации, [утверждена Указом Президента РФ № 646 от 5 декабря 2016], Москва 2016.

¹²³ Стратегия национальной безопасности Российской Федерации, [утверждена Указом Президента Российской Федерации от 2 июля 2021].

¹²⁴ A. Legucka, Wojna w sieci. Polityka Rosji w zakresie międzynarodowego bezpieczeństwa informacyjnego, „Biuletyn PISM” 2021, nr 111 (2309), s. 1–2.

¹²⁵ В. Булва, Международная информационная безопасность: от классической к сетевой дипломатии России. „Вестник Санкт-Петербургского университета. Международные отношения” 2024, № 17(3), s. 325–341.

unikając otwartej wojny¹²⁶. Jest to zatem przedłużeniem aktualnego postrzegania roli środowiska sieciocentrycznego. Istotnym pozostaje takżeróżnienie między operacjami cyber-technologicznymi (np. sabotaż infrastruktury) a operacjami cyber-psychologicznymi, które koncentrują się na wpływaniu na opinię publiczną, dezorientowaniu przeciwnika i prowadzeniu kampanii dezinformacyjnych¹²⁷. Przykładowo, atak na ukraińską sieć energetyczną w 2015 roku, pozbawiający prądu ponad 230 tys. osób¹²⁸, czy czasowe odcięcie obywateli Ukrainy od Diia¹²⁹ (ukr. Дія) w 2022 roku¹³⁰, ilustrują zastosowanie cyber-sabotażu. Natomiast działania takie jak kampania propagandowa przed inwazją w 2022 roku¹³¹ świadczą o kluczowej roli psychologicznych narzędzi wpływu.

Zarazem Rosja nie traktuje cyberwojny jako autonomicznej domeny, lecz jako integralny komponent wojny informacyjnej, część szerszej strategii kształtowania percepcji przeciwnika. Kiedy Zachód koncentruje się na cyberatakach jako formie destrukcji infrastruktury, Rosja skupia się na manipulacji informacją i aktywności poznawczej¹³². Obie strony wykorzystują podobne techniki, jednak każda z nich kładzie nacisk na inny obszar. W tym kontekście działania Rosji można postrzegać jako bardziej złożone i subtelne — choć niekoniecznie skuteczne. Jak wskazują niektóre źródła, dotychczas działania te nie przyniosły Moskwie oczekiwanych efektów strategicznych, co doprowadziło ostatecznie do eskalacji konwencjonalnej w lutym 2022 roku¹³³. Tak jaskrawa ocena może jed-

¹²⁶ G. Colom-Piella, *Cyber activities in the grey zone: an overview of the Russian and Chinese approaches*, [w]: *The Complex and Dynamic Nature of the Security Environment*, F. Cîrciumaru, I. Cojocaru (eds.), Bucharest 2024, s. 189–191; R. Burkholder, *Tackling Russian Gray Zone Approaches in the Post–Cold War Era*, „Journal of Advanced Military Studies” 2023, Vol. 14, No. 2, s. 151–154, 159–161.

¹²⁷ N. Kostyuk, E. Gartzke, *Why Cyber Dogs Have Yet to Bark Loudly in Russia’s Invasion of Ukraine*, „Texas National Security Review” 2022, Vol. 5, No. 3, s. 115–121.

¹²⁸ CISA, *Cyber-Attack Against Ukrainian Critical Infrastructure*, [IR-ALERT-H-16-056-01], 2021.

¹²⁹ Diia (ukr. Дія) — ukraińska platforma cyfrowych dokumentów, odpowiednik polskiego mObywatela; O. Kolodiziev i inni, *Digital transformation as a tool for creating an inclusive economy in Ukraine during wartime*, „Problems and Perspectives in Management”, Vol. 22, No. 3, s. 440, 442.

¹³⁰ СБУ: *Наразі відновлено роботу 95% сайтів, що постраждали від кібератаки на державні ресурси*; 17 січня 2022, „Служба безпеки України”, <https://ssu.gov.ua/novyny/sbu-narazi-vidnovleno-robotu-95-saitiv-shcho-postrazhdaly-vid-kiberataky-na-derzhavni-resursy>, [odczyt: 12.07.2025]; *Кібератака на сайти державних органів*, 14 січня 2022, „CERT-UA”, <https://cert.gov.ua/article/17899>, [odczyt: 12.07.2025].

¹³¹ O. Polegkyi, *Russian disinformation and propaganda before and after the invasion of Ukraine*, „Rocznik Instytutu Europy Środkowo-Wschodniej” 2023, nr 21, z. 1, s. 94–98, 100; Y. Savelyev, *Untruthful claims, real war, dire consequences: understanding the narrative of the Russian invasion of Ukraine*, „Journal of Contemporary Central and Eastern Europe” 2023, Vol. 31, No. 2, s. 469–476.

¹³² D. Dziwisz, *Rethinking Future Conflicts: The Cyber Grey Zone From the Russian Perspective*, „Politeja” 2024, nr 5 (92), s. 295–296.

¹³³ Tamże, s. 287, I. Gridina, M. Bulyk, *Russian-ukrainian war: the way how the "Gray war" in the east of Ukraine turned into a large-scale "black" one*, „Sci. J. Cahul St. U. Bogdan Petriceicu Hasdeu” 2022, No. 1 (15), s. 27–31; F. dos Reis, J. Grzybowski, *Moving ‘redlines’: The Russian–*

nak wynikać ze ściśle zachodniego spojrzenia na konflikty w cyberprzestrzeni. Wyobrażając je sobie jako serie spektakularnych operacji na miarę Stuxnet¹³⁴, wówczas rzeczywiście, wyniki zdają się być rozczarowujące. Jednakże spojrzenie z perspektywy rosyjskiej pozwala dostrzec synergę pomiędzy operacjami w cyberprzestrzeni (wojskowymi, działaniami służb specjalnych), działaniami politycznymi oraz kinetycznym wykorzystaniem sił zbrojnych. Co więcej, przedsięwzięcia w środowisku sieciocentrycznym budują stale powiększający się kapitał Rosji w zakresie wykorzystania złośliwego oprogramowania i technik cyberataków. Przyznają to zarówno źródła państwowe¹³⁵, jak i raporty sektora prywatnego¹³⁶, wskazując na m.in. liczne zakłócenia funkcjonowania ukraińskiej administracji i mediów, czy inne działania skierowane przeciwko Zachodowi. Dalsza intensyfikacja takich działań — choć daleka od popkulturowej wizji cyberwojny — może prowadzić do poważnych reperkusji i wzmacniania potencjału Federacji Rosyjskiej w środowisku sieciocentrycznym.

2.2.3. Chińskie koncepcje wykorzystania cyberprzestrzeni w konfliktach

Chiny traktują cyberprzestrzeń jako przedłużenie przestrzeni fizycznej, co implikuje konieczność obrony suwerenności i integralności państwa także w wymiarze cyfrowym. Stąd wynika dążenie do ustanowienia normy „suwerenności cybernetycznej”, która ma legitymizować działania państwa w zakresie kontroli treści i infrastruktury w internecie. W tym ujęciu cyberprzestępczość obejmuje nie tylko oszustwa czy handel narkotykami, lecz także treści uznane za zagrażające stabilności politycznej, w tym separatyzm, subwersję czy ekstremizm ideologiczny — kategorie często określane zbiorczo jako „terrorystyczne”¹³⁷. Chińska koncepcja walki w cyberprzestrzeni wywodzi się z szerszego ujęcia „bezpieczeństwa informacji” (chin. xinxī anquán — 信息安全). Wskazuje ono, że kluczowym aspektem cyberprzestrzeni nie jest wyłącznie obrona przed atakami na infra-

Ukrainian war and the pragmatic (mis-)use of international law, „Global Constitutionalism” 2024, Vol. 13 No. 2, s. 329–331.

¹³⁴ J.P. Farwell, R. Rohozinski, Stuxnet and the Future of Cyberwar, „Survival” 2011, Vol. 53, No. 1, s. 25–29.

¹³⁵ FBI, CISA, NSA i inni, *Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure*, [AA24-249A], 2024, s. 1–16; NSA, FBI, NCSC i inni, *Russian GRU Targeting Western Logistics Entities and Technology Companies*, [U/OO/157019-25, PP-25-2107], 2025, s. 1–4, 8–9.

¹³⁶ Microsoft, *Defending Ukraine: Early Lessons from the Cyber War*, [Report 22.06], 2022, s. 5–16; Unit42, *Russia-Ukraine Cyberattacks (Updated): How to Protect Against Related Cyberthreats Including DDoS, HermeticWiper, Gamaredon, Website Defacement, Phishing and Scams*, 22 February 2022, „Paloalto Networks”, <https://unit42.paloaltonetworks.com/preparing-for-cyber-impact-russia-ukraine-crisis/> [odczyt: 18.07.2025]; ESET Research, *APT Activity Report*, [OCT24-MAR25], 2025, s. 19–23.

¹³⁷ D. Broeders, L. Adamson, C. Creemers, *A coalition of the unwilling? Chinese and Russian perspectives on cyberspace*, [The Hague Program For Cyber Norms Policy Brief], Leiden 2019, s. 2–4.

strukturę, lecz ochrona suwerenności państwa poprzez kontrolę nad treścią i przepływem informacji. Jest to zatem podejście bliskie rosyjskiemu.

Podobieństw doszukiwać się można także w uzasadnieniu podjęcia działań w cyberprzestrzeni. Chiny wskazują na potencjalne zagrożenie wynikające z manipulacji informacją, zwłaszcza przez „wrogie siły zagraniczne”. Postrzegają to jako element wojny ideologicznej oraz prób destabilizacji ustroju poprzez media i platformy społecznościowe. W odpowiedzi na zagrożenia, Chiny deklarują prawo do stosowania tzw. „aktywnej obrony”, czyli działań wyprzedzających lub ofensywnych w celu neutralizacji wrogich operacji w cyberprzestrzeni¹³⁸.

Stąd rozwój i implementacja systemu filtrowania treści znanego jako Wielki Firewall Chin, mającego na celu zabezpieczenie przestrzeni informacyjnej przed niepożądanym wpływem. Jest to złożony system filtracji ruchu sieciowego, łączący standardowe techniki cenzury (m.in. filtrowanie adresów IP, resetowanie połączeń TCP) z bardziej wyrafinowanymi rozwiązaniami, takimi jak filtrowanie zawartości zapytań HTTP oraz analiza pakietów na poziomie warstwy aplikacyjnej. W szczególności system jest zdolny do inspekcji nagłówków HTTP i rozłączania połączeń, gdy wykryje frazy zakazane¹³⁹. Co istotne, blokady te nie są „sztywne”, często skutkując opóźnieniem lub niejednoznaczną reakcją, co może mylić użytkownika i zniechęcać do dalszego próbowania. Taka taktyka pozwala nie tylko odciąć dostęp, lecz także modelować zachowania użytkowników poprzez demotywację¹⁴⁰. Funkcjonalność ta uchodziła za jedną z najbardziej zaawansowanych już w pierwszej dekadzie XXI wieku, z czasem tylko zyskując na wyrafinowaniu i skuteczności.

Chińskie rozumienie operacji w cyberprzestrzeni wpisuje się w koncepcję „sieciowej potęgi państwa” (chin. wangluo qiangguo — 网络强国), łącząc rozwój technologii informatycznych z celami politycznymi i gospodarczymi. Głównym celem jest osiągnięcie światowego przywództwa w kluczowych sektorach takich jak sztuczna inteligencja czy półprzewodniki, a także zmniejszenie zależności od technologii amerykańskiej. Elementem tak budowanej strategii jest także cyfrowy komponent inicjatywy Pasa i Szlaku (tzw. Cyfrowy Jedwabny Szlak), mający na celu globalną ekspansję chińskiej infrastruktury cyfrowej¹⁴¹.

¹³⁸ Tamże.

¹³⁹ R. Ensafi, P. Winter, A. Mueen, J.R. Crandall, *Analyzing the Great Firewall of China Over Space and Time*, „Proceedings on Privacy Enhancing Technologies” 2015, No. 1, s. 63–68.

¹⁴⁰ R.C. Steven, S.J. Murdoch, R.N.M. Watson, *Ignoring the Great Firewall of China*, „Journal of Law and Policy for the Information Society” 2007, Vol. 3, No. 2, s. 289–291.

¹⁴¹ M.S. Erie, T. Streinz, *The Beijing Effect: China's Digital Silk Road as Transnational Data*

Należy jednak podkreślić, że podejście to postrzegać można jako próbę zrozumienia zachodnich oraz koncepcji rosyjskich, jak również odpowiedź na „wojnę hybrydową”. „Sieciowa potęga państwa” pojawiła się po raz pierwszy w 2014 roku, w czasie tworzenia Centralnej Grupy Wiodącej ds. Cyberbezpieczeństwa i Informatyzacji¹⁴², pełniąc wówczas pojemną funkcję — parasola, pod którym rozumiano wiele konceptów. Podejście to utwierdził sam Xi Jinping, przemawiając podczas konferencji roboczej ds. cyberbezpieczeństwa i informatyzacji w 2016 roku¹⁴³. I choć wraz z następnymi latami koncepcja ta zyskiwała na politycznym znaczeniu, to jej strategiczna wartość pozostała wątpliwa. Prawdopodobnie przez podobny efekt jak w przypadku wojny hybrydowej — uniwersalność, świeżość i medialną nośność — liczne źródła zaczęły traktować „sieciową potęgę państwa” jako istotny element Chińskiej działalności w cyberprzestrzeni, a nawet jako strategię¹⁴⁴.

Krytyczny głos wyrażony został m.in. w artykule *“Digital Silk Road” as a Slogan Instead of a Grand Strategy*¹⁴⁵. Jego autorzy podkreślają, że chińskie podejście do cyfryzacji — choć zakorzenione w języku strategicznym — jest w rzeczywistości fragmentaryczne, reaktywne i często motywowane względami propagandowymi lub oportuniźmem, a nie przemyślaną długofalową strategią. Mimo narracji o globalnym przywództwie technologicznym, praktyka działań chińskich raczej potwierdza chaotyczny charakter realizacji Cyfrowego Jedwabnego Szlaku¹⁴⁶. Autorzy krytycznie odnoszą się również do struktury decyzyjnej, zarówno w sektorze publicznym, jak i prywatnym. Brak centralnego nadzoru i wyraźnych priorytetów powoduje, że wiele inicjatyw cyfrowych Chin rozmywa się w praktyce, stając się bardziej lokalnymi eksperymentami niż częścią spójnego modelu ekspansji technologicznej. W efekcie „sieciowej potęgi państwa” rozmywa się

Governance, „Journal of International Law and Politics” 2021, Vol. 54, No. 1, s. 48–53.

¹⁴² R. Creemers, *Xi Jinping’s Speech at the National Cybersecurity and Informatization Work Conference*, 22 April 2018, „Digichina — Stanford Cyber Policy Center”, <https://digichina.stanford.edu/work/xi-jinpings-speech-at-the-national-cybersecurity-and-informatization-work-conference/> [odczyt: 18 maja 2024].

¹⁴³ X. Jinping, *Speech at the Work Conference for Cybersecurity and Informatization* [在网络安全和信息化工作座谈会上的讲话], 19 April 2016, The State Council PRC [中华人民共和国中央人民政府].

¹⁴⁴ D. Lewis, *China’s Global Internet Ambitions: Finding Roots in ASEAN*, „ICS” 2017, No. 14, s. 3–7; D. Broeders, L. Adamson, R. Creemers, *Coalition of the Unwilling...*, s. 3; E. La Bruyère, *The Network Great-Power Strategy: A Blueprint for China’s Digital Ambitions*, „Asia Policy” 2021, Vol. 16, No. 2, s. 5–12; D. Pan, *Storing data on the margins: making state and infrastructure in Southwest China*, „Information, Communication & Society” 2022, Vol. 25, Issue 16, s. 2413–2418.

¹⁴⁵ J. Cheng, J. Zeng, *“Digital Silk Road” as a Slogan Instead of a Grand Strategy*, „Journal of Contemporary China” 2024, Vol. 33, No. 149.

¹⁴⁶ Tamże, s. 824–825.

wśród innych sloganów oraz propagandowych ambicji, co stawia pod znakiem zapytania jej trwałość jako narzędzia geostrategicznego¹⁴⁷.

Szersza analiza źródeł wykazała jednak wyraźny trend zmian w postrzeganiu operacji w cyberprzestrzeni przez Chińską Armię Ludowo-Wyzwoleńczą (ALW). Transformacja strategii obronnej uwzględniała dynamiczne rozszerzenie roli technologii informacyjnych jako kluczowego komponentu siły militarnej. Począwszy od lat 90., Chiny przesuwały uwagę z konfliktów lądowych na operacje w warunkach wysokiej technologii¹⁴⁸. Coraz silniej podkreślano potrzebę dominacji w nowych domenach — przestrzeni kosmicznej i cybernetycznej — traktowanych jako strategiczne pola walki. Wyróżnić tu należy kolejne białe księgi (z 2013¹⁴⁹, 2015¹⁵⁰ i 2023¹⁵¹ roku), czy ustawę o cyberbezpieczeństwie z 2016¹⁵² roku. Towarzyszyło temu utworzenie w 2015 roku kolejnego komponentu ALW — Sił Wsparcia Strategicznego (chin. Zhanlue zhiyuan budui — 战略支援部队), który miał na celu scentralizowanie zdolności w zakresie wojny elektronicznej, cyberoperacji i operacji informacyjnych¹⁵³. Reforma ta była częścią szerszego procesu profesjonalizacji i unowocześnienia sił zbrojnych, z naciskiem na szybkie, zintegrowane działania w domenie cyfrowej. Rozwój zdolności w zakresie cyberprzestrzeni traktowany jest jako nieodzowny element koncepcji „obrony aktywnej”, umożliwiający działania uprzedzające, zakłócanie serwerów dowodzenia i kontroli (C2) przeciwnika, jak również realizację celów strategicznych bez fizycznej konfrontacji. W 2024 roku ALW przeszła restrukturyzację, a w miejsce SWS powołano nowe, niezależne komponenty: Siły Kosmiczne (chin. Junshì hangtian budui — 军事航天部队), Siły Wsparcia Informacyjnego (chin. Xinxi zhiyuan budui — 信息支援部队) oraz Siły Cyberprzestrzenne (chin. Wangluo kongjian

¹⁴⁷ Tamże, s. 829–831, 837.

¹⁴⁸ U.S Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2020*, Virginia 2020, s. 27; S.B. Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, McLean 2009, s. 10–12.

¹⁴⁹ State Council Information Office of the People's Republic of China [中华人民共和国国务院新闻办公室], *White Paper: The Diversified Employment of China's Armed Forces [中国武装力量的多样化运用]*, Beijing 2013, s. 4–5.

¹⁵⁰ State Council Information Office of the People's Republic of China [中华人民共和国国务院新闻办公室], *White Paper: China's Military Strategy [中国的军事战略]*, Beijing: 2015, s. 6, 11, 16–17.

¹⁵¹ State Council Information Office of the People's Republic of China [中华人民共和国国务院新闻办公室], *White Paper: China's Law-Based Cyberspace Governance in the New Era [新时代的中国网络法治建设]*, Beijing 2023, s. 1–3.

¹⁵² Zob. *Cybersecurity Law of the People's Republic of China [中华人民共和国网络安全法]*, [promulgated by the Standing Committee of the National People's Congress, Nov. 7, 2016, effective Jun. 1, 2017].

¹⁵³ K.L. Pollpeter, M.S. Chase, E. Heginbotham, *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations*, Santa Monica 2017, s. 1–3, 21–24.

budui — 网络空间不对). Dowodzi to powagi, z jaką potraktowano zarówno środowisko sieciocentryczne.

Chińska wizja obronności w erze informacyjnej koncentruje się na przejściu od siły liczebnej do przewagi systemowej opartej na informatyzacji, autonomii technologicznej i integracji cyberprzestrzeni z konwencjonalnymi domenami działań wojennych. W tym kontekście cyberprzestrzeń jawi się nie tylko jako przestrzeń operacyjna, ale także jako warstwa umożliwiająca uzyskanie przewagi strategicznej bez uciekania się do otwartego konfliktu.

Aktualnie chińskie operacje cybernetyczne koncentrują się głównie na celach ekonomicznych, takich jak kradzież własności intelektualnej czy danych biznesowych¹⁵⁴. Jednak w sytuacjach uznanych za zagrożenie dla kluczowych interesów narodowych — jak np. protesty w Hongkongu czy wybory na Tajwanie¹⁵⁵ — Pekin angażuje się także w działania dezinformacyjne oraz ataki techniczne (np. operacja Great Cannon skierowana przeciwko platformie GitHub¹⁵⁶).

Chińska perspektywa przyszłych konfliktów w cyberprzestrzeni, przedstawiona m.in. w raporcie *A Chinese Perspective on the Future of Cyberspace*¹⁵⁷, opiera się na wizji cyberprzestrzeni jako areny nie tylko rywalizacji technologicznej, lecz przede wszystkim ideologicznej, w której kształtuje się nowy ład globalny. Chińskie elity polityczne postrzegają kontrolę nad informacją jako kluczowy element suwerenności narodowej¹⁵⁸ i dążą do redefinicji zasad rządzących internetem. Nacisk położony jest na „cyber suwerenność”, czyli prawo państw do zarządzania własnym segmentem internetu bez zewnętrznej ingerencji.

Chińskie plany dotyczące cyberprzestrzeni obejmują nie tylko wzmacnianie zdolności obronnych wobec cyberataków, ale także budowę alternatywnej infrastruktury informacyjnej, opartej na chińskich technologiach i normach. Przykładem może być pro-

¹⁵⁴ NSA, CISA, FBI, *Chinese State-Sponsored Cyber Operations: Observed TTPs*, [U/OO/163624-21, PP-21-0971] 2021, s. 6–30; HC3, *Threat Profile: China-Based Threat Actors*, [202308161700] 2023, s. 6.

¹⁵⁵ J. Wu, *More than sharp power: Chinese influence operations in Taiwan, Hong Kong and beyond*, [w:] *China's Influence and the Center-periphery Tug of War in Hong Kong, Taiwan and Indo-Pacific*, B.C.H. Fong, J. Wu, A.J. Nathan (eds.), London 2020, s. 24–30; M.B. Manantan, *The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea*, „Issues & Studies: A Social Science Quarterly on China, Taiwan, and East Asian Affairs” 2020, Vol. 56, No. 3, s. 10–15.

¹⁵⁶ Zob. B. Marczak i inni, *An Analysis of China's "Great Cannon"*, [referat konferencyjny] *5th USENIX Workshop on Free and Open Communications on the Internet*, Washington 2015.

¹⁵⁷ X. Peixi, *A Chinese Perspective on the Future of Cyberspace*, [Cyberstability Paper Series, GCSC, HCSS], 2021.

¹⁵⁸ Tamże, s. 5–7.

mowanie koncepcji „Community of Shared Future”¹⁵⁹, która zakłada utworzenie globalnego ładu informacyjnego opartego na współpracy państw o podobnych wartościach — często w opozycji do zachodniego modelu otwartego internetu. Zarazem celem Chin nie jest cyberwojna jako taka, ale przekształcenie cyberprzestrzeni w narzędzie służące długofalowemu wpływowi geopolitycznemu¹⁶⁰.

W przeciwieństwie do Rosji, której strategia koncentruje się na działaniach destrukcyjnych, asymetrycznych i psychologicznych¹⁶¹, Chiny stawiają na długoterminowe kształtowanie architektury cyberprzestrzeni i jej regulacji. O ile Rosja wykorzystuje cyberprzestrzeń jako pole manewru w konfliktach szaro-strefowych, Chiny traktują ją jako „strategiczną domenę współpracy i rywalizacji” z naciskiem na instytucjonalne formy wpływu — np. w ramach struktur ONZ czy International Telecommunication Union (ITU)¹⁶². Istnieje jednak wspólna płaszczyzna: zarówno Rosja, jak i Chiny odrzucają zachodni uniwersalizm cyfrowy oraz obawiają się anglosaskiej dominacji nad infrastrukturą internetu¹⁶³. Szczegółne zastrzeżenie pojawia się jednak przy ocenie możliwości Pekinu. Choć chiński rozwój technologiczny jest imponujący, tak przyjęty model rozwoju oparty na kontroli i cenzurze może ograniczać innowacyjność oraz elastyczność w przypadku nieprzewidywalnych zagrożeń¹⁶⁴. W praktyce oznacza to, że chociaż Chiny mają ogromne możliwości technologiczne i polityczne (np. wpływ na globalne standardy 5G czy AI), ich strategia może okazać się mniej skuteczna w reagowaniu na szybko zmieniające się wyzwania cyberwojenne — co odróżnia ją od bardziej chaotycznego, ale też elastycznego podejścia rosyjskiego.

2.2.4. Udział podmiotów pozapaństwowych w konfliktach w cyberprzestrzeni

W erze cyfrowej asymetria podmiotów w konfliktach nabiera wyjątkowego znaczenia. Tradycyjna analiza sił zbrojnych opierała się na relatywnie symetrycznych porów-

¹⁵⁹ R.J.E.H. Creemers, F.N. Pieke, K. Iwabushi, *Common destiny in cyberspace: China's cyber diplomacy*, [w]: *The Global Square*, F.N. Pieke, K. Iwabushi (eds.), Berkeley 2021, s. 263–269; F. Zheng, G. Di, *Global Cyber Governance in China: Towards Building a Community of Shared Future in Cyberspace*, „Science, Technology and Society” 2022, Vol. 27, Issue 3, s. 460–467.

¹⁶⁰ P.S. Tona, *An Overview of China's Development in Cyberspace*, „International Journal of Cyber Diplomacy” 2024, Vol. 5, s. 42, 45–49; H. Liu, C. Miao, *Digital Geopolitics in a VUCA World: China Encounters a New Global Order*, „Global Policy” 2024, Vol. 15, Issue 56, s. 70–75.

¹⁶¹ D. Dziwisz, *Rethinking Future Conflicts...*, 295–299.

¹⁶² R.A. Hulvey, *Cyber Sovereignty: How China is Changing the Rules of Internet Freedom*, „IGCC” 2021, No. 2, s. 30–32, 38.

¹⁶³ G.J. Moore, *Huawei, Cyber-Sovereignty and Liberal Norms: China's Challenge to the West/Democracies*, „Journal of Chinese Political Science” 2023, Vol. 28, s. 151–163.

¹⁶⁴ M. Chansoria, *Defying Borders in Future Conflict in East Asia: Chinese Capabilities in the Realm of Information Warfare and Cyber Space*, „Journal of East Asian Affairs” 2012, Vol. 26, No. 1, s. 116–120.

naniach potencjału państwowego, podczas gdy w cyberprzestrzeni kluczowymi aktorami mogą być także niewielkie, elitarne grupy pozapaństwowe dysponujące relatywnie skromnymi zasobami, lecz wysoką specjalizacją techniczną i zdolnością do szybkiego działania. Małe zespoły hakerskie mogą dzięki znajomości specyfiki sieci, narzędzi automatyzacji i usług w chmurze prowadzić operacje o zasięgu globalnym, a ich działania często wykraczają poza granice tradycyjnej prywatności i jurysdykcji.

Atak ransomware na Colonial Pipeline w maju 2021 r. przeprowadzony przez DarkSide¹⁶⁵ ujawnił, że grupa złożona z kilkudziesięciu osób może zakłócić krytyczną infrastrukturę energetyczną i wywołać przerwy w dostawach paliw na południowym wschodzie USA¹⁶⁶. Efektem było wstrzymanie działalności zaatakowanego rurociągu (od 7 do 12 maja), co doprowadziło do paniki zakupowej i gwałtownego wzrostu cen benzyny. Pełną sprawność operacyjną przedsiębiorstwo odzyskało jednak dopiero 15 maja¹⁶⁷. Podobnie REvil¹⁶⁸, działając w czerwcu 2021 r., sparaliżowało ponad sto przedsiębiorstw poprzez podatności w oprogramowaniu Kaseya (CVE-2021-30116), które wykorzystywane było wówczas przez ponad 30 tysięcy dostawców usług dla od 800 tysięcy do 1 miliona podmiotów¹⁶⁹. Łączna wartość okupów wyniosła ponad 70 milionów USD¹⁷⁰. Największą sumę zapłaciło przedsiębiorstwo JBS Foods (amerykański oddział brazylijskiego JBS S.A.) — równowartość 11 milionów USD w Bitcoinach¹⁷¹. Analogicznie, atak na SolarWinds, przeprowadzony od września 2019 roku do marca 2020, stanowi przykład wysoce zaawansowanego ataku na łańcuch dostaw. Adwersarze¹⁷² zainfekowali oprogramowanie

¹⁶⁵ DarkSide — grupa hakerska, która opracowała złośliwe oprogramowanie RaaS — Ransomware as a Service — pod tą samą nazwą. Od 2020 roku prowadziła działania wymierzone w liczne przedsiębiorstwa charakteryzujące się dużymi obrotami; CISA, *DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*, [AA21-131A], 2021.

¹⁶⁶ L.P. Bradley, *Was the Colonial Cyberattack the First Act of Cyberwar Against the U.S.? Finding the Threshold of War for Ransomware Attacks*, „St. John's Law Review” 2022, Vol. 96, No. 2, s. 488–499, 509–514.

¹⁶⁷ J.R. Redeer, T. Hall, *Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack*, „Cyber Defense Review” 2021, Vol. 6, No. 1, s. 16–19, 31–33.

¹⁶⁸ REvil (znana także jako Sodinokibi) — grupa hakerska działająca najaktywniej w latach 2020–2021 (w 2021 roku będąc drugą najaktywniejszą grupą propagującą ransomware na świecie); Unit42, *2022 Ransomware Threat Report*, Santa Clara 2022, s. 16.

¹⁶⁹ S. Buhnia, M. Blackert, H. Deal, A. DePero, A. Patra, *Analyzing the 2021 Kaseya Ransomware Attack: Combined Spearphishing Through SonicWall SSLVPN Vulnerability*, „IET Information Security” 2025, Issue 1, s. 1–3.

¹⁷⁰ L. Iamandi, I.V. Virgolici, A.M. Ioniță, A. Drăgănescu, *Malicious Cyber Attacks*, „Journal of Danubian Studies and Research” 2022, Vol. 12, No. 1, s. 376.

¹⁷¹ G. Tielidze, *Russia's Changed Attack Tactics and Vectors in Cyberspace*, „Rondeli Foundation Expert Opinion” 2021, No. 171, s. 5.

¹⁷² Choć początkowa atrybucja była niejasna, to finalnie adwersarze zostali zidentyfikowani jako Nobelium (najczęściej spotykana nazwa, nadana przez Microsoft), alternatywnie: APT29 lub Cozy Bear. Łączy się ją z działalnością Służby Wywiadu Zagranicznego Federacji Rosyjskiej; A. Sisoyan, *New cybersecurity challenges: digital transformation and the political implications of their*

Orion — używane przez ponad 18 tysięcy podmiotów, w tym instytucje rządowe i firmy z sektora prywatnego — ukrytym kodem malware o nazwie Sunburst. Atak wyróżniał się wyjątkową precyzją: kod był testowany miesiącami, by pozostać niewykrywalnym przez systemy bezpieczeństwa, umożliwiając dostęp do danych i zdalne sterowanie systemami ofiar. Część organizacji wskazała, że skutki finansowe sięgały średnio 11% rocznych przychodów, a ponad 80% respondentów potwierdziło wzrost świadomości bezpieczeństwa po incydencie, co doprowadziło do większej współpracy międzysektorowej¹⁷³. SolarWinds odpowiedziało serią poprawek oraz zmianą mechanizmów aktualizacji, ale atak ukazał, jak głęboko zakorzenione ryzyko wiąże się z zaufaniem do dostawców oprogramowania infrastrukturalnego.

Powyższe ukazuje dwa zasadnicze problemy bezpieczeństwa w cyberprzestrzeni. Pierwszym z nich jest nieprzewidywalność środowiska, budująca głęboką niepewność. O ile bowiem działania państw dają się analizować, wpisywać w racje stanu, generalne strategie czy pewien racjonalizm, o tyle podmioty pozapaństwowe zwykle takiej możliwości nie dają. Nowe grupy hakerskie pojawiają się w sposób nieskoordynowany, konkurują między sobą lub współpracują bez szczególnych wzorców. Co więcej, brak właściwego scentralizowania badań ma własne reperkusje. Praca wielu podmiotów (często prywatnych) jest dublowana, a jej wyniki są trudne w porównywaniu. Najlepszym przykładem tego są próby identyfikacji adversarzy. Właściwie każde centrum badawcze stosuje własną nomenklaturę, często utrudniając szybkie przetwarzanie informacji. I choć zaobserwować można pierwsze próby ujednolicania taksonomii, to są one dalece niewystarczające¹⁷⁴. Kolejną istotną przeszkodą jest sama skuteczność identyfikacji. Ujęcie ataków na SolarWinds w niniejszej części rozdziału może być kwestionowane. Zależnie od źródeł, grupa Nobelium jest uważana albo za część struktur Służby Wywiadu Zagranicznego Federacji Rosyjskiej, za pozostającą pod jej wpływem, lub tylko powiązaną i wciąż realizującą własne cele¹⁷⁵. Nie pomaga też fakt, iż działalność państw w środowisku sieciocen-

implementation, „Journal of Political Science: Bulletin of Yerevan University” 2025, Vol. 4, No. 1(10), s. 114; NSA, CISA, FBI, *Russian SVR Targets U.S. and Allied Networks*, [U/OO/132340-21, PP-21-0292], 2021, s. 1–3.

¹⁷³ J. Martinez, J.M. Durian, *Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study*, „International Journal of Safety and Security Engineering” 2021, Vol. 11, No. 5, s. 539–540, 543; E.E. Chinwe, C.E. Alozie, *Adversarial Tactics, Techniques, and Procedures (TTPs): A Deep Dive into Modern Cyber Attacks*, „IRE Journals” Vol. 8, Issue 7, s. 554–557.

¹⁷⁴ Przykładem jest współpraca Microsoftu i CrowdStrike, zmierzająca do harmonizacji taksonomii adversarzy w cyberprzestrzeni; *How Microsoft names threat actors*, 31 July 2025, „Microsoft”, <https://learn.microsoft.com/en-us/unified-secops-platform/microsoft-threat-actor-naming> [odczyt: 01.08.2025].

¹⁷⁵ K. Zettl-Schabath, J. Bund, T. Gschwend, C. Borrett, *Advanced Threat Profile. APT29 — Stealth at Scale*, „European Repository of Cyber Incidents” 2023, 23 February, s. 1–3.

trycznym często wykorzystuje te same techniki i złośliwe oprogramowanie, co niezrzeszone grupy hakerskie oraz szeroko rozumiana cyberprzestępczość zorganizowana.

Stanowi to źródło asymetrii informacyjnej między podmiotami. Cele ataków są z reguły znane publicznie (w sensie identyfikacji), a wykorzystywane przez nich oprogramowanie albo jest informacją jawną, albo możliwą do wykrycia przed atakiem¹⁷⁶. W efekcie adversarze mogą planować działania z dużym wyprzedzeniem, zdobywając istotne informacje o swoim celu i zależnych podmiotach. Alternatywnie, ataki niejednokrotnie przeprowadzane są ad hoc, tam gdzie pojawi się taka sposobność. 28,3% podatności jest z powodzeniem wykorzystywana w ciągu mniej niż 24 godzin od opublikowania informacji na ich temat¹⁷⁷. Zarazem z punktu widzenia potencjalnych celów, adversarze identyfikowani mogą być tylko na podstawie przesłanek, często niejasnych informacji ze skanów urządzeń brzegowych lub dedykowanych pułapek wykrywających próby uzyskania nieautoryzowanego dostępu (tzw. honeypot). Niemal zawsze stawia to atakującego w dużo lepszej pozycji niż stronę broniącą się.

Co więcej, małe zespoły hakerskie często wykorzystują techniki „living off the land” (LotL). Zamiast używać zewnętrznego, złośliwego oprogramowania, a tym samym ryzykować wykrycie, atakujący bazują na legalnych i już obecnych w systemie komponentach operacyjnych. Celem LotL jest ukrycie działalności przed systemami wykrywania zagrożeń oraz maksymalna adaptacja do środowiska ofiary przy minimalnym śladzie. Wpisuje się w szerszy trend „systemowego survivalizmu”, w którym adversarz działa niejako jako pasożyt wykorzystujący organizm celu do własnych celów, nie wprowadzając do niego niczego obcego, co mogłoby zostać szybko zidentyfikowane¹⁷⁸. Ponadto wzrost dostępności narzędzi opartych na uczeniu maszynowym i automatyzacji pozwala na samonapędzające się kampanie rozprzestrzeniania się złośliwego kodu, mobilizujące zasoby chmurowe w charakterze „botnetów” tymczasowych, co zwiększa skalę i szybkość działań asymetrycznych.

Ataki hakerskie często łączone są z kampaniami dezinformacyjnymi, realizowanymi w mediach społecznościowych i za pomocą botów sieciowych. Przykładem może być, grupa Ghostwriter, prawdopodobnie działająca na rzecz rosyjskich i białoruskich

¹⁷⁶ W. Steingartner, D. Galinec, A. Kozina, *Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model*, „MDPI Symmetry”, 2021, No. 13, s. 4–8. 18–20.

¹⁷⁷ Zob. P. Garrity, *2025 Q1 Trends in Vulnerability Exploitation*, 24 April 2025, „Vuln Check” <https://www.vulncheck.com/blog/exploitation-trends-q1-2025> [odczyt: 20.07.2025].

¹⁷⁸ F. Barr-Smith, X. Ugarte-Pedrero, M. Graziano, R. Spolaor, I. Martinovic, *Survivalism: Systematic Analysis of Windows Malware Living-Off-The-Land*, [w:] *2021 IEEE Symposium on Security and Privacy (SP)*, L. O’Conner (ed.), Los Alamitos 2021, s. 1557–1560.

służb specjalnych¹⁷⁹. W 2022 r. rozsyłała ona spreparowane materiały mające podważyć zaufanie obywateli do procesów wyborczych w Niemczech i Łotwie¹⁸⁰. Takie działania pokazują, że ataki poznawcze są równie ważne jak techniczne, ponieważ mogą osłabić odporność społeczną i decyzje polityczne bez konieczności fizycznego naruszenia infrastruktury. Innym przykładem jest grupa Lizard Squad, która w 2014 roku przeprowadziła skoordynowane ataki DDoS na sieci PlayStation Network i Xbox Live, doprowadzając do wielodniowych przerw w dostępie do usług i wywołując falę krytyki pod adresem zarządów obu korporacji¹⁸¹. Choć atak nie zaowocował włamywaniem się do baz danych, to jednak skutecznie zachwiał wizerunkiem dostawców usług rozrywki online, a wiele osób zaczęło kwestionować ich zdolność do ochrony własnych systemów. Podobnie w 2015 roku, w wyniku ataku opublikowano wewnętrzne e-maile włoskiej firmy Hacking Team, specjalizującej się w sprzedaży oprogramowania do inwigilacji państwowej. Ujawnienie korespondencji z reżimami łamiącymi prawa człowieka spowodowało lawinę protestów społecznych oraz utratę kontraktów z licznymi rządami, co w efekcie doprowadziło do niemalże bankructwa przedsiębiorstwa¹⁸². Działania te wskazują, jak duży wpływ mogą osiągać grupy hakerskie, także w wywieraniu nacisków politycznych i zmiany praktyk biznesowych. Z tego względu adversarze coraz częściej łączą działania techniczne z precyzyjną operacją medialną.

Przeciwdziałanie powyższym zagrożeniom wymaga podejścia holistycznego, tj. obejmującego poziom sektora prywatnego, państwowego i współpracy międzynarodowej, jak również komplementarnego, czyli poruszającego najistotniejsze aspekty budowy bezpieczeństwa. Kluczową inicjatywą w tym zakresie jest Dyrektywa NIS2, przyjęta przez Parlament Europejski i Radę Unii Europejskiej w grudniu 2022 roku, będącej rozszerzeniem i wzmocnieniem wcześniejszych regulacji w zakresie bezpieczeństwa sieci i systemów informatycznych w UE. Jej celem jest poprawa ogólnej odporności państw członkowskich na incydenty cybernetyczne, zarówno w sektorze publicznym, jak i prywatnym. Zakres dyrektywy został znacząco poszerzony w porównaniu do pierwotnej dy-

¹⁷⁹ Insikt Group, *Ghostwriter in the Shell: Expanding on Mandiant's Attribution of UNC1151 to Belarus*, [CTA-2022-0318], 2022, s. 3–8.

¹⁸⁰ I. Karásková, U.A. Bērziņa-Čerenkova, K. Nēmečková, *Foreign Electoral Interference Affecting EU Democratic Processes*, [study requested by the Authority for European Political Parties and European Political Foundations], 2023, s. 49.

¹⁸¹ P. Wood, *2015 Internet Security Threat Report*, [04/15 21347933, Vol. 20], 2015, s. 28; M. Costa, *Exploring Hacktivism: The Role and Impact of Social Media*, „Advanced Research on Information Systems Security” 2025, Vol. 5, No. 1, s. 106–107.

¹⁸² S. Špaček, P. Čeleda, M. Drašar, M. Vizváry, *Analyzing an Off-the-Shelf Surveillance Software: Hacking Team Case Study*, [w:] *Proceedings of Conference SPI 2017: Security and Protection of Information*, J. Dočkal, M. Jirsa, J. Kaderka (eds.), Brno 2017, s. 143–145, 156–157.

rektywy NIS z 2016 roku, obejmując teraz znacznie większą liczbę podmiotów, w tym operatorów ważnych i kluczowych usług dla gospodarki, jak również z branż uznanych za istotne z punktu widzenia bezpieczeństwa (np. sektor zdrowia, energetyki, transportu, bankowości czy infrastruktury cyfrowej).

Jednym z fundamentalnych założeń NISz jest ujednolicenie wymagań w zakresie cyberbezpieczeństwa w całej Unii Europejskiej, co ma przeciwdziałać dotychczasowym różnicom w implementacji przepisów na poziomie krajowym. Dyrektywa zobowiązuje państwa członkowskie do wdrożenia jednolitych ram nadzorczych oraz sankcyjnych, a także do ustanowienia krajowych strategii cyberbezpieczeństwa zgodnych z wytycznymi unijnymi¹⁸³. Oznacza to nie tylko wzmocnienie zdolności operacyjnych organów publicznych, lecz również poprawę świadomości oraz odporności na poziomie instytucjonalnym i korporacyjnym. Dyrektywa NISz nakłada również konkretne obowiązki na przedsiębiorstwa, m.in. stosowania środków technicznych i organizacyjnych adekwatnych do ryzyka, regularnego raportowania incydentów, przeprowadzania audytów oraz zarządzania łańcuchem dostaw. Znaczące jest przy tym uwzględnienie perspektywy systemowej, w tym wymogu uwzględnienia zależności od podwykonawców oraz dostawców technologii, co odzwierciedla rosnące zrozumienie strukturalnej złożoności współczesnych środowisk cyfrowych¹⁸⁴. Podejście to może przyczynić się do ograniczenia efektu domina, w którym incydent w jednym ogniwie łańcucha wartości wywołuje zakłócenia w całym ekosystemie.

Należy przy tym podkreślić, że wpływ NISz jest dużo szerszy i wykracza poza granice UE. Przedsiębiorstwa spoza wspólnoty, które chcą świadczyć usługi w Europie lub współpracować z europejskimi partnerami, będą zmuszone do spełnienia wymogów dyrektywy, niezależnie od lokalnych regulacji. Tworzy to efekt „zewnątrznej europeizacji” norm cyberbezpieczeństwa, analogicznym do efektów wywołanych przez RODO¹⁸⁵. Firmy spoza UE będą musiały wdrożyć polityki zgodne z europejskimi oczekiwaniami, by utrzymać konkurencyjność i zapewnić zgodność kontraktową.

Dyrektywa NISz może również pośrednio wzmocnić międzynarodowy reżim normatywny w zakresie cyberbezpieczeństwa, ponieważ państwa trzecie, chcąc zachować interoperacyjność technologiczną i prawną z UE, mogą wdrażać zbliżone przepisy. W sytuacji braku wspólnej konwencji międzynarodowej dotyczącej cyberprzestrzeni, regio-

¹⁸³ NIS2, rozdział II, art. 8–13, rozdział III, art. 14–19, rozdział IV, art. 20–25.

¹⁸⁴ ENISA, *Technical Implementation Guidance*, Luxembourg 2025, s. 2–3.

¹⁸⁵ P. Trimintzios i inni, *Cybersecurity in the EU Common Security and Defence Policy (CSDP) Challenges and risks for the EU*, [EPRS/STOA/SER/16/214N], Brussels 2017, s. 7–9 57–59.

nalne standardy o szerokim zasięgu, takie jak NIS2, mogą odgrywać rolę de facto wyznacznika oczekiwanych standardów postępowania w środowisku cyfrowym. Dotyczy to nie tylko aktorów państwowych, ale także dużych podmiotów korporacyjnych i sektora infrastruktury krytycznej.

Wreszcie, dyrektywa ma także wymiar poznawczy i kulturowy. Zmuszając podmioty do opracowywania strategii, procedur reagowania i mechanizmów komunikacji, NIS2 przyczynia się do zwiększenia świadomości zagrożeń cybernetycznych wśród rządów i decydentów. To szczególnie ważne w kontekście rosnącej liczby zagrożeń poznawczych, gdzie granica między technicznym incydentem a manipulacją społeczną ulega zatarciu. Zwiększenie odporności organizacyjnej może więc nie tylko chronić przed atakami, lecz także przed kampaniami dezinformacyjnymi.

Należy jednak podkreślić, że choć efekty te są prawdopodobne i spodziewane, to implementacja NIS2 na poziomie krajowym przebiegała w sposób problematyczny. Nie wiele państw wdrożyło przepisy krajowe na czas (17 października 2024). W maju 2025 roku Komisja Europejska wysłała noty w tej sprawie do Bułgarii, Czech, Danii, Niemiec, Estonii, Irlandii, Hiszpanii, Francji, Cypru, Łotwy, Luksemburgu, Węgier, Holandii, Austrii, Polski, Portugalii, Słowenii, Finlandii i Szwecji¹⁸⁶. Co więcej, same propozycje implementacji mogą osiągać efekt przeciwny do intencji NIS2. Polska przedstawiła łącznie pięć projektów nowelizacji Ustawy o Krajowym Systemie Cyberbezpieczeństwa (stan na połowę 2025 roku). Ostatni z nich, z 7 lutego 2025 roku, wprowadził pewne odstępstwa dla podmiotów ważnych będących podmiotami publicznymi — tj. wyłączył część obowiązków na rzecz innych, opisanych w załączniku nr 4¹⁸⁷. Niemniej, ustawodawca wciąż zachował ogólnie restrykcyjne przepisy, które względem NIS2 wykazują nadregulację, m.in. w zakresie surowszych sankcji, niż to wymagane przez UE, zasady wstrzymywania koncesji, zezwoleń i działalności gospodarczej, jak również rozbudowane obowiązki dotyczące usuwania sprzętu i oprogramowania od podmiotów z państw spoza Unii Europejskiej i NATO¹⁸⁸. Wynika to z faktu objęcia ustawą aż 18 sektorów gospodarki. Rozszerza

¹⁸⁶ *Commission calls on 19 Member states to fully transpose the NIS2 Directive*, 7 May 2025, „European Commission”, <https://digital-strategy.ec.europa.eu/en/news/commission-calls-19-member-states-fully-transpose-nis2-directive> [odczyt: 23.07.2025].

¹⁸⁷ *Ustawa z dnia (...) 2025 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw*, projekt z dnia 7 lutego 2025 r. [projekt UC32], s. 164–168.

¹⁸⁸ K. Mączka, *Dyrektywa NIS2 jako wytyczna do wdrożenia systemu zarządzania bezpieczeństwem informacji w organizacji*, „Ochrona Ludności i Dziedzictwa Kulturowego” 2024, nr 5, s. 116–117.

to katalog podmiotów objętych regulacją z obecnych 378 operatorów usługi kluczowej¹⁸⁹, do łącznie ponad 6000 podmiotów ważnych i kluczowych¹⁹⁰.

Wiązać się to może z niewystarczającą liczbą ekspertów ds. cyberbezpieczeństwa, bezpieczeństwa informacji oraz ciągłości działania. Co więcej, należy wziąć pod uwagę wysokie koszty wdrażania systemów zarządzania bezpieczeństwem informacji (np. w zakresie normy PN-EN ISO/IEC 27001:2023) lub ciągłości działania (np. PN-EN ISO 22301:2020) — zwłaszcza w sektorze publicznym¹⁹¹. Istotny pozostaje także długi czas potrzebny na wdrożenie i uzyskanie przynajmniej podstawowej dojrzałości przez takie systemy. Rodzi to obawy, że wiele z tych podmiotów skorzysta z usług firm oferujących gotowe dokumentacje oraz szybkie wdrożenia — kierując się próbą uniknięcia najpoważniejszych konsekwencji. Prowadzić to może do myślenia o cyberbezpieczeństwie jako zgodności, którą da się nabyć, zamiast o ciągłym procesie. Stoi to wprost w sprzeczności z intencją NIS2, jak również dotychczasową praktyką wdrażania RODO. Jednym z największych sukcesów tego rozporządzenia było bowiem nie tylko wdrożenie zasad ochrony danych osobowych, lecz powszechna zmiana sposobu myślenia o ich zabezpieczeniu. RODO wymusiło przejście z postrzegania tego obszaru jako pojedynczego pozyskania zgodności, do ustanowienia stale pracującego systemu, który wymaga doskonalenia.

Podsumowanie

Rekapitulując powyższe rozważania należy stwierdzić, że asymetria — pomimo swej długiej tradycji w historii wojskowości — wciąż stanowi pojęcie o płynnych granicach, potencjalnie wymagające precyzyjnego wyznaczenia ram analitycznych. Przedstawione przykłady, od starożytnych wojen partyzanckich po współczesne starcia w cyberprzestrzeni, ukazują, że asymetria może przejawiać się zarówno w dysproporcji technologicznej czy materialnej, jak i w odmiennej legitymizacji walki, strukturze organizacyjnej, normatywnych ograniczeniach aktorów, czy samej przestrzeni operacji.

¹⁸⁹ *Liczba operatorów usług kluczowych (OUK) z podziałem na sektory*, 7 lipca 2025, „Serwis Rzeczypospolitej Polskiej”, https://dane.gov.pl/pl/dataset/3409,liczba-operatorow-uslug-kuczowych-z-podzialem-na-sektory/resource/68232/table?page=1&per_page=50&q=&sort= [odczyt: 7 lipca 2025].

¹⁹⁰ Dokładna liczba podmiotów nie jest znana, a sama autoidentyfikacja podmiotu jako objętego nową ustawą o krajowym systemie cyberbezpieczeństwa jest jednym z często podnoszonych problemów. Szacunkową liczbę przedstawili eksperci z PwC; *NIS2, czyli nowe wymogi dotyczące cyberbezpieczeństwa*, 25.07.2025, „PwC”, <https://www.pwc.pl/pl/uslugi/nis2-nowe-wymogi-dotyczace-cyberbezpieczenstwa.html> [odczyt: 01.08.2025].

¹⁹¹ *Ocena skutków regulacji*, 3 października 2024, [projekt UC32], s. 22–29, w tym: *Załącznik nr 4 do OSR: podsumowanie wydatków dla poszczególnych części budżetowych w zł*, s. 1–6.

W konfliktach minionych asymetria przybierała zwykle formę nierównowagi sił pomiędzy konwencjonalnymi armiami oraz oddziałami nieregularnymi. Współczesne asymetryczne formy konfliktów, uwzględniające jednocześnie użycie narzędzi konwencjonalnych, niekonwencjonalnych i informacyjnych, potwierdzają, że asymetryczność nie jest jedynie kategorią historyczną, lecz fundamentalną właściwością konfliktów XXI wieku. Kluczowe było tu wskazanie, że samo rozszerzenie pojęcia asymetrii o nowe środki — od improwizowanych materiałów wybuchowych przez wirusy komputerowe po arsenał atomowy — nie zawsze wzbogaca analizę; nie każda dysproporcja będzie asymetrią sensu stricto, zwłaszcza kiedy jest elementem trwałej równowagi strategicznej.

W odniesieniu do asymetrii podmiotów, uwypuklona została rola aktorów pozapaństwowych, którzy dzięki dostępowi do zaawansowanych narzędzi cyfrowych i mobilności operacyjnej mogą zadawać szkody o randze strategicznej. Cyberprzestrzeń przyniosła w tym kontekście równie wiele szans, co zagrożeń. Wydaje się, że toczony w niej starcia będą coraz częściej wywoływane przez niewielkie, wysoko wyspecjalizowane grupy pozapaństwowe, lub z nimi współpracujące. Dzięki elastyczności operacyjnej i wykorzystaniu złożonych mechanizmów technicznych oraz psychologicznych, mogą one skutecznie destabilizować infrastrukturę, naruszać zaufanie obywateli i wpływać na procesy polityczne — bez użycia tradycyjnej siły zbrojnej. Zarazem nieprzewidywalność takich aktorów sama w sobie stanowi odrębne wyzwanie, potencjalnie redefiniujące anarchię¹⁹² środowiska międzynarodowego.

Wydaje się zatem, że przyszłe konflikty w cyberprzestrzeni będą więc charakteryzować się eskalacją asymetrycznych działań, w których przewaga nie będzie wynikać z liczebności czy budżetu, lecz z elastyczności, wiedzy specjalistycznej i możliwości wykorzystania zaawansowanych technologii (np. AI, automatyzacja ataków, Internet Rzeczy). Z tego powodu wymagane jest interdyscyplinarne podejście, łączące wiedzę z obszaru inżynierii oprogramowania (bezpieczne projektowanie systemów, szyfrowanie, segmentacja sieci), prawa międzynarodowego (ramy odpowiedzialności, proporcjonalności reakcji, współpraca międzyjurysdykcyjna), psychologii politycznej (manipulacja poznawcza, odporność społeczna) oraz nauk o bezpieczeństwie (modelowanie ryzyka, strategia odstraszania). Tylko skoordynowana analiza wszystkich tych wymiarów pozwoli opracować

¹⁹² Rozumianej jako anarchia w teorii relacji międzynarodowych, tj. jako dynamiczna i samoorganizująca się struktura, w której różnorodne podmioty międzynarodowe współtworzą trwałe normy i procesy kooperacji, lub konkurują i prowadzą konflikty — bez odwołania się do jednego nadrzędnego arbitra. Współcześnie to także pluralistyczne spojrzenie na porządek światowy, od historycznych przypadków heteronomii, do współczesnych zgrupowań w cyberprzestrzeni, czy ukrytych struktur społecznych; zob. J. Havercroft, A. Prichard, *Anarchy and International Relations theory: A reconsideration*, „Journal of International Political Theory” 2017, Vol. 13, No. 3.

skuteczne mechanizmy służące zapobieganiu asymetrycznym atakom oraz budowaniu długotrwałej odporności społeczno-technicznej.

Budowanie bezpieczeństwa w środowisku sieciocentrycznym — zarówno defensywy, jak i możliwości operacyjnych — wymaga akceptacji współpracy ponadpaństwowej. Złożone łańcuchy dostaw i dywersyfikacja możliwości produkcyjnych nowoczesnej technologii na całym świecie, w praktyce uniemożliwiają pojedynczemu państwu na zapewnienie całkowitej samodzielności cyfrowej. Gdyby jednak hipotetycznie założyć taką możliwość dla struktur publicznych, to problemem pozostaje sektor prywatny. Co więcej, immanentna transgraniczność cyberprzestrzeni, jak również kompatybilność technologii, sprzyjają budowaniu wspólnych standardów bezpieczeństwa czy międzynarodowej wymianie informacji o zagrożeniach. Przykład dyrektywy NIS2 pokazuje, jak legislacja może odegrać istotną rolę w zwiększeniu ogólnej odporności — wymuszając na operatorach krytycznych usług wdrażanie zaawansowanych środków technicznych, organizacyjnych oraz procedur zarządzania ryzykiem. Rozszerzenie jej zakresu na podmioty prywatne i transgraniczną współpracę CSIRT-ów, ma szansę zredukować skuteczność asymetrycznych ataków przez minimalizację luk w łańcuchach dostaw i zwiększenie prędkości reagowania. Jednak nawet najskuteczniejsze regulacje nie zastąpią rozwoju kompetencji poznawczych i kulturowej odporności społeczeństw, które muszą nauczyć się rozpoznawać i odpierać manipulacje informacyjne. Przyszłe strategie bezpieczeństwa będą więc musiały integrować technologie obronne z programami edukacyjnymi, transparentnymi ścieżkami komunikacji kryzysowej i mechanizmami demokratycznej kontroli. Obecne operacje dezinformacyjne oraz propagandowe, prowadzone przeciwko państwom Zachodu, dowodzą tego jak dużą szkodę wyrządzić może nadmierne skupienie się na zabezpieczeniach infrastruktury lub próbie osiągnięcia przewagi technologicznej. Obiektywnie szybsze procesory Zachodnie (w porównaniu do rosyjskich czy chińskich), nowocześniejsze narzędzia cyfrowe lub bardziej zaawansowane narzędzia pola walki (jak bezzałogowe pojazdy), zdają się dawać pewną przewagę. W praktyce jednak to Zachód pada ofiarą wpływu na jego procesy demokratyczne, a możliwości działań odwetowych są ograniczone — właśnie przez pominięcie komponentu społeczno-psychologicznego.

W perspektywie długofalowej asymetria pozostanie siłą napędową ewolucji konfliktów, dlatego wyzwaniem dla badaczy oraz praktyków bezpieczeństwa będzie ciągle dostosowywanie paradygmatów analitycznych i operacyjnych do dynamicznie zmieniającej się natury zagrożeń — w szczególności tych, które manifestują się w cyberprzestrzeni jako asymetryczne, wielowymiarowe i nieregularne formy agresji.

Rozdział III

Porównanie i krytyka koncepcji hybrydowości i asymetryczności

Niniejszy rozdział podejmuje krytyczną analizę koncepcji „wojny hybrydowej” i „wojny asymetrycznej”. Oba terminy zyskały na znaczeniu po 2000 roku, zwłaszcza w dyskursie anglojęzycznym, gdzie wykorzystywane są zarówno w debacie akademickiej, jak również w języku politycznym oraz medialnym. Choć w sferze publicznej dominację zyskało pojęcie wojny hybrydowej, to jego semantyczna pojemność i definicyjna nieostrość budzą poważne zastrzeżenia metodologiczne. Spotkać można się z krytyką, że wojna hybrydowa jest jedynie frazesem lub hasłem-wytrychem i nie wnoszeni niczego wyrażnie nowego do debat politycznych¹. Medialna popularność tego pojęcia może wynikać z jego metaforyczności, umożliwiającej łatwe przedstawienie złożonych zjawisk w sposób przystępny i medialnie atrakcyjny. Koncepcja „hybrydy” jest bowiem relatywnie łatwa do zrozumienia, a przy tym dostatecznie pojemna, by można było jej użyć w celach politycznych.

Pojęcie wojny asymetrycznej, jakkolwiek również szerokie i wieloznaczne, ma nieco bardziej ugruntowane podstawy w teorii strategii i studiach nad siłą relacyjną w konflikcie². W literaturze asymetryczność bywa traktowana nie jako odrębny typ konfliktu, lecz jako jego cecha — właściwość wynikająca z nierównowagi potencjałów, celów lub norm działania stron. Asymetria dotyczy zarówno zdolności wojskowych, jak i politycznej woli i ograniczeń liberalnych demokracji³. Przecenianie pojęcia asymetrii jako odrębnej kategorii może prowadzić do uproszczeń analitycznych i pomijać fakt, że więk-

¹ A. Bilal, *Hybrid Warfare — New Threats, Complexity, and ‘Trust’ as the Antidote*, „NATO Review”, 30 November 2021, <https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html> [odczyt: 10.07.2025].

² Por. I. Arreguín-Toft, *How the Weak Win Wars: A Theory of Asymmetric Conflict*, „International Security” 2001, Vol. 26, No. 1.

³ G. Merom, *How Democracies Lose Small Wars State, Society, and the Failures of France in Algeria, Israel in Lebanon, and the United States in Vietnam*, Cambridge 2003, s. 11–14.

szość konfliktów ma elementy asymetryczne. Jak wykazano w poprzednich rozdziałach — dotyczy to nie tylko współczesnego sposobu prowadzenia walki, lecz także przeszłego.

Celem niniejszego rozdziału jest porównanie i krytyczne zderzenie obu koncepcji — hybrydowości i asymetryczności — w ich różnych ujęciach teoretycznych, z uwzględnieniem przykładów praktycznych. Analiza ma na celu nie tylko wykazanie, w jakim zakresie pojęcia te mogą być przydatne w opisie i interpretacji współczesnych zjawisk militarnych i pozamilitarnych, lecz także zidentyfikowanie ich ograniczeń poznawczych. Zostaną omówione zarówno genezy terminów, jak i ich obecność w zachodnich, rosyjskich i chińskich doktrynach oraz analizach strategicznych. Szczególny nacisk położony zostanie na wykazanie, że „wojna hybrydowa” jako termin analityczny jest nie tylko wewnętrznie niespójna, lecz także podatna na instrumentalizację polityczną. W przypadku wojny asymetrycznej podjęta zostanie próba przesunięcia uwagi z klasyfikacji konfliktów ku rozpoznaniu asymetrii jako uniwersalnego i zmiennego parametru działań zbrojnych, który nie powinien być traktowany jako osobny typ wojny, lecz jako wymiar obecny w różnym nasileniu w niemal każdym konflikcie. Co więcej, niniejszy rozdział odnosi się także do relacji hybrydowości i asymetrii względem strategii oraz doktryn państw i roli, którą odgrywają na takim szczeblu.

Wartym podkreślenia jest, że w toku analizy źródeł dostrzeżono, iż koncepcja wojny hybrydowej jest bardziej odległa w przypadku chińskiego definiowania konfliktów. Z tego względu omówienie materiałów strategicznych i akademickich, w przypadku Chin koncentruje się na wojnie asymetrycznej.

3.1. Analiza pojęcia hybrydowości i jej krytyka

Od rosyjskiej inwazji na Ukrainę w 2014 roku, liczba analiz i komentarzy dotyczących wojny hybrydowej nieustannie przybywa⁴. Co więcej, źródła bardzo często dokładnie tak określają ten konflikt — a jednak nie wpisuje się on w wiele aspektów hoffmannowskiej terminologii⁵. Jednakże trudno byłoby zarzucić autorom, iż to uproszczenie wynikało z ogólnej popularności pojęcia, lecz z braku jednej, autorytatywnej definicji (lub choćby pretendującej do niej). Tym bardziej nie istniał żaden holistyczny model. Dlatego teza, iż elementy wojny hybrydowej nie są nowe wydaje się słuszna. Jak wcześniej wskazano — rzeczywiście występują one od starożytności.

⁴ Niektóre źródła mówią nawet o wykładniczym przyroście. Jednakże termin *hybrid war* wyszukiwany w Google Scholar wykazuje trend spadkowy liczby publikacji — znaczny od początku pandemii Covid-19 (ponad dwukrotny). Podobnie *hybrid warfare*. Zob. J.K. Wither, *Making Sense of Hybrid Warfare*, „Connections: The Quarterly Journal” 2016, No. 2, s. 73.

⁵ A. Krzak, *Wojny przyszłości po rosyjsku...*, s. 28.

Ale fakt określenia ich jako takie, z wykorzystaniem jednej lub wielu perspektyw teoretycznych — zachodnich, wschodnich czy dalekowschodnich — wydaje się nie mieć szczególnej wartości analitycznej poza samym tematem. Liczne opisy konfliktów „hybrydowych”, „złożonych” (kompozytowych), czy „nieliniowych” nie służą wyjaśnieniu problematyki wojen, a wręcz przeciwnie — komplikują teorie i proponują podejścia dostatecznie różne, by trudno było mówić o ich kompatybilności. Dlatego istotnym będzie nie tylko rozważenie bieżącego stanu wiedzy na temat rozumienia wojny hybrydowej, lecz także poddanie tego terminu krytyce.

3.1.1. Teoria strategiczna

Całość należy zacząć od narysowania ram teoretycznych, w których osadzone zostaną dalsze definicje. Wobec problematyki wojen zastosowanie ma teoria strategiczna. Dzięki pracom m.in. Thomasa Schellinga⁶ czy Colina Graya⁷, w ciągu ostatnich 40 lat pojęcie to było sukcesywnie adaptowane w dyscyplinie stosunków międzynarodowych, politologii i bezpieczeństwa, stając się metodą analizy⁸. Jest zarazem coraz częściej stosowane, pomagając w zrozumieniu procesu podejmowania decyzji — przez rozważenie możliwości oraz sił, kosztów i skali ryzyka, jak również konsekwencji dla wszystkich stron⁹. Zatem stanowi ona doskonały punkt wyjściowy dla analizy systemu politycznego ogólnie, z rozumieniem wojen jako przedłużenia polityki¹⁰.

⁶ Thomas Crombie Schelling (ur. 14 kwietnia 1921, zm. 13 grudnia 2016), amerykański ekonomista, badacz polityki zagranicznej, bezpieczeństwa narodowego oraz strategii nuklearnej oraz kontroli nad arsenałem atomowym na Uniwersytecie Marylandu w College Park. W 2005 roku otrzymał Nagrodę Banku Szwecji im. Alfreda Nobla w dziedzinie ekonomii za poszerzenie zrozumienia konfliktu i współpracy poprzez analizę teorii gier; W. Grimes, *Thomas C. Schelling Dies at 95; Used Game Theory to Explain Nuclear Strategy*, „New York Times” 2016, December 14, s. B14; zob. T. Schelling, *The Strategy of Conflict*, Cambridge 1980.

⁷ Colin Spencer Gray (ur. 29 grudnia 1943, zm. 27 lutego 2020), brytyjsko-amerykański politolog, badacz relacji międzynarodowych, strategii i geopolityki na Uniwersytecie Reading, założyciel Narodowego Instytutu Polityki Publicznej w Waszyngtonie. Współpracował z agencjami rządowymi USA w charakterze eksperta, opracowując wewnętrzne raporty; K.B. Payne, *On Deterrence, Defense and Arm Control: In Honor of Colin S. Gray*, „NIFPP Information Series”, 2020, No. 461, s. 1, 10–11; zob. C.S. Grey, *Strategic Studies: A Critical Assessment*, Westport 1982; C.S. Grey, *Modern Strategy*, Oxford 1999.

⁸ Bynajmniej nie można im przypisać pierwotnego autorstwa, a jedynie popularyzację i współczesne spojrzenie na teorię strategiczną. Jej podstawy położyli Carl von Clausewitz, Alfred Thayer Mahan oraz Julian Stafford Corbett — czy jak wskazują inni, także Sun Tzu. Por. S. Fitzsimmons, *Evaluating the Masters of Strategy: A Comparative Analysis of Clausewitz, Sun Tzu, Mahan, and Corbett*, „Innovations: A Journal of Politics” 2007, Vol. 7, s. 27–29; C.S. Grey, *Modern Strategy...*, s. 36.

⁹ H.R. Yarger, *Strategic Theory of for the 21 st Century: The Little Book on Big Strategy*, Carlisle 2006, s. 2.

¹⁰ J.M. Guerra, *An Introduction to Clausewitzian Strategic Theory: General Theory, Strategy, and Their Relevance for Today*, „Infinity Journal” 2012, Vol. 2, Issue 3, s. 31.

Teoria strategiczna zakłada, iż wszystkie konflikty charakteryzują się pewnymi wspólnymi cechami, które zapewniają możliwość ich porównywania czy badania z jednego, wspólnego punktu widzenia. Interesując się tak organizacją wszystkich zazębiających się elementów systemu, jak również jego środowiskiem, zakłada tworzenie strategii skutecznej, tj. zezwalającej na odpowiednie użycie siły¹¹. Przy tym podkreśla się, iż podejście to nie jest ściśle związane z jednym kontekstem historycznym, a raczej rozumie ono ewolucję procesów¹². Stanowi więc próbę wyjaśnienia tego, co już było, jak również implikacji dla teraźniejszości i przyszłości, tworząc obraz uniwersalnych i wiecznych cech zapewniania podstawowej potrzeby człowieka: bezpieczeństwa¹³.

O ile jednak teoria strategiczna jest dość dobrze opisana w źródłach, to strategia sama w sobie stanowi pojęcie szeroko używane, ale zarazem niejednorodne w rozumieniu — podobnie jak sama hybrydowość. Jej opisy odnajdujemy nie tylko w wymienionych dyscyplinach, lecz np. ekonomii czy zarządzaniu. Postrzeganie niemal wszystkiego jako strategii — o ile w pewnym zakresie umożliwiające opis rzeczywistości — rabuje ją ze znaczenia¹⁴. Nawet jednak w badaniach nad bezpieczeństwem należy zauważyć, że nie istnieje jedna formuła opisująca strategię i — przede wszystkim — jej przyszłe wyniki. Jest to bezpośrednim następstwem faktu, iż nauki społeczne oraz polityczne rzadko bywają oszczędne w swoich teoriach¹⁵. Złożoność analizowanych przez nie zjawisk, przy ograniczonej wiedzy na ich temat, skutkuje ustanowieniem niewielu praw. O ile w tak szybko rozwijającym się świecie można jeszcze liczyć na to, że zdolni będziemy kiedykolwiek osiąść pełną wiedzę na temat danej problematyki. Dlatego realnie możliwe będzie raczej podanie prawdopodobieństwa dla następstw określonych założeń.

Nie stanowi to bynajmniej myśli nowej — już Clausewitz mówił, iż pozytywna doktryna wojny jest niemożliwa, gdyż w konfliktach wszystko jest niepewne. Wszelkie obliczenia wykonywane są przy stale zmieniających się wartościach, a same działania militarne stanowią przeplatanie się siły fizycznej i efektów psychologicznych¹⁶. John Garnett zauważa nawet, że dotychczas najużyteczniejsze teorie nie spełniają ściśle „naukowych” wymogów, gdyż nie są wprost predykcyjne, stanowiąc raczej zbiory pojęć negatywnych¹⁷.

¹¹ F.P.B. Osinga, *Science, Strategy and War*, London 2006, s. 11.

¹² M.L.R. Smith, J. Stone, *Explaining Strategic Theory*, „Infinity Journal” 2011, Vol. 1, No. 4, s. 30.

¹³ C.S. Gray, *The Future of Strategy*, London 2015, s. 28.

¹⁴ H. Strachan, *The Direction of War: Contemporary Strategy in Historical Perspective*, Cambridge 2013, s. 27.

¹⁵ G. King, R.O. Keohane, S. Verba, *Designing Social Inquiry*, Princeton 1994, s. 20.

¹⁶ C. von Clausewitz, *O wojnie...*, s. 136–141.

¹⁷ J.C. Garnett, *Commonsense and the Theory of International Politics*, London 1984, p.46.

W omawianiu teorii strategicznej nie można jednak pominąć funkcji eksplanacyjnej, szczególnie użytecznej w wyjaśnianiu potencjalnych strat, zysków, czy też tworzenia polityki i jej oceny. Jest instrumentem nie tylko wykorzystywanym przez dowódców czy osoby stojące na czele państw, lecz także ich kształcącym. Bo przez wzgląd na swoją naturę, często nie udziela ona odpowiedzi, lecz izoluje elementy składowe w danej problematyce. Dzięki temu pozwala stawiać trafne pytania, czy sugeruje związki między sprawami pozornie różnymi¹⁸. Jednocześnie za najważniejsze spośród nich to pragmatyczne „czy pomysł zadziała?”. Dlatego tym bardziej pytanie o zasadność pojęcia wojny hybrydowej powinno być poprzedzone rozważaniami na temat właśnie tej teorii.

Wcześniej należy jednak doprecyzować rolę samej strategii, szczególnie w pojęciu ewoluowania jej relacji z systemem politycznym, szczególnie w rozumieniu „wielkiej strategii” (ang. grand strategy). W XIX wieku koncept ten nie był jeszcze szeroko rozposzechniony, choć dostrzegano jego wartość — czym zajmował się m.in. William Tecumseh Sherman¹⁹. Jednak to w 1911 roku pojawiło się zasadnicze rozróżnienie na strategię „wielką” i „małą”. Podczas wykładu na ówczesnym Royal Naval War College, Julian Corbett mówił o tym, iż holistyczne spojrzenie na zasoby całego państwa w czasie wojny jest strategią „wielką”²⁰.

Dyskusje o szerszym pojmowaniu strategii miały miejsce szczególnie po I Wojnie Światowej. Wśród literatury autorstwa Johna F.C. Fullera, Edwarda M. Earle’a czy André Beaufre’a oraz Liddella Harta, wyróżnić można tego ostatniego, dobrze podsumowującego ówczesną myśl. Poza rozszerzaniem zakresu strategii „wielkiej” zaznaczał on, że „podczas gdy horyzonty strategii są ograniczone wojną, wielka strategia wykracza poza wojnę, ku późniejszemu pokojowi. Powinna nie tylko łączyć różne instrumenty, ale także regulować ich użycie, aby uniknąć szkody dla przyszłego pokoju — dla jego bezpieczeństwa i dobrobytu”²¹. Także to jakie rezultaty naród osiągnie podczas konfliktu, warunkowało przede wszystkim przygotowanie w czasie pokoju. Z kolei ujmowanie elementów zupełnie pozamilitarnych, a jednak z myślą o potencjalnym wykorzystaniu w wojnie — to co dziś nazwalibyśmy hybrydowym podejściem — pojawiło się w literaturze już w połowie II Wojny Światowej²². Zgadza się z tym Colin S. Gray, który dodatkowo uważa, że „każda strategia to wielka strategia” i nie można mówić o podejściu prawdziwie strategicznym,

¹⁸ C.S. Grey, *Modern Strategy...*, s. 36.

¹⁹ Zob. J.T. Palmer, L.J. Fullenkamp, *Battle Command in the 1864 Campaign for Atlanta: the emergence of William Tecumeshh Sherman as a Strategic Leader*, Carlisle Barracks 1996.

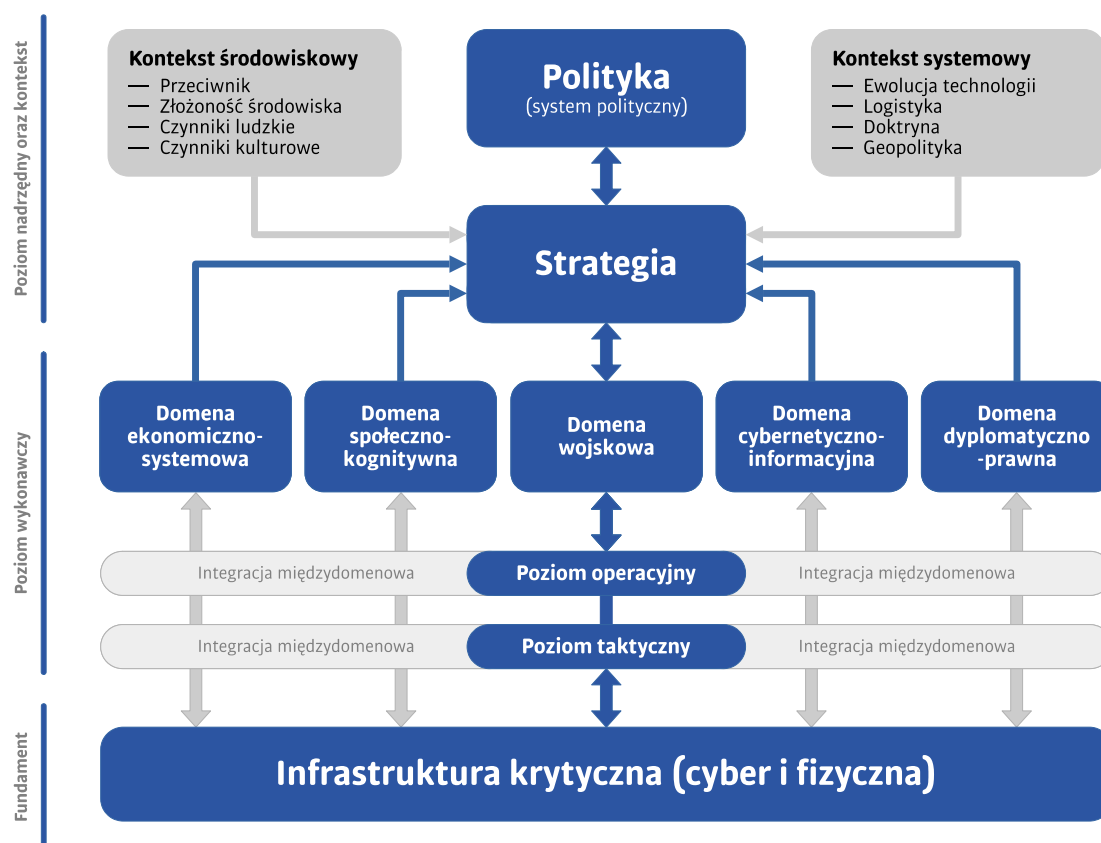
²⁰ H. Strachan, *The Direction of...*, s. 32.

²¹ B.L. Hart, *Strategy. Second revised edition*, London 1991. s. 322.

²² E.M. Earle, *Makers of Modern Strategy from Machiavelli to Hitler*, Princeton 1943, s. VIII.

jeśli nie jest ono holistyczne. Każda cecha i zasób podmiotu — niezależnie czy państwowego, czy też nie — będzie mieć znaczenie w razie wojny. Według niego, podmiot wewnętrznie spójny musi opracować wielką strategię, by móc zwiększyć szansę sukcesu²³.

Strategia ze swej definicji i pełnionej roli winna obejmować wiele obszarów, m.in. ekonomię, sprawy społeczne, informacyjne, czy dyplomację. Zatem rozbitcie jej na „wielką” oraz „małą” traci na znaczeniu. Natomiast podczas tworzenia lub analizy strategii należy zwrócić uwagę na kluczowe aspekty, będącymi ośmioma wymiarami, występującymi we wszystkich wojnach. Są to pojęcia: przeciwnika, stopnia złożoności, człowieka, kultury, technologii, geografii, logistyki i doktryny. Ich względna waga będzie zależeć od kontekstu czy sposobu prowadzenia danej wojny, lecz każdy z tych wymiarów odgrywa rolę — choć niejednokrotnie zmieniającą się w czasie konfliktu (patrz: rys. 1.). Jednakże skoro tak, to zasadnym jest zadanie pytania o elementy, których wojna hybrydowa w ogóle ma dotyczyć, jak również w jakim zakresie.



Rys. 1. Poziomy planowania i prowadzenia działań, z uwzględnieniem integracji międzydomenowej, kontekstu oraz fundamentu²⁴.

²³ C.S. Gray, *The Strategy Bridge: Theory for Practice*, New York 2010, s. 28.

²⁴ Opracowanie własne, na podstawie: M. Caliskan, *Hybrid warfare through the lens of strategic theory*, „Defense & Security Analysis” 2019, Vol. 35, No. 1, s. 45.

3.1.2. Rewolucja w sprawach wojskowych — porównanie perspektywy zachodniej z chińską

Jak wspomniano we wstępie do niniejszego rozdziału, pierwsze próby sformułowania pojęcia „wojny hybrydowej” były podejmowane już pod koniec XX wieku. Działo się to w kontekście „rewolucji w sprawach wojskowych” — RMA (Revolution in Military Affairs) — doktryny i systemu rozwoju Sił Zbrojnych USA. Koncepcja ta mówiła o znaczącym zwrocie w sposobie prowadzenia konfliktów, wywołanym innowacyjnym wykorzystaniem nowoczesnych technologii w walce oraz dzięki zasadniczymi zmianami strategicznymi i operacyjnymi²⁵. W formułowaniu RMA wyróżniano też trzy naczelne czynniki: szybki rozwój technologiczny, przenoszący wojskowość z ery industrialnej do ery informacyjnej, zakończenie zimnej wojny, jak również systematyczne zmniejszanie budżetów na obronność²⁶. Szybko jednak skrytykowano to podejście i zauważano, że nie można pominąć natury wojny, rozumianej jako kompleksowej interakcji celów politycznych, ludzkich emocji, wpływów kulturowo-etnicznych czy zdolności militarnych. Jednakże sam postęp technologiczny jest tutaj wyłącznie środkiem do osiągnięcia celów²⁷.

Warto przy tym wskazać, iż powyższą koncepcję rozszerzano w środowisku akademickim, ze względu na braki w „szczegółach technicznych”. Według O’Hanlona RMA tworzyło pewną filozofię, w ramach której funkcjonowały cztery szkoły myślenia. Pierwszą był „system systemów”, który opisuje kompleksową hierarchię struktur dowodzenia i technologii we wszystkich służbach, a zatem jest szkieletem operacji łączonych. Drugą: „dominacja przez wiedzę o przestrzeni bitewnej”, stwierdzającą jakoby technologia miała pozwolić na uzyskanie kompleksowej wiedzy o danym polu walki, bez jakiegokolwiek niepewności. Trzecia szkoła dotyczy „globalnego zasięgu, globalnej potęgi”, czyli rozwinięciem poprzedniej myśli o założenie, że USA mogłoby zidentyfikować dowolny cel na zie-

²⁵ Przytoczone stanowisko zostało wyrażone w memorandum pierwszego dyrektora Office of Net Assessment, wewnętrznego think-tanku Pentagonu, funkcjonującego pod Departamentem Obrony USA. Było ono powszechnie uznane i wielokrotnie przytaczane, także w programach akademickich wojskowych uczelni wyższych USA. Co istotne, zgodnie z Dyrektywą 5111.11, tego rodzaju oceny nie wyrażały prywatnego stanowiska, lecz były faktycznym materiałem analitycznym, na podstawie którego siły zbrojne USA mogły identyfikować pojawiające się oraz przyszłe zagrożenia. Jednocześnie dyrektywa ta zastępowała wcześniejsze (upraszczając je), które łącznie regulowały tę sprawę w podobny sposób. Zob. A.W. Marshall, *Some Thoughts on Military Revolutions*, Memorandum Office of Net Assessment, 29.08.1993; *Director of Net Assessment*, 22 August, [DoDD 5111.11], 2001; *Program for Joint Education (PJE)*, U.S. Army War College, Carlisle Barracks 1996; *Revolution in Military Affairs. A selected Bibliography*, U.S. Army War College, Carlisle Barracks 1996.

²⁶ E.H. Tilford, *The Revolution in Military Affairs: Prospects and Cautions*, Carlisle Barracks 1995, s. 7.

²⁷ Por. O. Nassauer, D. Plesch, *NATO Strategy Review: Out of Step with Events*, „Armed Forces Journal International” 1991, No. Oct. s. 50-52

mi w czasie bliskim do rzeczywistego, z możliwością zniszczenia go. Ostatnią z kolei była „podatność na zagrożenia” — przyjmująca, iż nowe technologie nie zostaną zmonopolizowane przez potęgi militarne, ale w końcu „wyciekną” i rozpowszechnią się²⁸.

RMA nie było bynajmniej koncepcją oryginalną, a jej genezy można doszukiwać się w Rosji końca lat 70²⁹. Marszałek Nikołaj Ogarkow, ówczesny szef Sztabu Generalnego Sił Zbrojnych ZSRR pisał o „wojskowej rewolucji technicznej” w słowach, że jest to: „proces (...) który tworzy jakościowo nowe rodzaje uzbrojenia i techniki wojskowej, a także unowocześnia konwencjonalne (klasyczne) środki walki i znacząco podnosi ich możliwości bojowe”³⁰. Integralne postrzeganie prowadzenia konfliktów oraz wykorzystania technologii były według niego kluczowe, gdyż to właśnie postęp w samym sprzęcie stanowił zasadniczy powód dla zmian doktrynalnych w sprawach wojskowych³¹. Jak się później okazało, rosyjskie spojrzenie na sprawę bynajmniej nie było tyle ich dążeniem do uzyskania technologicznej przewagi, lecz systematycznym badaniem myśli i działań USA w tym obszarze. Miało to na celu skuteczniejsze przewidywanie tego, jak prowadzone będą przyszłe konflikty³².

Chiny także nie pozostały obojętne i od początku lat 80. studiowały działania USA oraz ZSRR ws. wdrażania RMA, wydając w tym czasie liczne publikacje na temat zbliżających się rewolucyjnych zmian w działaniach wojennych. Zmiany na arenie międzynarodowej i wydarzenia związane z technologiczną rewolucją pokryły się z momentem, kiedy przywództwo Armii Ludowo-Wyzwoleńczej (ALW) nie był silnie ograniczone przez ideologię partyjną. Pozwoliło to na realistyczną i — co istotne — powszechną ocenę RMA³³. Koncepcja ta może nie została wprost zaadaptowana przez Chiny (z powodu braku realnej możliwości), lecz przyczyniła się do zmian w sposobie myślenia ALW. Stało się ono dużo bardziej otwarte i pragmatyczne³⁴.

Skonkretyzowanie podejścia chińskiego sprowadzało się w tamtym czasie do Trzech Szkół Myśli ALW. Pierwszą była „wojna ludu”, czerpiąca z maoistycznej wizji, lub w niektórych wariantach — z teorii Dèng Xiǎopíng. Oceniała ona ALW jako zacofaną

²⁸ M.E. O’Hanlon, *Technological Change and the Future of Warfare*, Washington 2000, s. 11–19.

²⁹ E.A. Cohen, *A Revolution in Warfare*, „Foreign Affairs” 1996, Vol. 75, No. 2, s. 37–54.

³⁰ H.B. Огарков, *Военная наука и защита социалистического Отечества*, „Коммунист” 1978, № 7, s. 115.

³¹ H.B. Огарков, *Всегда в готовности к защите отечества*, Москва 1982, s. 30.

³² Y. Ji, *The Revolution in Military Affairs and the Evolution of China’s Strategic Thinking*, „Contemporary Southeast Asia” 1999, Vol. 21, No. 3, s. 345.

³³ Z. Zhen, *Guanyu wojun zhanyi lilun de jige wenti* [Kilka pytań dotyczących teorii kampanii ALW], [w:] *Tongxiang shengli de tansou* [Odkrywając drogi do zwycięstwa], Editorial Group (ed.), Pekin 1987, s. 16 [tłum. za: tamże, s. 345–346].

³⁴ Y. Ji, *The Revolution in Military Affairs...*, s. 347.

technologicznie, a przez to pozbawioną innego wyjścia, jak tylko polegać na sile i liczebności ludzi oraz bieżącym sprzęcie, celem udaremniania inwazji wroga. Drugą szkołę stanowiła „wojna zaawansowanej technologii”, która obecna była w ówczesnej chińskiej strategii obrony narodowej. Ta wprawdzie rozpoznawała już wojnę informacyjną oraz cyberprzestrzeń, ale zakładała, iż nie jest potrzebna pilna i gruntowna przebudowa armii. Śledząc zmiany w metodzie prowadzenia konfliktów, skupiano się na rozwoju technologicznym, lecz wciąż osadzonym w bardziej klasycznym podejściu do konfliktów. Ostatnią ze szkół było po prostu RMA — przyjmowane w sposób podobny do Zachodniego. Wówczas liczba zwolenników takiego podejścia pozostawała niewielka. Przewidywano jednak, że jeżeli awansują oni w hierarchii wojskowej, a starzy teoretycy odejdą, to rozwój ALW podąży w kierunku przynajmniej zbliżonym do RMA³⁵. Wydaje się to odnajdywać potwierdzenie w dzisiejszych planach Chin, by do 2035 roku osiągnąć kamień milowy „pełnej modernizacji”. Na XIX Kongresie Narodowym Chińskiej Partii Komunistycznej, który miał miejsce w 2017 roku, Xi Jinping przedstawił raport mówiący m.in. o koncepcji stworzenia „światowej klasy wojska” do 2050 roku. Miałoby to zrównać ALW z armią USA, jednak nie przez próbę naśladownictwa, lecz stanie się liderem nowej rewolucji w sprawach wojskowych.

Chińczycy proponują koncept „inteligentnej” wojny (chin. 智能化战争 — zhi-nenghua zhanzheng), czyli przejścia od konfrontacji systemów, do konfrontacji „algorytmów” [walki]. Strona z przewagą „algorytmu” miałaby dominować w wojnie przez hybrydę ludzko-komputerową, podejmowanie decyzji w sieciach neuronowych, czy użyciem technologii „mózgu w chmurze”. Wprawdzie teoretycy chińscy nie sądzą, że sztuczna inteligencja zastąpi człowieka w dowodzeniu, lecz będzie „cyfrowym oficerem sztabowym”, masowo zbierającym, przetwarzającym i prezentującym informacje operacyjne oraz wywiadowcze³⁶.

W tym kontekście zauważyć należy, że chińska refleksja strategiczna — choć często interpretowana przez zachodnich autorów jako zbliżona do pojęcia wojny hybrydowej — w istocie koncentruje się wokół zagadnienia asymetrycznego wykorzystania przewagi technologicznej i poznawczej, a nie na samym łączeniu różnych domen działań w sposób „hybrydowy” w ujęciu zachodnim. Pojęcie „wojny hybrydowej”, które w dyskursie euroatlantyckim opisuje jednoczesne użycie środków konwencjonalnych, niekonwen-

³⁵ Tamże, s. 347–348.

³⁶ E.J. Burke, K. Gunness, C.A. Cooper, M. Cozad, *People's Liberation Army Operational Concepts*, Santa Monica 2020 s. 21; E.B. Kania, *The PLA's Latest Thinking on the Three Warfares*, „China Brief” 2016, Vol. 16, No. 13, s. 10–14.

cjonalnych, informacyjnych i ekonomicznych³⁷, nie znajduje bezpośredniego odpowiednika w chińskiej doktrynie. Kluczowe dla niej są natomiast pojęcia „wojny nielimitowanej” (która zostanie omówiona w dalszej części) oraz przytoczonej „inteligentnej wojny”. Podkreślają one bowiem nie tyle mieszanie środków, co celowe i selektywne wykorzystanie asymetrii w czasie, przestrzeni oraz technologii.

W chińskiej literaturze wojskowej wyraźnie dominuje przekonanie, że skuteczność działań zależy nie od hybrydowości środków, lecz od „systemowego wyprzedzenia” przeciwnika w obszarze informacyjnym i decyzyjnym³⁸. Oznacza to, że przewaga nie musi polegać na jednoczesnym operowaniu w wielu domenach, lecz na zakłóceniu procesu poznawczego przeciwnika i wykorzystaniu tego zakłócenia do przełamania jego odporności systemowej. Koncepcja ta jest spójna z wcześniejszymi chińskimi ujęciami wojny psychologicznej, medialnej i prawnej, które ujęte zostały w ramach tzw. „trzech wojen”. Te zostaną omówione w dalszej części niniejszego rozdziału.

Z tego względu, chińskie podejście do konfliktu znacznie bliższe jest operacjonalizacji asymetrii niż zachodniemu modelowi hybrydowości. Hybryda, jako pojęcie szerokie i niedookreślone, nie oddaje precyzji i intencjonalności chińskich strategii, które zakładają dokładne określenie punktów wrażliwości przeciwnika i atakowanie ich w sposób niedostrzegalny lub trudny do sklasyfikowania na gruncie tradycyjnych kategorii wojennych. Wydaje się, że celem Chin nie jest eskalacja poprzez łączenie środków, lecz deeskalacja poprzez osiągnięcie celu przed wybuchem wojny.

3.1.3. Zachodnie spojrzenie na „wojnę hybrydową”

W kontekście takiego rozumienia zmian wojskowych, Frank Hoffman skonkretyzował wcześniejsze zręby koncepcji „wojny hybrydowej” przez serię publikacji: *The Rise of Hybrid Wars*, *Hybrid Warfare and Challenges*, *Hybrid vs. Compound War*, *Neither Omnipotent Nor Unbeatable*, a także *On Not-So-New Warfare*. Zagrożenia hybrydowe zdefiniował jako „każdego przeciwnika (adwersarza), który w sposób równoległy stosuje unikalne połączenie użycia: broni konwencjonalnej, nieregularnej taktyki działania, terroryzmu i zachowań o charakterze kryminalnym, w ramach szeroko rozumianego pola bitwy”³⁹. Zarazem, według Hoffmana, wojny hybrydowe łączą wysiłki regularne i niere-

³⁷ F.G. Hoffman, *Hybrid Warfare and Challenges*, „Joint Force Quarterly” 2009, Issue 52, s. 36–39.

³⁸ E.B. Kania, *Artificial intelligence in China's revolution in military affairs*, „Journal of Strategic Studies”, 2021, Vol. 44, No. 4, s. 520–522, 529–534; E.B. Kania, *Battlefield singularity. Artificial intelligence, military revolution, and china's future military power*, Washington 2017, s. 11–12. 33–38; K.E. Morgan, K.P. Mueller, E.S. Medeiros, K.L. Pollpeter, R. Cliff, *Dangerous Thresholds: Managing Escalation in the 21st Century*, Santa Monica 2008, s. 51–58; D. Shats, *Chinese Views of Effective Control: Theory and Action*, Montgomery 2022, s. 5–9.

³⁹ F. Hoffman, *Conflict in the 21st Century...*, s. 7.

gularne, podejmowane tak przez państwa, jak również podmioty niepaństwowe. Tych aktorów mogą z kolei stanowić niewielkie grupy lub nawet pojedyncze jednostki — lecz kierowane operacyjnie i taktycznie w głównej przestrzeni walki, dla synergicznego osiągnięcia celów wojny⁴⁰. Zatem dostrzec tu można konwergencję wszystkich dostępnych środków, celem zmuszenia przeciwnika do ulegnięcia własnemu celowi politycznemu. Łatwo zauważyć, iż wprost wpisuje się to w Clausewitzową definicję prowadzenia wojny, a zatem nie można hybrydowości postrzegać jako pojęcia nowego. Mówił o tym sam Hoffmanm nowatorskiego ujęcia doszukując się w metodach oraz szczeblu podejmowania działań. Wcześniej hybrydowość była domeną strategii, teraz miała wejść w użycie na poziomie operacyjnym i taktycznym — za sprawą „rozmycia”⁴¹.

Dla Organizacji Traktatu Północnoatlantyckiego, wojna hybrydowa wyznaczyła nowy cel po zimnej wojnie i pozwoliła ponownie skupić się na tradycyjnej misji Sojuszu. Z jednej strony rozumiano to jako nowe wyzwanie w postaci przeciwnika mogącego podejmować dwa różne podejścia strategiczne jednocześnie⁴². Zarazem jednak dostarczało to narzędzi porównawczych (w perspektywie doktrynalnej) dla południowych i wschodnich flank NATO, prowadząc do wypracowania myśli, iż struktury Sojuszu muszą być w gotowości do szybkiej adaptacji, celem radzenia sobie z nowymi zagrożeniami. W jednym z raportów ideę tę ujęto jako zaadaptowanie, dostosowanie i doskonalenie (ang. *adapt, adapt, adept*)⁴³. Dlatego przyjęto, że „wojna hybrydowa” to „szerokie, złożone, adaptacyjne, oportunistyczne i często zintegrowane kombinacje metod konwencjonalnych i niekonwencjonalnych”. Dalej: „działania te mogą być jawne lub ukryte, angażując wojskowe, paramilitarne, zorganizowane siatki przestępcze i podmioty cywilne we wszystkich elementach władzy”⁴⁴.

Przyczynkiem do podjęcia kroków w stronę przyjęcia przedmiotowej koncepcji była inwazja Rosji na Ukrainę w 2014 roku. Podczas Szczytu NATO w Walii uznano, że fundamentalnie zmieniło to postrzeganie bezpieczeństwa w Europie⁴⁵. Powstałe w ten sposób zagrożenie wymaga zatwierdzenia „Planu działania na rzecz gotowości” (ang. *Readiness Action Plan — RAP*), który precyzował przedsięwzięcia w bliskiej perspektywie

⁴⁰ Tamże, s. 2.

⁴¹ Tamże, s. 29.

⁴² C. Bell, *Hybrid warfare and its metaphors*, „Humanity: An International Journal of Human Rights, Humanitarianism, and Development” 2012, Vol. 3 (2), s. 225–246.

⁴³ J.M. Calha, *Hybrid warfare? NATO's new strategic challenge*, NATO Parliamentary Assembly Defence and Security Committee General Report, 10 October [166 DSC 15 E bis], 2015, s. 8–9.

⁴⁴ *Next Steps in NATO's Transformation: To the Warsaw Summit and Beyond*, [White Paper — NATO Transformation Seminar], Washington 2015, s. 5.

⁴⁵ H. Bayley, *A citizen's guide to NATO's priorities after the Wales Summit*, Brussels 2014, s. 13.

i adaptację metod działania w dłuższej⁴⁶. Jako istotne wskazano środki odstraszające, m.in. przez Łączoną Grupę Zadaniową Bardzo Wysokiej Gotowości (ang. Very High Readiness Joint Task Force — VJTF), która przede wszystkim wzmacniałaby zdolność komunikacji strategicznej, a także zwiększenia wydatków na obronność⁴⁷. Z kolei dwa lata później, w 2016 roku, potwierdzono uprzednie dążenia i zapowiedziano stworzenie Łączonego Wydziału Wywiadu i Bezpieczeństwa (Joint Intelligence and Security Division — JISD)⁴⁸, a w 2017 roku powołano Pion ds. Analizy Hybrydowości (ang. Hybrid Analysis Branch)⁴⁹. Co więcej, podczas Szczytu w Brukseli NATO uregulowało sprawy działań poniżej progu wojny, jakie towarzyszą działaniom hybrydowym — w razie ich wystąpienia pozwalając Sekretarzowi Sojuszu powołać się na artykuł 5⁵⁰. Uwzględniając w tym także podmioty niepaństwowe, NATO prowadziło silną narrację o utrzymywaniu dotychczasowej jedności oraz aktualności względem nowych wyzwań, jako gwaranta bezpieczeństwa dla swoich członków⁵¹.

Mimo jasnego podejścia teoretycznego Sojuszu tj. postrzegania wojny hybrydowej przez pryzmat wojskowy, w praktyce wyłania się inne spojrzenie na problematykę, typowo polityczne. W identyfikowaniu zagrożeń hybrydowych NATO posługuje się bowiem siedmioma wskaźnikami. Są to: (1) bezpieczeństwo energetyczne, (2) presja i wpływy polityczne, (3) wrogie działania wywiadowcze oraz sabotażowe, (4) działania cybernetyczne, (5), operacje informacyjne, (6) „miękka siła” — czyli wpływ organizacji pozarządowych, działalność kulturowa, religijna, a także (7) postawa wojskowa w dyskursie strategicznym⁵². Jak widać, tylko jeden ze wskaźników bezpośrednio porusza sprawy militarne. Co więcej, niektórzy przedstawiciele NATO wprost utożsamiają „wojnę hybrydową” z „wojną informacyjną”. Rysuje to obraz zróżnicowania w interpretacji hybrydowości, który może rodzić uzasadnione pytania o zdolność Sojuszu do skutecznego działania,

⁴⁶ *Wales Summit Declaration*, 5 September, [NATO Press Release (120)], 2014, §5, 13.

⁴⁷ Tamże, § 7–14.

⁴⁸ *Warsaw Summit Communiqué*, 9 July, [NATO Press Release (100)], 2016, § 79.

⁴⁹ A.F. von Loringhoven, *Adapting NATO Intelligence in Support of “One NATO”*, „Gandirea Militara Romaneasca” 2017, Issue 3(4), s. 153–157.

⁵⁰ Por. *Brussels Summit Declaration*, 11 July, [NATO Press Release (brak numeru)], 2018, § 21, 33; *Brussels Summit Communiqué*, 14 June, [NATO Press Release (086)], 2021, §21, 31–34, 35.

⁵¹ T. Flockhart, *Towards a strong NATO narrative: from a “practice of talking” to a “practice of doing”*, „International politics” 2012, No. 49 (1), s. 78–79.

⁵² Stanowisko to wyrażone zostało podczas serii 18 pogłębionych wywiadów, przeprowadzonych przez badaczy Université Catholique de Louvain z urzędnikami NATO, którzy zajmowali się koncepcją hybrydowości po inwazji Rosji na Ukrainę w 2014 roku; M. Caliscan, M. Liégeois, *The concept of ‘hybrid warfare’ undermines NATO’s strategic thinking: insights from interviews with NATO officials*, „Small Wars & Insurgencies” 2020, Vol. 32, No. 2, wywiad 14, s. 300.

sকoro wazni jego przedstawiciele⁵³ nie mogą zgodzić się co do spójnych ram teoretycznych. Z drugiej strony publicznie udzielone informacje nie muszą odzwierciedlać faktycznych modeli niejawnych, którymi zapewne NATO się posługuje. Za hipotezą o uchyleniach w postępowaniu Sojuszu przemawia jednak wspomniany „Plan działania na rzecz gotowości”, który szczebel taktyczny traktuje powierzchownie⁵⁴, a to skupienie na nim byłoby oczekiwane w sprawach wojny hybrydowej⁵⁵. Nie jest to bynajmniej problem wyłącznie NATO, lecz obserwować go można w innych podejściach zachodnich⁵⁶.

Także Unia Europejska zajęła w tej sprawie stanowisko, które jest bardzo podobne do wyrażanego przez Sojusz, tym samym dziedzicząc co do zasady te same problemy. W ramach wyznaczania wspólnych ram przeciwdziałania zagrożeniom hybrydowym, zauważa, że są one „różnie definiowane i definicje te należy formułować w sposób elastyczny, tak by uwzględniały one zmienny charakter tego rodzaju zagrożeń, pojęcie to oznacza kombinację represyjnych oraz wywrotowych działań, konwencjonalnych i niekonwencjonalnych metod (tj. dyplomatycznych, militarnych, ekonomicznych, czy technologicznych), które mogą być stosowane w sposób skoordynowany przez podmioty państwowe i niepaństwowe, by osiągnąć określone cele, przy czym działania te są prowadzone poniżej progu oficjalnie wypowiedzianej wojny”⁵⁷.

Jednak zasadniczo UE stroni od skupiania się na czynnikach militarnych konfliktów hybrydowych, co wyraża np. „Wspólna polityka bezpieczeństwa i obrony”. Wynika to z prowadzenia autonarracji pokazującej Wspólnotę jako biegunowo przeciwną wojnie. Dlatego nawet w omawianym obszarze preferowane jest podejście z perspektywy zarządzania kryzysowego⁵⁸, skupiającego się na prewencji. W dodatku stanowisko UE jest ra-

⁵³ Wśród osób z którymi przeprowadzano wywiady, 10 z nich było wojskowymi, a w relacji do wiedzy o wojnie hybrydowej, było to: 6 generałów, 5 osób związanych z rozwojem, 5 z wykonawstwem i 2 osoby pracowały w obu tych obszarach; Tamże, *Appendix A. Note for Interviews*, s. 318.

⁵⁴ *Wales Summit Declaration...*, § 5–13; X. Pintat, *NATO's Readiness Action Plan: Assurance and Deterrence for the post-2014 Security Environment*, NATO Parliamentary Assembly Defence and Security Committee Report, 10 October, [167 DSCFC 15 E bis], 2015, s. 10–11.

⁵⁵ J.M. Arnold, *NATO's Readiness Action Plan: Strategic Benefits and Outstanding Challenges*, „Strategic Studies Quarterly” 2016, Vol. 10, No. 1, s. 84–88, 91–92.

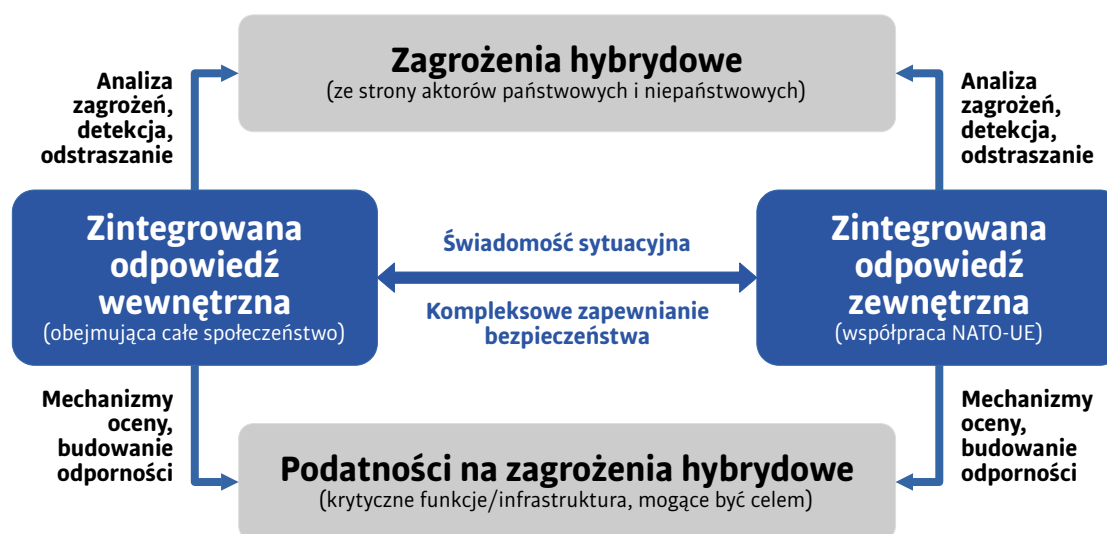
⁵⁶ D. Stroker, C. Whiteside, *Blurred Lines: Gray-Zone Conflict and Hybrid War — Two Failures of American Strategic Thinking*, „Naval War College Review” 2020, Vol. 73, No. 1, s. 3.

⁵⁷ Definicję przytoczono w jej oficjalnym tłumaczeniu na język polski, *Wspólny komunikat do Parlamentu Europejskiego i Rady: Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym*, 6 April, [JOIN (2016) 018], 2016, s. 2.

⁵⁸ Zob. C. Moser, S. Blockans, *The extent of the European Parliament's competence in Common Security and Defence Policy*, Brussels 2022; *Countering Hybrid Threats. Working document of the European External Action Service*, 13 May, [EEAS (2015) 731], 2015.

czej ramowe, wyznaczające generalny kierunek dla całej Wspólnoty, gdyż zagrożenia bywają zupełnie różne dla poszczególnych państw członkowskich⁵⁹.

Wkład UE w system bezpieczeństwa opiera się raczej na monitorowaniu i ewaluowaniu niebezpieczeństw, jak również sugerowaniu pewnych rozwiązań, m.in. przez Hybrid Fusion Cell⁶⁰ — komórkę działającą w ramach Centrum Wywiadu i Sytuacji (ang. EU Intelligence and Situation Centre — EU INTCEN), będącego częścią Europejskiej Służby Działań Zewnętrznych (ang. European External Action Service — EEAS). Zatem UE stara się pełnić rolę badawczo-informacyjną, jednak swoje struktury i możliwości wykorzystuje nie tylko na potrzeby wewnętrzne, lecz także w ramach współpracy z NATO⁶¹ (zob. rys. 2.). Wspólnie zauważają, że koniecznym pozostaje kolektywne zrozumienie zagrożeń hybrydowych, wymagających regularnego zaangażowania w ramach odpowiednich struktur UE i NATO oraz między nimi. Wciąż jednak każde państwo musi ocenić własne podatności, aby zrozumieć rodzaj hybrydowych niebezpieczeństw, które mogą być skierowane przeciwko niemu⁶².



Rys. 2. System współpracy NATO-UE, opracowany w ramach kompleksowego podejścia do zagrożeń hybrydowych⁶³.

⁵⁹ *EU strategic communication to counteract anti-EU propaganda by third parties*, 21 November, [P8_TA (2016) 0441], 2016, pkt. B, D, I–K, § 3, 14–16, s. 2–3, 4, 6.

⁶⁰ *Joint Staff Working Document. EU operational protocol for countering hybrid threats*, 5 July, [SWD (2016) 227 z późn. zm. — wersja finalna], 2016, s. 2–5, 7.

⁶¹ *Zob. Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*, 8 July, [NATO Press Release (119)], 2016.

⁶² Tamże.

⁶³ A. Hagelstam, K. Narinen, *Cooperating to counter hybrid threats*, „NATO Review”, 23.11.2018, <https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html> [odczyt: 07.08.2022].

Tym na co należy zwrócić uwagę przy ogólnym podsumowaniu myśli zachodniej, to szerokie spektrum środków pozawojzkowych, które teoretycy tej części świata wskazują jako elementy wojny hybrydowej. Rodzi to problemy (i zarazem ryzyko) z odróżnieniem zwykłej konkurencji międzypaństwowej od faktycznych działań wojennych. Oczywiście tak długo, jak działania te byłyby składową większych operacji militarnych, przyznanie iż wchodzą w ich skład jest łatwe — choćby na poziomie teorii polemologicznych, jeżeli same definicje prawa międzynarodowego nie wystarczają. Ale co kiedy środki te zostaną użyte jako rodzaj „hybrydowego uderzenia wyprzedającego”? Obecne teorie mówią o identyfikacji działań poniżej progu wojny — choć charakteryzują je bardzo podobnie do metod prowadzenia klasycznych konfliktów, lecz bez formalnego zrywania pokoju. Wskazuje się głównie na „wyłom w prawie międzynarodowym”. Jednakże niedoprecyzowania i brak zgody co do definicji sprawiają, że taki system pojęciowy tworzy kolejny próg, poniżej którego można potencjalnie operować. Wówczas rozpoznanie takich przedsięwzięć jako hybrydowych staje się zupełnie uznaniowe, a wypracowane teorie „wojny hybrydowej” tracą na znaczeniu. Stwierdzenia, iż „Zachód znajduje się w trwałej wojnie hybrydowej z Rosją” także nie ułatwiają tworzenia skutecznych modeli⁶⁴.

3.1.4. Rosyjskie spojrzenie na „wojnę nieliniarną” i konflikty „nowej generacji”

W przeciwieństwie do teoretyków zachodnich, w rosyjskiej literaturze niełatwo jest odnaleźć istotne informacje na temat pozamilitarnych środków nacisku w kontekście zagrożeń hybrydowych. Wprawdzie pojawiają się one w dokumentach strategicznych, lecz po prostu jako metody działania innych państw, a nie element wojny hybrydowej⁶⁵. Np. *Strategia Bezpieczeństwa Narodowego Federacji Rosyjskiej* z 2021 roku, wśród niebezpieczeństw z Zachodu wymienia m.in. wykorzystywanie środków ekonomicznych do osłabiania Rosji⁶⁶, okcydentalizację (przyjmowanie zachodnich wzorców), dezinformację, czy „kolorową rewolucję” które mogłyby wpływać na wewnętrzną destabilizację⁶⁷. Oczywiście wskazuje też wojskowy charakter zagrożeń ze strony NATO i USA⁶⁸, lecz trudno tu się doszukać spójnego wpasowania w jakąkolwiek teorię wojny hybrydowej. Zamiast tego, Strategia proponuje uniezależnianie się Rosji (jako zabezpieczenie przed

⁶⁴ R. Thornton, *The Changing Nature of Modern Warfare. Responding to Russian Information Warfare*, „The RUSI Journal” 2015, Vol. 160, No. 4, s. 46.

⁶⁵ M.Ç. Güler, A. Shakirova, *Deciphering Russia's 2021 National Security Strategy Document*, „SETA | Perspective” 2021, No. 67, s. 2–3.

⁶⁶ *Стратегия национальной безопасности Российской Федерации*. Утверждена Указом Президента Российской Федерации от 2 июля 2021 г. № 400, s. 38.

⁶⁷ Tamże, s. 34–38.

⁶⁸ Tamże, s. 11–14.

konkurencją ze strony innych państw), a także zwiększanie potencjału własnych sił zbrojnych, przede wszystkim przez inwestowanie w rozwój nowych technologii rozwoju sprzętu i uzbrojenia⁶⁹.

Aby lepiej zrozumieć takie podejście Rosji, należy cofnąć się do rozpadu Związku Radzieckiego i następnych lat. Walki w Iraku w 1990 roku pokazały, że niewielkie siły, odpowiednio wykorzystujące niekonwencjonalne metody walki, czy też technologie (dostarczane przez Zachód), mogą stawić czoła uprzedniej „potędze militarnej”, za jaką ZSRR się uważał. Wiele konfliktów na tle etnicznym, które eskalowały na kanwie braku dotychczas wspólnej siły politycznej, czy kryzys finansowy z 1998 roku (i trwające ograniczanie wydatków na wojsko)⁷⁰, nie ułatwiły budowania nowych systemów. Problem stanowiło także tworzenie strategii, gdyż w poradzieckiej Rosji, której uprzednimi podstawami ideologicznymi był marksizm i leninizm, pojawiła się próżnia⁷¹. Później zapełniano ją naśladownictwem reszty Europy, ówczesznie nawet podziwianej. Emulację tego widać choćby we wczesnych wizjach integracji przez „Wspólnotę Niepodległych Państw”⁷², wzorowanych na strukturach UE⁷³. W takim kontekście rozwijały się myśli rosyjskich teoretyków wojskowych⁷⁴.

Do przełomu mileniów, należałoby wyróżnić m.in. Machmuta Garijewa, który był jednym z głównych doradców podczas wycofywania się wojsk radzieckich z Afganistanu. Wraz z nabywaniem doświadczenia jako wojskowy, zmieniał też swoje poglądy na konflikty zbrojne. O ile klasyczne starcia postrzegał jako ich trzon, to zauważał pozostałe komponenty. Sądził, iż „wojna jest złożonym zjawiskiem społecznym i politycznym, które obejmuje wszystkie sfery życia narodów zaangażowanych różnymi środkami walki z wrogiem, w tym środkami przemysłowymi, politycznymi oraz psychologicznymi,

⁶⁹ A.M. Dyner, *Strategia bezpieczeństwa narodowego Rosji*, „Biuletyn PISM” 2021, Nr 131 (2329), s. 1.

⁷⁰ S. Perlo-Freeman, O. Ismail, C. Solmirano, E. Sköns, C. Solmirano, *Military expenditure*, [w:] *SIPRI Yearbook 2010. Armaments, Disarmament and International Security*, B. Gill i inni (eds.), Oxford 2010, s. 163.

⁷¹ M. Light, *In search of an identity: Russian foreign policy and the end of ideology*, „Journal of Communist Studies and Transition Politics” 2003, Vol. 19, Issue 3, s. 43.

⁷² Wspólnota Niepodległych Państw (ros. Содружество Независимых Государств), miała redukować reperkusje rozpadu ZSRR i wspierać poradziecką współpracę w sferach polityki, gospodarki i bezpieczeństwa. Jednak już po dekadzie była oceniana raczej jako porażka — z brakiem aktywnego uczestnictwa państw członkowskich, a także faworyzowaniem przez Rosję stosunków bilateralnych, zamiast wielostronnych; P. Kubicek, *The Commonwealth of Independent States: an example of failed regionalism?*, „Review of International Studies” 2009, No. 35, s. 251–256.

⁷³ M. Light, *In search of an identity...*, s. 44.

⁷⁴ Mimo adaptacyjnego podejścia do aparatu pojęciowego, rosyjscy teoretycy przystosowali go do swoich potrzeb, wynikających m.in. z kultury i tradycji; J. Darczewska, *Diabeł tkwi w szczegółach. Wojna informacyjna w świetle doktryny wojennej Rosji*, Warszawa 2015, s. 15.

wśród których dominujący jest konflikt zbrojny”⁷⁵. Jednocześnie uważał, że „natura” wojny jest niezmienna, nawet w obliczu broni atomowej — choć dostrzegał trudność użycia jej jako przedłużenia polityki, gdyż mogła być narzędziem eskalacji samozagłady⁷⁶. W swym paradygmacie niezmienności mówił też o samych celach wojny: gospodarczych, terytorialnych i zasobach naturalnych. Wszystkie pozostałe przyczyny, np. polityczne lub religijne, były dla niego tylko fasadą. Zaś technologia była mnożnikiem siły, a nie substytutem wojny⁷⁷.

W następstwie Operacji Pustynna Burza w 1991 roku, rosyjski generał Wołodymir Slipczenko wprowadził koncepcję „wojen szóstej generacji”, wspomnianą już w pierwszej części niniejszego rozdziału. To właśnie ten konflikt, jego zdaniem, miał stanowić przejaw nowego rozdziału w historii wojen — choć niepokazujący jeszcze pełnego ich potencjału⁷⁸. Slipczenko wskazywał na „informatyzację” wojny konwencjonalnej, jak również rozwój precyzyjnych systemów uderzeniowych w ewolucji pola walki, lecz postrzegał je w kontekście strategicznego impasu nuklearnego⁷⁹. Dlatego wierzył, że obserwowano wówczas pierwsze przejawy „wojny bezkontaktowej” i to ona miała stać się przyszłością⁸⁰.

W 2000 roku Federacja Rosyjska opublikowała swoją *Doktrynę Bezpieczeństwa Informacyjnego*, w którym wymieniła cyberprzestrzeń jako jedno z pól walki. Co jednak istotne, kiedy inne państwa postrzegały środowisko sieciocentryczne za miejsce działalności służb specjalnych, Rosja już wtedy mówiła o potrzebie jej militaryzacji⁸¹.

W kontekście tych zmian, Sergiej Bogdanow, we współpracy z innymi teoretykami, rozszerzył twórczość Slipczenki. Zgodzenie się z propozycją wojen niekontaktowych, lecz zarazem doprecyzował sposób osiągania przewagi. Uważał, że państwa muszą dbać o bezpieczeństwo informacyjne, pod groźbą utraty suwerenności politycznej, ekonomicznej lub po prostu strategicznej przewagi w walce⁸². Całość może prowadzić do powstania „konfliktów niekonwencjonalnych”, w których przemoc już nie implikuje użycia

⁷⁵ M.A. Gareyev, *If War Comes Tomorrow? The Contours of Future Armed Conflict*, Y.V. Fomenko (trans.), J.W. Kipp (ed.), London 1998, s. VIII.

⁷⁶ Tamże, s. 70–81.

⁷⁷ Tamże, s. 19–37.

⁷⁸ В.И. Слипенченко, *Война будущего* (прогностический анализ), Москва 1999, s. 36–39.

⁷⁹ Zob. В.И. Слипенченко, *К какой войне должны готовиться вооружённые силы*, „Отечественные записки” 2002, № 8(9).

⁸⁰ В.И. Слипенченко, *Войны нового поколения: дистанционные бесконтактные*, Москва 2004, s. 32–34, 49–50.

⁸¹ R. Deibert, R. Rohozinski, *Control and Subversion in Russian Cyberspace*, [w:] *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, R. Deibert, J. Palfrey, R. Rohozinski, J. Zittrain (eds.), Cambridge 2010, s. 32.

⁸² С.Г. Чекинов, С.А. Богданов, *Влияние не прямых действий на характер современной войны*, „Военная мысль” 2011, № 6, s. 10.

wszelkich dostępnych form walki zbrojnej. Dzięki technologicznym innowacjom, możliwym staje się skuteczne osłabianie przeciwnika innymi metodami, dziś rozumianymi jako „hybrydowe”⁸³. Istotną publikacją wydaje się *Natura i treść wojny nowej generacji*, którą zachodni teoretycy postrzegają niczym plan aneksji Krymu z 2014 roku. Wraz z Czekinowem autor argumentuje, że Arabska Wiosna zaczęła nowy rozdział w historii wojen: możliwe jest obalenie obcej władzy w sposób pośredni. Dokonywać ma się tego przez użycie wojny psychologicznej, informacyjnej, mobilizacji społecznej (łącznie wysiłki mediów, dyplomatów i służb specjalnych). Dopiero później można mówić o wprowadzaniu wojsk, choć ich wsparcie lub częściowy udział jest możliwy już wcześniej⁸⁴.

To jednak nie było pierwszym przedstawieniem koncepcji „wojen nowej generacji”, gdyż po raz pierwszy przedstawił je 25 stycznia 2013 roku szef Sztabu Generalnego Sił Zbrojnych FR, Walerij Gierasimow. W pewnym sensie zaprezentował on rosyjski punkt widzenia, systematyzując dotychczasowe poglądy, choć zachodni obserwatorzy niesłusznie okrzyknęli to „doktryną Gierasimowa”⁸⁵. U podstaw jego koncepcji legło stwierdzenie, że po tzw. „kolorowych rewolucjach” doszło do głębokich zmian w świecie, które zatęrzyły linię między wojną a stabilnym pokojem⁸⁶. Prowadzi to, jego zdaniem, do powstania nowego modelu wojny, tworzącej „permanentny obszar operacji” przez wpływ informacyjny na społeczeństwa. Sprawia to, iż metody pozamilitarne i militarne będą używane w proporcjach 4:1⁸⁷. Wobec tego „wojny nowej generacji” nie skupiają się na przejmowaniu terytoriów, czy niszczeniu sił zbrojnych nieprzyjaciela, ale na osłabianiu obcego państwa przez systemowy rozkład wszystkich jego struktur⁸⁸. Aparat pojęciowy metod działania — pośrednich i pozawojсковych — został zapożyczony od zachodnich teoretyków. Wymienił tutaj przedsięwzięcia ekonomiczne, informacyjne i polityczne, humanitarne

⁸³ В.Н. Горбунов, С.А. Богданов, *О характере вооруженной борьбы в XXI веке*, „Военная мысль” 2009, № 3, s. 2–15.

⁸⁴ В.Н. Горбунов, С.А. Богданов, *Природа и содержание войны нового поколения*, „Военная мысль” 2013, № 4, s. 12–23.

⁸⁵ M. Galeotti, *The mythical ‘Gerasimov Doctrine’ and the language of threat*, „Critical Studies on Security” 2019, Vol. 7, No. 2, s. 158–160; C.K. Bartles, *Getting Gerasimov Right*, „Military Review” 2016, Vol. 96, No. 1, s. 30; R.N. McDermott, *Does Russia Have a Gerasimov Doctrine?*, „The US Army War College Quarterly: Parameters” 2016, Vol. 46, No. 1, s. 103–105; O. Fridman, *On the ‘Gerasimov Doctrine’. Why the West Fails to Beat Russia to the Punch*, „PRISM” 2019, Vol. 8, No. 2, s. 106–107; K. Jóhár, A. Rácz, *Contemporary Russian Military Thinking on Conflicts of the 21st Century: Beyond the ‘Gerasimov Doctrine’*, [w:] *Conflicts in the Gray Zone A Challenge to Adapt*, A.P. Kiss (ed.), Budapest 2017, s. 111–113.

⁸⁶ И.В. Бочарников, С.В. Лемешев, Г.В. Люткене, *Современные концепции войн и практика военного строительства*, Москва 2013, s. 65–67.

⁸⁷ O. Johnson, *The Russian Understanding of War: Blurring the Lines between War and Peace*, Washington 2019, s. 73.

⁸⁸ В. Герасимов, *Ценность науки в предвидении*, „Военно-промышленный курьер” 2013, № 8, s. 2.

— rozumiane przez kontyngenty międzynarodowych sił pokojowych, rzekomo mających chronić prawa człowieka, a także „potencjał protestu” w państwach będących celem agresji⁸⁹. Dopiero po tym nastąpi użycie sił zbrojnych.

Gierasimow uważa zatem, że przyszłe wojny odbywać się będą w trzech lub czterech zasadniczych etapach⁹⁰. Pierwszy jest faza przygotowawcza: rozpoznanie wywiadowcze, infiltrowanie systemów przeciwnika, działania dezinformacyjne oraz psychologiczne, jak również sabotaże, terroryzm czy dywersja. Drugi etap to faza trwałej i aktywnej destabilizacji wewnętrznej, wraz z prowadzeniem do izolacji w środowisku międzynarodowym. Dalej następuje eskalacja konfliktu przez działania zbrojne poniżej progu wojny, z użyciem separatystów, buntowników, najemników lub sił specjalnych. Dopiero ostatnia, czwarta faza, to uderzenie z wykorzystaniem wszystkich rodzajów wojsk, a także z użyciem broni precyzyjnego rażenia⁹¹, mających na celu zniszczenie potencjału gospodarczego i wojskowego przeciwnika⁹². Wciąż jednak istotne pozostaje prowadzenie walki psychologicznej i informacyjnej, czy nierezygnowanie z metod asymetrycznych oraz nieregularnych⁹³.

Tym co winno się rzucać w oczy jest fakt, iż nawet „gibridnaja wojna” Gierasimowa nie wyklucza konwencjonalnych konfliktów, choć prowadzonych w sposób inny niż uprzednio — bo z większym znaczeniem metod „nieregularnych”. Wciąż jest to tylko ewolucja, a nie rewolucja. Istnieją też przesłanki aby sądzić, że rosyjscy teoretycy nigdy nie uważali koncepcji hybrydowości za uniwersalną⁹⁴. Staje się to szczególnie jaskrawe w kontekście rozwoju rosyjskiej myśli wojskowej, a przede wszystkim wcześniejszych publikacji w tym zakresie. Gdy wziąć pod uwagę prace np. Garijewa, to w inwazji na Ukrainę z 2022 roku nie ma niczego zaskakującego.

⁸⁹ M. Wojanowski, *Mit „wojny hybrydowej”. Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku*, „Przegląd Bezpieczeństwa Wewnętrznego 2015”, wyd. spec. „Wojna hybrydowa”, s. 28.

⁹⁰ Interesujący wykaz korelacji między militarnymi oraz niemilitarnymi środkami oddziaływania, tabelarycznie porządkujący koncepcję Gierasimowa, został przedstawiony w publikacji Mickiewicza i Kasprzyckiego, P. Mickiewicz, D.D. Kasprzycki, *Od „konfliktu hybrydowego” do działań konwencjonalnych? Koncepcja oddziaływania militarnego Rosji, ze szczególnym uwzględnieniem zmian po 2018 roku*, „Przegląd Bezpieczeństwa Wewnętrznego” 2021, Nr 25 (13), s. 15.

⁹¹ M. Wojanowski, *Koncepcja „wojny nowej generacji” w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego” 2015, Nr 7 (13), s. 15.

⁹² A. Krzak, *Wojny przyszłości po rosyjsku...*, s. 26.

⁹³ В. Герасимов, *Ценность науки...*, s. 3.

⁹⁴ M. Kofman, M. Rojansky, *A Closer look at Russia's Hybrid War*, „Kennan Cable” 2015, No. 7, s. 4–5.

3.1.5. Wojna „hybrydowa”, czy „gibridnaja”? Krytyka pojęcia

Mimo, iż pojęcia „wojny hybrydowej” w ujęciu zachodnim i rosyjskim wydają się być podobne, to istnieją między nimi fundamentalne różnice. Pierwsze prace teoretyków amerykańskich przedstawiały tę metodę prowadzenia konfliktów przede wszystkim z perspektywy wojskowej. Rozpoznając uwarunkowania polityczne, skupiali się na osiągnięciu celów militarnych w nowy sposób, łączący działania regularne i nieregularne — poniżej progu wojny. Wydaje się więc, że dla Zachodu, „wojna hybrydowa” jest przedmiotem przynależnym przede wszystkim polemologii⁹⁵. Natomiast rozumienie tego zjawiska jako „wojny politycznej” zaczęło pojawiać się dosyć późno.

Tymczasem w omawianym obszarze, myśli rosyjskiej od zawsze było bliżej do „wojny buntowniczej”⁹⁶ Jewgienija Messnera. Według jego konceptu, „powstała nowa forma konfliktów zbrojnych, (...) w której walczący to nie tylko (i nie tyle) wojska, co ruchy ludowe. To nowe zjawisko powinno być rozpatrywane z różnych punktów widzenia, lecz przede wszystkim psychologicznego. Jeżeli w klasycznych wojnach morale armii miało znaczenie, wówczas w obecnej erze sił i ruchów ludowych, czynniki psychologiczne stają się dominujące”⁹⁷. Kreuje to pole bitwy, na którym walka toczy się o zdevastowanie spójności społeczno-kulturowej. Z istotą elementów psychologicznych, podejmuje się działania nieregularne, powoli wyniszczające przeciwnika, a przez to wywierające na niego nacisk. Dlatego „wojna buntownicza” i „gibridnaja wojna” to właściwie dwie strony tego samego medalu, obrazującego użycie m.in. terroryzmu międzynarodowego, separatyzmu, ekstremizmów, czy działalności przestępczej⁹⁸. Jednakże „gibridnaja wojna” nie jest bezpośrednim następcą semantyki Messnera, a stanowi raczej sposób postrzegania amerykańskiej „hybrid war” przez pryzmat rosyjskiej myśli wojskowej.

⁹⁵ O. Firdman, *Hybrid Warfare or Gibridnaya Voyna? Similar, But Different*, „The RUSI Journal” 2017, Vol. 162, No. 1, s. 46.

⁹⁶ Wojna buntownicza (ros. Мятёжевойна) — w dosłownym tłumaczeniu „wojna rebeliancka”. O ile taki przekład w pewnym stopniu oddaje metody działania, to angielskie źródła tłumaczą tę koncepcję jako „subversion war” (spopularyzowane przez Oferę Fridmana), upatrując w niej pośrednich sposobów wywierania nacisku na inne państwa, dążąc do ich osłabienia. Ze względu na głębię pojęcia oraz trudność jego przełożenia na język polski, w rodzimej literaturze spotyka się „miałieżewojnę”. Por.: O. Jonsson, *The Russian Understanding of War...*, s. 77; O. Fridman, *Old Wine in a New Bottle: The Cold-War Origins of the Concept of Gibridnaya Voyna*, [w:] *Russia and the former societ space. Instrumentalizing Security, Legitimizing Intervention*, V. Rotaru, M. Troncotă (eds.), Cambridge 2017, s.114; K. Kraj, *Wojny asymetryczne czy miałieżewojna Jewgienija Messnera zagrożeniem dla bezpieczeństwa w XXI wieku*, „Bezpieczeństwo. Teoria i Praktyka” 2012, Nr 3, s. 33–39. P. Ochmann, J. Wojaś, *Wojna hybrydowa jako przykład...*, s. 103.

⁹⁷ В.И. Марченкова, *Хочешь мира, победи мятежевойну! Творческое наследие Е. Э. Месснера*, Москва 2005, s. 97.

⁹⁸ K. Kraj, *Wojny asymetryczne czy miałieżewojna...*, s. 39.

Należy podkreślić, że nieuprawnionym byłoby stwierdzenie, jakoby zachodni teoretycy dopiero teraz dojrzeliby do rozpoznania istoty wymiaru politycznego w konfliktach hybrydowych — a rosyjscy pominęli etap koncepcji militarnych, od razu formułując współczesną formę „gibridnej wojny”. Podstaw tego stanu rzeczy należałoby się dopatrywać wyłącznie w różnicach kulturowych, tj. zupełnie innym podejściu do sposobu osiągania celów politycznych. Zaje się to potwierdzać tło historyczne, w tym spuścizna Zimnej Wojny oraz późniejszych wydarzeń⁹⁹.

Dużo istotniejszym problemem jest przeznaczenie samego pojęcia — zbyt inkluzywnego¹⁰⁰ i plastycznego¹⁰¹, aby uznać je za przydatne analitycznie. Obejmuje ono właściwie każdą formę agresji, tak długo jak tylko nie jest ona opisywalna jako pojedyncza (odosobniona) forma walki. Prowadzi to do tak kuriozalnych sytuacji jak nazwanie słów Ławrowa „wojną hybrydową”, kiedy ten skrytykował niemiecką policję za brak przejrzystości ws. gwałtu na 13-letniej Rosjance w Berlinie¹⁰². Komentatorzy przyjęli taki dyskurs, gdyż „hybrydowość” jest modna oraz wygodna w użyciu, pozwalając przypiąć łatkę do wielu pozawojzkowych działań¹⁰³.

Należy zadać sobie pytanie: czy niemilitarne metody naprawdę są działaniami wojennymi? A jeżeli tylko w określonych przypadkach, to czy definicje „wojny hybrydowej” nie powinny tego precyzować, zamiast pozostawiać w sferze niedopowiedzenia i arbitralnej uznaniowości? Rodzi to bowiem obawy, że elementy zwykłej konkurencji między państwami będą nosić znamiona „wojny hybrydowej”, mimo iż nie stwarzają realnego zagrożenia dla bezpieczeństwa narodowego (ponad dopuszczalne granice), lub nie grożą użyciem siły¹⁰⁴. W takim wypadku koncept hybrydowości nabiera znamion mało wiarygodnej ideologii, nie różniąc się zbytnio od stanowiska Rosji, jakoby była ona w stanie „wojny” z zachodnią demokracją, kulturą i wartościami — przez okcydentalizację oraz „kolorowe rewolucje”¹⁰⁵. Problemy te wynikają z faktu, iż definicja Hoffmana jest zbyt wąska, pomijając np. aspekt propagandowy. Późniejsze dodanie do niej pojęć działań nieregularnych, asymetrycznych i podobnych, spowodowało otrzymanie terminu opisującego

⁹⁹ O. Firdman, *Hybrid Warfare or Gibridnaya Voyna...*, s. 45–46.

¹⁰⁰ C.S. Gray, *Categorical Confusion? The Strategic Implications of Recognizing Challenges Either as Irregular or Traditional*, Carlisle 2012, s. 41.

¹⁰¹ E. Tenenbaum, *Le piège de la guerre hybride*, „Focus stratégique” 2105, No. 63, s. 43.

¹⁰² B. Renz, H. Smith, *Russia and Hybrid warfare - going beyond the label*, „Aleksanteri Papers” 2016, No. 1, s. 18.

¹⁰³ J. Bērziņš, *A New Generation of Warfare*, „Per Concordiam” 2015, Vol. 6, No. 3, s. 24.

¹⁰⁴ J.K. Wither, *Making Sense of Hybrid Warfare...*, s. 79.

¹⁰⁵ Zob. Y. Nikitina, *The “Color Revolutions” and “Arab Spring” in Russian Official Discourse*, „Connections” 2014, Vol. 14, No. 1.

każdy szkodliwy wpływ poza stanem wojny¹⁰⁶. Nie oznacza to, że binarne pojmowanie starć klasycznych oraz „nieregularnych” jest właściwsze, gdyż mamy do czynienia z całym spektrum. Jednakże według Strachana „etykiety, których używamy do opisu konfliktów — wojny wielkie i małe, regularne i nieregularne, manewrowe, przeciwpartyzanckie, czy humanitarne — w pierwszej kolejności zakładają, że poprawnie skategoryzowaliśmy samą ‘wojnę’, kiedy to wcale nie musi być prawdą. Może to prowadzić do przyjęcia stanowiska, że wojny nie zmieniają się w czasie ich trwania. A jeśli to robią, wówczas etykietowanie może wydłużyć zrozumienie, iż konflikt przeszedł z jednej kategorii w inną — tak jak w Iraku w 2003 roku”¹⁰⁷. Zatem rodzi to niebezpieczeństwo, że „wojna hybrydowa” tworzy zbędną kategorię — zbyt wąską by w porę dostrzec groźbę regularnego konfliktu masowego, bądź zbyt szeroką na skuteczne zastosowanie jej w walce. Szczególnie ostatnie jest istotnym problemem, gdyż koncept „wojny hybrydowej” nie zmienia praktyki operacyjnej, choćby *modus operandi* państw członkowskich NATO. Wprowadza nową nomenklaturę opisującą tak wiele zagrożeń, że właściwie należałoby się zastanowić, czy w ogóle można opracować skuteczną strategię przeciwko wszystkiemu¹⁰⁸.

Oceniając „wojnę hybrydową” z pozycji teorii strategicznej można dojść do wniosku, iż cała ta koncepcja jest nieprzydatna dla powtarzalnego osiągnięcia zwycięstw w walce — przez swoją „przeciwestrategiczność”¹⁰⁹. Wynika to z faktu, iż po odarciu propozycji hybrydowości do faktycznych metod tego „jak działać”, otrzymamy wskazówki dotyczące poziomu taktycznego oraz operacyjnego¹¹⁰. Oryginalna koncepcja Hoffmana pomija wiele czynników pozamilitarnych, będąc przydatną co najwyżej dla ramowych wytycznych w doktrynach. Można byłoby ją zatytułować „trendami konwergencji w taktyce”¹¹¹. Z kolei próba dopisania do niej innych elementów doprowadzić może albo do „rozwodnienia” teorii, albo opisanie tego, czym strategia jest z samej swej definicji — nie potrzebując przy tym dodatkowej kategoryzacji lub opisu nową nomenklaturą. Co więcej, nie ułatwia to Zachodowi zrozumienia działań rosyjskich. Bo przecież nie potrzeba nowej i niejasnej kategorii aby stwierdzić, iż w Rosji przywiązuje się szczególną uwagę do działań prowa-

¹⁰⁶ R. Kristi, P. Järvenpää, *A New Era of EU-NATO Cooperation: How to Make the Best of a Marriage of Necessity*, Tallinn 2017, s. 12.

¹⁰⁷ H. Strachan, *On War, Joint Warfare*, „The RUSI Journal” 2009, Vol. 154, No. 4, s. 20.

¹⁰⁸ M. Caliskan, M. Liégeois, *The concept of ‘hybrid warfare’...*, wywiad 7, s. 304.

¹⁰⁹ S. Rinelli, I. Duyvesteyn, *The Missing Link: Civil-Military Cooperation and Hybrid Wars*, [w:] *A Civil-Military Response to Hybrid Threats*, E. Cusumano, M. Corbe (eds.), London 2018, s. 17–40.

¹¹⁰ M. Caliskan, *Hybrid warfare through the lens of...*, s. 49.

¹¹¹ D.G. Cox, T. Bruscinio, A. Ryan, *Why Hybrid Warfare Is Tactics Not Strategy: A Rejoinder to “Future Threats and Strategic Thinking”*, „Infinity Journal” 2012, Vol. 2, No. 2, s. 28.

dzonych przed interwencją zbrojną, ze szczególnym wpływem czynników geopolitycznych (przestrzennego rozumienia przebiegu konfliktów)¹¹².

Należałoby jeszcze zastanowić się nad przyczynami stworzenia pojęcia „wojen hybrydowych”, co pomogłoby go lepiej zrozumieć ich miejsce w nauce. Ciekawe światło rzuca Maria Mälksoo, która mówi o jej ontologicznych podstawach, jako źródło wskazując niepewność w stosunkach międzynarodowych i zarządzania dylematem bezpieczeństwa państw. W sprawach zarządzania zagrożeniami hybrydowymi, czyli studium mocno skoncentrowanym na polityce oraz wojskowości, zaproponowana perspektywa systematyzuje i konceptualizuje dynamikę lęku, jak również radzenia sobie z nim. Zdaniem autorki, „wojna hybrydowa” podważa dotychczasowe struktury poznawcze na temat tego czym wojna jest, przez to dezorganizując życie i relacje społeczne¹¹³. Jawi się to jako uosobienie ontologicznej niepewności, czyli „głębokiego, paraliżującego stanu niewiedzy, którym zagrożeniom stawić czoła, a które ignorować, czyli jak sobie radzić w świecie”¹¹⁴. To co rozumiane jest jako zagrożenia hybrydowe, instytucjonalizuje niepewność i epistemologicznie burzy binarność czasu wojny oraz pokoju, przy tym stawiając pod znakiem zapytania dotychczasowe strategie „bycia” czy „działania”¹¹⁵. Co więcej, hybrydowość płącze ze sobą wojnę oraz politykę, zagrażając skompromitowaniem i tak już rozmytego rozróżnienia¹¹⁶. Uwydatnia to paradoks obrony społeczeństw demokratycznych, ponieważ skuteczność przeciwdziałania zagrożeniom może podważać etyczne podstawy samych demokracji. Choć np. Foucault uważa, iż „wojna hybrydowa” po prostu uwypukliła utrzymywanie potęgi we współczesnym świecie, gdyż pokój w społeczeństwie obywatelski musi być rozumiany jako tajna wojna. Jest ona bowiem zasadą i motorem sprawowania władzy politycznej¹¹⁷.

A zatem wysuwa się wniosek, że początkowe zainteresowanie koncepcją wojen hybrydowych mogło być odpowiedzią na ontologiczną niepewność, w myśl iż jakiegokolwiek wyjaśnianie świata jest lepsze niż żadne. Zarazem być może stanowiło ono uspra-

¹¹² M. Wojanowski *Mit „wojny hybrydowej”*. *Konflikt na terenie...*, s. 37.

¹¹³ M. Mälksoo, *Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO*, „European Security” 2018, Vol. 27, No. 3, s. 374–375.

¹¹⁴ Oryg. Ontological insecurity refers to the deep, incapacitating state of not knowing which dangers to confront and which to ignore, i.e. how to get by in the world; J. Mitzen, *Ontological security in world politics: state identity and the security dilemma*, „European Journal of International Relations” 2006, No. 12 (3), s. 345.

¹¹⁵ T. Flockhart, *The problem of change in constructivist theory: ontological security seeking and agent motivation*, „Review of international studies” 2016, No. 42 (5), s. 799–816.

¹¹⁶ M. Mälksoo, *Countering hybrid warfare as ontological...*, s. 386.

¹¹⁷ M. Foucault, *“Society must be defended”*. *Lectures at the Collège de France*, trans. D. Macey, London 2003, s. 15–18.

wiedliwienie podejmowania wątpliwych działań przez współczesne demokracje, co wyjaśniałoby zachodnią genezę pojęcia. Mimo, że żaden z tych przypadków nie broni braków „wojny hybrydowej”, to daje ciekawy wgląd w lepsze zrozumienie przyczyn powstania i rozwoju tej koncepcji.

3.2. Analiza pojęcia asymetryczności i jej krytyka

Jak wskazano powyżej, od starożytności ludzkość poszukiwała środków i metod skuteczniejszego dominowania nad innymi, celem osiągania własnych celów. Oznacza to, że także wykorzystanie asymetrii lub w ogóle występowanie tego zjawiska jest dla wojen zupełnie naturalne. Zdecydowanie zwiększa się udział czynników asymetrycznych w konfliktach, lecz one same zdają się pozostawać takie same. Największe państwa wciąż stosują dotychczas znaną sztukę wojenną, której nowoczesne oblicze pola walki fundamentalnie nie zmienia. Clausewitz przedstawiał zbiór reguł sztuki wojennej, uwzględniając w nim: *zmasowanie, cel, ekonomię sił, prostotę, zaskoczenie, jedność dowodzenia, ubezpieczenie, ofensywę* (rozumianą nie jako aktywność, posiadanie inicjatywy) oraz *manewr*¹¹⁸. Wszystkie te zasady wciąż pozostają w mocy, a reagowanie na zjawiska asymetryczne albo ten zbiór poszerza, albo traktuje go ramowo, jedynie doprecyzowując aplikowanie tychże reguł względem „Nowych Wojen”. Punktem wyjściowym dla analizy samej asymetryczności będzie więc prześledzenie tego, w jaki sposób koncepcja ta kształtowała się na przestrzeni dekad.

Jednocześnie podkreślić należy, że podobnie jak w analizie hybrydowości, także i tu występuje problem określenia co wojną jest. Konflikty asymetryczne wykorzystują wszelkie możliwe środki, co wiąże się z brutalizacją pola walki, szczególnie przy zaangażowaniu podmiotów pozapaństwowych. Zacierają to granice między pokojem i wojną¹¹⁹, choć zarazem każe zadać pytanie: czy takiego zatarcia spodziewać się należy zawsze? Zdaje się bowiem, że wiele konfliktów po prostu klasyczną wojną nie miały być, a zjawisko asymetrii (lub hybrydowości) nie było tego powodem, lecz jedynie narzędziem wykorzystanym w danych okolicznościach. Wojna w Ukrainie trwająca od 2022 roku pokazuje, jak istotne są klasyczne formy walki, a także jak komplementarnie uzupełniają je nowoczesne technologie i taktyki.

Jest to jednak starcie między dwoma państwami i odróżnić je należy od konfliktów asymetrycznych, w których duży udział mają podmioty pozapaństwowe. Za Münk-

¹¹⁸ C. von Clausewitz, *O wojnie*, s. 143.

¹¹⁹ A. Wejksznier, *Wojny XXI wieku. Istota współczesnych konfliktów asymetrycznych*, [w:] *Zagrożenia asymetryczne współczesnego świata*, S. Wojciechowski, R. Fiedler (red.), Poznań 2009, s. 125–127.

rem¹²⁰, Epplerem¹²¹ można też wskazać, że konflikty takie będą mieć tendencję do przeciągania się latami. Ani nie sprzyjają one budowaniu kapitału stron konfliktu, ani umacnianiu państwowości — jak to miało miejsce w przypadku poprzednich wojen. Dlatego jedynym sposobem do ich zakończenia może być interwencja zewnętrzna. Eppler będący badaczem-pacyfistą, sam wzywa do ponownego przemyślenia znaczenia pacyfizmu w czasach nowych wojen. Szczególnie, że w powstrzymaniu sprywatyzowanej przemocy nieefektywne będą rozwiązania pokojowe. Co więcej, takie konflikty charakteryzują się niewielką podatnością na tradycyjne metody przeciwdziałania, np. przez odstraszenie lub przymus (zarówno w formie groźby, jak i jego użycia)¹²². Przeciwnicy asymetryczni pozostają rozproszeni, wymagając działań niekonwencjonalnych¹²³, a przez to kluczowych zmian w sposobach prowadzenia walki szczebla taktycznego i niejednokrotnie operacyjnego.

3.2.1. Rozwój koncepcji asymetryczności

Ze względu na powszechność posługiwania się terminem asymetryczności, trudno jednoznacznie wskazać moment, w którym zaczęła być używana. Możliwe jest jednak wskazanie wzrostu jej popularności w literaturze naukowej oraz w dokumentach z lat 90. XX wieku. Analitycy wojskowi i badacze zaczęli wówczas poszukiwać terminów opisujących nowe formy konfliktów po zakończeniu zimnej wojny. Rozpad Związku Radzieckiego oraz zmiana charakteru konfliktów międzynarodowych na bardziej lokalne i nieregularne, wymusiły analizę taktyk stosowanych przez słabsze podmioty, w tym grupy terrorystyczne.

W odpowiedzi na te wyzwania, Departament Obrony USA wprowadził definicję wojny asymetrycznej, wskazując że walka asymetryczna to: „próby obejścia lub osłabienia mocnych stron przeciwnika, przy jednoczesnym wykorzystaniu jego słabości, przez użycie

¹²⁰ Herfried Münkler (ur. 15 sierpnia 1951) — niemiecki politolog, profesor teorii politycznej na Uniwersytecie Humboldta w Berlinie. Historyk myśli politycznej i badacz teorii wojny, szczególnie Machiavellego; Munzinger Archiv GmbH, *Internationales Biographisches Archiv*, 19/2021 vom 11. Mai 2021 (bo), Eintrag „Münkler, Herfried”, <https://www.munzinger.de/search/go/document.jsp?id=00000024700> [dostęp: 10 sierpnia 2023].

¹²¹ Erhard Eppler (ur. 9 grudnia 1926, zm. 19 października 2019) — niemiecki polityk, publicysta, nauczyciel i myśliciel zaangażowany w rozwój środowiska i ruchy pokojowe. Założyciel che Gesellschaft für Internationale Zusammenarbeit (GIZ) (Niemiecka Agencja Współpracy Międzynarodowej), minister współpracy gospodarczej; Munzinger Archiv GmbH, *Internationales Biographisches Archiv*, 16/2020 vom 14. April 2020 (la), Eintrag „Eppler, Erhard”, <https://www.munzinger.de/search/go/document.jsp?id=00000012072> [dostęp: 10 sierpnia 2023].

¹²² M. Madej, *Terroryzm i inne zagrożenia asymetryczne w świetle współczesnego pojmowania bezpieczeństwa narodowego i międzynarodowego — próba teoretycznej konceptualizacji*, [w:] *Porządek międzynarodowy u progu XXI wieku*, R. Kuźniar (red.), Warszawa 2005, s. 509.

¹²³ K. Piątkowski, *Wojna nowego typu?*, „Polska w Europie” 2002, nr 1, s. 37–38.

metod znacznie różniących się od zwykłego sposobu działania przeciwnika”¹²⁴. Warto przy tym wskazać, że Departament Obrony rozszerzał powyższą definicję i podejmował próbę identyfikacji źródeł: technologicznych lub kulturowych¹²⁵.

Definicja Centralnej Agencji Wywiadowczej USA była bardziej precyzyjna i skupiała się ponadto na aspekcie technologicznym, naturalnym dla jej charakterystyki działania. Według CIA, walka asymetryczna to: „stosowanie innowacyjnych strategii, taktyk i technologii przez słabsze państwo lub podpaństwo przeciwnika, których celem jest uniknięcie mocnych stron i wykorzystanie potencjalnych słabości większych i technologicznie lepszych przeciwników. Obejmuje to: 1) selektywne użycie broni lub zasobów wojskowych przez państwo lub grupę podpaństwową w celu przeciwdziałania, odstraszenia lub ewentualnego pokonania licznie lub technologicznie lepszych sił; 2) wykorzystanie zasobów dyplomatycznych i innych niemilitarnych zasobów lub taktyk przez państwo lub grupę podpaństwową w celu zniechęcenia lub ograniczenia działań wojskowych przez silniejsze siły”¹²⁶.

Termin "asymmetric warfare" zaczął być szczególnie widoczny w analizach takich autorów jak Ivan Arreguín-Toft (2001). W swoim artykule *How the Weak Win Wars: A Theory of Asymmetric Conflict* krytykuje on tradycyjne teorie, takie jak natura aktora, dyfuzja broni i asymetria interesów, uznając je za niewystarczające do wyjaśnienia rosnącego trendu przegrywania asymetrycznych wojen przez główne mocarstwa. Arreguín-Toft wprowadza nową hipotezę, opartą na interakcjach strategicznych. Argumentuje, że interakcja podobnych podejść strategicznych sprzyja silnym aktorom, podczas gdy przeciwnie podejścia strategiczne (użycie strategii niekonwencjonalnych) sprzyjają słabym¹²⁷. Wykorzystując analizę statystyczną i historyczne studia przypadków, wykazuje, że interakcja strategiczna jest najlepszym predyktorem wyników asymetrycznych konfliktów, zapewniając niuansowe zrozumienie dynamiki wojny¹²⁸. Takie spojrzenie było zarazem

¹²⁴ Oryg. Attempts to circumvent or undermine an opponent's strengths while exploiting his weaknesses using methods that differ significantly from the opponent's usual mode of operation; D. J. Wurzel, K.R. McGruther, W. R. Murray, *A Survey of Unclassified Literature on the Subject of Asymmetric Warfare*, Sherman Oaks 1998, s. 13.

¹²⁵ Tamże, s. 7.

¹²⁶ Oryg. The use of innovative strategies, tactics, and technologies by a 'weaker' state or substate adversary that are intended to avoid the strengths and exploit the potential vulnerabilities of larger and technologically superior opponents. This includes: 1. The selective use of weapons or military resources by a state or substate group to counter, deter, or possibly defeat a numerically or technologically superior force. 2. The use of diplomatic and other non-military resources or tactics by a state or substate group to discourage or constrain military operations by a superior force; CIA, *Statement of Work for Asymmetric Warfare Threats to US Interests: Expert Panel Support*, Washington 1998, s. 2.

¹²⁷ I. Arreguín-Toft, *How the Weak Win Wars...*, s. 104–110.

¹²⁸ Tamże, s. 96–99, 110–118, 124–128.

odpowiedzią na nowe wyzwania, jakie stawiały konflikty w takich miejscach jak Somalia, Afganistan czy Irak, gdzie tradycyjne siły militarne nie zawsze odnosiły sukcesy mimo przewagi technologicznej i liczebnej.

Ważną zdaje się także być praca Davida L. Buffaloe'a (2006) *Defining Asymmetric Warfare*, gdyż dostarcza dość kompleksowej analizy koncepcji wojny asymetrycznej, której doszukuje się w czasach starożytnych, a przejawów jej koncepcji w ostatnich stuleciach¹²⁹. Dalej autor wskazuje on m.in. konkretne cechy tego rodzaju walk, takie jak:

- metody niekonwencjonalne — takie jak wojna partyzancka, terroryzm;
- operacje psychologiczne — stosowane w celu osłabienia morale przeciwnika, a jednocześnie wzmocnienia determinacji własnych sił;
- wykorzystanie terenu i zasobów cywilnych — przez słabszą stronę, co utrudnia skuteczne zaangażowanie strony przeważającej¹³⁰.

Pozwoliło to Buffaloe'wi zaproponować szczegółową definicję wojny asymetrycznej jako „populacyjnie skoncentrowanej, nietypowej wojny prowadzonej między militarnie przeważającą potęgą a jedną lub większą liczbą słabszych potęg, obejmującej wszystkie następujące aspekty: ocenę i pokonanie zagrożenia asymetrycznego, prowadzenie operacji asymetrycznych, zrozumienie asymetrii kulturowej i ocenę asymetrycznego kosztu”¹³¹.

Choć kompleksowa, definicja ta wprowadza pewną niejednoznaczność, zwłaszcza przez wzgląd na zdefiniowanie poszczególnych jej składowych, takich jak asymetrii kulturowej, czy asymetrycznego kosztu. W analizie Buffaloe'a dostrzec można mocne skoncentrowanie się na armii USA i jej doświadczeniach, a także — mimo wszystko — amerykańskim kontekście kulturowym. Uwidacznia się to również w zaproponowanym wzorze na wojnę asymetryczną¹³². Mimo podjęcia próby empirycznej parametryzacji tego zjawiska, opiera się on na kategoriach podlegających subiektywnej ocenie, co w tym przypadku uniemożliwia uzyskanie wyniku obiektywnego.

Powyższe podejście zbytnio skupia się też na podkreślaniu uzyskiwaniu przewagi mniejszego aktora, co tworzy niepełny obraz zjawiska. Przeciwnicy równi sobie również

¹²⁹ D.L. Buffaloe, *Defining Asymmetric Warfare*, „The Land Warfare Papers” 2006, No. 58, s. 7–13.

¹³⁰ Tamże, s. 1–13.

¹³¹ Oryg. *Asymmetric warfare is population-centric nontraditional warfare waged between a militarily superior power and one or more inferior powers which encompasses all the following aspects: evaluating and defeating asymmetric threat, conducting asymmetric operations, understanding cultural asymmetry and evaluating asymmetric cost*; tamże, s. 17.

¹³² Ze względu na niewykorzystanie wzoru w dalszej części niniejszej dysertacji, przez jego nieprzydatność, odstąpiono od szczegółowego jego opisanie. Objaśnienie zaproponowanego $AW=AT+AO+CA+AC$ odnaleźć można w cytowanej pracy; tamże, s. 18.

mogą wykorzystać zjawisko asymetrii, by skuteczniej osiągać swoje cele. W taki właśnie sposób Michael Breen i Joshua A. Geltzer definiują wojnę asymetryczną, ilustrując, jak może być skutecznie stosowana przez silniejsze państwa. Autorzy postrzegają strategię asymetryczną jako tę, które przekształcają postrzegane mocne strony przeciwnika w słabości, często poprzez ujawnianie własnych postrzeganych słabości jako mocnych stron¹³³. W takim rozumieniu wojna asymetryczna staje się czymś więcej niż bronią słabych, podkreślając jej strategiczną użyteczność dla silnych państw. Jako przykład wskazać można działania Chin i Rosji skierowane w stronę Stanów Zjednoczonych: przez zmianę postrzegania zaawansowanej infrastruktury technologicznej z siły tego państwa, do jego słabości. Efekt ten jest osiągany bez konwencjonalnych konfrontacji¹³⁴.

Cyberprzestrzeń odgrywa tutaj kluczową rolę, gdyż rozwiązana i technologicznie zaawansowana natura współczesnych społeczeństw znacząco zwiększają „powierzchnię ataku”. Już w 2011 roku Breen i Geltzer wskazali, że Chiny i Rosja wówczas opracowały wyrafinowane zdolności cybernetyczne, aby wykorzystać wskazane podatności i użyć cyberprzestrzeni jako mnożnika siły w swoich asymetrycznych strategiach. Anonimowość i zaprzeczalność operacji cybernetycznych (problem atrybucji) sprawiają zarazem, że są one atrakcyjną opcją dla państw, które chcą rzucić wyzwanie silniejszym przeciwnikom bez wywoływania odpowiedzi militarnej w pełnej skali¹³⁵.

Z taką diagnozą rozkładu sił trudno się nie zgodzić, a późniejsze przykłady tylko to potwierdzają. Społeczeństwa państw Zachodnich, a w szczególności USA, mierzą się z problemem znaczącego wpływu obcych wywiadów. Od stopniowej polaryzacji¹³⁶, przez wzmacnianie szkodliwych ruchów, np. skoncentrowanych wokół teorii spiskowych¹³⁷, po bezpośredni wpływ na wybory¹³⁸. Należy przy tym podkreślić, że problem ten dodatkowo komplikują fundamentalne różnice kulturowe, które tworzą środowisko wyjątkowo nie-sprzyjające państwom Zachodnim. Społeczeństwa rosyjskie i chińskie przejawiają wyższą akceptację dla znaczącej kontroli państwowej nad różnymi domenami ich życia, także w przejawach stojących w opozycji do indywidualizmu jednostki¹³⁹. Znacząco ułatwia to

¹³³ M. Breen, J.A. Geltzer, *Asymmetric Strategies as Strategies of the Strong*, „Parameters” 2011, Vol. 41, No. 1, s. 41.

¹³⁴ Tamże, s. 43–44.

¹³⁵ Tamże, s. 48.

¹³⁶ G. Cosentino, *Social Media and the Post-Truth World Order The Global Dynamics of Disinformation*, Cham 2020, s. 5–16.

¹³⁷ S. Radnitz, *Solidarity through Cynicism? The Influence of Russian Conspiracy Narratives Abroad*, „International Studies Quarterly” 2022, No. 66, s. 7–12.

¹³⁸ V.C. Keating, O. Schmitt, *Ideology and influence in the debate over Russian election interference*, „International Politics” 2021, Vol. 58, No. 5, s. 4–16.

¹³⁹ C. Owen, *Participatory authoritarianism: From bureaucratic transformation to civic* →139

akceptację silnych mechanizmów kontroli i wpływu w cyberprzestrzeni, takich jak nadzoru (podśluchu), propagandy, czy cenzury¹⁴⁰. Skutkiem tego jest powstanie systemów trudnych do zinfiltrowania przez zewnętrzny nacisk. Odwrotnie sytuacja wygląda w państwach Zachodnich. Wolność słowa, niska kontrola nad komunikacją oraz ogromna swoboda osobista sprawiają, iż w społeczeństwa te łatwo przeniknąć z przekazem propagandowym lub destabilizującym. Jakikolwiek działania dążące do objęcia cyberprzestrzeni cyfrowej nadzorem, będą tworzyć opór społeczeństwa i zaostrzać nastroje przeciw rządowe, co państwa takie jak Rosja z pewnością by wykorzystały. Natomiast brak właściwych akcji pozostawi przeciwnikowi więcej przestrzeni na prowadzenie szkodliwych kampanii. Tworzy to obraz głębokiej asymetrii między mocarstwami, która już teraz jest wykorzystywana na szeroką skalę, mimo że zdajemy się stać dopiero u progu wykorzystania potencjału cyberprzestrzeni.

Breen i Geltzer proponowali, by odpowiedzią na powyższe było proaktywne oraz innowacyjne podejście. Sugerowali, że Stany Zjednoczone powinny nie tylko skupić się na obronie przed atakami asymetrycznymi, ale także opracować własne strategie asymetryczne, dążące do tworzenia strategicznych niespodzianek i wykorzystywania podatności przeciwników. Autorzy podkreślają też potrzebę kompleksowego zrozumienia krajozobu asymetrycznego, w tym motywacji i taktyk adwersarzy, przyjmując bardziej elastyczne i adaptacyjne nastawienie¹⁴¹.

Wychodząc od skupienia uwagi na czynniku ludzkim, interesująca jest również analiza zjawiska walki asymetrycznej z punktu widzenia darwinowskiej biologii ewolucyjnej. Zakłada ona, że modelowanie konfliktów skupia się głównie na sile militarnej, pomijając istotny element dynamiki ewolucyjnej konkurujących populacji: procesu *adaptacji przez selekcję naturalną*. Jej reguły nie odnoszą się wyłącznie do mechanizmów biologicznych, lecz bytów ogólnie (włączając w to maszyny), pogody itd., tak długo jak znaczenie mogą mieć trzy warunki: *różnorodność, selekcja i replikacja*¹⁴². To właśnie one warunkować mają istotę walki asymetrycznej. *Różnorodność* bowiem zapewnia większą pulę cech w danej populacji (np. zróżnicowanie umiejętności, pochodzenia, wykształcenia), co zapewnia potencjalnie wyższy wskaźnik innowacyjności („mutacji”), a tym samym

participation in Russia and China, „Review of International Studies” 2020, Vol. 46, Issue 4, s. 18–35; J. Richter, W.F. Hatch, *Organizing Civil Society in Russia and China: A Comparative Approach*, „International Journal of Politics, Culture, and Society” 2013, Vol. 26, s. 328–333, 343–344.

¹⁴⁰ V. Weber, *The Worldwide Web of Chinese and Russian Information Controls*, „Centre for Technology and Global Affairs: Working Paper Series” 2019, No. 11, s. 4–6.

¹⁴¹ M. Breen, J.A. Geltzer, *Asymmetric Strategies...*, s. 51–52.

¹⁴² D. Johnson, *Darwinian selection in asymmetric warfare: the natural advantage of insurgents and terrorists*, „2010 Journal of the Washington Academy of Sciences” 2010, Vol. 95, No. 3, s. 89.

premiuje przetrwanie. Stoi to zarazem w opozycji do relatywnie bardziej zamkniętego katalogu cech, które wynikać mogą z umiejętności pożądanых przez konwencjonalne siły, czy też zunifikowanych systemów szkolenia żołnierzy¹⁴³. Co więcej, próba przełamania tego konwencjonalną przewagą siły sprawia, iż mechanizm *selekcji* naturalnie pozbędzie się jednostek słabszych, pozostawiając mocniejsze. To z kolei znacząco podniesie adaptację ogółu słabszej strony¹⁴⁴. Finalnie *replikacja* odnajdywana jest w samym sposobie zarządzania ludźmi. Jednostki wewnątrz słabszej strony konfliktu zazwyczaj pozostają na polu walki dłużej, premiując zdobywanie doświadczenia, wiedzy i w efekcie skuteczniej przystosowując się. Mogą także przenieść to na jednostki nowe. Konwencjonalne siły stosują natomiast szybszą rotację żołnierzy, opierając się w dużej mierze na szkoleniu ogólnym, które modyfikowane jest o doświadczenia z pola walki¹⁴⁵. Autor wskazuje więc na pewnego rodzaju odgórny (arbitralny) transfer doświadczeń, zamiast oddolnego (naturalnego). To właśnie ten drugi pozwala na szybszą akumulację adaptacji, stanowiącej kluczowy argument za istotą substytutu siły u słabszych stron. Wynika to z faktu, że wszelkie przystosowanie jest odpowiedzią na pewne zdarzenia, a zatem immanentnie jest to mechanizm funkcjonujący za późno. Jednak odpowiednie nagromadzenie takich reakcji w wąskiej populacji może doprowadzić do wypracowania nowych technik¹⁴⁶.

Trudno jednak w pełni zgodzić się z tymi założeniami. O ile podnoszą one istotny głos w ocenie wpływu ludzkiej natury na konflikty, to np. tak duży nacisk na adaptację zupełnie pomija inne czynniki, jak choćby strategiczną przewagę w znajomości pola walki i trafnego lokowania wojsk, czy wpływ wsparcia międzynarodowego. Co więcej, stosowanie darwinowskiego podejścia presuponuje racjonalność wszystkich jednostek i wynikającą z niego chęć przystosowania się do przetrwania. W praktyce jednak widzimy znaczący wpływ ideologii czy religii, indukującej motywacje irracjonalne¹⁴⁷. Co więcej, te mogą być tak samo skutecznie wykorzystywane zarówno przez słabszego adwersarza, jak i mocniejszego — szczególnie w kontekście patriotyzmu lub nacjonalizmu¹⁴⁸. Niepomijalnym jest też fakt, iż mimo wyzwań adaptacyjnych, silniejsza strona nadal cechuje się znaczącą przewagą zasobów i zdolności wojskowych. Te odgrywają szczególną rolę

¹⁴³ Tamże, s. 96–98.

¹⁴⁴ Tamże, s. 98–99.

¹⁴⁵ Tamże, s. 99.

¹⁴⁶ Tamże, s. 107–109.

¹⁴⁷ J.L. Maynard, *Ideology and armed conflict*, „Journal of Peace Research” 2019, Vol. 56, No. 5, s. 636, 638; R. Nalbandov, *Irrational Rationality of Terrorism*, „Journal of Strategic Security” 2013, Vol. 6, No. 4, s. 93–95.

¹⁴⁸ V. Nedzinskaitė-Mitkė, *Modern National Identity and Patriotism*, „Filosofija. Sociologija” 2022, Issue 3, s. 255–257.

w osiąganiu ogólnych celów wojny, nawet jeśli mogą być równoważone w pewnych jej fragmentach. Przyznać autorowi należy, że w określonych warunkach dynamiki poziomu mikro (skupienia się na indywidualnych jednostkach) zapewniają słabszej stronie przewagę lub przynajmniej zrównują ją z silniejszym adwersarzem. Darwinowskie podejście pomija jednak poziom makro, tj. wpływ polityki międzynarodowej, ekonomii czy czynników społecznych w szerszym ujęciu.

Należy zatem podkreślić, że chociaż podejście to zapewnia cenny wgląd w dynamikę asymetrycznych działań wojennych, to pozostaje jedną z wielu struktur stosowanych do zrozumienia złożoności współczesnych konfliktów. Niepomijana pozostaje rola asymetrii materialnych, strategicznych i zacierania się tradycyjnych granic wojennych.

Powyżej przytoczone koncepcje, choć poruszające asymetryczność w sposób zróżnicowany i interesujący, nie zapewniają pełnego obrazu. Z tego względu istotnym staje się porównanie sposobu definiowania asymetrii pomiędzy spojrzeniem szerzej rozumianego Zachodu, Rosji i Chin.

3.2.2. Zachodnie spojrzenie na zagrożenia asymetryczne

W połowie XX wieku Basil Liddell Hart promował „podejście pośrednie” w strategii, opowiadając się za unikaniem mocnych stron wroga, upraszczaniem działań i celowaniem w słabości¹⁴⁹. Edward N. Luttwak rozszerzył tę koncepcję o „logikę paradoksalną”, u podstaw której legła ludzka natura. Zakłada ona możliwość odwrócenia przeciwności, w których to zagrożenia pozornie nieznaczące mogą urosnąć do rangi istotnych, a ogromne potencjały siły okazać się mogą bezskuteczne¹⁵⁰. Broń wydatnie użyteczna na początku wojny, w późniejszej jej fazie może utracić na znaczeniu. Podobnie adwersarz niestanowiący zagrożenia, może wyrządzić wielkie straty dużo silniejszej od siebie stronie konfliktu. Tę przebiegłość i wywrotowość asymetrycznego przeciwnika później podkreślił George W. Bush, w słowach „nie możemy pozwolić, aby zagraniczni wrogowie wykorzystują fora wolności, aby zniszczyć samą wolność”¹⁵¹.

W kresie zimnej wojny asymetria stanowiła istotny element amerykańskiej myśli strategicznej, choć rzadko definiowana pod tą nazwą. Dostrzegano wówczas różnice przewagi ilościowej w Europie, jaką miał Związek Radziecki, do przewagi jakościowej Stanów Zjednoczonych i NATO. Pierwsze wyraźne skupienie się na współcześnie rozumianych konfliktach asymetrycznych pojawia się w amerykańskiej Wspólnej Doktrynie

¹⁴⁹ B.L. Hart, *Strategy...*, s. 5.

¹⁵⁰ E.N. Luttwak, *Strategy: The Logic of War and Peace*, Cambridge 1987, s. 5.

¹⁵¹ *Remarks to the United States Attorneys Conference*, „Weekly Compilation of Presidential Documents” [R04], 2001, Vol. 37, No. 48, s. 1728.

z 1995 roku. Wtedy jednak rozumiano je dość wąsko, jako starcia między siłami o różnym potencjale¹⁵², szczególnie w rozumieniu przestrzeni walki (powietrze kontra ziemia, itd.). Podobnie w literaturze starcia te definiowano jako „konflikt, w którym biorą udział dwa państwa o nierównych ogólnych zasobach militarnych i gospodarczych”¹⁵³. Jednakże opublikowana w tym samym roku Narodowa Strategia Wojskowa USA wyraźnie wskazywała na terroryzm czy proliferację broni masowego rażenia, a także wyzwania związane z wojną informacyjną¹⁵⁴. Zatem zaczęto oddzielać nowe definicje konfliktów asymetrycznych od po prostu różnicy potencjału między państwami. Jest to o tyle istotne, że niemalże każda wojna z udziałem USA (lub szerzej NATO) byłaby z definicji pozbawiona symetrii przez poziom zaawansowania technologii wojskowych, sił i środków. Podobnie zbytne skupienie się na tylko wykorzystaniu słabości jako jakiegoś novum byłoby nieprawdziwe, gdyż stanowi to podstawę prowadzenia wojen¹⁵⁵.

Rozumienie przedmiotowych konfliktów rozwijało się o kolejne elementy, aż w latach 90. XX wieku zaczęło zmieniać postrzeganie środowiska bezpieczeństwa po zimnej wojnie. Uznawanie rosnącego potencjału asymetrii zagrożeń dla Stanów Zjednoczonych (ze strony mniejszych podmiotów) oraz asymetrii globalnego rozkładu władzy sprawiły, że konflikty i strategie asymetryczne będą naturalną ewolucją.

Asymetria zaczęła przenikać dyskusje w kręgach obronnych i politycznych USA, a przez to także pozostałych państw NATO. Jednak powszechność użycia tego terminu prowadziła do nieporozumień i błędnych interpretacji, gdyż definicje nie były spójne. Przeciwnie, skupiały się raczej na obszarach bardzo ogólnych lub selektywnych, jak np. konkretne uzbrojenia czy taktyki¹⁵⁶. Stawienie czoła wieloaspektowej naturze takich konfliktów zaczęło wykraczać poza uproszczone kategoryzacje i obejmować zniuansowaną dynamikę. Wymaga to holistycznego podejścia, które uwzględnia nie tylko bezpośrednie implikacje dla bezpieczeństwa, ale także szersze konsekwencje polityczne i etyczne.

Istotnym wydarzeniem były ataki z 11 września na World Trade Center. W odpowiedzi na nie, Kenneth F. McKenzie Jr zredefiniował konflikt asymetryczny jako „wykorzystanie słabszej siły taktycznej lub operacyjnej przeciwko [słabościom] silniejszego

¹⁵² G.A. Harrison, *Overlord: A classic Joint and Combined Operation*, [w:] *Joint Warfare of the Armed Forces of the United States [Joint Pub. 1]*, Washington 1995, s. IV-10–11.

¹⁵³ T.V. Paul, *Asymmetric Conflicts: War Initiation by Weaker Powers*, Cambridge 1994, s. 20.

¹⁵⁴ *National Military Strategy of the United States of America. A Strategy of Flexible and Selective Engagement*, Washington 1995, s. 3–10.

¹⁵⁵ W.H. von Heinegg, *Asymmetric Warfare: How to Respond?*, „U.S. Naval War College, International Law Studies” 2011, Vol. 87, s. 464–465.

¹⁵⁶ S. Lambakis, J. Kiras, K. Kolet, *Understanding „Asymmetric” Threats to the United States, „Comparative Strategy”* 2002, Vol. 21, No. 4, s. 253–257.

przeciwnika celem osiągnięcia nieproporcjonalnego efektu w celu osłabienia woli [przeciwnika] dla osiągnięcia celów strategicznych aktora asymetrycznego”¹⁵⁷. Na tę nieproporcjonalność położono szczególny nacisk, gdyż była kluczem do „osiągania celów strategicznych poprzez zastosowanie skromnych zasobów”¹⁵⁸. Co więcej, autor podkreślał nie tylko zastosowanie asymetrii na wszystkich trzech poziomach prowadzenia walki (strategicznym, operacyjnym i taktycznym), lecz także ich wzajemne przenikanie się (np. jak duży wpływ taktyka może mieć bezpośrednio na strategię)¹⁵⁹.

W 2003 roku NATO wprowadziło do własnego słownika terminów i definicji (AAP-6) pojęcie *zagrożeń hybrydowych*, identyfikowanych jako „zagrożenie wynikające z możliwości zastosowania różnych środków i metod w celu obejścia lub neutralizacji silnych punktów przeciwnika, wykorzystując jednocześnie jego słabości w celu uzyskania niewspółmiernych wyników”¹⁶⁰. Od tamtej pory w terminie tym nie wprowadzono żadnych zmian.

Aneksja Krymu przez Rosję w 2014 roku skłoniła NATO do wzmocnienia swoich zdolności odstraszenia w celu ochrony wschodniej flanki. NATO miało jednak trudności z zajęciem się pozamilitarnymi aspektami wojny hybrydowej, takimi jak cyberataki, zakłócenia gospodarcze i manipulacja informacjami. Luka ta doprowadziła do wzmożonych wezwań do współpracy między NATO, rządami europejskimi i społeczeństwem obywatelskim w celu stawienia czoła tym wieloaspektowym zagrożeniom. Na początku 2015 r. potrzeba zaangażowania UE w przeciwdziałanie zagrożeniom hybrydowym zyskała na znaczeniu¹⁶¹, co zaowocowało nową polityką bezpieczeństwa i utworzeniem organów takich jak Grupa Zadaniowa *East StratCom*¹⁶², których zadaniem jest przeciwdziałanie rosyjskiej dezinformacji.

¹⁵⁷ Z ang. *leveraging inferior tactical or operational strength against American vulnerabilities to achieve disproportionate effect with the aim of undermining American will in order to achieve the asymmetric actor's strategic objectives*; K.F. McKenzie, Jr., *The Revenge of the Melians: Asymmetric Threats and the Next QDR*, Wasington 2000, s. 2.

¹⁵⁸ Tamże.

¹⁵⁹ Tamże, 8–9.

¹⁶⁰ *Słownik terminów i definicji NATO*, [AAP-6], 2017, s. 66.

¹⁶¹ *European Council meeting (19 and 20 March 2015) — Conclusions*, 20 March, [Cover note EUCO 11/15], 2015, s. 4–6.

¹⁶² East StratCom Task Force (ESCTF) jest częścią Służby zewnętrznej Unii Europejskiej (European External Action Service, EEAS), a konkretniej Wydziału Komunikacji Strategicznej i Analizy Informacji (Strategic Communications and Information Analysis Division, AFFGEN.7), w której funkcjonuje razem z m.in. Grupą Zadaniową Zachodnie Bałkany oraz Grupą Zadaniową Południe; *Questions and Answers about the East StratCom Task Force*, „The Diplomatic Service of the European Union”, 27.10.2021, https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11235, [odczyt: 31.02.2024].

Podczas szczytu w Madrycie w czerwcu 2022, NATO dalej wskazywało na zagrożenia asymetryczne bez podania ogólnej kategorii. Wymieniono wyłącznie terroryzm, uznając go za najbardziej bezpośredni wyraz niebezpieczeństw asymetrycznych, skierowanych przeciwko obywatelom, międzynarodowemu pokojowi, a także rozwojowi i dobrobytowi¹⁶³. Co więcej, podkreślono istotę odstraszenia jako jednego z trzech rdzeni dalszej działalności NATO¹⁶⁴ — obok zarządzania i przeciwdziałania kryzysom¹⁶⁵ oraz kooperatywnej ochrony¹⁶⁶. To właśnie odstraszanie zdaje się stanowić istotny aspekt relacji między NATO i Federacją Rosyjską, gdyż obie te strony używają złożonych mechanizmów zniechęcania adversarza do podejmowania działań. O ile konwencjonalne siły wojskowe i potencjał atomowy stanowią bardzo istotny składnik, to zachód stale bada wpływ domen informacyjnych, politycznych, ekonomicznych czy środowiska sieciocentrycznego¹⁶⁷. Ma to istotne implikacje dla sedna problemu, gdyż uznanie wagi nowoczesnych kategorii sprawia, iż braki w klasycznych wymiarach (sile militarnej, zaawansowaniu technologicznym wojska) mogą być zastąpione wzmożonymi działaniami w domenach nowych, np. przez ofensywne działania w cyberprzestrzeni¹⁶⁸ (cyberataki, dezinformację, propagandę), szeroko rozumiane formy wpływu społecznego, itd.

W stanowisku Unii Europejskiej trudno jest odnaleźć odniesienia do walki asymetrycznej sensu stricto, gdyż ta jest traktowana wymiennie z walką hybrydową, bezkontaktową, nieokreśloną, a także „Nowymi Wojnami”, czy też wojnami: nieliniowymi, pełnego spektrum, bezkontaktowymi, itd¹⁶⁹. Dlatego ogólna reakcja Unii na zagrożenia hybrydowe ewoluowała w drodze różnych inicjatyw, w tym komunikacji strategicznej, reagowania kryzysowego i budowania odporności. W ich drodze nakreślono konkretne działania mające na celu ulepszenie systemów wczesnego ostrzegania i świadomości sy-

¹⁶³ NATO 2022 *Strategic Concept*, Madrid 2022, s.4.

¹⁶⁴ Tamże, s. 1, 3, 6–8.

¹⁶⁵ Tamże, s. 9.

¹⁶⁶ Tamże, s. 9–11.

¹⁶⁷ K. Mallory, *New Challenges in Cross-Domain Deterrence*, Santa Monica 2018, s. 5–23; A. Lambi, V. Vijayaraghavan, *Cross-Domain Deterrence in the Cyber World*, „International Journal for Research in Applied Science & Engineering Technology” 2022, Vol. 10, Issue IX, s. 387–389; N. Katagiri, Two explanations for the paucity of cyber-military, cross-domain operations, „Journal of Cybersecurity” 2022, Vol. 1, Issue 10, s. 1–5; E. Lonergan, M. Montgomery, *What is the Future of Cyber Deterrence?*, „SAIS Review of International Affairs” 2021, Vol.41, No. 2, s. 68–71.

¹⁶⁸ M. Keinonen, *Using Military Cyber Operations as a Deterrent*, [w:] *Proceedings of the 18th International Conference on Cyber Warfare and Security*, R.L. Wilson, B. Curran (ed.), Reading 2023, s. 488–489, 495.

¹⁶⁹ H. Smith, *Countering Hybrid Threats*, [w:] *The EU and NATO: The Essential partners*, G. Lindstrom, T. Tardy (eds.), Paris 2019, s. 17; *Final Joint Framework on countering hybrid threats. A European Union response*, 6 April, [Joint communication JOIN(2016)18 | CELEX: 52016JC0018], 2016, s. 3–18.

tuacyjnej. UE i NATO zinstytucjonalizowały swoją współpracę za pomocą wspólnych deklaracji z 2016 i 2018 r., których celem było zamknięcie luk w bezpieczeństwie wykorzystywanych przez zagrożenia hybrydowe¹⁷⁰. Zarazem wskazało to na pewien podział ról, gdzie Unia Europejska przejęła zakres reagowania kryzysowego i zadań dyplomatycznych w zwalczaniu zagrożeń, w tym asymetrycznych. Pomimo przeszkód politycznych, ograniczających bezpośrednią wymianę danych wywiadowczych, UE i NATO przeprowadzają skoordynowane oceny, korzystając z informacji z otwartych źródeł i danych wywiadowczych państw członkowskich. Ich współpraca, zwłaszcza w dziedzinie cyberobrony, obejmuje regularne spotkania informacyjne i wspólne ustalenia techniczne¹⁷¹.

3.2.3. Rosyjskie spojrzenie na zagrożenia asymetryczne

Zmiany w globalnej potęgze po zakończeniu zimnej wojny i postęp w technologii wojskowej stworzyły nierówność siły między Stanami Zjednoczonymi oraz Federacją Rosją. Zakwestionowało to dotychczasową stabilność strategiczną w rozumieniu kontroli zbrojeń, która ówczesnie opierała się na parytecie (równoważności) arsenału nuklearnego. Wobec niekorzystnej pozycji gospodarczej, ekonomicznej i militarnej, Rosja poszukiwała rozwiązań redukujących tę różnicę. Wówczas nastąpił rozwój broni hipersonicznej oraz taktycznych pocisków nuklearnych. Podejście to jednak podważało samą zasadę parytetu, którą Rosja pragnęła utrzymać¹⁷². Analiza traktatów INF i New START ukazuje, że mimo iż te porozumienia miały na celu stabilizację, ich ograniczenia oraz rozwój nowoczesnych systemów, prowadziły do destabilizacji¹⁷³. W szczególności, upadek traktatu INF umożliwił Rosji opracowanie pocisków średniego zasięgu, co dodatkowo skomplikowało ramy kontroli zbrojeń. Nowy Traktat START, choć korzystny dla Rosji, nie rozwiązał problemu asymetrii obronnych, zwłaszcza w kontekście amerykańskich systemów obrony przeciwrakietowej. W kontekście tych wyzwań, poza rozwijaniem zaawansowanych technologii broni konwencjonalnej, Rosja dywersyfikowała budowę własnej pozycji przez

¹⁷⁰ *Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*, 8 July, [PR: (2016) 119], 2016; *Joint Declaration on EU-NATO Cooperation, by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*, 10 July, [PR: (2018) 095], 2018.

¹⁷¹ P. Cullen, *A perspective on EU hybrid threat early warning efforts*, [w:] *Hybrid Warfare. Security and Asymmetric Conflict in International Relations*, M. Weissmann, N. Nilsson, B. Palmertz, P. Thunholm (eds.), London 2021, s. 53–54.

¹⁷² M. Svobodová, *Russia's approach to arms control: caught between asymmetry and the desire for strategic stability*, „European Security” 2023, Vol. 33, Issue 1, s. 152–155.

¹⁷³ V. Putin, *Statement by Vladimir Putin on additional steps to de-escalate the situation in Europe after the termination of the Intermediate-Range Nuclear Forces Treaty (INF Treaty)*, 26 October 2020, „President of Russia”, <http://en.kremlin.ru/events/president/news/64270>, [odczyt: 15.08.2024]; M. Svobodová, *Russia's approach to arms control...*, s. 156–161.

stosowanie technik walki nieregularnej, które stały się integralnym elementem jej strategii. Spotkało się to z odpowiedzią NATO, które tego rodzaju niekonwencjonalne działania uznało za zagrożenie dla bezpieczeństwa zbiorowego¹⁷⁴. Odpowiedź Rosji, pogłębiająca wykorzystanie asymetrii, tylko przyczyniła się do zwiększenia tzw. niestabilności międzydomenowej, gdzie ataki mogą łączyć różne obszary, takie jak cyberprzestrzeń, politykę i gospodarkę. Zarazem, rosyjskie postrzeganie NATO jako zagrożenia wzrosło na przestrzeni lat, a obawy te zostały jeszcze bardziej wzmocnione podczas wojny na Ukrainie. Obie strony wyrażają zaniepokojenie destabilizującymi działaniami w różnych domenach. Jednakże przez wzgląd na brak wspólnego zrozumienia granic między zwykłą konkurencją i nieregularną agresją, utrudniona jest budowa stabilizacji we współczesnym środowisku bezpieczeństwa¹⁷⁵.

Szczególnie przebieg wojny w Ukrainie pokazał, że Federacja Rosyjska nie jest gotowa na pełnoskalowe, kinetyczne starcie z NATO. Odnoszone w czasie konfliktu sukcesy i tak pozostają osiągnięciami osadzonymi w szczególnym kontekście. Ukraina była osłabiana przez lata, a wsparcie Zachodu nie zastąpi szkolenia i doświadczenia w użyciu sprzętu, które mają państwa sojuszu. Istotną rolę odgrywają też lotnictwo i rozwój technologiczny, lecz co najważniejsze: obrona przeciwlotnicza. To braki w niej po obu stronach konfliktu pozwoliły na tak szerokie użycie dronów, czy to produkcji irańskiej, czy nawet amatorskiej (po obu stronach), także w sytuacjach bojowych¹⁷⁶. Spodziewać się można bowiem, że mniejsze statki bezzałogowe byłyby trudniejsze do przechwycenia, a przez to skuteczniejsze w rekonesansie czy odwracaniu uwagi. Czyniłoby je wciąż zdolnymi do użycia w starciu z NATO.

Skala wykorzystania amatorskich i komercyjnych pojazdów bezzałogowych nie dowodzi, że dotychczasowi teoretycy wojskowi pomylili się, kiedy podkreślali znaczenie profesjonalnych, wojskowych dronów rekonesansowych i bojowych¹⁷⁷. Wyjawszy fakt, że nietrudno odszukać źródła przeczące takiej tezie¹⁷⁸, to najważniejszym pozostaje rozróż-

¹⁷⁴ NATO 2022 *Strategic Concept*, s. 3–7.

¹⁷⁵ А.Г. Арбатов, *Украинский кризис и стратегическая стабильность*. „Полис. Политические исследования” 2022, № 4, s. 25–30.

¹⁷⁶ K. Chávez, O. Swed, *Emulating underdogs: Tactical drones in the Russia-Ukraine war*, „Contemporary Security Policy” 2023, Vol. 44, No. 4, s. 592–593.

¹⁷⁷ K. Anderson, *Rise of the Drones: Unmanned Systems and the Future of War*, Subcommittee on National Security and Foreign Affairs, Committee on Oversight and Government Reform, US House of Representatives, 23 March, [11th Congress, 2nd Session] 2010, s. 1–13; A. Gilli, M. Gilli, *The diffusion of drone warfare? Industrial, organizational, and infrastructural constraints*. „Security Studies” 2016, Vol. 25, No. 1, s. 50–84.

¹⁷⁸ T. Zieliński, *Drones in Military Conflicts. Are Unmanned Aircraft Systems the Future of Wars?*, [w:] *Challenges to National Defence in Contemporary Geopolitical Situation*, S. Bekesiene, S. Hoskova-Mayerova (eds.), Wilno 2022, A. Calcara, A. Gilli, M. Gilli, R. Marchetti, I. Zaccagnini, *Why* →147

nienie między podejściem odgórnym i oddolnym. W sprawie strategicznego oraz operacyjnego wykorzystania pojazdów bezzałogowych nic się nie zmieniło. Taktyczne użycie konstrukcji amatorskich lub komercyjnych wynika z inicjatyw oddolnych. Żołnierze od zawsze wykorzystywali wszelkie siły i środki, włączając w to zdobyty od przeciwnika sprzęt czy rozwiązania komercyjne, by chronić swoje życie lub skuteczniej realizować cele. Rozwój technologiczny daje im większe możliwości, lecz sam w sobie nie odменя w pełni sposobu prowadzenia wojny.

Doktryna Wojskowa Federacji Rosyjskiej z 2014 roku uznaje Zachód za potężnego konkurenta i źródło większości zagrożeń wojskowych. Rozszerza ona pojęcie ryzyka wojskowego o wykorzystanie technologii informacyjnych i komunikacyjnych do celów wojskowo-politycznych, w tym cyberataków i operacji wpływu¹⁷⁹. Z kolei *Strategia Bezpieczeństwa Narodowego Federacji Rosyjskiej* z 2021 roku wyraźnie stanowi, że Rosja zastrzega sobie prawo do użycia symetrycznych i asymetrycznych działań w celu neutralizacji wrogich operacji, jeśli zagrożone są interesy państwa. Wśród źródeł takiego niebezpieczeństwa wymienia m.in. technologie IT, tworzenie chaosu informacyjnego, czy podważanie wiarygodności władz rosyjskich. W odpowiedzi, strategia przewiduje środki takie jak tworzenie suwerennego segmentu Internetu, wzmocnienie zabezpieczeń przed cyberatakami i rozwój sił i środków konfrontacji informacyjnej¹⁸⁰.

Między innymi to z powyższych względów, asymetria mająca na celu uniknięcie lub zmniejszenie konsekwencji bezpośredniego starcia nie jest dla Rosji jedynie opcjonalną taktyką, lecz koniecznością strategiczną. Federacja Rosyjska postrzega siebie jako militarnie ustępującą stronę w konfrontacji z zaawansowanym technologicznie przeciwnikiem, takim jak USA lub NATO. To postrzeganie własnej względnej słabości wymusza innowacyjne podejście do wojny, gdzie intelektualna przewaga i niestandardowe metody stają się kluczowe dla osiągnięcia celów politycznych bez ponoszenia nieakceptowalnych kosztów konwencjonalnego konfliktu. Asymetria staje się więc sposobem na przekształcenie słabości w siłę poprzez wykorzystanie wrażliwości przeciwnika. Zarazem nie wyklucza się konwencjonalnej siły militarnej w innych kierunkach strategicznych, czego dowodzi inwazja Rosji na Ukrainę w 2022 roku.

Wartym podkreślenia jest także fakt, że powyższy wywód opierał się na zachodnim sposobie opisanie praktyki działań rosyjskich — dla zachowania spójności definicyj-

Drones Have Not Revolutionized War. The Enduring Hider-Finder Competition in Air Warfare, „International Security” 2022, Vol. 46, No. 4, s. 33–35.

¹⁷⁹ *Военная доктрина Российской Федерации*, 25 декабря, Москва 2014.

¹⁸⁰ *Стратегия национальной безопасности Российской Федерации*, 2 июля, Москва 2021.

nej w porównywaniu. W rosyjskiej literaturze, przymiotnik „asymetryczny” jest wykorzystywany wymiennie z „pośrednim” („nie wprost”, z ang. indirect)¹⁸¹. Źródeł takiego podejścia doszukiwać się można w mocnym oparciu rosyjskiej literatury — w przedmiotowej tematyce — na pracy Basila Liedella Harta *Strategy: The Indirect Approach*. Szczególnie cytowane jest jego rozumienie podejścia pośredniego jako dominacji domeny psychologicznej nad kinetyczną¹⁸².

3.2.4. Chińskie spojrzenie na zagrożenia asymetryczne

Chiny postrzegają wojnę asymetryczną jako kluczową strategię równoważenia przewagi przeciwnika, zwłaszcza Stanów Zjednoczonych, poprzez wykorzystanie informacji, cyberprzestrzeni i taktyk hybrydowych, zakorzenionych w tradycyjnej chińskiej myśli wojskowej. Stoi to w pewnej opozycji do większości zachodnich definicji, które skupiają się na wykorzystaniu niekonwencjonalnych metod przez słabszych aktorów. Źródeł doszukiwać się można w doświadczeniach z konfliktów. Operacje w byłej Jugosławii, Pustynna Burza czy późniejsze zaangażowanie w Irak i Afganistan, utwierdziły Stany Zjednoczone w określonym postrzeganiu asymetrii. Chiński kontekst pozostaje jednak różny, zarówno w długiej perspektywie historycznej, jak również ostatnich dekadach. Choć źródła sięgające Sun Tzu zostały omówione w poprzednich częściach niniejszej pracy, to wyłącznie jego wspomnienie nie oddawałoby istoty Chińskiego postrzegania asymetrii.

Ta towarzyszyła państwu środka przez wieki, głównie jednak na poziomie strategicznym. Dlatego w czasach cesarskich istotne było dzielenie wroga przez strategiczne sojusze, przekupywanie elit, budowanie fizycznych barier oraz dopiero w ostateczności — prowadzenie wojny zbrojnej, również wykorzystującej pewne asymetryczne techniki¹⁸³. Przyczyniło się to do budowania skomplikowanego podejścia w konkurencji międzypaństwowej, które współcześnie wyewoluowało w multipolaryzm (chin. 多极化 — duojihua)¹⁸⁴.

¹⁸¹ С.Г. Чекинов, С.А. Богданов, *Асимметричные действия по обеспечению военной безопасности России*, „Военная Мысль” 2010, № 3, s. 19.

¹⁸² B.L. Hart, *Strategy: The Indirect Approach*, London 1967, s. 24; С.Г. Чекинов, С.А. Богданов, *Влияние непрямых действий на характер современной войны*, „Военная мысль” 2011, № 6, s. 4.

¹⁸³ A. Jash, *Fight and Win Without Waging a War: How China Fights Hybrid Warfare*, „CLAWS Journal” 2019, Vol. 12, No. 2, s. 98–99.

¹⁸⁴ R.D. Ewing, *Hu Jintao: The Making of a Chinese General Secretary*, „The China Quarterly” 2003, Vol. 173, s. 17–18, 29–31; P. Ciborek, *Political and Economic Activities of the PRC on the Balkan Peninsula Romania: A Case Study*, [w:] *New Dynamics in Asia*, K. Żakowski (ed.), Łódź 2020, s. 114–115.

Prowadzi to do szerszego postrzegania koncepcji asymetrii w ogólnej konkurencji międzypaństwowej, które wprost wynika z regionalnych uwarunkowań. Chiny mierzą się bowiem z Indiami, postrzegając je jako „mniejszego” rywala, mogącego jednak przeszkodzić w realizacji ich długoterminowych celów dominacji w Azji¹⁸⁵. Ta percepcja asymetrii nie wynika wyłącznie z różnicy potencjału militarnego i gospodarczego, lecz również z historycznych uprzedzeń wobec indyjskiej państwowości i roli w regionie¹⁸⁶. Wynika to z faktu, że Indie, choć słabsze w ujęciu konwencjonalnym, mogą stosować strategie balansowania — np. zbliżenie z USA i Japonią — które mają na celu utrudnienie chińskiej hegemonii w Azji Południowej i Wschodniej.

W takim kontekście zrodziła się chińska koncepcja „Trzech wojen” (chin. 三战 — san zhan), obejmująca wojnę psychologiczną (chin. 心理战 — xinli zhan), wojnę opinii publicznej (chin. 舆论战 — yulun zhan) oraz wojnę prawną (chin. 法律战 — falü zhan), stanowiąc istotny komponent współczesnej strategii bezpieczeństwa państwa i doktryny operacyjnej Chińskiej Armii Ludowo-Wyzwoleńczej (ALW). Jej geneza opiera się zarówno na tradycyjnej myśli strategicznej, jak również na analizie współczesnych konfliktów, w tym wojen z udziałem Stanów Zjednoczonych. Pierwszą i kluczową publikacją było *Unrestricted Warfare*¹⁸⁷ z 1999 roku, postulujące wykorzystanie wszelkich dostępnych metod — militarnych i pozamilitarnych — w celu osiągnięcia strategicznych celów. Z pozycją tą musieli zapoznać się istotni oficerowie ALW, jak również Chi Haotian, ówczesny minister obrony, czy sam przewodniczący Chińskiej Republiki Ludowej — Jiang Zemin¹⁸⁸. Szybka popularyzacja przyczyniła się do dużego wpływu tej publikacji na sposób kształtowania ALW.

Oficjalne przyjęcie koncepcji Trzech wojen nastąpiło bowiem już w grudniu 2003 roku, kiedy to Centralna Komisja Wojskowa i Komitet Centralny Komunistycznej Partii Chin zatwierdziły nowelizację *Regulaminu Pracy Politycznej ALW*, w którym jasno wskazano zadania prowadzenia działań psychologicznych, propagandowych i prawnych¹⁸⁹. Poszczególne obszary definiowano jako:

¹⁸⁵ M.S. Pardesi, *Explaining the asymmetry in the Sino-Indian Strategic Rivalry*, „Australian Journal of International Affairs” 2021, Vol. 75, No. 3, s. 342, 347–348.

¹⁸⁶ J.W. Garver, *Protracted Contest: Sino-Indian Rivalry in the Twentieth Century*, Washington 2001, s. 5–31.

¹⁸⁷ Q. Liang, W. Xiangsui, *Unrestricted Warfare (超限战) 2nd ed.*, Wuhan, 2011, s. 41.

¹⁸⁸ D. Cheng, *Unrestricted Warfare: Review Essay II*, „Small Wars and Insurgencies” 2000, No. 11(1), s. 122.

¹⁸⁹ A. Singh, *China's 'Three Warfares' and India*, „Journal of Defence Studies” 2013, Vol. 7, No. 4, s. 27–33; D. Cheng, *China's Active Defense Strategy and Its Regional Impact*, 27 January, [U.S.-China Economic and Security Review Commission Hearing], 2011, s. 6–7.

- wojna psychologiczna — operacje mające na celu wpływanie na stan psychiczny i zachowania przeciwnika przez kontrolowane rozpowszechnianie informacji, tj. dyskredytowanie przeciwnika i jego władz¹⁹⁰;
- wojna opinii publicznej — koncentrowanie się na pozyskiwaniu poparcia społecznego w kraju i za granicą przy użyciu mediów tradycyjnych i cyfrowych, tj. obniżanie morale przeciwnika¹⁹¹;
- wojna prawna — mobilizacja prawa krajowego i międzynarodowego do uzyskania przewagi politycznej i strategicznej, tj. tworzenie podstaw do późniejszych działań konfliktowych¹⁹².

Wszystkie trzy komponenty koncepcji mogą być wykorzystywane na poziomie taktycznym, operacyjnym oraz strategicznym, przy czym wojna psychologiczna uznawana jest za najbardziej fundamentalną, ponieważ jej efekty są celem zarówno działań medialnych, jak i prawniczych¹⁹³. Co więcej, wojna psychologiczna może być rozumiana w sposób podobny jak zachodnie definicje wojny informacyjnej, na co wskazują liczne źródła¹⁹⁴. Niemniej, przez wzgląd na wspomnianą fundamentalność, także cała koncepcja Trzech wojen jest postrzegana jako wojna informacyjna¹⁹⁵ — choć takie podejście wydaje się nieostre i co najmniej niepełne.

Za realizację Trzech wojen odpowiadają zarówno struktury partyjne, państwowe (w rozumieniu struktur cywilnych) oraz wojskowe. Kluczową rolę odgrywają instytucje propagandowe, które dysponują instrumentami nadzoru nad przekazem medialnym, zarówno w wymiarze wewnętrznym, jak i zagranicznym. Działania te mają na celu kształtowanie korzystnego otoczenia międzynarodowego dla realizacji interesów strategicznych Chin. Praktycznymi ich przykładami są reformy prawa morskiego (np. ustawa o ochronie wysp), intensyfikacja propagandy zagranicznej (w tym ekspansję mediów

¹⁹⁰ S. Lee, *China's 'Three Warfares': Origins, Applications, and Organizations*, „Journal of Strategic Studies” 2014, Vol. 37, No. 2, s. 203–204.

¹⁹¹ Tamże, s. 204.

¹⁹² Tamże, s. 204–205.

¹⁹³ Tamże, s. 204–205; N. Beauchamp-Mustafaga i inni, *Deciphering Chinese Deterrence Signalling in the New Era: An Analytic Framework and Seven Case Studies*, [RR-A1074-1], Santa Monica 2021, s. 35.

¹⁹⁴ Z. Yuliang, *The Science of Campaigns* [战役学], Beijing 2006, s. 107, 155; PLA Academy of Military Science, Military Strategy Department [军事科学院战略研究部] — S. Zhaoli (ed.), *Science of Military Strategy* [战略学], Beijing 2013, s. 130; D. Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, California 2017, s. 51; P. Behrendt, *San Zhong Zhanfa or Three Warfares. Chinese Hybrid Warfare* „Kwartalnik Boyma” 2022, nr 1 (11), s. 29–32.

¹⁹⁵ L.M. Wortzel, *The Chinese People's Liberation Army and Information Warfare*, Carlisle Barracks 2014, s. 29–30; C. Neculcea, *China's Three Warfare Strategy. Origins, evolution, applicability*, „Journal of Defense Resources Management” 2023, Issue 1, s. 22.

państwowych na rynki zewnętrzne), rozwój dyplomacji publicznej oraz instrumenty ekonomiczne i wojskowe służące wywieraniu presji psychologicznej¹⁹⁶. Aktualnie obserwuje się chińskie działania, mające na celu podważenie zaufania społeczeństwa tajwańskiego do jego instytucji politycznych, wzbudzenie chaosu oraz osłabienie determinacji w obronie państwa¹⁹⁷. W przypadku eskalacji konfliktu można spodziewać się intensyfikacji tych operacji, zwłaszcza w państwach goszczących siły amerykańskie. W ramach wojny opinii publicznej, Pekin może rozpowszechniać narracje o rzekomych nadużyciach wojsk USA wobec lokalnej ludności — zarówno wyolbrzymione, jak i całkowicie sfabrykowane — w celu wywołania społecznego sprzeciwu wobec współpracy z Waszyngtonem. Takie wykorzystanie opinii publicznej czy wpływu psychologicznego, celem kształtowania percepcji i postaw społecznych w sposób sprzyjający interesom, doskonale wpisuje się w ramy Trzech wojen.

3.2.5. Wojna asymetryczna, czy asymetria w wojnie — krytyka pojęcia

Współczesny świat sprzyja powstawaniu asymetrii bardziej niż przedtem, gdyż stała się ona środkiem balansującym światowe systemy¹⁹⁸ w stanie równowagi dynamicznej¹⁹⁹. Skuteczność takich środków zdaje się determinować konflikty, zwiększając udział komponentu asymetrycznego. Indukują to także współczesne, wielowymiarowe łańcuchy zależności międzypaństwowych, w których coraz istotniejszą rolę odgrywają też duże podmioty pozapaństwowe. Zarazem jednak rozmywa się granica między konfliktem i konkurencją międzypaństwową. Asymetria jest bowiem używana jako punkt wyjścia, z którego dalsza eskalacja (lub jej brak) jest przedmiotem starannej orkiestracji działań. Za Münklerem²⁰⁰, Epplerem²⁰¹ można też wskazać, że przedmiotowe dla tej pracy konflik-

¹⁹⁶ S. Lee, *China's 'Three Warfares'...*, s. 206–209.

¹⁹⁷ J.Y.M. Cheng, *The Challenges Taiwan Faces in Cognitive Warfare and Its Impact on US–Taiwan Relations*, „Journal of Indo-Pacific Affairs” 2025, Vol. 8, No. 1, s. 93–100.

¹⁹⁸ Rozumianych w podobnym zakresie co systemy definiowane przez Immanuela Wallersteina. Wskazał on na głęboką asymetrię potencjału ekonomicznego, społecznego i ogólnych możliwości państw. Wyróżnił trzy grupy państw lub regionów: rdzeń (np. Europa Zachodnia, Ameryka Północna), półperyferie (np. Ameryka Łacińska) i peryferie (np. Afryka Subsaharyjska i Środkowa, Azja Południowa); zob. I. Wallerstein, *The modern World System I: Capitalist Agriculture and the Origins of the European World-Economy in the Sixteenth Century*, New York 1974.

¹⁹⁹ M. Rozumny, *The Logic of Multilateral Asymmetric Conflicts: The Russia-Ukraine War Case*, „Online Journal Modelling the New Europe” 2023, No. 42, s. 28–30.

²⁰⁰ Herfried Münkler (ur. 15 sierpnia 1951) — niemiecki politolog, profesor teorii politycznej na Uniwersytecie Humboldta w Berlinie. Historyk myśli politycznej i badacz teorii wojny, szczególnie Machiavellego; Munzinger Archiv GmbH, Internationales Biographisches Archiv, 19/2021 vom 11. Mai 2021 (bo), Eintrag „Münkler, Herfried”, <https://www.munzinger.de/search/go/document.jsp?id=00000024700> [dostęp: 10 sierpnia 2023].

²⁰¹ Erhard Eppler (ur. 9 grudnia 1926, zm. 19 października 2019) — niemiecki polityk, publicysta, nauczyciel i myśliciel zaangażowany w rozwój środowiska i ruchy pokojowe. Założyciel che Gesellschaft für Internationale Zusammenarbeit (GIZ) (Niemiecka Agencja Współpracy

ty będą mieć tendencję do przeciągania się latami. Ani nie sprzyjają one budowaniu kapitału stron konfliktu, ani umacnianiu państwowości — jak to miało miejsce w przypadku poprzednich wojen. Rodzi to dodatkowy problem, gdyż jak podają autorzy, jedynym sposobem do zakończenia takich wojen może być interwencja zewnętrzna. Eppler będący badaczem-pacyfistą, sam wzywa do ponownego przemyślenia znaczenia pacyfizmu w czasach nowych wojen. Szczególnie, że w powstrzymaniu sprywatyzowanej przemocy nieefektywne będą rozwiązania pokojowe.

Należałoby też zastanowić się, czy takie przedstawianie asymetrii jest w ogóle istotne z punktu widzenia bezpieczeństwa państw. Być może lepsze jest jej aprioryczne przyjęcie i skupienie się raczej na skutkach lub definiowaniu obszarów, które są szczególnie narażone na takie zagrożenia. Argument w tej sprawie odnaleźć można w pracy *Pozimnowojenny paradygmat bezpieczeństwa*:

(...) wątpliwy z logicznego punktu widzenia wydaje się rozpowszechniony przez wielu autorów pogląd o występowaniu po zimnej wojnie tzw. zagrożeń asymetrycznych dla bezpieczeństwa państw. Gdyby uznać tę rację, to należałoby zapytać, czy istnieją zagrożenia symetryczne, a więc czy występowanie symetrii np. w posiadanym potencjale obronnym dwóch państw tworzy zagrożenie²⁰².

Pomimo dominującej obecności pojęcia „wojny asymetrycznej” (rozumianej jako asymmetric war lub asymmetric warfare) w literaturze strategicznej i bezpieczeństwa, jego użyteczność analityczna może być kwestionowana. Asymetria nie stanowi bowiem odrębnego typu konfliktu, lecz jest jego immanentną cechą — obecnie bardziej widoczną z racji warunków strukturalnych współczesnego świata, ale niemającą charakteru konstytutywnego dla wojny jako takiej.

Z perspektywy państw, racjonalnym wyborem staje się więc prowadzenie konfliktu poniżej progu otwartej wojny — szczególnie wtedy, gdy przeciwnik posiada porównywalny potencjał konwencjonalny. W takich warunkach asymetria staje się nie tyle ryzykiem, co strategiczną okazją do osiągania celów politycznych przy minimalizacji kosztów — poprzez działania nieregularne, w domenie informacyjnej, cyberprzestrzeni lub przez presję ekonomiczną. Osadzenie całości w przestrzeni społecznej sprawia też, że to informacja staje się głównym nośnikiem wpływu²⁰³.

Międzynarodowej), minister współpracy gospodarczej; Munzinger Archiv GmbH, Internationales Biographisches Archiv, 16/2020 vom 14. April 2020 (la), Eintrag „Eppler, Erhard”, <https://www.munzinger.de/search/go/document.jsp?id=00000012072> [dostęp: 10 sierpnia 2023].

²⁰² R. Zięba, *Pozimnowojenny paradygmat bezpieczeństwa*, [w:] *Bezpieczeństwo międzynarodowe po zimnej wojnie*, R. Zięba (red.), Warszawa 2008, s. 25–26.

²⁰³ L. Jones, *The Future of Warfare Is Irregular*, „Fletcher Forum of World Affairs” 2022, Vol. 46, No. 2, s. 110.

Należy zatem uznać, że asymetria jest raczej właściwością relacyjną konfliktów niż ich odrębnym modelem. Ma ona charakter dynamiczny i kontekstowy, może przyjmować różne formy — technologiczne, organizacyjne, poznawcze, doktrynalne — i w sposób istotny wpływać na przebieg działań. Nie stanowi jednak wystarczającej podstawy do wyodrębnienia osobnej kategorii wojny. Co więcej, traktowanie asymetrii jako typu konfliktu grozi rozmyciem precyzji analitycznej i skupieniem się na pojęciu, a nie na jego skutkach. Lepszym podejściem byłoby przyjęcie asymetrii jako zmiennej ryzyka — i skoncentrowanie się na analizie jej skutków w poszczególnych obszarach systemu bezpieczeństwa państwa.

Asymetria jednak nie działa w próżni a jej skuteczność zależy od strukturalnych właściwości danego obszaru bezpieczeństwa. Przykładowo, w przestrzeni militarnej asymetria potencjału wykazuje dużą inercję — nie da się w ciągu tygodni czy miesięcy zdublować przewagi w liczbie batalionów pancernych, marynarki wojennej czy lotnictwa. Już dziś produkcja nowoczesnego uzbrojenia mierzy się z wieloletnimi opóźnieniami. Najbardziej zaawansowane technologie — jak myśliwce V generacji — mają ograniczoną dostępność nie tylko ze względu na koszt, lecz czas wytwarzania²⁰⁴. Spodziewana, rosnąca złożoność i stopień zaawansowania przyszłych systemów uzbrojenia mogą ten problem jedynie zaostriżyć. To z kolei będzie istotnym komponentem kosztów prowadzenia otwartej wojny. Nawet przy zapewnieniu wystarczających zasobów finansowych, państwo nie może kupić czasu, a zatem zastępować uzbrojenia zniszczonego w boju w sposób adekwatny. W tej sytuacji przewaga asymetryczna w konwencjonalnym sensie jest trudna do osiągnięcia w krótkim terminie.

Sytuacja jest odmienna w cyberprzestrzeni, gdzie relatywnie niskie bariery wejścia umożliwiają szybką akumulację środków ofensywnych i wywieranie wpływu o operacyjnej lub potencjalnie strategicznej skali. W tym środowisku asymetria może być generowana niemal natychmiastowo — poprzez wykrycie luk w systemach, przejęcie kontroli nad infrastrukturą krytyczną, destabilizację systemów finansowych czy wykorzystanie dezinformacji do osiągnięcia efektów społeczno-politycznych. Taka zmienność i dynamika asymetrii czynią z niej czynnik ryzyka, który powinien być przedmiotem ciągłej analizy, a nie statycznego definiowania.

Zamiast więc koncentrować się na definiowaniu wojny asymetrycznej jako typu konfliktu, należałoby przesunąć punkt ciężkości ku analizie odporności poszczególnych

²⁰⁴ H.R. Penney, *The Future of Fighter Force Our Nation Requires: Building a Bridge*, Arlington 2021, s. 5, 10–11, 17; J. Venable, *Expensive F-15EX Does Not Deliver: Congress Should Nix Its Purchase*, „Issue Brief: Center for National Defense” 2020, No. 6009, s. 5–7.

komponentów państwa na działania asymetryczne. Kluczowe pytania nie powinny dotyczyć tego, „czy asymetria występuje”, ale „gdzie może być wykorzystana najskuteczniej przez przeciwnika” oraz „jakie mechanizmy kompensacyjne należy uruchomić, by zniwelować jej skutki”. Takie podejście bardziej odpowiada rzeczywistości strategicznej XXI wieku niż próby klasyfikowania konfliktów na podstawie dominującej formy przewagi jednej ze stron.

Podsumowanie

Rekapitułując należy stwierdzić, że koncepcje „wojny hybrydowej” i „wojny asymetrycznej” różnią się nie tylko genezą i zakresem, lecz przede wszystkim stopniem przydatności metodologicznej oraz użytecznością w opisie współczesnych konfliktów. Wojna hybrydowa, mimo swej popularności w narracjach politycznych i medialnych, nie spełnia podstawowych kryteriów pojęcia analitycznego. Zbyt duża pojemność semantyczna, nieostrość definicyjna oraz niejednoznaczność w odniesieniu do poziomów operacyjnych, strategicznych i taktycznych stanowią oś problemu. W efekcie termin ten staje się jedynie etykietą służącą legitymizacji działań obronnych lub ofensywnych w sferze komunikacji politycznej. Natomiast nie wnosi wiele więcej do samych studiów nad bezpieczeństwem, będąc raczej „ślepą uliczką”. Wydaje się zatem, że pojęcie „wojny hybrydowej” zaczęto stosować w sposób tautologiczny.

Zgoła inaczej przedstawia się sytuacja w przypadku wojny asymetrycznej. Choć również pojęcie to cierpi na nadmiar interpretacji i uproszczeń, jego podstawy teoretyczne są silniej zakorzenione w refleksji strategicznej — zarówno w klasycznych analizach relacyjnej siły, jak i w studiach nad wojną nieregularną, partyzancką, cybernetyczną, czy wojnami zastępczymi. Wspólnym mianownikiem wszystkich tych form jest przewaga jednej ze stron w określonej domenie (technologicznej, operacyjnej, poznawczej, czasowej lub normatywnej) oraz dążenie drugiej strony do zrekompensowania tej przewagi za pomocą środków alternatywnych, często niekonwencjonalnych. Zamiast jednak ujmować asymetrię jako odrębny typ konfliktu, bardziej zasadne wydaje się postrzeganie jej jako nieodłącznego i zmiennego parametru każdego konfliktu, który warunkuje jego dynamikę i logikę eskalacyjną. Perspektywa ta koresponduje z przytaczany wcześniej ujęciem I. Arreguína-Tofta, który wskazuje, że skuteczność asymetrii wynika nie z samej nierównowagi, lecz z wyboru skutecznej strategii jej wykorzystania²⁰⁵.

²⁰⁵ I. Arreguín-Tofta, *How the Weak Win Wars...*, s. 117–131.

Współcześnie asymetria manifestuje się w sposób szczególnie wyraźny w domenach innych niż kinetyczna. W przestrzeni militarnej asymetria wykazuje dużą inercję: przewagi nie da się zbudować natychmiast, a produkcja zaawansowanego uzbrojenia wymaga czasu, nakładów i infrastruktury. W cyberprzestrzeni czy sferze informacyjnej, asymetria nie jest obciążona takimi ograniczeniami. Dlatego szczególnie w tym kontekście bardziej trafne wydaje się traktowanie jej jako zmiennej ryzyka, a nie klasyfikatora konfliktu. Podejście to pozwala skoncentrować się na odporności konkretnych sektorów — infrastruktury krytycznej, łańcuchów dostaw, systemów dowodzenia czy opinii publicznej — zamiast na próbie stworzenia sztywnej typologii wojen.

Analiza komparatywna pokazała również, że sposób rozumienia asymetrii i hybrydowości zależy od kontekstu doktrynalnego i kultury strategicznej. W ujęciu zachodnim wojna hybrydowa zyskała status swoistej diagnozy współczesnych zagrożeń, szczególnie po aneksji Krymu. W doktrynie rosyjskiej jednak nie występuje jako samodzielna koncepcja — to raczej Zachód przedstawiany jest jako użytkownik takich środków, zaś Rosja opiera swoje strategie na całościowej koncepcji konfliktu nielinearnego i wojny nowej generacji. Z kolei w refleksji chińskiej dominuje podejście poznawczo-asymetryczne, z naciskiem na wojnę „inteligentną” i wykorzystanie przewag informacyjnych oraz technologicznych. Chińskie źródła rzadko operują pojęciem wojny hybrydowej — zamiast tego rozwijają koncepcje „wojny nielimitowanej” oraz dominacji poznawczej.

W świetle powyższych ustaleń, niniejszy rozdział prowadzi do wniosku, że pojęcie „wojny hybrydowej” powinno zostać ograniczone w użyciu do funkcji opisowych lub retorycznych i nie powinno pełnić roli głównego narzędzia analizy konfliktów. Znacznie bardziej produktywnie — teoretycznie i praktycznie — jest przyjęcie ram asymetrycznych, traktowanych jednak nie jako typologia, lecz jako instrument rozpoznawania i opisu zagrożeń w perspektywie systemowej. Takie podejście umożliwia lepsze uchwycenie złożoności współczesnych konfliktów oraz realistyczną ocenę zdolności państw do ich zapobiegania, adaptacji i reagowania.

Rozdział IV

Analiza konfliktów czasów rewolucji cyfrowej

W odróżnieniu od wcześniejszych epok, w których technologie komunikacyjne pełniły głównie funkcję wspierającą, współczesne konflikty coraz częściej przybierają formę sieciocentryczną, w której cyberprzestrzeń jest nie tylko areną, lecz zarazem narzędziem walki. Niezwykle istotnym staje się komponent informacyjny i teleinformatyczny, będący już integralnym elementem prowadzenia działań zarówno militarnych, jak i pozamilitarnych. Dlatego w niniejszym rozdziale przeanalizowano przypadki obejmujące tak bieżące wydarzenia, jak również sięgające początków transformacji cyfrowej. Pozwoliło to uchwycić proces ewolucji strategii, taktyk i doktryn w tym obszarze.

Wojny XIX i pierwszej połowy XX wieku opierały się na masowej mobilizacji zasobów ludzkich i przemysłowych, a o ich przebiegu decydowały czynniki takie jak produkcja uzbrojenia, zdolność logistyczna czy skala zaangażowania armii w działania konwencjonalne. W tym modelu przewaga militarna była w znacznej mierze funkcją potencjału ekonomicznego i zdolności przemysłowych, co determinowało zarówno długość, jak i intensywność konfliktów. Zimna wojna przyniosła jakościową zmianę w sposobie myślenia o przewadze strategicznej. Obok tradycyjnych sił zbrojnych coraz większe znaczenie zyskiwały środki wywiadowcze, operacje psychologiczne oraz rozwój technologii teleinformatycznych, które umożliwiały oddziaływanie na przeciwnika bez konieczności bezpośredniego starcia kinetycznego. Pojęcie „wojny informacyjnej” zaczęło wówczas funkcjonować w dyskursie wojskowym, a infrastruktura komunikacyjna stała się jednym z kluczowych elementów potencjału obronnego. Niemniej podkreślić należy, że w każdym z tych konfliktów wykorzystywano działania nieregularne, asymetryczne, czy choćby „hybrydowe”. Jak wykazano jednak w poprzednich rozdziałach, odbywało się to w innym kontekście i często w innych celach niż współcześnie.

Wraz z nadejściem rewolucji cyfrowej i gwałtownym rozwojem globalnej sieci komputerowej nastąpiło przejście do modelu konfliktów, w których przestrzeń operacyjna obejmuje zarówno fizyczne pole walki, jak i cyberprzestrzeń. Doktryna sieciocen-

tryczności, rozwijana m.in. przez siły zbrojne USA od lat 90. XX wieku, opiera się na założeniu, że przewaga informacyjna — rozumiana jako zdolność do szybkiego pozyskiwania, przetwarzania i dystrybucji danych — może przełożyć się na przewagę operacyjną. Równolegle wzrosło znaczenie precyzyjnych, małoskalowych operacji o dużym zasięgu strategicznym, których skutki mogą być równie destrukcyjne jak działania prowadzone w wymiarze kinetycznym. Co więcej, przejście od wojen przemysłowych do sieciocentrycznych oznacza także przesunięcie punktu ciężkości z ilości zasobów na ich jakość. Kluczowym elementem przewagi stała się wiedza, a nie wyłącznie masa wojsk czy potencjał produkcyjny. W cyberprzestrzeni przewagę można zyskać dzięki lepszemu oprogramowaniu, skuteczniejszej analizie danych czy wykorzystaniem zaawansowanych socjotechnik. Otworzyło to pole do działania aktorom pozapaństwowym, którzy — dysponując relatywnie niewielkimi zasobami materialnymi — są w stanie przeprowadzać operacje o skutkach globalnych, podważając tradycyjne hierarchie siły w stosunkach międzynarodowych.

W rezultacie współczesne konflikty coraz częściej przybierają formy, które łączą konwencjonalne działania w domenach lądowej, morskiej, powietrznej i kosmicznej, z operacjami w cyberprzestrzeni i przestrzeni informacyjnej. Granice między tymi obszarami ulegają zatarciu, a przewaga w jednej z domen może decydować o wyniku starcia w pozostałych. Zarazem wykorzystywane techniki sprawiają, że rozmywa się także tożsamość aktorów. Metodyka działań sił zbrojnych w cyberprzestrzeni może nie być odróżnialna od działań przestępczych grup hakerskich. Takie ujęcie wymusza konieczność nowego, wielowymiarowego spojrzenia na strategię obronne i ofensywne, w którym cyberprzestrzeń nie jest już jedynie narzędziem wsparcia. Jest równorzędnym polem walki, które nie tylko znacząco wpływa na pozostałe obszary, lecz samo w sobie wnosi wyjątkowe wyzwania.

Punktem wyjścia dla rozważań było wcześniejsze omówienie hybrydowości i asymetrii konfliktów. Przeanalizowano implikacje tez stawianych przez autorów takich jak Ivan Arreguín-Toft, który badał relacje sił w starciach między nierównymi przeciwnikami, czy Frank G. Hoffman, kształtujący pojęcie wojny hybrydowej, integrującej działania kinetyczne z operacjami informacyjnymi i cybernetycznymi. W toku rozważań uwzględniony został również dorobek Mary Kaldor¹, wskazującej na specyfikę „nowych wojen” — zdecentralizowanych, często pozapaństwowych, opartych na sieciach i przepływach informacji. Szczególna uwaga zostanie poświęcona zacieraniu granic między wojną oraz

¹ M. Kaldor, *New and Old Wars: Organized Violence in a Global Era*, Cambridge 2012.

pokojem, czy światowym przemianom ery industrialnej i cyfrowej². Wykorzystane w tym celu zostały obserwacje Johana Schota oraz Laura Kanger³, dotyczące — ich zdaniem — współcześnie zachodzącej, głębokiej transformacji. Jest ona fundamentalną zmianą kierunku rozwoju współczesnych systemów społeczno-technicznych. Stanowi też odpowiedź na narastające problemy ekologiczne i społeczne, wywołane przez epokę industrializacji i intensywnego wzrostu gospodarczego. Wiąże się to ze zmianami politycznymi, takimi jak wzrost potencjału aktorów pozapaństwowych, czy zmiany w systemach państwowych dążące do wielopoziomowych instytucji o regionalnym lub globalnym zasięgu⁴. Finalnie, znaczenie zyskują również rozważania nad samą konkurencją między państwową, kontestowaniem siły oraz utrzymywaniem wpływu. Poza omówioną wcześniej walką informacyjną, uwzględniono także *Cyber power* Josepha Nye’a, akcentującą rolę informacji jako zasobu strategicznego i instrumentu wpływu na procesy polityczne oraz społeczne⁵.

Skonfrontowano wspomniane koncepcje z praktyką, badając, w jaki sposób założenia teoretyczne materializują się w konkretnych działaniach operacyjnych, kampaniach dezinformacyjnych, czy cyberatakach o skutkach strategicznych. Ich analiza ma na celu nie tylko opis mechanizmów działania, ale także ocenę skuteczności i trwałości efektów, jakie wywierają one na bezpieczeństwo międzynarodowe oraz stabilność polityczną państw.

We wcześniejszych częściach dysertacji wykazano, że współczesne konflikty, w których komponent cyfrowy odgrywa rolę decydującą, cechują się wysokim stopniem asymetrii podmiotów, niejednoznacznością identyfikacji sprawców oraz przenikaniem się działań o charakterze technicznym i poznawczym. Taka konfiguracja wymaga przyjęcia perspektywy interdyscyplinarnej. W rezultacie, niniejszy rozdział nie ogranicza się do opisu przypadków, lecz traktuje je jako materiał empiryczny umożliwiający weryfikację dotychczasowych teorii oraz identyfikację nowych trendów w prowadzeniu działań w cyberprzestrzeni. Wskazano także czynniki, które mogą kształtować oblicze przyszłych konfliktów — od rosnącej roli aktorów pozapaństwowych, poprzez rozwój narzędzi automatyzacji i sztucznej inteligencji, po zmiany w regulacjach prawnych i standardach bezpieczeństwa na poziomie międzynarodowym.

² Tamże, s. 74–76, 78–79, 93; M. Kaldor, *In defence of new wars*, „Stability: International Journal of Security and Development” No. 2 (1), s. 2–3, 14.

³ J. Schot, L. Kanger, *Deep transitions: Emergence, acceleration, stabilization and directionality*, „Research Policy” 2018, No. 47, s.1045-1059.

⁴ Tamże, s. 1050–1054.

⁵ J.S. Nye Jr., *Cyber Power*, [OMB No. 0704-0188], 2010, s. 5–9.

4.1. Geneza konfliktów epoki cyfrowej: zmieniające się pole walki oraz postrzeganie konfliktów

Kontrola nad informacją i narracją towarzyszyła konfliktom zbrojnym od najdawniejszych czasów, co wykazano w poprzednich rozdziałach. Już w starożytności dowódcy zdawali sobie sprawę, że odpowiednie kształtowanie obrazu przeciwnika ma istotne znaczenie dla uzyskania strategicznej przewagi. Dotyczyło to zarówno postrzegania go w oczach własnych żołnierzy i obywateli, jak również w percepcji sojuszników czy neutralnych obserwatorów. Przekaz informacyjny, niezależnie od użytego medium, miał podtrzymywać morale, legitymizować działania oraz delegitymizować przeciwnika. Przez większą część historii dyskurs ten charakteryzował się jednak znaczną inercją. Rozprzestrzenianie informacji było powolne, a możliwości dotarcia do masowego odbiorcy pozostawały ograniczone technicznie i organizacyjnie⁶. Nawet pojawienie się nowoczesnych środków łączności, takich jak telegraf, telefon czy radio, nie zlikwidowało całkowicie barier czasowych i przestrzennych — choć miało znaczący wpływ⁷. Dopiero kolejne dekady przyniosły istotne skrócenie dystansu pomiędzy wydarzeniem a odbiorcą, co stopniowo zaczęło zmieniać dynamikę oddziaływania informacyjnego.

W XX wieku, wraz z rozwojem mediów masowych, pole walki informacyjnej poszerzyło się o sferę percepcji społecznej w skali nieznanej wcześniej w historii⁸. Informacja przestała być wyłącznie narzędziem dowodzenia wojskowego i propagandy wewnętrznej; stała się także elementem kształtowania opinii międzynarodowej, a przez to narzędziem wywierania presji politycznej i psychologicznej. W efekcie, kontrola nad przepływem danych i interpretacją wydarzeń zaczęła być rozpatrywana jako zasób strategiczny, którego utrata mogła prowadzić do poważnych konsekwencji militarnych i politycznych. Transformacja ta doprowadziła do stopniowego odchodzenia od tradycyjnego modelu, w którym to państwo i wojsko monopolizowały narrację o przebiegu konfliktu. W kolejnych dekadach — od zimnej wojny, przez okres globalizacji, po erę cyfrową — proces ten ulegał coraz większej decentralizacji.

Przełom w tym względzie przyniosły lata 90. XX wieku, gdyż technologia umożliwiła niemal natychmiastowe dotarcie przekazu do globalnej publiczności, a nowe formy

⁶ I. Fang, *A History of Mass Communication Six Information Revolutions*, New York 1997, s. xvii–xviii, xxi–xxii, 28–29, 51–55, 240–243.

⁷ Y. Kaukiainen, *Shrinking the world: Improvements in the speed of information transmission, c. 1820-1870*, „European Review of Economic History” 2001, Vol. 5, No. 1, s. 8–19.

⁸ G.R. Sullivan, J.M. Dubik, *War in the information age*, „Strategic Studies Institute” 1994, Vol. 94, No. 4, s. 2–3, 11–15.

mediów zaczęły podważać dotychczasowe mechanizmy kontroli. To właśnie wówczas zestrojono działanie militarne z zarządzaniem informacją i formatem 24-godzinnych wiadomości telewizyjnych. Doprowadziło to do utworzenia nowej, „oglądalnej” dramaturgii konfliktu: transmisji na żywo, konferencji prasowych jako rytmu dnia, wizualizacji precyzyjnych uderzeń oraz wrażenia „czystej” wojny. Ten paradygmat, wpisujący się w potrzeby legitymizacji międzynarodowej, zyskał na znaczeniu podczas konfliktu w byłej Jugosławii. Telewizja cechowała się wówczas ambiwalencją między rzeczywistością przemocy oraz jej medialną prezentacją⁹. Co więcej, operatorzy kanałów telewizyjnych byli raczej nieliczni, w dużej części stanowiąc podmioty państwowe, a przez to otwierając nowe możliwości kontroli przekazu. Już wtedy zauważono, że medium telewizyjne pozostawia trwalsze wspomnienia i skuteczniej kształtuje postawy¹⁰. Późniejsze badania potwierdziły, że telewizja miała znaczący wpływ na postrzeganie zdarzeń przez ludzi, jak również wyrabianie opinii na ich temat¹¹. Metody skutecznego wykorzystania telewizji stopniowo ewoluowały, a wraz z mechanizmami globalizacji i upadkiem Związku Radzieckiego, wkroczyły w erę silniejszego, ponadnarodowego wpływu na społeczeństwa.

Kolejny istotny punkt zwrotny nastąpił w pierwszej dekadzie XXI wieku, kiedy doszło do symbolicznego upadku dotychczasowego aparatu kontroli informacyjnej. Wydarzenia w więzieniu Abu Ghraib w 2004 roku (ujawnione w formie zdjęć wykonanych przez samych sprawców) pokazały, że państwowe i wojskowe struktury nadzoru nie były w stanie nadążyć za dynamiką obiegu cyfrowych obrazów. W tym samym okresie rozwój koncepcji Web 2.0¹² radykalnie zmienił architekturę komunikacji. Żołnierze, dziennikarze obywatelscy i cywile otrzymali narzędzia do natychmiastowego publikowania materiałów i organizowania się w sieci. Blogi, fora dyskusyjne oraz pierwsze media społeczno-

⁹ R. Bilski, *Kocioł Bałkański*, Warszawa 2000, s. 10; M. Waldenberg, *Rozbicie Jugosławii: jugosłowiańskie lustro międzynarodowej polityki*, Warszawa 2005; s. 186–193; J. Kiper, *Remembering the Causes of Collective Violence and the Role of Propaganda in the Yugoslav Wars*, „Nationalities Papers” 2024, Vol. 52, No. 1, s. 83–84, 98–99.

¹⁰ P. Greenfield, J. Beagles-Roos, *Radio vs. Television: Their Cognitive Impact on Children of Different Socioeconomic and Ethnic Groups*, „Journal of Communication” 1988, Vol 38, No. 2, s. 82–89.

¹¹ H. Ivanov, *Inside Propaganda Serbian Media in the Yugoslav Wars 1991–1995*, London 2021, s. 21–23; J.W. Cheng, H. Mitomo, T. Otsuka, S.Y. Jeon, *Cultivation effects of mass and social media on perceptions and behavioural intentions in post-disaster recovery — The case of the 2011 Great East Japan Earthquake*, „Tematics and Informatics” 2016, Vol. 33, Issue 3, s. 765–769; C.H. Liao, *Exploring the Influence of Public Perception of Mass Media Usage and Attitudes towards Mass Media News on Altruistic Behavior*, „Behavioral Sciences” 2023, Vol. 13, No. 621, s. 14–17.

¹² Web 2.0 — koncepcja interaktywnej przestrzeni informacyjnej, w której użytkownicy nie tylko konsumują, lecz także tworzą treści, a sieciowe platformy (media społecznościowe, blogi, mikroblogi) stają się polem operacyjnym dla działań dezinformacyjnych, propagandowych i asymetrycznych. Środowisko sieciocentryczne cechuje się w takim ujęciu relatywnie niskim progiem wejścia, decentralizacją źródeł informacji oraz architekturą sprzyjającą szybkiemu rozprzestrzenianiu się treści; D. Patrikarakos, *Web 2.0: The New Battleground*, „Armed Conflict Survey” 2018, Vol. 4, No. 1, s. 51, 54–58.

ściowe stworzyły równoległą przestrzeń informacyjną, w której treści powstawały i rozprzestrzeniały się oddolnie, bez centralnego filtrowania. Skala i tempo tej produkcji doprowadziły do erozji tradycyjnej hierarchii przekazu oraz osłabienia skuteczności mechanizmów cenzury. W efekcie zaobserwowano przejście od „wojny zarządzanej” do „wojny partycypacyjnej”¹³, w której kontrola nad narracją stała się polem rozproszonego, wielopodmiotowego sporu.

Trzeci przełomowy moment nastąpił w drugiej dekadzie XX wieku, gdy cyberprzestrzeń stała się areną działań asymetrycznych aktorów, w tym grup hakerskich, organizacji pozapaństwowych, a nawet pojedynczych osób. Postęp technologiczny, powszechny dostęp do narzędzi ofensywnych oraz globalny zasięg sieci sprawiły, że zdolność do wpływania na bieg wydarzeń przestała być domeną wyłącznie państw. Pojedynczy, wysoko wykwalifikowany specjalista lub mała grupa działająca z dowolnego miejsca na świecie może dziś zakłócić funkcjonowanie infrastruktury krytycznej, przeprowadzić złożoną kampanię dezinformacyjną czy pozyskać wrażliwe dane o znaczeniu strategicznym — co wstępnie zarysowano w poprzednich rozdziałach. W rezultacie równowaga sił w sferze informacyjnej i cybernetycznej uległa dalszej destabilizacji, a pole walki stało się bardziej złożone niż kiedykolwiek wcześniej.

Powyższe pozwala spojrzeć na „nowe wojny”, tj. konflikty ery cyfrowej i popularyzacji cyberprzestrzeni¹⁴, przez pryzmat trzech okresów:

- d) zarządzanie informacją w wojnie — przekaz odgórny, kontrolowany głównie przez wojsko i państwo;
- e) rozpad monopolu — zburzenie tradycyjnego modelu kontroli narracji w wyniku rewolucji technologicznej i pojawienia się mediów oddolnych;
- f) tworzenie się nowego układu sił — wzrost znaczenia asymetrycznych aktorów w cyberprzestrzeni, w tym podmiotów pozapaństwowych i jednostek.

W każdym z powyższych okresów wskazać można przykłady reprezentatywnych wydarzeń, oddających istotę przemian, zastosowane techniki oraz wywoływane skutki. Wybrane zdarzenia i konflikty przedstawiono w poniższej tabeli (1).

¹³ O. Biuchak, A. Hoskins, *My war: participation in warfare*, „Digital War” 2022, No. 3, s. 1–4.

¹⁴ Poza kryterium popularyzacji dostępu do cyberprzestrzeni (komputery domowe, sieć Internet), kierowano się także kryterium czasowym „nowych wojen”, które jest najpowszechniej przyjętym w źródłach. Wskazują one na upadek Związku Radzieckiego, czy operację Pustynna Burza. Ponadto wzięto pod uwagę aspekt informacyjny, tj. źródła, odbiorców, metod sprawowania kontroli oraz sposobów rozprzestrzeniania się informacji. Na podstawie tych przesłanek, dokonano wyboru zakresu od lat 90. XX wieku do współczesności; H. Münkler, *Old and new wars* [w:] *The Routledge Handbook of Security Studies*, M.D. Cavelty, V. Mauer (eds.), Abingdon-New York 2010, s. 191–192; P. Bryczek-Wróbel, M. Moszczyński, *The evolution of the concept of information warfare in the modern information society of the post-truth era*, „Defence Science Review” 2022, No. 13, s. 51–52.

Okres	Lata	Wydarzenie	Przełomowy aspekt technologiczno-taktyczny
Zarządzanie informacją w wojnie: wojsko dominuje przekaz	1991	Wojna w Zatoce Perskiej	Wojna ta ustanowiła model ścisłego zarządzania informacją. System „pool” z akredytowanymi reporterami, codzienne briefingi i transmisje CNN 24/7, zbudowały „wojnę na żywo” pod kontrolą wojska. Przełomem stało się również widowiskowe użycie precyzyjnej amunicji kierowanej i nagrań wideo z urządzeń celowniczych jako narzędzi narracyjnych. To pierwszy konflikt śledzony równocześnie przez masową publiczność, gdzie kontrola przepływu obrazów stała się elementem operacji. Efekt: odczarowanie „syndromu Wietnamu” i utrwalenie modelu odgórnego zarządzania mediami jako standardu kolejnych interwencji.
	1999	Kosowo	NATO powtórzyło model informacyjny z 1991 roku: operacja lotnicza z silnie reglamentowanym dostępem mediów i naciskiem na przekaz o „chirurgicznej precyzji”. Kontrola narracji minimalizowała polityczne koszty braku mandatu Rady Bezpieczeństwa, a obrazy trafień precyzyjnych wzmacniały przekaz o „wojnie humanitarnej”. Skala zastosowania środków precyzyjnych i briefingi wojskowe budowały wizerunek skuteczności, mimo kontrowersji wokół błędów i strat cywilnych. Efektem było ugruntowanie przekonania, że przewaga informacyjna i medialna może współdecydować o powodzeniu kampanii bez użycia sił lądowych.
	2001	Ataki z 11 września oraz wojna w Afganistanie	Początek globalnej „Wojny z Terroryzmem”, narodziny systemu nadzoru cyfrowego. Atak na World Trade Center z 11 września uruchomił globalną Wojnę z Terroryzmem, łącząc siły specjalne, precyzyjne uderzenia i wsparcie lotnicze z nową infrastrukturą nadzoru cyfrowego. Przełomem była skala integracji wywiadu, łączności i rozpoznania z operacjami kinetycznymi oraz sposób relacjonowania 24/7, emocjonalne, w czasie realnym. Skutek: trwała rozbudowa reżimów prawnych i technologicznych nadzoru oraz militaryzacja walki informacyjnej jako stałego komponentu operacji.
	2003	Wojna w Iraku	„Shock and awe”: teatr wojenny transmitowany na żywo, blogi żołnierzy, militarna produkcja narracji. Kulminacja wojny jako spektaklu: reporterzy towarzyszący żołnierzom i ofensywa wizualna miały zsynchronizować percepcję z tempem działań. Przełomem była też profesjonalizacja własnej produkcji treści przez siły zbrojne, armia stała się nadawcą, a nie tylko nadzorcą lub obiektem relacji. Skala telewizyjnej inscenizacji i kontroli dostępu osłabiła zdolność mediów do kwestionowania narracji politycznej.

Okres	Lata	Wydarzenie	Przełomowy aspekt technologiczno-taktyczny
Rozpad monopolu: zburzenie tradycyjnego modelu kontroli narracji	2004–2010	Upadek kontroli informacyjnej — Abu Ghraib oraz Web 2.0	Zdjęcia tortur wykonane przez samych sprawców w Abu Ghraib pokazały, że aparat kontroli nie nadąża za obiegiem cyfrowych obrazów. Web 2.0 dał żołnierzom i cywilom narzędzia do natychmiastowego publikowania i organizowania się; blogi, fora i wczesne media społecznościowe stały się równoległą sferą wojny. Skala oddolnej produkcji treści zburzyła hierarchię komunikacji i osłabiła skuteczność tradycyjnej cenzury. Wywołało to przejście z wojny zarządzanej do partycypacyjnej, gdzie kontrola narracji stała się rozproszona.
	2010	Wikileaks oraz dziennikarstwo obywatelskie	Transparentność wojny — ujawnienie dokumentów wojennych jako forma nowej kontroli społecznej. Wikileaks zinstrumentalizował cyfrową infrastrukturę do masowych wycieków (Collateral Murder, Afghan War Logs, Iraq War Logs), redefiniując relację między tajemnicą państwową oraz interesem publicznym. Przełom polegał na hurtowej, surowej publikacji materiałów i modelu kooperacji z redakcjami. Skutkiem była globalna debata o granicach jawności i bezpieczeństwie operacyjnym oraz wzmocnienie praktyk dziennikarstwa danych w sprawach wojny.
	2010–2017	Wzrost znaczenia dronów i cyberoperacji	Drony wprowadziły teleobecność i stałe ISTAR ¹⁵ , łącząc rozpoznanie z selektywną projekcją siły („assassination by joystick”). Cyberoperacje — od Estonii w 2007 roku i Gruzji w 2008 roku, po Stuxnet w 2010 roku — pokazały, że infrastruktura krytyczna i systemy przemysłowe są polem rażenia porównywalnym z kinetyką. Skala i częstotliwość ataków wymusiły doktrynalne uznanie cyberprzestrzeni za domenę działań i rozbudowę adekwatnych zdolności. Efekt: rozszczelnienie granicy wojny i pokoju. Zaostrzenie konkurencji międzypaństwowej w środowisku sieciocentrycznym, wzrost popularności koncepcji konfliktu poniżej progu wojny.
	2011–2015	Gaza, Syria i wojna partycypacyjna	Smartfony, platformy i streaming sprawiły, że każda strona konfliktu (armie, milicje, dziennikarze obywatele, diaspory) stała się producentem narracji w czasie rzeczywistym. Przełom dotyczył nie tylko dystrybucji, ale i taktyki: operacje planowano z myślą o kamerze, a obrazy stawały się efektami operacyjnymi (odstraszanie, rekrutacja, delegitymizacja przeciwnika). Skala globalnego uczestnictwa widowni i wolontariuszy OSINT przekształciła odbiorców w aktorów. Wojna o teren zarazem była wojną o uwagę, a Facebook i Twitter stały się istotnymi źródłami wiedzy.

¹⁵ ISTAR (ang. intelligence, surveillance, target acquisition, and reconnaissance) — integracja informacji wywiadowczych i z rozpoznania w celu wsparcia działań wojskowych.

Okres	Lata	Wydarzenie	Przełomowy aspekt technologiczno-taktyczny
	2014–2017	ISIS i wojna wiralna	ISIS zbudowało fabrykę treści: wysokiej jakości montaż, język memów i seryjne formaty przemocy pod algorytmy platform. Przełomowe było sprzężenie propagandy z taktyką: treści rekrutowały, zastraszaly i koordynowały, a przemoc stawala się widowiskiem zaprojektowanym do udostępniania. Skala dyfuzji (wiele języków, tysiące kanałów) wymusiła kontrdziałania: blokady kont, kampanie cyberoperacji wykorzystujących podatności w systemach, ściganie węzłów dystrybucji. W efekcie platformy stały się polami bitew, a moderacja — narzędziem bezpieczeństwa.
Tworzenie się nowego układu sił: wzrost znaczenia asymetrycznych aktorów w cyberprzetworzeniach	2015–2020	Żołnierz udoskonalony oraz militaryzacja AI	Eksperymenty z technologią noszoną (ang. wearables), wykorzystaniem rzeczywistości rozszerzonej, egzoskieletami i BCI ¹⁶ oraz automatyzacją ISTAR zapowiadały „wojnę algorytmiczną”. Miała ona przynieść krótsze ścieżki decyzyjne, więcej źródeł danych, mniej ludzi w tejże ścieżce. Przełom polegał na łączeniu danych z wielu sensorów z półautonomicznym wykonawstwem (drony lądowe, powietrzne i morskie). Zaczęto szerzej dyskutować o w pełni autonomicznych systemach bojowych. Zaczęło dochodzić do przesunięcia ciężaru przewagi z platform kinetycznych na przewagę obliczeniową i architekturę danych.
	2020–2022	Covid-19 i popularyzacja pracy zdalnej	Pandemia wymusiła gwałtowne przejście na zdalne łańcuchy pracy, szkolenia i utrzymania, rozszerzając powierzchnię cyberataków. Zaobserwowano wzrost kampanii ransomware i ataki na łańcuchy dostaw, a przeciążone zespoły IT operowały w trybie kryzysowym. Kryzys półprzewodników uderzył w łańcuchy modernizacyjne i produkcję obronną, wymuszając rewizję strategii pozyskań i zapasów. Skutkiem tego był gwałtowny wzrost cen półprzewodników na rynku cywilnym. W skali społecznej przyspieszyła normalizacja teleobecności (telemedycyna, teleedukacja, zdalna administracja), co przełożyło się na nowe wektory wpływu informacyjnego i zależność od platform.

¹⁶ BCI (ang. brain-computer interface) — technologie łączące bezpośrednio elektronikę z sygnałami z ludzkiego mózgu metodami skanowania lub wszczepu elektrod.

Okres	Lata	Wydarzenie	Przełomowy aspekt technologiczno-taktyczny
	2020–2025	Rosnąca polaryzacja społeczna w demokracjach	Algorytmiczna segmentacja i agresywne formaty krótkich treści spotęgowały polaryzację, a aktorzy państwowi i niepaństwowi wykorzystywali mikrotargetowanie ¹⁷ , botnety ¹⁸ i operacje wpływu. Skutkiem stała się erozja zaufania do instytucji państwa oraz dotychczasowych konsensusów publicznych (społecznych). Przełomem jest skala i precyzja personalizacji przekazów, które omijają tradycyjne bramki weryfikacji, rozciągając spór informacyjny na codzienne życie. Skutek militarny jest pośredni, ale realny: trudniejsza koordynacja polityk bezpieczeństwa, większa podatność na operacje psychologiczne i kryzysy legitymizacji decyzji o użyciu siły.
	2022–2025	Konflikt w Ukrainie	Pierwszy konwencjonalny konflikt z masową, obustronną integracją dronów (w tym improwizowanych, niskiego i średniego pułapu) oraz walką radioelektroniczną, która w czasie rzeczywistym kształtuje taktykę. Przełomowe było połączenie tanich platform, oprogramowania otwartoźródłowego, czy finansowania z inicjatywy społecznej, z pominięciem państwa. Wykorzystano także komercyjną infrastrukturę satelitarną dla łączności i rozpoznania. Skala użycia, tj. tysiące dronów miesięcznie, ciągła adaptacja środków walki radioelektronicznej czy dalekosiężne uderzenia precyzyjne, redefiniują pojęcie przewagi ogniowej. Działania w cyberprzestrzeni toczą się równolegle, ale w samym konflikcie największe znaczenie ma ją sensoryka, walka kinetyczna i walka radioelektroniczna. Stają się one nowym trójkątem przewagi.

Tab. 1. Wybrane wydarzenia reprezentatywne dla okresów „nowych wojen” (ery cyfrowej)¹⁹.

¹⁷ Mikrotargetowanie — rozumiane jako docieranie do konkretnych, niewielkich grób odbiorców lub pojedynczych osób ze starannie wyselekcjonowanymi treściami. Są to działania oparte o zaawansowane algorytmy dostarczające treści, przede wszystkim w mediach społecznościowych. We wskazanym okresie zaobserwowano także wzrost wykorzystania mikrotargetowania w wyborach, np. parlamentu polskiego w 2023; K. Mrocza, K. Żarna, M. Nowakowski, *Wykorzystanie algorytmów i narzędzi sztucznej inteligencji w kampanii wyborczej w Rzeczypospolitej Polskiej i Republice Słowacji — analiza case studies*, „Studia politologiczne” 2024, nr 72, s. 279–299; M. Cześnik, R. Miśta, M. Żerkowska-Balas, *Uczestnictwo i mobilizacja w wyborach parlamentarnych 2019 roku*, „Studia Socjologiczne” 2020, nr 4, s. 91–120.

¹⁸ Grupy urządzeń zainfekowanych złośliwym oprogramowaniem w ukryciu przed użytkownikiem, tworzące zdalnie kontrolowaną sieć. Grupy te są następnie wykorzystywane w dalszych atakach. Choć początkowo pojęcie to wiązano głównie z komputerami, to popularyzacja internetu rzeczy (IoT — ang. internet of things) doprowadziła do coraz częstszego wykorzystania niewielkich smart-urządzeń; M. Gelgi i inni, *Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques*, „Sensors” 2024, No. 24, Issue 11, s. 9–10, 28–29.

¹⁹ Opracowanie własne.

4.1.1. Okres zarządzania informacją: dominacja wojska w przekazie

W debacie publicznej lat 80. ugruntował się mit, że Wietnam przegrano „na ekranie” — przez obrazy ofiar i ambiwalentnych relacji z frontu²⁰. Sformułowanie takie upraszcza jednak złożoność konfliktu, redukując go do roli mediów. W rzeczywistości decydujące były błędy strategiczne, niedoszacowanie przeciwnika i brak dostosowania doktryny do realiów wojny partyzanckiej²¹. Wietkong i armia północnowietnamska, wspierane przez ZSRR i Chiny, prowadziły długotrwałą, wyniszczającą kampanię, której USA nie potrafiły skutecznie przeciwdziałać, mimo przewagi technologicznej. Media przyspieszyły erozję poparcia społecznego, ujawniając brak postępów i sprzeczności w przekazie władz²², lecz były raczej katalizatorem kryzysu legitymizacji niż jego przyczyną. Porażka wynikała z połączenia czynników militarnych, politycznych i społecznych, a nie wyłącznie z „wojny na ekranie”.

Mimo to, konsekwencją wojny w Wietnamie było dążenie do minimalizacji kosztów ludzkich i do ścisłej kontroli przekazu. Praktyczny wzorzec dostarczyła Brytania na Falklandach w 1982 roku: reglamentowany dostęp, wstępna weryfikacja korespondentów, ścisły nadzór transmisji i cenzura *ex ante*. Działania te zostały ujęte w patriotyczne ramy, które media głównego nurtu współtworzyły, wpisując się w logikę operacji²³. Pierwsze podobne działania ze strony USA zostały podjęte w 1983 roku na Grenadzie. W pierwszych dwóch dniach operacji wykluczono zupełnie przekazywanie informacji przez prasę. Miało to służyć zaskoczeniu militarnemu, zminimalizować rozpraszanie żołnierzy obecnością prasy, a także wykluczyć konieczność poświęcenia części sił na ochronę reporterów²⁴. Takie podejście spotkało się jednak z potępieniem i oskarżeniami o zamach na wolność słowa. Podobne ograniczenia nakładane na dziennikarzy towarzyszyły inwazji USA na Panamę w 1989 roku. Grupom akredytowanym odmawiano transportu i dostępu do operacji, która zaczęła się w międzyczasie. Z kolei samolotom czarterowym z dziennikarzami śledczymi na pokładzie zabraniano lądowania, co tłumaczono zbyt dużym zagrożeniem²⁵. Mimo krytycznej oceny mediów, wojsko zaczęło osiągać zamierzone rezultaty,

²⁰ M. Mandelbaum, *The Television War*, „Daedalus” 1982, Vol. 111, s. 157–163; P.C. Rollins, *The Vietnam War: Perceptions Through Literature, Film, and Television*, „American Quarterly”, 1984, Vol. 36, No. 3, s. 423–431.

²¹ H.G. Summers, *On Strategy: A Critical Analysis of the Vietnam War*, New York 1995, s. 110–125.

²² R. Singsank, *Skepticism and Exposure: Television Coverage of the Vietnam*, „Armstrong Undergraduate Journal of History” 2020, Vol. 10: Issue 2, s. 93–94.

²³ C.R. Ellerby, *British Interests in the Falkland Islands: Economic Development, The Falkland Lobby and the Sovereignty Dispute. 1945 to 1989*, Oxford 1990, s. 283–285.

²⁴ R.W. Pincus, *Press access to military operations: Grenada and the need for a new analytical framework*, „University of Pennsylvania Law Review” 1987, Vol. 135(813), s. 813–814.

²⁵ D.A. Frenznick, *First Amendment on the Battlefield: A Constitutional Analysis of Press Access* →168

tylko wzmacniając przekonanie, że USA potrzebny jest dopracowany, powtarzalny system zarządzania informacją — nawet przy sprzeciwie agencji prasowych, telewizyjnych i radiowych.

I wojna w Zatoce Perskiej (1990–1991) była dla USA symbolicznym przepracowaniem traumy Wietnamu: szybkim wygranym i technologicznie sprawnemu działaniu, towarzyszyło nowe podejście do mediów. Zakładano wówczas równoległe prowadzenie dwóch wojen: kinetycznej na Bliskim Wschodzie i globalnej, tj. informacyjnej. Tę ostatnią adresowano do trzech grup odbiorców: krajowej (morale i poparcie), koalicyjnej (legitymizacja) i wrogiej (demoralizacja). Wymagało to odmiennej kalibracji treści, lecz jednolitej infrastruktury przekazu. Zbudowano ją w oparciu o:

- polityczne odprawy w Waszyngtonie i Londynie²⁶;
- ściśle kontrolowane odprawy wojskowe z Dhahranu i Rijadu²⁷;
- tzw. pool system — ograniczoną akredytację wybranych (głównie angloamerykańskich) dziennikarzy, skupionych w jednostkach reporterskich, z towarzyszącymi cenzorami i „forward transmission units” o prawie do wstrzymywania materiałów²⁸.

W praktyce bezpośrednia cenzura była rzadka, ponieważ bliskość operacyjna i zależność logistyczna sprzyjały autokontroli, a tempo działań naziemnych utrudniało bieżące nadawanie. Jednocześnie wysiłki militarne i dyplomatyczne (budowa koalicji „Desert Shield” i wymuszenie rezolucji RB ONZ) były od początku splecione z operacją

to Military Operations in Grenada, Panama and the Persian Gulf, „McGeorge Law Review” 1991, Vol. 23, Issue 2, s. 325–326.

²⁶ W.H Parks, *The Gulf War: A Practitioner's View*, „Penn State International Law Review/Penn State International Law Review” 1992, Vol. 10(3), s. 416–417.

²⁷ Kontrolowano również informacje przekazywane przez dziennikarzy rządowej Saudyjskiej Agencji Prasowej (SPA, arab. وكالة الأنباء السعودية). Ograniczono ich dostęp do obszarów działań wojennych, a raporty przysyłano do Wspólnego Biura Informacyjnego (JIB — ang. Joint Information Bureau). Biuro to przetwarzało też informacje z Dhahranu i Rijadu, a czasami także z codziennych odpraw saudyjskiego wojska; AM. Al Kahtani, *The Performance of the Saudi Arabian Press During the Gulf Conflict, 1990-1991*, Leeds 1999, s. 3–4.

²⁸ System pool został opracowany przez Pentagon w odpowiedzi na wcześniejsze ograniczenia medialne, m.in. podczas interwencji w Grenadzie w 1983 roku. W ramach tego systemu wybrani przedstawiciele mediów (tzw. „pool reporters”) otrzymywali możliwość relacjonowania wydarzeń z frontu, a ich materiały były następnie udostępniane reszcie dziennikarzy. Należy podkreślić, że choć system miał zapewnić bezpieczeństwo i kontrolę nad przepływem informacji, w praktyce często ograniczał dostęp do kluczowych wydarzeń. Np. w bitwa o Khafji, najlepiej poinformowani byli tzw. „pool busters” — dziennikarze działający poza oficjalnym systemem. Finalnie system prowadził do licznych napięć między mediami i wojskiem. Niemniej, wśród akredytowanych dziennikarzy dostrzeżono nawiązywanie relacji z żołnierzami, co skutkowało tworzeniem bardziej patriotycznych treści; D.H. Mould, *Press pools and military-media relations in the Gulf War: a case study of the battle of Khafji, January 1991*, „Historical Journal of Film, Radio and Television” 1996, Vol. 16, No. 2, s. 136–138; S. Oates, *War Propaganda and the Patriotic Model of the News in the 21st Century*, „Journalism & Communication Monographs” 2021, Vol. 23(4), s. 330–331.

perswazyjną skierowaną do opinii publicznych. Warunek „wyjścia z Wietnamu” — rozumiane jako szybkie zwycięstwo o niskich kosztach — miał być komunikowalny oraz wiarygodny²⁹. Kulminacją tej logiki była konstrukcja „idealnego” scenariusza: dominacja w powietrzu, wstrząsowy ostrzał infrastruktury, czy krótka, 100-godzinna kampania. Dzięki temu uzyskano format, który równie dobrze mieścił się w planie operacyjnym, jak i w harmonogramie przekazu do globalnej publiczności.

Nowością była zdolność telewizyjnej infrastruktury, do utrzymania nieprzerwanego rytmu relacji „na żywo”: studia, eksperci, raporty z regionu, konferencje w rytmie dobowym, a nawet transmisje z Bagdadu. Wytworzyło to modernistyczną obietnicę „wojny jako transmisji”, czyli ciągłego, zsynchronizowanego spektaklu. Precyzyjne uderzenia i obrazy „inteligentnych” bomb budowały wrażenie higieny przemocy: wysokiej kontroli skutków i minimalizacji ofiar cywilnych. W publicznym odbiorze rodziło to figurę „czystej wojny”³⁰, nawet jeśli sposób prowadzenia konfliktów pozostawał niezmienny. Co do zasady wojna polegała na destrukcji infrastruktury i giną w niej cywile, lecz przez dobór materiałów, kadr i języka, skutecznie unikano eksponowania tych aspektów³¹. Telewizja „wojenna” lat 90. różniła się od Wietnamu nie tylko rytmem, lecz także materiałami: szybka teletransmisja zastąpiła filmową zwłokę i montaż po dobie. Nie tylko przyspieszyło to obieg, lecz przede wszystkim ujednoliciło format.

Taka medialność sprzyjała także redefinicji ról: generałowie jako narratorzy dnia, operatorzy telewizyjni jako posłańcy dostarczający „dowody skuteczności”, a publiczność jako audytorium spektaklu, mniej jako krytyczny odbiorca. Wytwarzaniu społecznej akceptacji wojny w Zatoce Perskiej towarzyszyła także fabrykacja materiałów wysoce emocjonalnych. Przykładem jest „świadeństwo” 15-letniej Nayiry z 1990 roku, która zeznała ona przed Kongresem USA, że była świadkiem zbrodni dokonywanych przez irackich żołnierzy. Jedną z nich miało być wydobycie noworodków z inkubatorów w szpitalu al-Addan i pozostawienie ich na śmierć na szpitalnej posadzce³². Materiał nagłośniony został przez stacje sieciowe i był wielokrotnie przywoływany w debacie senackiej oraz przez prezydenta. Siła narracyjna tej fabuły, mimo braku weryfikacji, stała się jednym z kluczo-

²⁹ G.C. Herring, *Reflecting the Last War: the Persian Gulf and the „Vietnam Syndrome”*, „Journal of Third World Studies” 1993, Vol. 10, No. 1, s. 45.

³⁰ D. Arav, *Trauma and Nostalgia in the Israeli Televised Memory of the First Gulf War*, [w]: *Trauma and Nostalgia. Practices in Memory and Identity*, L. van Liere, S. Sremac (eds.), Amsterdam 2024, s. 47.

³¹ K. Aryal, *The Gulf War as Simulacra: An Analysis of Vishwa Ghatana [World Affairs] on Nepal Television*, „Journal of Arts & Humanities” 2023, Vol. 5, No. 1, s. 69–70.

³² M.S. Sweeney, *The Military and the Press: An Uneasy Truce*, Evanston 2006, s. 163–64.

wych zasobów mobilizacyjnych poparcia³³. Fragmenty tych zeznań w formie wideo trafiły wówczas do ok. 35 milionów odbiorców, wywołując zamierzoną reakcję³⁴. Dopiero pod koniec konfliktu ujawniono, że Nayira była córką ambasadora Kuwejtu w USA, a jej „świadeństwo” zostało spreparowane przez prywatną firmę Hill & Knowlton, która specjalizuje się w public relations³⁵. Przykład ten ukazuje, iż potencjalna „czystość” nie jest właściwością samych działań wojskowych, lecz efektem informacyjnej kontroli i selekcji oraz dramaturgii medialnej. Poza poparciem w społeczeństwie, skutkiem było także powstanie rosnącej potrzeby podjęcia działań zmierzających do niezależnej weryfikacji danych czy zachowania transparentności źródeł.

Pod koniec dekady system odgórnego zarządzania informacją został odtworzony w kampanii NATO podczas konfliktu w byłej Jugosławii. W warunkach interwencji lotniczej powtarzano wcześniejsze rozwiązania: centralne odprawy, kontrolę dostępu i obrazowanie skuteczności uderzeń jako główny nośnik legitymizacji. W kontekście koalicji i sporów prawnych o mandat użycia siły, komunikacja była nie tylko „wsparciem operacji”, ale polem, na którym rozstrzygano sensowność interwencji³⁶. To z kolei miało istotne znaczenie, gdyż wojska Paktu Północnoatlantyckiego podjęły interwencję w ramach administracji prezydenta USA Billa Clintona, czyniąc to bez aprobaty ONZ. Decyzję o „wojnie prewencyjnej” uzasadniano przesłankami o niedopuszczeniu do katastrofy humanitarnej, ludobójstwa kosowskich Albańczyków oraz okrucieństw porównywalnych do II Wojny Światowej³⁷. Ponownie dokonano tego w rytmie całodobowych transmisji i języka technologicznej skuteczności działań NATO.

Wartym podkreślenia jest, że Siły Sojuszu zbombardowały wówczas 17 z 19 nadajników, jak również budynki Radio-Telewizji Serbii (RTS, serb. Radio Televizija Srbije — Радио-телевизија Србије): siedziby w Belgradzie (23 kwietnia 1999 roku) oraz w Nowym Sadzie (3 maja 1999 roku)³⁸. Zachodnie media silnie demonizowały Serbów, czyniąc z zarzucanej im działalności główny wątek medialny. Były to często materiały sfabryko-

³³ D. Walton, *Appeal to Pity: A Case Study of the Argumentum Ad Misericordiam*, „Argumentation” Vol. 9, No. 5, s. 772–773.

³⁴ A.E. Rowse, *How to Build Support for War*, „Columbia Journalism Review” 1992, No. 31, s. 28.

³⁵ S.A. Roschwalb, *The Hill & Knowlton Cases: A Brief on the Controversy*, „Public Relations Review” 1994, Vol. 20, No. 3, s. 268, 271–272.

³⁶ D.K. Thussu, *Legitimizing Humanitarian Intervention? CNN, NATO and the Kosovo Crisis*, „European Journal of Communication” 2000, Vol. 15, No. 3, s. 348–351.

³⁷ N. Mihaljinac, A. Vujošević, *The Representation of the NATO Bombing of Yugoslavia in Foreign Artistic and Mass Media Texts: Unjustified War or Justified Intervention?*, „TEME: Časopis za društvene nauke” 2021, Vol. XLV, No 2, s. 464.

³⁸ P. Hammond, *Reporting "Humanitarian" Warfare: propaganda, moralism and NATO's Kosovo war*, „Journalism Studies” 2000, Vol. 1, No. 3, s. 368–369.

wane, jak np. filmowane przez Cable News Network (CNN) transporty rannych, którzy tak naprawdę nie byli poszkodowani³⁹. Z kolei wystąpienia rzecznika NATO, Jamiego Shea, podczas 78-dniowej operacji Allied Force w Jugosławii⁴⁰, stały się jednym z najbardziej krytykowanych przykładów manipulacji medialnej w zachodnich mediach. Codzienne konferencje prasowe, transmitowane na żywo, były, jak sam przyznał, elementem „wojny informacyjnej”⁴¹. Początkowo działania te krytykowane były m.in. przez media rosyjskie, które starały się ukazać rzeczywistych uchodźców uciekających przed bombardowaniami⁴². Dopiero później podjęto szerszą krytykę operacji NATO, wskazując m.in. na brak szacunku do ofiar przez uczynienie „show” z wojny oraz brak szacunku do ofiar⁴³.

Spójność logiczna analizowanego okresu dominacji wojska nad informacją, ujawnia jej podatność na tzw. „efekt tunelowy” — czyli skłonność do faworyzowania obrazów zgodnych z założeniami operacyjnymi, nawet jeśli pomijają one złożone konsekwencje humanitarne i polityczne. W narracji skupionej na „precyzyjnych uderzeniach” systemowo niwelowano dysonans wynikający z rozbieżności między wizualnym przekazem oraz rzeczywistymi skutkami. Aby zrozumieć, jak wojna została przekształcona w doświadczenie medialne na Zachodzie w latach 90., należy dostrzec, że kluczową rolę odegrała tu przede wszystkim „inżynieria widzialności” — a nie sama technologia militarna. To właśnie skrupulatna dominacja w przekazie umożliwiła skuteczne legitymizowanie interwencji z lat 1991 i 1999. Jednak ten model zaczął załamywać się w epoce Web 2.0, gdy instytucje straciły monopol na produkcję i kontrolę informacji.

³⁹ G. Civikov, *Proces Miloszewicia. Relacja obserwatora*, Warszawa 2009, s. 170–172.

⁴⁰ Operacja prowadzona przez NATO w okresie od 24 marca do 20 czerwca 1999 roku. Miała doprowadzić do zakończenia czystek etnicznych na terenie Kosowa, a także wymuszenia procesu demokratyzacji Jugosławii, M.W. Lamb Sr., *Operation Allied Force. Golden Nuggets for Future Campaigns*, Alabama 2002, s. 2–7.

⁴¹ *The Balkans: quo vadis? Jamie Shea: Kosowo — wówczas i obecnie*, 25 August 2008, „NATO Review”, <https://www.nato.int/docu/review/pl/articles/2008/08/25/jamie-shea-kosowo-wowczas-i-obecnie/index.html> [odczyt: 1 sierpnia 2025], wywiad: od minuty 2:20 do 8:00.

⁴² P. Hammond, L. Nizamova, I. Savelieva, *Consensus and Conflict in the Russian Press*, [w:] *Degraded Capability: The Media and the Kosovo Crisis*, E.S. Herman, P. Hammond (eds.), London 2000, s. 181–182.

⁴³ Należy podkreślić, że do dziś większa część źródeł publikowanych na Zachodzie, które krytycznie odnoszą się do działań NATO w Jugosławii, jest autorstwa naukowców z Europy Wschodniej i Bałkanów; O. Fridman, *Memories of the 1999 NATO Bombing in Belgrade, Serbia*, „Südosteuropa” 2016, Vol. 64, No. 4, s. 451; D. Trbojević, *Unearthing memories: 1999 bombing of FR Yugoslavia between crisis, trauma and nostalgia*, „Ethnologia Slovaca et Slavica” 2024, T. 45, s. 67–70; A. Mitić, *Reflection of the 1999 NATO Aggression in the Strategic Narratives of Global Powers and the Context of Multipolarity*, [w:] *History and Cultural Memory*, J. Janijić, M. Pesić (eds.), Belgrade 2024, s. s. 400–401.

4.1.2. Okres rozpadu monopolu: zburzenie tradycyjnego modelu kontroli narracji

Inwazja na Irak w 2003 roku wyznaczyła punkt zwrotny w zdolności wojska do utrzymania centralnej kontroli nad przekazem informacji. Model ściśle zarządzanej komunikacji zaczął erodować wskutek nowych możliwości technologicznych, jak również rosnącej kultury uczestnictwa w sieci. Już sama możliwość dokumentowania działań przez żołnierzy zaczęła stanowić wyzwanie dla hierarchii informacyjnej wojska. Symbolicznym momentem tej zmiany była afera w więzieniu Abu Ghraib w 2004 roku. Fotografie tortur wykonane przez samych sprawców⁴⁴ (amerykańskich żołnierzy) nie przedostały się do opinii publicznej dzięki tradycyjnym mediom, lecz przez wyciek cyfrowych plików, które błyskawicznie krążyły w internecie⁴⁵. Należy przy tym podkreślić, że już wcześniej istniały przykłady „nieautoryzowanych” materiałów w obiegu, jak np. amatorskie nagrania wojen w Czeczenii⁴⁶. Jednakże tym co odróżnia je od przełomowego momentu jest nie sam fakt dotarcia do szerszej publiczności, lecz fundamentalne nienadążanie kontroli wojskowej nad skutkami rozwoju cyberprzestrzeni.

W latach 2004–2006 ukształtował się ekosystem określany mianem Web 2.0 — zbiór platform i usług nastawionych na treści generowane przez użytkowników (ang. user-generated content) oraz na interakcję sieciową⁴⁷. Popularne wówczas blogi i fora, serwisy wideo, jak również wczesne media społecznościowe, stworzyły równoległą sferę informacyjną, nad którą wojsko nie miało bezpośredniej kontroli. Również żołnierze zaczęli wówczas prowadzić tzw. milblogs, publikować zdjęcia w serwisach typu Flickr czy krótkie filmy na YouTube⁴⁸. Każdy taki wpis mógł zawierać dane operacyjne, fragmenty codziennego życia na misji, czy podważać oficjalną narrację (także nieświadomie). Próby cenzurowania tych treści okazały się problematyczne, a zakazy publikacji często prowadziły do „efektu Streisand” — większego zainteresowania zakazaną treścią i jej migracji na serwisy poza jurysdykcją władz wojskowych⁴⁹. Bynajmniej dynamiki zmian nie należy jednak przeceniać w charakterze wzrostu „oddolnego oporu” wobec kontroli. Badania przedstawione w pracy *Like War: The Weaponization of Social Media* wskazują, że armie

⁴⁴ K. Andén-Papadopoulos, *The Abu Ghraib torture photographs: News frames, visual culture, and the power of images*, „Journalism” 2008, Vol. 9, No. 1, s. 11–21.

⁴⁵ D. Apel, *Torture Culture: Lynching Photographs and the Images of Abu Ghraib*, „Art Journal” 2005, Vol. 64, No. 2, s. 96, 99–100.

⁴⁶ S. Abraham, *Chechnya: Between War and Peace*, „Human Rights Brief” 2001, Vol. 8, Issue 2, s. 11; A. Politkovskaya, *A Dirty War: A Russian Reporter in Chechnya*, New York 2001, s. xvii–xviii.

⁴⁷ M. Allen, *What was Web 2.0? Versions as the dominant mode of internet history*, „New Media & Society” 2012, Vol. 15, No. 2, s. 260–261, 266–268.

⁴⁸ J.H. Lehman, *Military Engagement with Social Media*, [OMB No. 0704-0188] 2011, s. 5–6.

⁴⁹ S.C. Jansen, B. Martin, *The Streisand Effect and Censorship Backfire*, „International Journal of Communication” 2015, No. 9, s. 658–659.

zaczęły świadomie wchodzić w ten obieg, używając blogów czy Facebooka do operacji psychologicznych oraz rekrutacji⁵⁰. Oznacza to, że rozpad monopolu nie był procesem liniowym i jednokierunkowym, a władze wojskowe starały się adaptować do nowych realiów.

Kulminacją tego okresu było powstanie i globalny rozgłos Wikileaks — platformy, która wykorzystwała infrastrukturę cyfrową do publikacji masowych przecieków w surowej, nieprzetworzonej formie, redefiniując relację między tajemnicą państwową a interesem publicznym. Warto wyróżnić tutaj serię materiałów — od wideo *Collateral Murder* (kwiecień 2010)⁵¹, przez *Afghan War Logs* (lipiec 2010)⁵², po *Iraq War Logs* (październik 2010)⁵³, które opublikowano w WikiLeaks. Przyniosła ona bowiem dwa główne skutki:

- g) społeczny — wzmocnienie ruchów na rzecz jawności i rozwój dziennikarstwa opartego na analizie dużych zbiorów danych (tzw. data journalism);
- h) operacyjny — ujawnienie szczegółów działań taktycznych, nazwisk informatorów czy lokalizacji baz, co według wielu wojskowych komentatorów stwarzało ryzyko dla bezpieczeństwa operacyjnego⁵⁴.

Warto przy tym odnotować różnice interpretacyjne: choć często podkreśla się wartość demokratyzującą tego typu przecieków, to część publikacji akcentuje realne za-

⁵⁰ P.W. Singer, E.T. Brooking, *Like War: The Weaponization of Social Media*, Boston 2018, s. 22, 205–209.

⁵¹ *Collateral Murder* jest nagraniem 2007 roku, przedstawiającym atak amerykańskiego śmigłowca Apache w Bagdadzie, w którym zginęli cywile (w tym dwaj dziennikarze agencji Reuters). Zestawiono w nim kontrastujące perspektywy wizualne, obrazujące brutalność wojny. Publikacja nagrania w 2010 roku wywołała globalną debatę o przejrzystości działań wojskowych, etyce wojny oraz roli mediów w ujawnianiu przemocy ukrytej za militarnym językiem i technologią; J. Tidy, *Visual regimes and the politics of war experience: Rewriting war 'from above' in WikiLeaks' 'Collateral Murder'*, „Review of International Studies” 2016, Vol. 43, s. 95–103.

⁵² *WikiLeaks Afghan War Logs*, znane również jako *Afghan War Diary*, to zbiór ponad 91 000 tajnych raportów wojskowych USA dotyczących wojny w Afganistanie w latach 2004–2010, opublikowany przez WikiLeaks 25 lipca 2010 roku. Publikacja, uznana za jeden z największych przecieków w historii amerykańskiego wojska, rzuciła nowe światło na skalę przemocy, nieudokumentowane ofiary cywilne oraz niepokojące aspekty międzynarodowej współpracy w konflikcie; J. O'Loughlin, F.D.W. Witmer, A.M. Linke, N. Thorwardson, *Peering into the Fog of War: The Geography of the WikiLeaks Afghanistan War Logs, 2004–2009*, „Eurasian Geography and Economics” 2010, Vol. 51, No. 4, s. 472–483.

⁵³ *Iraq War Logs* — zbiór około 400 000 tajnych raportów wojskowych USA z lat 2004–2009, opublikowany przez WikiLeaks w październiku 2010 roku. Ujawniono systematyczne przypadki przemocy wobec ludności cywilnej, tortur stosowanych przez irackie siły oraz skalę nieudokumentowanych ofiar wojny. Ujawnienie tych danych wywołało debatę o odpowiedzialności instytucji publicznych i przejrzystości działań administracji w kontekście konfliktów zbrojnych; A. Roberts, *WikiLeaks: the illusion of transparency*, „International Review of Administrative Sciences” 2012, Vol. 78, No. 1, s. 117–121.

⁵⁴ M.D. Horvath, *Wikileaks.org—An Online Reference to Foreign Intelligence Services, Insurgents, or Terrorist Groups?*, [NGIC-2381-0617-08], 2008, s. 5–7; R.O. Vlad, *The perils of presidential openness: strikes, secrecy and performative opacity*, „Intelligence and National Security” 2023, Vol. 38, No. 6, s. 964; A. Bejar, *Balancing Social Media with Operations Security (OPSEC) in the 5a. CONTRACT NUMBER 21st Century*, [OMB No. 0704-0188], 2010, s. 6, 12.

grożenia wynikające z niefiltrowanej publikacji niejawnych dokumentów⁵⁵. Zatem choć celem była decentralizacja władzy nad informacją, scentralizowana pozycja samego Wikileaks czyniła ten serwis de facto nowym źródłem „miękkiej” władzy.

Należy też podkreślić, że przedmiotowy rozpad dotychczasowego monopolu nie oznaczał jedynie zwiększenia pluralizmu źródeł (choć czasem wciąż skoncentrowanych). Stworzył on warunki, w których każdy aktor konfliktu — od państwa, przez NGO, po grupy terrorystyczne — mógł prowadzić własną operację medialną w skali globalnej. W Syrii czy w Strefie Gazy smartfony, media społecznościowe i narzędzia transmisji na żywo pozwoliły milicjom, dziennikarzom obywatelskim i diasporom, na konstruowanie narracji w czasie rzeczywistym⁵⁶. To, co wcześniej było efektem ubocznym działań wojennych, stało się jednym z celów operacyjnych: inscenizacje dla kamer, publikacje wideo z ataków, czy tzw. kampanie hashtagowe⁵⁷.

W latach 2014–2017 powyższą metodę działania doprowadziło do skrajności tzw. Państwo Islamskie (ISIS). Budując rozbudowane „fabryki treści”, łączyło ono estetykę memów i wysokobudżetowego montażu z brutalnymi inscenizacjami przemocy — umyślnie projektowanymi pod kątem nadużycia algorytmów platform. ISIS osiągnęło niespotykany wcześniej poziom sprzężenia taktyki wojskowej z operacjami informacyjnymi. Nagrania egzekucji nie tylko zastraszały przeciwników, ale także rekrutowały i koordynowały działania sympatyków w wielu krajach⁵⁸, włączając to poparcie oraz zaangażowanie kobiet⁵⁹. Reakcją państw i platform było wprowadzenie masowych blokad kont, operacje cybernetyczne wymierzone w infrastrukturę dystrybucji oraz penalizacja propagandy terrorystycznej. W praktyce Facebook, Twitter czy YouTube stały się de facto „polami bitew” informacyjnych, a moderacja treści zaczęła pełnić funkcję narzędzia bezpieczeństwa narodowego.

⁵⁵ M.D. Horvath, *Wikileaks.org—An Online Reference...*, s. 21–22; M. Fenster, *Disclosure's Effects: WikiLeaks and Transparency*, „UF Law Scholarship Repository” 2012, No. 97, Rev. 753, s. 788–789; Y. Benkler, *A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate*, „Harvard Civil Liberties Law Review” 2011, Vol. 46, Rev. 311, s. 319–321.

⁵⁶ M. Blumenthal, *The 51 Day War: Resistance and Ruin in Gaza*, London 2015, s. 11–17.

⁵⁷ Należy przez to rozumieć wykorzystanie hashtagów do promowania narracji, mobilizacji wsparcia i walki o dominację informacyjną prze różne strony konfliktu: państwa, organizacje, grupy zbrojne i obywateli.

⁵⁸ T. Neer, M.E. O'Toole, *The Violence of the Islamic State of Syria (ISIS): A Behavioral Perspective*, „Violence and Gender” 2014, Vol. 1, No. 4, s. 150–151; H.M. Vitale, J.M. Keagle, *A Time to Tweet, as Well as a Time to Kill: ISIS's Projection of Power in Iraq and Syria*, „Defense Horizons” 2014, No. 77, s. 7–8.

⁵⁹ M. Abu Rumman, H. Abu Hanieh, *Infatuated with martyrdom: female jihadism from Al Qaeda to the “Islamic State”*, Amman 2017, s. 36, 129–131; M. Shorer, *Mobilization of Women to Terrorism: Tools and Methods of ISIS*, „International Annals of Criminology” 2018, No. 56, s. 99–101.

Upadek monopolu wojskowego nad przekazem to nie tylko zmiana techniczna, lecz przede wszystkim transformacja paradygmatu komunikacyjnego. Dawny model scentralizowanej władzy informacyjnej, w którym wojsko kontrolowało dostęp do danych i narracji, został zastąpiony przez otwarty, rozproszony system. Odbiorcy stali się współtwórcami i aktywnymi weryfikatorami treści. Rewolucja Web 2.0 w latach 2004–2010 przyspieszyła ten proces, wprowadzając technologie i platformy oparte na treściach tworzonych przez użytkowników. Trwale zmieniło to układ sił informacyjnych — wojsko straciło kontrolę nad powstawaniem i dystrybucją przekazu. Zjawisko to zyskało kilka określeń, takich jak „wojna rozproszona”⁶⁰, „wojna radykalna”⁶¹, „wojna kognitywna” (zwana również „poznawczą”)⁶², czy jako część „wojny hybrydowej”⁶³. W praktyce oznaczało to, że kontrola narracji przestała być pojedyńkiem pomiędzy nadawcami instytucjonalnymi (np. oficjalnymi materiałami wojskowymi) oraz masowymi mediami. Zamiast tego wyłonił się rozproszony ekosystem tysięcy i milionów źródeł. Żołnierskie, prywatne blogi, dziennikarze obywatelscy czy lokalne społeczności stające się operatorami i kuratorami własnego przekazu, wykorzystwały narzędzia mobilne i sieciowe do przekazywania swojej wersji wydarzeń. W rezultacie proces komunikacyjny w kontekście wojny zaczął przypominać rozproszoną rywalizację narracyjną, w dużej części znosząc skuteczność tradycyjnej cenzury.

Rozszerzenie możliwości publikowania treści w czasie rzeczywistym wymusiło modyfikację strategii wojskowych. Coraz częściej planowano operacje „pod kamerę” — uwzględniając ich potencjalny efekt wizualny i narracyjny w mediach społecznościowych⁶⁴. W tym nowym środowisku informacyjnym obrazy stawały się równorzędnymi celami operacyjnymi — mogły odstraszać przeciwnika, budować morale własnych sił lub legitymizować działania wobec opinii publicznej. Ponadto same platformy społecznościowe zaczęły pełnić funkcję areny walki: zarówno w charakterze kanału komunikacji, a zarazem przestrzeni, w której prowadzono ofensywne i defensywne operacje narracyj-

⁶⁰ A. Hoskins, B. O’Loughlin, *War and Media. The Emergence of Diffused War*, Cambridge 2010, s. 4–10.

⁶¹ M. Ford, A. Hoskins, *Radical War. Data, Attention and Control in the Twenty-First Century*, Oxford 2022, s. 11–12.

⁶² B. Claverie, F. Du Cluzel, „Cognitive Warfare”: *The Advent of the Concept of “Cognitics” in the Field of Warfare* [w]: *Cognitive Warfare*, B. Claverie, B. Prébot, N. Buchler, F. Du Cluzel (eds.), Neuilly 2022, s. 2.2–2.4.

⁶³ I. Anghel, *Social Media as Hybrid Warfare Tool — Putting Russia’s Informational Strategy in Context*, „Romanian Military Thinking” 2020, No. 1, s. 52–61; M. Kamionka, *Rosyjska wojna hybrydowa w mediach społecznościowych na przykładzie portalu Facebook*, „Wiedza Obronna” 2023, t. 282, nr 1, s. 65–67.

⁶⁴ C. Ornatowski, *Retoryka uzbrojona: walka o świadomość we współczesnej przestrzeni medialnej*, „Res Rethorica” 2021, Nr 8(4), s. 15–16, 33.

ne. Przytoczony przykład ISIS ukazuje zintegrowanie produkcji treści z taktyką bojową, tworząc wysoko zorganizowany aparat medialny o cechach:

- a) wielojęzyczności przekazu — celem zapewnienia globalnego zasięgu;
- b) wykorzystania wiralowości — celem maksymalizacji efektu udostępniania materiałów i ich propagacji przez odbiorców;
- c) profesjonalizmu tworzenia treści — celem zapewnienia spójnej identyfikacji wizualnej oraz jak najskuteczniejszego wykorzystania algorytmów platform.

W tym kontekście platformy społecznościowe stały się aktywnym polem bitwy. Blokady kont, algorytmiczne filtrowanie treści i operacje cybernetyczne przeciwko infrastrukturze ISIS stanowiły nowy wymiar reagowania państw na zagrożenie. Moderacja treści zyskała natomiast status elementu bezpieczeństwa narodowego.

Co więcej, taka zmiana modelu dystrybucji informacji miała skutki wykraczające poza sferę komunikacji. Demokratyzacja produkcji treści rozmyła monopol państwa na kreowanie obrazu konfliktu. Zacieranie granicy między uczestnikiem a obserwatorem wciągnęło globalną opinię publiczną w aktywne współtworzenie narracji wojennych. Jednakże przyspieszenie obiegu informacji zwiększyło zarazem ryzyko błędnych interpretacji i manipulacji, zanim możliwa była rzetelna weryfikacja. Tym samym lata 2004–2010 były okresem, w którym wojsko przestało być jedynym centrum dyspozycji narracyjnej. Rozpoczął się proces, który w kolejnych latach doprowadził do sytuacji, w której niewielcy, asymetryczni aktorzy zyskują potencjał wpływu porównywalny z państwami.

4.1.3 Okres tworzenia się nowego układu sił: wzrost znaczenia asymetrycznych aktorów w cyberprzestrzeni

W latach 2015–2025 zarządzanie informacją (oraz jej postrzeganiem) zaczęło stawać się najważniejszym mnożnikiem siły dla aktorów asymetrycznych. Choć „natura” wojny pozostawała taka sama, to postępowały zmiany jej charakteru — a co ważne, znaczenie działań poniżej progu otwartego konfliktu⁶⁵. Kluczowe znaczenie zyskała nie masa środków, lecz zdolność do łączenia pozyskiwania, fuzji i dystrybucji danych z efektami kinetycznymi, elektromagnetycznymi i psychologicznymi, w dużej mierze poprzez infrastrukturę cywilno-platformową. W takim ujęciu państwa tracą możliwość hierarchicznego sterowania obiegiem informacji, a przewaga przesuwa się ku tym, którzy szybciej zamykają pętle decyzyjne⁶⁶ i lepiej zarządzają niepewnością atrybucji w cyberprzestrzeni.

⁶⁵ A. Ayalon, E. Popovich, M. Yarchi, *From Warfare to Imagefare: How States Should Manage Asymmetric Conflicts With Extensive Media Coverage*, „Terrorism and Political Violence” 2016, No. 28, s. 255–266

⁶⁶ Pętle decyzyjne w rozumieniu koncepcji Johna Richarda Boyda, czyli cyklicznego modelu procesu decyzyjnego. Wyróżnia on cztery fazy: obserwację, orientację, decyzję i działanie, które służą →177

Interesujące były także eksperymenty z technologiami noszonymi, rzeczywistością rozszerzoną, egzoszkielecikami, interfejsami domózkowymi oraz automatyzacją ISTAR. Zapowiadały skrócenie ścieżek decyzyjnych przez integrację wielu sensorów z półautonomicznym wykonawstwem (drony lądowe, powietrzne, morskie). Autorzy wskazują na przesuwanie przewagi z platform kinetycznych na architekturę danych i moc obliczeniową: kto lepiej filtruje szum, dekonfliktuje sensory i automatyzuje dystrybucję zadań, ten szybciej generuje efekty na polu walki⁶⁷. Jednakże logika „wojny algorytmicznej” zdaje się wzmacniać aktorów asymetrycznych, gdyż pozwala im korzystać z tanich, komercyjnych komponentów i oprogramowania otwartoźródłowego, aby budować własne pętle informacji poza kontrolą państwowych systemów dowodzenia i kontroli.

Istotnym wydarzeniem, które zwiększyło rolę cyberprzestrzeni był wybuch pandemii wirusa SARS Cov-2. Następująca wówczas normalizacja pracy zdalnej i teleobecności przeniosła kluczowe aspekty codziennego funkcjonowania do środowisk cyfrowych. Niezależnie od potencjalnego odwrotu od takiej formy, jej wpływ wywarł trwały efekt. Organizacje zostały zmuszone do zaadaptowania rozwiązań cyfrowych, m.in. obiegu codziennej dokumentacji, zmian w sposobie świadczenia usług, czy własnej zależności⁶⁸. Kluczowe stały się bowiem łańcuchy dostaw rozwiązań w cyberprzestrzeni, tj. oprogramowania, infrastruktury i platform, zarówno jako instalacji rozwiązań lokalnych (on-premise), jak również w formie usług chmurowych. Nie mniejsze znaczenie ma także świadomość samych użytkowników cyberprzestrzeni co do wyzwań, zagrożeń i szans, jakie niesie za sobą środowisko sieciocentryczne. Z punktu widzenia zarządzania informacją, obrona przestała być problemem pojedynczego perymetru, a stała się problemem całego ekosystemu. Słabymi ogniwami są podwykonawcy, dostawcy oprogramowania, firmy świadczące usługi — a więc węzły, w które aktorzy asymetryczni mogą uderzać z niskim kosztem i mniejszym ryzykiem atrybucji. Szczególnie w Unii Europejskiej dostrzec można szybką reakcję. Przytaczana wcześniej dyrektywa NIS 2 oraz rozporządzenie DORA⁶⁹

do szybkiego reagowania w dynamicznym środowisku operacyjnym. Podobnie jednak pętle te mogą być postrzegane w cyklu Williama E. Deminga, tj. planowanie, wykonywanie, sprawdzanie, doskonalenie; W.J. Kittel, *Koncepcja pętli decyzyjnej Johna Richarda Boyda — „OODA Loop”*, „Kwartalnik Bellona” 2022, nr 4, s. 48–50.

⁶⁷ E. Luna, J. Calderón, P. Cataña, M. Ponce, *Advances in Technologies for the Soldiers of the Future*, „Revista Athenea” 2025, Vol. 6, Issue 20, s. 36–39; B. Denby, i inni, *Silent speech interfaces*, „Speech Communication” 2009, No. 52, s. 275–282; M. Wu, *Intelligent Warfare: Prospects of Military Development in the Age of AI*, New York 2022, s. 110–113.

⁶⁸ S. Paavola i inni, *Transformed knowledge work infrastructures in times of forced remote work*, „Information and Organization” 2025, No. 35, s. 2, 11–12.

⁶⁹ Zob. *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011*, →178

kładą nacisk na bezpieczeństwo całego łańcucha dostaw, budowę „odporności cyfrowej” i kształtowanie postaw cyberhigieny. W sposób holistyczny nakładają ramowe obowiązki w zakresie cyberbezpieczeństwa w kluczowych aspektach działalności przedsiębiorstw oraz instytucji, starając się wymusić działania niwelujące opisane powyżej problemy.

Niepomijalny jest także kryzys półprzewodników, do którego doszło podczas pandemicznej cyfryzacji. Wzrost popytu przy relatywnie niewielkiej możliwości zwiększenia podaży skutkował przeciążeniem możliwości produkcyjnych, w szczególności Tairwan Semiconductor Manufacturing Company (TSMC)⁷⁰. Poza skutkami ekonomicznymi, doprowadziło to do zmniejszenia przejrzystości pochodzenia komponentów oraz utrudnienia kontroli cyklu życia oprogramowania. Dla asymetrycznych aktorów było to okazją do ataków ukrytych, np. wykorzystania internetu rzeczy oraz oferowania tańszych alternatyw wobec braku renomowanych. Takie produkty, usługi i oprogramowanie narażyły użytkowników na złośliwe oprogramowanie, które wbudowywano w systemy prywatne i organizacyjne. Skutkiem był wzrost cyberataków w czasie pandemii⁷¹.

W utracie monopolu władzy nad informacją i utworzeniu nowego układu sił znaczenie mają również formaty krótkich treści, które prezentowane są użytkownikom przez algorytmy, a nie klasyczne wyszukiwanie. Obniżyło to bariery dotarcia do szerszego grona, w tym niszowych odbiorców, a przy tym rozproszyło metody skutecznej weryfikacji treści. Są to zatem warunki sprzyjające rozwojowi celowej dezinformacji, propagandy, fake newsów oraz innych form zafałszowywania informacji⁷². Platformy takie jak TikTok, czy moduły krótkich treści (np. YouTube Shorts, Instagram Reels) strukturalnie premiują ofensywę informacyjną i zaskoczenie narracyjne. Jednocześnie utrudniają każdorazową weryfikację materiałów przez użytkowników samym mechanizmem szybkiego angażowania i przełączania do kolejnego filmiku⁷³. W takim kontekście obrona opierająca się

Eur. Lex. PE/41/2022/INIT [DORA].

⁷⁰ W. Xiong, D.D. Wu, J.H.Y. Yeung, *Semiconductor supply chain resilience and disruption: insights, mitigation, and future directions*, „International Journal of Production Research” 2024, Vol. 63, No. 9, s. 3444–3445.

⁷¹ H. Albustanji, *COVID-19 Pandemic Impact on Cyber Threats*, [w:] *The impact of COVID-19 crisis on diverse democratic perspectives through gender perspective*, M. Pucelj (ed.), Novo Mesto 2024, s. 50–51, 55–57; S. Lindroos, A. Hakkala, S. Virtanen, *The COVID-19 pandemic and remote working did not improve WLAN security*, „Procedia Computer Science” 2022, No. 201, s. 159–160, 162–165; H.S. Lallie i inni, *Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic*, „Computers and Security” 2021, No. 105, s. 8–13.

⁷² H. Ren, *Network Warfare and Information Communication: the role and Challenge of New Media in the conflict in Ukraine*, „International Journal of Social Sciences and Economic Management” 2024, Vol. 5, Issue 2, s. 35–37.

⁷³ R. Romański, *Mechanisms of Disinformation Amplification in Hybrid Warfare: The Case of the Conflict in Ukraine*, „Bulletin of Carol I National Defence University” 2025, No. 2, s. 19–20, 27–29.

o działania *ex post*, tj. sprostowania, demaskowanie i rekontekstualizacje pozostają nie-skuteczne. Aktywna kontrofensywa wymaga głębszego zrozumienia algorytmów, odpowiednich sił, a przy tym może podburzyć zaufanie własnych obywateli do państwa podejmującego przedmiotowe działania. Z kolei skuteczność zupełnej kontroli nad takimi platformami jest raczej wątpliwa w zglobalizowanym środowisku. Łącznie przesuwają to nadzór nad przekazem coraz bardziej poza możliwości wielu państw, gdyż szczególnie platformy prezentujące krótkie treści umożliwiają narzucenie rytmu reakcji instytucjom, które działają wolniej i pod presją dowodową. Co więcej, problem ten dotyczyć będzie bardziej społeczeństw otwartych oraz demokracji, które mniej akceptują ingerencję państwową sferę informacyjną, niż podmioty autorytarne⁷⁴.

W konsekwencji rośnie znaczenie pomiaru i modulacji przepływów informacji (telemetria platform, wskaźniki zaangażowania) jako funkcji obronnej. Paradoks polega na tym, że te same metryki, które służą do optymalizacji komunikacji publicznej, są dźwignią dla przeciwnika. Pozwalają bowiem szybko iterować przekazy i unikać filtrów instytucjonalnych. To problem nie tylko polityczny, lecz przede wszystkim operacyjny: wzrost podatności na działania psychologiczne obniża jakość informacji wejściowych do procesów decyzyjnych i wydłuża pętlę OODA po stronie państwowej⁷⁵.

Niektóre wnioski formułowane po napaści Rosji na Ukrainę w 2022 roku wskazywały, że sztuka wojenna cofnęła się przed erą technologiczną i marzenia o cyfrowym żołnierzu⁷⁶. Choć podkreślić należy, iż inne dostrzegały konieczność oceny synergii oraz balansu między podejściem konwencjonalnym i opartym o nowoczesną technikę⁷⁷. Wkrótce zaczęto jednak zauważać, jak ogromne znaczenie mają wymiana informacji, rodzaj przekazu oraz nowoczesne środki, takie jak wykorzystanie na masową skalę dronów (w tym improwizowanych)⁷⁸. Od samego początku, równoległe do konfliktu kinetycznego, w przestrzeni cyfrowej toczyła się wojna informacyjna. Poza standardowymi jej celami, takimi jak dyskredytacja przeciwnika i podnoszenie morale, istotne stały się przekazy prosto z frontu, nagrania z kamer na mundurach, czy rozpowszechnianie konkretnego

⁷⁴ D. Finkelstein i inni, *Information manipulation on TikTok and its relation to American users' beliefs about China*, „Frontiers in Social Psychology” 2024, Vol. 2, s. 2, 14.

⁷⁵ A. Marjanović, D. Smiljanić, *Cognitive warfare—the human mind as the new battlefield*, „Proceedings of the Defence and Security Conference” 2025, Vol. 1, No. 1, s. 88–91, 99–100.

⁷⁶ S. Biddle, *Back in the Trenches: Why New Technology Hasn't Revolutionized Warfare in Ukraine*, „Foreign Affairs” 2023, No. 102, s. 153–156.

⁷⁷ Z. Śliwa, *The Synergy Between Technology and Soldiers in Warfare—The Russian Armed Forces Image During the War in Ukraine*, „Wiedza obronna”, t. 281, nr 4, s. 55–58.

⁷⁸ H. Bender, M. Kanderske, *Consumer Drone Warfare: Practices, Aesthetics and Discourses of Consumer Drones in the Russo-Ukrainian War*, [w:] *Drones in Society. New Visual Aesthetics*, E. Serafinelli (ed.), Cham 2024, s. 148–152.

przekazu wśród cywilów. Wymieniać tu można zarówno ostrzeżenia lub oddolne organizowanie obrony cywilnej, jak również wymienianie się metodami wytwarzania środków walki⁷⁹.

Wykorzystanie technologii w Ukrainie dowiodło (nie pierwszy raz), że taktyka pola walki jest kształtowana przez sprzężenie sensoryki (punktów zbioru informacji), zdolności dystrybucji informacji w polu elektromagnetycznym, ich przechwytywania oraz zagłuszania. Przewaga informacyjna polega na tym, by utrzymać fuzję danych oraz dystrybucję rozkazów, a więc zarządzać pasmami łączności, redundancją kanałów, czy samą architekturą przetwarzania danych. W ujęciu strategicznym oznacza to, że komercyjna infrastruktura łączności i rozpoznania staje się współzależną częścią prowadzenia działań. W tym kontekście znaczący okazał się udział systemu Starlink, który zapewnił skuteczną komunikację na polu walki i odegrał istotną rolę w obronności samej Ukrainy⁸⁰. W sposób szczególny dowiódł tego nieudany atak dronów na Krym, który jak się później okazało, wynikał z celowego wyłączenia infrastruktury na osobiste polecenie Elona Muska⁸¹. Sytuacja ta dowodzi jednak kolejnego problemu: próżni ze strony państw w technologii, decyzyjności lub innowacji, wypełnianej przez sektor prywatny. W konsekwencji dochodzi do utraty kontroli nad strategicznymi zasobami, co do których decyzje podejmowane są w silnie autorytarnej strukturze (hierarchii korporacyjnej). Tym bardziej przesuwają to możliwości decyzyjne poza aktorów państwowych, jednakże w zakresie o znacznie większym wpływie, niż przy poprzednio wskazanej utracie kontroli nad samą informacją.

Jednocześnie wyraźnie rośnie rola operacji pozostających poniżej progu wojny. Argument, że przyszłość cyberoperacji będzie w większym stopniu skryta i trudna do atrybucji, wynika z logiki zarządzania eskalacją: widoczne, przypisywalne ataki zwiększają ryzyko niekontrolowanej spirali, podczas gdy „ciche” zakłócenia infrastruktury, lub operacje eksfiltracji⁸² danych, mogą przynieść efekt operacyjny bez kosztów politycznych. To właśnie przestrzeń, w której niepaństwowi i sponsorowani pośrednio aktorzy dysponują największą dźwignią względem państw. Na szeroką skalę efekt ten wykorzy-

⁷⁹ K. Zarembko, J. Knodt, J. Kachel, *Smartphone resilience: ICT in Ukrainian civic response to the Russian full-scale invasion*, „Media, War & Conflict” 2025, Vol. 18, No. 3, s. 313–315, 319–320; T.O. Sithole, *The use of digital platforms by citizen aid actors during the Ukraine humanitarian crisis*, „Frontiers in Human Dynamics” 2024, Vol. 6, s. 3–4, 6–7.

⁸⁰ J. Abels, *Private infrastructure in geopolitical conflicts: the case of Starlink and the war in Ukraine*, „European Journal of International Relations” 2024, Vol. 30, No. 4, s. 852–854, 861.

⁸¹ G. Small, *The Rogue Private Company and National Defense Emergencies*, „Duke Journal of Constitutional Law & Public Policy” 2025, Vol. 20, s. 107–109.

⁸² Rozumianej jako kradzież informacji z systemów informatycznych przez złośliwe oprogramowanie (eksfiltracja automatyczna) i/lub podmiot (eksfiltracja manualna).

stują Chiny przez opłacane grupy przestępcze oraz (najprawdopodobniej) służby specjalne. Ich działania są przykładem systematycznego i długofalowego podejścia do eksfiltracji danych oraz infiltracji infrastruktury krytycznej. Podmioty te stosują zaawansowane techniki utrzymywania dostępu, takie jak modyfikacja list kontroli dostępu (ACL)⁸³, wykorzystanie niestandardowych portów, tunelowanie ruchu przez GRE/IPsec⁸⁴ czy uruchamianie poleceń w kontenerach Linux na urządzeniach sieciowych⁸⁵. Świadczy to o wysokim poziomie technicznego przygotowania i strategicznej cierpliwości aktorów sponzorowanych przez państwo. Co istotne, działania te są często trudne do wykrycia i przypisania, co dodatkowo wzmacnia ich użyteczność w kontekście zarządzania eskalacją.

W tym kontekście szczególnie niepokojące jest wykorzystywanie zaufanych połączeń między dostawcami usług telekomunikacyjnych oraz manipulowanie konfiguracjami urządzeń sieciowych w celu przechwytywania danych uwierzytelniających i ruchu sieciowego. Tego rodzaju operacje, choć technicznie złożone, umożliwiają pozostanie niewykrytym zwykle przez długi czas, w szczególności przez problem atrybucji. W efekcie, państwa demokratyczne stają przed wyzwaniem nie tylko technologicznym, ale również strategicznym: jak skutecznie przeciwdziałać działaniom, które formalnie nie naruszają zasad prawa międzynarodowego, lecz w praktyce podważają suwerenność cyfrową i zdolność do autonomicznego działania w przestrzeni informacyjnej.

Rywalizacja przesuwana się bowiem ku „cichemu” zarządzaniu informacją: standaryzacji detekcji anomalii w przepływach danych, odporności łańcuchów dostaw oprogramowania, a także koordynacji sojuszniczej mimo niepełnej atrybucji. Publikacja NATO wskazuje 2030 rok jako okres, w którym odporność informacyjna ekosystemów (łączyjących państwowe i komercyjne zasoby) stanie się główną determinantą przewagi⁸⁶. Wymusza to nowe mechanizmy współpracy publiczno-platformowej i zarządzania zależnościami krytycznymi⁸⁷. Bez tego przeciwnik może wykorzystywać technikę wymuszania

⁸³ Technika ta wykorzystuje dodanie adresów IP atakujących do Access Control List (ACL), co zezwala na ruch sieciowy z tych adresów i pozwala ominąć ustanowione polityki kontroli; NSA i inni, *Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System*, [U/OO/198904-25, PP-25-3703], 2025, s. 8.

⁸⁴ Wykorzystywane są tunele sieciowe takie jak Generic Routing Encapsulation (GRE), Multipoint GRE (mGRE) lub IPsec, które umożliwiają hermetyzację wielu protokołów warstwy sieciowej w jednym tunelu. Pozwala to tworzyć ukryte kanały transmisji danych, wtapiające się w normalny ruch sieciowy. Co więcej, niektóre z tych działań mogą pozwalać ukrywać adresy IP adwersarzy w logach, przez rejestrowanie ich lokalnymi adresami IP; tamże, s. 9.

⁸⁵ Operacje te pozwalają atakującemu na prowadzenie złośliwych działań bez wykrycia, ponieważ działania i dane w kontenerach nie są ściśle monitorowane; tamże, s. 9–10.

⁸⁶ J. Bellasio, E. Silfversten, *The Impact of New and Emerging Technologies on the Cyber Threat Landscape and Their Implications for NATO*, [w:] *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, A. Ertan, K. Floyd, P. Pernik, T. Stevens (eds.), Tallin 2020, s. 98–103.

⁸⁷ C. Whang, *Refocusing Export Control Regimes to Effectively Address Cyber Security* →182

nieproduktywnej eskalacji proceduralnej. Uderzenie w obszary mało istotne z punktu widzenia prowadzi do wszczęcia działań kryzysowych przez zaatakowanego, kierując tam zasoby (infrastrukturę, ludzi, oprogramowanie, finanse i czas) w sposób nieskoordynowany. Sytuacja taka skutkuje ogólnym chaosem po stronie podmiotów broniących się, co stwarza kolejne szanse ataku dla adversarza w obszary odsłonięte i pozbawione zasobów. Kluczowe zatem staje się sprzęgnięcie komunikacji publicznej z zarządzaniem informacją operacyjną: jasne progi reakcji, szybkie korygowanie dezinformacji i przejrzyste kryteria atrybucji⁸⁸, przy jednoczesnym utrzymaniu odporności infrastruktury na przerwę w ciągłości działania.

Należy jednak podkreślić zastrzeżenia co do tezy o coraz większej „skrytości” przyszłych cyberoperacji. O ile jest ona dobrze uargumentowana w literaturze strategicznej (ryzyko eskalacyjne, opłacalność cichych efektów), to opiera się głównie na studiach przypadków i dedukcji z teorii interakcji strategicznej. Wydaje się, że w przyszłości przydatne staną się szersze analizy porównawcze, których celem będzie odróżnienie trendów ogólnych od korelacji specyficznych dla wybranych obszarów działań. Wprawdzie rysujący się obraz cyberoperacji jest spójny, lecz niewykluczone, że brakuje jeszcze danych wejściowych. Wyróżnić tu należy stosunkowo nową sztuczną inteligencję oraz dopiero tworzący się wpływ na pole walki czy działania w cyberprzestrzeni: wojska, służb specjalnych oraz szeroko rozumianego sektora publicznego i prywatnego.

Co więcej, obserwując przesunięcie sprawczości z platform kinetycznych na przepływy danych i ekologie platform, rzeczywisty wpływ asymetrycznych aktorów pozapaństwowych wciąż pozostaje przedmiotem dyskusji. Ten sam problem atrybucji, który daje im przewagę, nie pozwala jednoznacznie stwierdzić, czy dane grupy przestępcze nie są sponsorowane przez państwo, lub nie stanowią fasady dla działań służb specjalnych. Choć analiza źródeł i obserwacje empiryczne, w tym w przedstawionym powyżej zakresie, raczej potwierdzają aktywność przestępczą, to zasadnym wydaje się wskazanie tej luki (tak aby nie ekstrapolować wniosków w sposób nadmierny).

Finalnie zaobserwować można, że nowy układ sił w cyberprzestrzeni opiera się na przewadze obliczeniowej, projektowaniu odpornej architektury danych, jak również zdolności do skrytego zarządzania przepływami informacji w złożonych ekosystemach publiczno-prywatnych. Asymetryczni aktorzy wykorzystują algorytmiczną selekcję uwagi, niepewność atrybucji i rozproszone łańcuchy dostaw informacji, by wymuszać na

Concerns, [w:] *Cyber Threats and NATO 2030...*, s. 227–228.

⁸⁸ L.B. Weissinger, *The Challenge of Networked Complexity to NATO's Digital Security*, [w:] *Cyber Threats and NATO 2030...*, s. 241–245.

państwach kosztowne reakcje i degradować ich pętle decyzyjne. Odpowiedzią nie może być powrót do centralnego monopolu informacyjnego, lecz budowa odporności ekosystemowej, standardów interoperacyjności i zdolności „cichej” projekcji efektów w cyberprzestrzeni, tak by przywrócić przewagę w tempie i jakości decyzji.

4.2 Konsekwencje dla bezpieczeństwa międzynarodowego — konflikty w epoce cyfrowej

Cyberprzestrzeń okazała się środowiskiem, w którym granica między pokojem oraz wojną zaciera się, a działania poniżej progu otwartego konfliktu prowadzone są permanentnie. Kreuje to potrzebę nowego spojrzenia na bezpieczeństwo: nie tylko w kategoriach siły militarnej, ale także odporności systemów informacyjnych, komunikacyjnych i infrastrukturalnych. Dzieje się to przy równoczesnym rozproszeniu odpowiedzialności za bezpieczeństwo. Ta tradycyjnie spoczywała na państwach i siłach zbrojnych, a obecnie kluczowe zasoby (łączność satelitarna, chmury obliczeniowe czy platformy społecznościowe) pozostają w gestii sektora prywatnego.

Znaczenie środowiska sieciocentrycznego rośnie również w wymiarze rozwoju technologicznego. Sztuczna inteligencja i automatyzacja wspierają obronę systemów, lecz jednocześnie umożliwiają ofensywne operacje na niespotykaną dotąd skalę: od masowej produkcji treści dezinformacyjnych po precyzyjne ataki w cyberprzestrzeni⁸⁹. W tym kontekście szczególnego znaczenia nabiera infrastruktura krytyczna. Atak na systemy energetyczne, finansowe czy transportowe może sparaliżować państwo bez konieczności użycia tradycyjnych sił zbrojnych. Przykłady ostatnich lat dowodzą, że takie działania są efektywne właśnie dlatego, że wywołują chaos gospodarczy i polityczny, wciąż nie przekraczając progu wojny⁹⁰. To powoduje, że cyberprzestrzeń staje się obszarem, w którym najtrudniej zarządzać eskalacją: brak jednoznacznej atrybucji utrudnia reakcję, a jednocześnie brak odpowiedzi ośmiela przeciwnika do dalszych działań.

Konsekwencje dla bezpieczeństwa międzynarodowego mają zatem kilka wymiarów. Po pierwsze, normatywny: prawo międzynarodowe oraz zobowiązania sojusznicze muszą dostosować się do realiów operacji cyfrowych. Po drugie, instytucjonalny: Unia Europejska i NATO redefiniują swoją rolę w kontekście wspólnej obrony przed zagrożeniami w sieci. Po trzecie, operacyjny: współpraca państw i sektora prywatnego staje się

⁸⁹ E. Pauwels, *Preparing for next-generation information warfare with generative AI*, „CIGI Papers” 2024, No. 310, s. 8–11.

⁹⁰ K. Tsantikidou, N. Sklavos, *Threats, Attacks, and Cryptography Frameworks of Cybersecurity in Critical Infrastructures*, „Cryptography” 2024, Vol. 8, No. 7, s. 4–5, 14–17.

koniecznością. Po czwarte, technologiczny: sztuczna inteligencja, automatyzacja i ekosystemowe zależności tworzą nowe pola ryzyka oraz potencjalnej przewagi. Zarysowane w ten sposób procesy ukazują, iż konflikt w epoce cyfrowej nie jest zjawiskiem wyłącznie technologicznym, lecz wymaga szerszego ujęcia prawnego, politycznego i strategicznego.

4.2.1. Wyzwania dla prawa międzynarodowego i NATO

Cyberprzestrzeń jako nowy wymiar rywalizacji strategicznej stawia poważne wyzwania zarówno dla prawa międzynarodowego, jak również dla struktur bezpieczeństwa zbiorowego (takich jak NATO). Kluczowy problem wynika z faktu, że zatarciu uległy tradycyjne kategorie wojny i pokoju, agresji oraz samoobrony, czy też konfliktu zbrojnego i działań poniżej progu wojny. W cyberprzestrzeni trudno bowiem zdefiniować, kiedy incydent staje się aktem agresji, kto jest sprawcą i jaką reakcję można uznać za proporcjonalną. Brak jednoznacznych norm prawnych powoduje, że każde zdarzenie staje się przedmiotem interpretacji, co osłabia zdolność państw i sojuszy do wspólnej reakcji.

Dobitnym przykładem tego problemu był cyberatak na Estonię w 2007 roku, powszechnie uznawany za jeden z pierwszych przypadków cyberoperacji o charakterze politycznym na dużą skalę⁹¹. Paraliż administracji publicznej i sektora bankowego w Tallinie wywołał poważny kryzys wewnętrzny, jednak żaden z sojuszników NATO nie zdecydował się na uznanie incydentu za atak zbrojny w rozumieniu art. 5 Traktatu Waszyngtońskiego. Brak jednoznacznej atrybucji sprawił, że reakcja ograniczyła się do wsparcia technicznego i politycznego, bez uruchomienia mechanizmów obrony zbiorowej⁹². Warto jednak zaznaczyć, iż wiele wskazywało na rosyjskie zaangażowanie w działania hakerów, m.in. przez zawieszenie części handlu z Estonią i odmówienie współpracy w śledztwie Tallina ws. ataków⁹³. Wydarzenie to obnażyło fundamentalny problem: cyberatak o poważnych skutkach może nie spełniać formalnych kryteriów agresji zbrojnej, a brak normatywnej jasności prowadzi do fragmentarycznych i spóźnionych reakcji.

Podobne trudności ujawniły się w 2010 roku, kiedy irański program nuklearny został zaatakowany złośliwym oprogramowaniem Stuxnet. Operacja ta była technicznie przełomowa. W skuteczny sposób zakłóciła pracę wirówek w Natanz i opóźniła rozwój potencjału nuklearnego Iranu, czyniąc to w sposób wówczas niespotykany, przede

⁹¹ S. Herzog, *Ten Years after the Estonian Cyberattacks. Defense and Adaptation in the Age of Digital Insecurity*, „Georgetown Journal of International Affairs”, 2017, Vol. 18, No. 3, 73–74.

⁹² W. Goodman, *Cyber Deterrence: Tougher in Theory than in Practice?*, „Strategic Studies Quarterly” 2010, Vol. 4, No. 3, s. 110.

⁹³ M. Terlikowski, *Cyber attacks on Estonia. Implications for International and Polish Security*, „Polish Quarterly of International Affairs” 2007, Vol. 16, No. 3, s. 71.

wszystkim pod kątem zaawansowania⁹⁴. W efekcie Stuxnet okrzyknięto pierwszą cyberbronią, choć należy podkreślić, że jego skutki były raczej ograniczone i pozbawione długofalowego wpływu. Dlatego o ile zdaje się, iż rzeczywiście rozpoczął on erę cyberbroni, to był zarazem bardzo wczesnym jej etapem. Najistotniejsze jednak pozostają implikacje: żadne państwo nie przyznało się do autorstwa⁹⁵, a społeczność międzynarodowa nie potrafiła uzgodnić, czy atak tego rodzaju można uznać za użycie siły w świetle Karty Narodów Zjednoczonych⁹⁶. Brak reakcji ze strony ONZ czy NATO pokazał, że prawo międzynarodowe pozostaje w tyle wobec innowacyjnych metod działań. De facto zaakceptowano nową formę operacji ofensywnej, co w dłuższej perspektywie otworzyło drogę do militaryzacji cyberprzestrzeni.

Wątpliwości narastają także wokół kwestii proporcjonalności i odpowiedzi. Cyberatak na sieć energetyczną Ukrainy w 2015 roku⁹⁷, przypisywany grupie Sandworm powiązanej z rosyjskim wywiadem⁹⁸, pozbawił prądu setek tysięcy osób w środku zimy. Z punktu widzenia prawa humanitarnego był to incydent uderzający w ludność cywilną, a więc wprost naruszający podstawowe zasady prawa konfliktów zbrojnych. Problem polega jednak na tym, że w przypadku braku ofiar śmiertelnych i trudnej atrybucji, reakcja środowiska międzynarodowego ograniczyła się do potępienia i sankcji (głównie przeciwko poszczególnym oficerom GRU i członkom Sandworm⁹⁹).

Problem odpowiedzialności państw przy rozmytej atrybucji pozostaje nierozwiązany do dziś. Ukazują to cyberincydenty wywoływane przez takie grupy jak przytaczane APT28 (znane jako Fancy Bear, Rosja)¹⁰⁰, czy Grupa Lazarus (Korea Północna)¹⁰¹. Do-

⁹⁴ R. Bania, *Wojny w cyberprzestrzeni — przypadek Iranu* [w:] *Bezpieczeństwo narodowe i międzynarodowe w regionie Bliskiego Wschodu i Północnej Afryki (MENA) u progu XXI wieku*, R. Bania, K. Zdulski (red.), Łódź 2012, s. 195.

⁹⁵ C. Stevens, *Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet*, „Contemporary Security Policy” 2020, Vol. 41, No. 1, s. 143.

⁹⁶ J.P. Farwell, R. Rohozinski, *Stuxnet and the Future of Cyber War*, „Survival: Global Politics and Strategy” 2011, Vol. 53, No. 1, s. 32–36.

⁹⁷ R.M. Lee, M.J. Assante, T. Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, Washington 2016, s. 4–6.

⁹⁸ Działalność grupy Sandworm jest wiązana z Jednostką 26165 Głównego Zarządu Wywiadowczego Federacji Rosyjskiej (podobnie jak Fancy Bear), która specjalizuje się w uderzeniach przeciwko infrastrukturze innych państw; C. Melella, F. Ferazza, K. Mersinas, *Disjointed Cyber Warfare: Internal Conflicts among Russian Intelligence Agencies*, „ACIG” 2024, Vol. 4, No. 2, s. 16; NSA i inni, *Russian GRU Targeting Western Logistics Entities and Technology Companies*, [U/OO/157019-25, PP-25-2107], 2025, s. 3–5.

⁹⁹ *Rozporządzenie Wykonawcze Rady (UE) 2020/1125 z dnia 30 lipca 2020 r. wykonujące rozporządzenie (UE) 2019/796 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim*, Eur. Lex. L 246/4, s. 6.

¹⁰⁰ Patrz: przypis dotyczący Sandworm.

¹⁰¹ Grupa aktywna od 2009 roku i odpowiadająca m.in. za atak na Sony Pictures Entertainment w 2014 roku oraz nielegalną eksfiltrację danych dotyczących programów nuklearnych; CNMF i inni, →186

wodzą one, że choć w operacjach w cyberprzestrzeni na dużą skalę wykorzystuje się liczne podmioty pozostające co najmniej pod wpływem państw, to nie sposób wykazać dokładne powiązania i związki przyczynowe, finansowe, organizacyjne lub osobowe. Również samo przypisanie ataków do grup jest trudne, zwłaszcza w przypadku aktorów z Korei Północnej, gdzie choćby atrybucja Lazaurus pokrywa się z innymi adwersarzami¹⁰². W praktyce blokuje to skuteczne wykorzystanie mechanizmów prawa międzynarodowego. NATO próbowało odpowiedzieć na ten problem, deklarując na szczycie w Warszawie (2016), że cyberprzestrzeń jest nową domeną operacyjną Sojuszu¹⁰³. Jednak brak wypracowanych procedur i kryteriów uznania ataku cyfrowego za równoważny militarnemu, ograniczyły znaczenie tego zobowiązania w sensie praktycznym.

Z punktu widzenia NATO kluczowym wyzwaniem jest również eskalacja i odstraszanie, czego przykład stanowi incydent Colonial Pipeline (2021 — patrz: rozdział II). Pokazał on, że ataki na infrastrukturę krytyczną mogą prowadzić do realnych skutków gospodarczych i społecznych, nawet jeśli nie są prowadzone bezpośrednio przez państwo. Choć administracja USA jednoznacznie wskazała na grupę DarkSide jako sprawcę, jej powiązania z rosyjską przestrzenią cyberprzestępczą wywołały pytania o granice odpowiedzialności Moskwy. NATO znalazło się tu w impasie: czy incydent wywołany przez „prywatnych” aktorów, działających w państwie trzecim, ale tolerowanych przez jego władze, może być potraktowany jako atak na sojusznika? Brak jednoznacznej odpowiedzi osłabia wiarygodność odstraszania, gdyż potencjalny agresor może liczyć na to, że spór o kwalifikację prawną opóźni lub uniemożliwi adekwatną reakcję.

Dopełnieniem tego obrazu jest problem „szarej strefy” działań poniżej progu wojny. Kampanie dezinformacyjne i ingerencje w procesy wyborcze nie wpisują się w klasyczne definicje agresji. Jako przykład takowych wskazać można działania grupy Ghostwriter wobec Niemiec i Łotwy (omówione w rozdziale II), czy operacje wpływu podczas wyborów w USA w 2016 roku¹⁰⁴. Ich skutki polityczne są daleko idące: podważają legitymację instytucji demokratycznych i zdolność państw do podejmowania decyzji strategicznych. Brak jasnych norm prawnych powoduje, że reakcja sojuszników ogranicza się

North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs, [AA24-207A], 2024, s. 26.

¹⁰² W efekcie niektórzy autorzy stosują Lazaurus jako wspólne określenie dla klastrow grup z Korei Północnej (takich jak BeagleBoyz, Bluenoroff, Andariel); A. Gulyás, „Lazarus” *The North Korean Hacker Group*, [w:] *Proceedings of the International Scientific Conference Strategies XXI. The Complex And Dynamic Nature of The Security Environment*, F. Cîrciumaru, C.C. Ioniță (eds.), Bucharest 2021, s. 75, 77.

¹⁰³ J. Shea, *How is NATO Meeting the Challenge of Cyberspace?*, „PRISM” 2017, Vol. 7, No. 2, s. 22.

¹⁰⁴ K. Nalewaj, *Rosyjska ingerencja w wybory prezydenckie w USA w 2016 r.*, „Com.press” 2024, nr 1, s. 91–95.

do działań defensywnych i sankcji dyplomatycznych, które nie zawsze są skuteczne w powstrzymaniu długofalowych operacji wpływu.

Przedstawione powyżej wyzwania epoki cyfrowej — dla prawa międzynarodowego i NATO — można ująć w kilku wymiarach:

- a) brak definicji cyberataku i progów eskalacyjnych utrudnia wykorzystanie istniejących mechanizmów prawnych;
- b) problem atrybucji osłabia możliwość przypisania odpowiedzialności państwom i stosowania zasady samoobrony;
- c) wzrost roli podmiotów pozapaństwowych stawia pytanie o zakres odpowiedzialności państwa-gospodarza;
- d) działania poniżej progu wojny podważają stabilność polityczną i społeczną, pozostając poza regulacją prawa humanitarnego.

Choć NATO dostrzegło wagę problemu, to wciąż zмага się z niedopasowaniem swoich struktur do dynamiki cyberprzestrzeni. Jednakże impas pozwala przeciwnikom na wykorzystanie efektu przewagi atakującego. Jak wskazywano w poprzednich rozdziałach, cyberprzestrzeń premiuje działania agresorów, którzy często mogą próbować „do skutku” bez szczególnych konsekwencji. Z kolei jeden błąd broniącego się może przynieść dotkliwe reperkusje. W efekcie obserwujemy coraz częstsze ataki w cyberprzestrzeni skierowane m.in. przeciwko zachodnim demokracjom, w szczególności na infrastrukturę krytyczną¹⁰⁵. Dlatego ostatecznie można stwierdzić, że prawo międzynarodowe i mechanizmy sojusznicze stoją przed istotnym dylematem: jak dostosować się do konfliktu, w którym tradycyjne kategorie „wojny” i „pokoju” tracą ostrość, a działania przeciwnika są trudne do wykrycia, przypisania i zakwalifikowania. Wyzwanie to nie dotyczy wyłącznie kwestii technicznych, lecz fundamentalnie podważa dotychczasowe rozumienie suwerenności, odpowiedzialności państw i kolektywnej obrony. Dopóki nie zostaną wypracowane nowe normy i mechanizmy reakcji, cyberprzestrzeń pozostanie obszarem, w którym przewagę mają ci, którzy potrafią najlepiej wykorzystać lukę między prawem a praktyką. To z kolei zdaje się premiować autorytaryzmy.

¹⁰⁵ M. Ojdana-Kościuszko, *Ewolucja i wyzwania polskiego systemu cyberbezpieczeństwa*, „De Securitate et Defensione” 2024, nr 1, s. 133; O.O. Val i inni, *Strengthening Cybersecurity Measures for the Defense of Critical Infrastructure in the United States*, „Asian Journal of Research in Computer Science” 2024, Vol. 17, No. 11, s. 27, 30.

4.2.2. Znaczenie sektora prywatnego w budowie bezpieczeństwa międzynarodowego

Współpraca między sektorem państwowym i prywatnym stała się kluczowym elementem zapewnienia bezpieczeństwa w cyfrowej epoce. W obliczu rosnącej integracji infrastruktury krytycznej i usług cyfrowych należących do podmiotów prywatnych, państwa nie mogą dłużej polegać wyłącznie na własnych zasobach. Jednakże zaangażowanie firm technologicznych, operatorów telekomunikacyjnych i dostawców rozwiązań IT w mechanizmy obrony, reagowania i rekonfiguracji systemów, stawia zupełnie nowe wyzwania. Przytoczony wcześniej przykład wyłączenia Starlink nad Ukrainą w kluczowym momencie operacji poddaje w wątpliwość dotychczasowe podejście do racjonalności podmiotów międzynarodowych¹⁰⁶. W sytuacji, gdy korporacja o globalnym zasięgu ma tak duży wpływ na działalność państw, to wydaje się słusznym by uznać ją za jednego z aktorów relacji międzynarodowych — nawet mimo sprzeciwu definicyjnego czy teoretycznego ze strony badaczy¹⁰⁷. Choć formalnie korporacje te podległe są państwom, to zasięg skutków ich wpływu przekracza granice postrzegania ich jako „niższego poziomu” (od struktur władzy). Dodatkowo uzasadnia to sposób zaangażowania sektora prywatnego w politykę, czego najjaskrawszym przykładem są wybory w USA z 2024 roku i udział Elona Muska. Zarazem sektor ten wnosi istotne szanse dla państw, zarówno pod kątem zdywersyfikowania możliwości obronnych i ofensywnych, jak również indukowania rozwoju technologicznego.

Istotnym jest przytoczenie przykładu dzielenia się wiedzą o zagrożeniach oraz wspólnych działaniach w ramach inicjatywy Cybersecurity Tech Accord, do której dołączyły Microsoft, Cisco, IBM i inne firmy technologiczne. Ich rola w analizie incydentów, ostrzeganiu przed zagrożeniami oraz szybkim udostępnianiu środków naprawczych znacząco zwiększa skalę i jakość reakcji na cyberataki. Wartym wyróżnienia jest tutaj „termometr cyberbezpieczeństwa” — metodologia oceny stanu środowiska sieciocentrycznego. Zakłada ona trzy poziomy:

- a) cyber-stabilności (poniżej 0°) — niewielka liczba państwowych cyberoperacji, ograniczone zagrożenia ze strony innych aktorów;
- b) cyber-konfliktu (od 0° do 99°) — nieodpowiedzialne cyberoperacje państw, regularne zagrożenia ze strony innych aktorów, negatywny wpływ na dyplomację;

¹⁰⁶ C.H. Achen, *Realism and Rationality*, „Critical Review” 2024, Vol. 35, No. 4, s. 545–546.

¹⁰⁷ M. Babic, J. Fichtner, E.M. Heemskerk, *States versus Corporations: Rethinking the Power of Business in International Politics*, „The International Spectator” 2017, Vol. 52, No. 4, 28–31, 39–40.

- c) cyber-wojny (powyżej 100°) — użycie cyberoperacji w sprzeczności z prawem międzynarodowym i przyjętymi normami, nieskuteczne odstraszanie¹⁰⁸.

W 2023 roku wskazanie termometru wyniosło 100°, a w 2024 i 2025 101°¹⁰⁹. Choć wyniki tych analiz są raczej przeglądem, aniżeli pogłębioną diagnozą cyberprzestrzeni, to wciąż mogą stanowić ważne źródło informacji w zakresie uświadamiania podmiotów i budowy współpracy. Jej efektem jest wytworzenie oraz dystrybuowanie materiałów mających na celu zwiększenie poziomu bezpieczeństwa w środowisku sieciocentrycznym, czy proaktywne działania w procesach ustawodawczych. W tym zakresie ocena skali wpływu Cybersecurity Tech Accord na faktyczne działania polityków ma znaczenie drugorzędne. Zgromadzenie wśród sygnatariuszy największych firm technologicznych i aktywne publikowanie jest przykładem skutecznej, oddolnej inicjatywy, która może wesprzeć działania państwa w budowaniu bezpiecznej przestrzeni cyfrowej¹¹⁰.

Za równie interesujący uznać należy przykład współpracy w ramach NATO — inicjatywy Cyber Defence Pledge, którą ustanowiono podczas szczytu w Warszawie w 2016 roku¹¹¹. W jej ramach zachęca się członków sojuszu do współpracy z sektorem prywatnym w zakresie ochrony infrastruktury współdzielonej — np. platform chmurowych, systemów satelitarnych czy centrów danych. Taki model współdziałania umożliwia integrację zdolności analitycznych firm z procesem decyzyjnym Sojuszu. Jej mocną stroną jest przede wszystkim formalizacja zobowiązań politycznych i operacyjnych, które skłaniają państwa do inwestycji w infrastrukturę, szkolenia oraz zdolności reagowania na incydenty. Wprowadzenie siedmiu bazowych wymogów odporności oraz utworzenie struktur takich jak NATO Cyber Operations Centre czy Rapid Reaction Teams świadczy o rosnącej instytucjonalizacji cyberbezpieczeństwa w ramach Sojuszu¹¹². Jednakże słabością Cyber Defence Pledge jest brak mechanizmów egzekwowania zobowiązań oraz asymetria zdolności między państwami członkowskimi, co prowadzi do nierównomiernego wdrażania postanowień. Ponadto problemem pozostaje niejednoznaczność w zakresie stosowania artykułu 5 w kontekście cyberataków¹¹³, co — jak wskazano wcześniej — osłabia potencjał odstraszania. Dlatego inicjatywa ta, choć ambitna, wymaga dalszej konsoli-

¹⁰⁸ CTA, *Year 7 Report*, [b.m.w.] 2025, s. 5;

¹⁰⁹ Tamże, s. 3–4.

¹¹⁰ Y. Cho, J. Chung, *Bring the State Back In: Conflict and Cooperation Among States in Cybersecurity*, „Pacific Focus” 2017, Vol. 32, No. 2, s. 293.

¹¹¹ *Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016*, [PR (2016) 100], 2016, art. 71, s. 15–16.

¹¹² R.J. Atkinson, *NATO Cyber Defence, 2000-2022*, Londyn (Canada) 2023, s. 117, 156.

¹¹³ Tamże, s. 134–137.

dacji politycznej i operacyjnej, tak aby mogła skutecznie odpowiadać na dynamicznie ewoluujące zagrożenia w cyberprzestrzeni.

Warto przy tym wspomnieć dyrektywę NISz (omówioną w rozdziale II), której celem jest integracja i koordynowanie działań poprawiających poziom cyberbezpieczeństwa między podmiotami publicznymi i prywatnymi. W tym kontekście wyróżnić należy zamiar systemowego zwiększania bezpieczeństwa m.in. przez koncept zachowania cyberhigieny. Rozumieć przez nią należy zespół dobrych nawyków, postaw, praktyk i świadomości, które nie wymagają specjalistycznej wiedzy, lecz pozwalają skuteczniej reagować na zagrożenia przez pracę oddolną¹¹⁴. Dotychczasowe badania wskazują na istotną rolę cyberhigieny w budowaniu krajobrazu cyberbezpieczeństwa¹¹⁵ — tak państwa, jak i wspólnoty UE. Wynika to z faktu, iż postrzeganie cyberbezpieczeństwa jako zabezpieczeń technicznych oraz architektury systemów jest obrazem połowicznym. Za równie istotny należy uznać czynnik ludzki, z punktu ściśle cyberprzestrzeni: jako najsłabsze ogniwo, a z punktu widzenia państwa: jako cel obcych działań informacyjnych. Brak spójnych ram edukacyjnych, kreowania cyfrowej „obrony cywilnej” oraz skutecznych kampanii społecznych łącznie sprawiają, że przeniesienie odpowiedzialności za wdrażanie cyberhigieny na sektor prywatny było kluczowe. Z kolei NISz ustanawia kluczowe ramy dla centralnego zarządzania tym procesem. Niezależnie od ogólnej oceny skuteczności tej dyrektywy, na którą czekać trzeba będzie jeszcze lata, jako jej zdecydowanie pozytywny aspekt należy wskazać przełom w sposobie myślenia o cyberbezpieczeństwie, na miarę zmiany w postrzeganiu prywatności, który zapewniło RODO.

Co więcej, współpraca publiczno-prywatna staje się tym bardziej konieczna, że coraz trudniej oddzielić odpowiedzialność państwa od działalności firm. Cyberprzestrzeń to środowisko współdzielone. Atak na dostawcę chmurowego, platformę komunikacyjną albo usługę satelitarną może mieć skutki równie poważne jak atak na państwową infrastrukturę¹¹⁶. Przykłady współpracy międzysektorowej dowodzą otwarcia dostępu do zasobów i kompetencji, których państwo samo nie posiada, lub dysponuje ich zbyt ograniczoną liczbą. Firmy dostarczają eksperckie zespoły incident response, mechanizmy

¹¹⁴ ENISA, *Technical Impelentation Guidance On Commission Implementing Regulation (EU) 2024/2690 laying down rules for the application of NIS2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures*, Luxembourg 2025, s. 111–113.

¹¹⁵ A. Vishwanath i inni, *Cyber hygiene: The concept, its measure, and its initial tests*, „Decision Support Systems” 2020, No. 128, s. 111–113; A. Fikry, *Defining the Beauty of Cyber Hygiene: A Retrospective Look*, „Engineering Management Review” 2024, Vol. 52, Issue 2, s. 175–177.

¹¹⁶ O. Bures, *Contributions of Private Businesses to the Provision of Security in the EU: Beyond Public-Private Partnerships*, [w:] *Security Privatization How Non-security-related Private Businesses Shape Security Governance*, O. Bures, H. Carrapicio (eds.), [b.m.w.] 2018, s. 23–25, 28–29, 34–37.

threat intelligence i narzędzia automatyzacji¹¹⁷. Dzięki temu odporność operacyjna wzrasta, a państwo może reagować skuteczniej, przede wszystkim za sprawą koordynacji działań, np. z użyciem zespołów CSIRT. Jednak istnieje też niebezpieczeństwo: gdy sektor prywatny przejmuje zbyt wiele kluczowych funkcji, państwa stają się podatne na decyzje korporacyjne. Stąd istotne pozostaje utrzymanie zdolności państwowych do zapewnienia alternatywnej łączności i kontroli.

4.2.3. Rosnąca rola sztucznej inteligencji oraz automatyzacji w atakach

Choć odporność państw w cyberprzestrzeni w coraz większym stopniu zależy od współpracy z sektorem prywatnym, to dynamika środowiska cyfrowego nie sprowadza się jedynie do kwestii podziału odpowiedzialności. Równie istotnym zjawiskiem, które w ostatniej dekadzie przybrało na sile, jest rosnące wykorzystanie AI oraz automatyzacji w planowaniu i przeprowadzaniu ataków. Pozwala to na przełamywanie dotychczasowych ograniczeń skali i szybkości działań, przy jednoczesnym otwarciu nowej sfery dzięki AI — zdolności do adaptacji w czasie rzeczywistym i autonomicznego wyszukiwania słabości. W konsekwencji, obrona oparta na tradycyjnych modelach reakcji staje się coraz mniej wystarczająca.

Pierwszym wymownym przykładem były kampanie phishingowe, które z prymitywnych, masowych wiadomości ewoluowały do wysoce spersonalizowanych komunikatów, generowanych przez modele językowe. Badania IBM wskazują w tym kontekście, że użycie systemów AI pozwala na automatyczne profilowanie ofiar, analizę ich obecności w mediach społecznościowych oraz tworzenie treści pozornie wiarygodnych¹¹⁸. Daje to przewagę asymetrycznym aktorom, którzy bez dużych zasobów mogą przeprowadzać złożone ataki, trudne do odróżnienia od autentycznej komunikacji. Oznacza to, że klasyczne metody detekcji — filtrowanie słów kluczowych czy analiza adresów IP — tracą skuteczność¹¹⁹.

¹¹⁷ A. Calcara, R. Marchetti, *State-industry relations and cybersecurity governance in Europe*, „Review of International Political Economy” 2021, Vol. 29, No. 4, s. 1239–1249.

¹¹⁸ C. Singleton i inni, *X-Force Threat Intelligence Index 2021*, Armonk 2021, s. 3, 6.

¹¹⁹ Q. Qi, Z. Wang, Y. Xu, Y. Fang, C. Wang, *Enhancing Phishing Email Detection through Ensemble Learning and Undersampling*, „Applied Sciences” 2023, No. 13, s. 3–5; S.K. Birthriya, P. Ahlawat, A.K. Jain, *Detection and prevention of spear phishing attacks: A comprehensive survey*, „Computers & Security” 2025, No. 151, s. 5–6.

Warto również wskazać na ataki wykorzystujące bibliotekę Log4j¹²⁰, gdzie skala i szybkość wykrywania nowych wektorów ataku nie byłaby możliwa bez narzędzi opartych na uczeniu maszynowym. Atakujący używali botnetów zdolnych do automatycznego skanowania internetu w poszukiwaniu podatnych systemów i natychmiastowego wdrażania exploitów¹²¹. Agencje rządowe podkreślały, że w ciągu kilku dni od ujawnienia podatności, miliony systemów zostały zagrożone, a sama reakcja obronna musiała zostać zautomatyzowana, aby nadążyć za tempem działań przeciwnika¹²². Co więcej, badania NATO CCDCOE (2020) wskazują, że zdolność botnetów do rekonfiguracji w oparciu o dane środowiskowe, a nawet do omijania systemów detekcji, stanowi nową jakość zagrożenia¹²³. Wnioskiem płynącym z tego przypadku jest to, że automatyzacja nie jest już jedynie przewagą napastnika — staje się koniecznością także po stronie broniącej się. Od tamtej pory potencjał AI w zakresie ataków na systemy i infrastrukturę krytyczną tylko się rozwinął, czego dowodzi ransomware PromptLock. To złośliwe oprogramowanie wykorzystuje uczenie maszynowe do analizy komputera ofiary i wygenerowanie zindywidualizowanych skryptów, na podstawie których przeprowadzany jest atak¹²⁴. Głównym wyzwaniem jest tutaj brak wskaźników ataku (IoC — ang. Indicators of Compromise), czyli śladów lub artefaktów wskazujących na potencjalne naruszenie bezpieczeństwa systemu lub sieci. Wykorzystywane przez oprogramowanie monitorujące i reagujące na zdarzenia (SIEM, EDR, XDR) do wykrywania złośliwej działalności, wskaźniki te stają się przynajmniej częściowo nieprzydatne w przypadku PromptLock. Sam moment ataku może bowiem skutkować każdorazowo innym efektem, co znacząco utrudnia śledzenie uniwersalnych identyfikatorów dla przedmiotowego zagrożenia.

Rosnącą rolę odgrywa także zastosowanie AI w kampaniach deepfake, które coraz częściej wykorzystywane są jako narzędzie operacji informacyjnych. Nagrania generowa-

¹²⁰ Log4j — otwartoźródłowa biblioteka programistyczna, opracowana w języku Java, służąca do rejestrowania zdarzeń (logowania) w aplikacjach. Umożliwia elastyczne zarządzanie komunikatami diagnostycznymi i błędami poprzez konfigurację poziomów logowania, formatów oraz miejsc docelowych zapisu (np. pliki, konsola, serwery zdalne). Dzięki modularnej architekturze i możliwości konfiguracji zewnętrznej, Log4j jest szeroko stosowany w systemach produkcyjnych oraz korporacyjnych; R. Hiesgen, M. Nawrocki, T.C. Schmidt, M. Wählisch, *The Log4j Incident: A Comprehensive Measurement Study of a Critical Vulnerability*, „Transactions on Network and Service Management” 2024, Vol. 21, No. 6, s. 5921–5922.

¹²¹ J. Khoury, M.S. Pour, E. Bou-Harb, *A Near Real-Time Scheme for Collecting and Analyzing IoT Malware Artifacts at Scale*, [w:] *Proceedings of the 17th International Conference on Availability, Reliability and Security*, D. Engel, M. Fischer (eds.), Vienna 2022, s. 4–5.

¹²² CISA i inni, *Mitigating Log4Shell and Other Log4j-Related Vulnerabilities*, [AA21-356A], 2021, s. 1–2.

¹²³ M. Kuzlu, C. Fair, O. Guler, *Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity*, „Discover” 2021, Vol. 1, s. 5–7, 11.

¹²⁴ Zob. ThaiCERT, *“PromptLock”: First-Ever Ransomware Leveraging AI for File Encryption Discovered*, [311/68] 2025.

ne algorytmicznie były już wykorzystywane w kampaniach dezinformacyjnych w Europie Środkowo-Wschodniej, m.in. w celu podważania zaufania do instytucji rządowych¹²⁵. Europol ostrzegał, że w połączeniu z kampaniami automatycznego rozpowszechniania, deepfake mogą destabilizować procesy polityczne szybciej, niż jest możliwe ich zweryfikowanie¹²⁶. W tym kontekście problem nie dotyczy tylko cyberprzestrzeni w wąskim sensie, lecz szerzej: odporności społecznej i politycznej państw. Pozwala to bowiem kształtować odbiór wykorzystania AI w ofensywnych operacjach wojskowych, przesuwając kontrolę nad informacją jeszcze bardziej nie tylko poza państwa, lecz poza możliwości obrońcy w ogóle. Może to skutkować ułatwieniem wykorzystania AI w celach wojskowych, przy jednoczesnym kontrolowaniu reakcji społeczeństwa. Co więcej, symulacje RAND Corporation (2021) wskazują, że systemy zdolne do autonomicznego zakłócania łączności i modyfikacji sygnałów radarowych mogą znacząco utrudnić przeciwnikowi ocenę sytuacji. Automatyzacja decyzji w zakresie walki radioelektronicznej może prowadzić do sytuacji, w której eskalacja następuje szybciej niż człowiek jest w stanie ją kontrolować¹²⁷. Jednocześnie pojawia się problem etyczny i prawny. Kwestia autonomicznych systemów uzbrojenia (LAWS — ang. Lethal Autonomous Weapon Systems) od lat budzi kontrowersje w ONZ. Automatyzacja ataku oznacza bowiem nie tylko większą skuteczność, lecz także utratę pełnej kontroli człowieka nad decyzją o użyciu siły¹²⁸. W takim wypadku brak jasnych mechanizmów przypisywania odpowiedzialności stanowi poważne wyzwanie dla systemu prawa międzynarodowego¹²⁹, a zarazem doboru adekwatnych środków reakcji. Szczególną tego formą byłoby wykorzystanie LAWS przez podmiot asymetryczny — małą grupę przestępczą lub terrorystyczną, albo nieznanego aktora, który rozszerzyłby problem atrybucji w cyberprzestrzeni na kinetyczne skutki użycia środków cyfrowych.

¹²⁵ D. Kuźnicka-Błaszowska, N. Kostyuk, *Emerging need to regulate deepfakes in international law: the Russo-Ukrainian war as an example*, „Journal of Cybersecurity” 2025, Vol. 11, Issue 1, s. 4–7.

¹²⁶ Europol, *Facing reality? Law enforcement and the challenge of deepfakes, an observatory report from the Europol Innovation Lab*, Luxembourg 2022, s. 5, 8.

¹²⁷ J. Black i inni, *Strategic competition in the age of AI Emerging risks and opportunities from military use of artificial intelligence*, Santa Monica-Cambridge 2024, s. 22, 75–76; Z. Burdette i inni, *An AI Revolution in Military Affairs? How Artificial Intelligence Could Reshape Future Warfare*, [WR-A4004-1], 2025, s. 5, 37–39.

¹²⁸ Wskazać tu należy zróżnicowane podejścia. Rząd USA lobbuje za niskim stopniem uregulowania przypadków wykorzystania LAWS, gdzie inne państwa, w szczególności potencjalnie zagrożone, sprzeciwiają się temu; zob. USA-GOV, *Humanitarian benefits of emerging technologies in the area of lethal autonomous weapon systems*, [CCW/GGE.1/2018/WP.4], 2018; M.R. Choudhury, *Letter dated 8 March 2021 from the Panel of Experts on Libya established pursuant to resolution 1973 (2011) addressed to the President of the Security Council*, [S/2021/229], 2021; UN General Assembly, *Lethal autonomous weapons systems. Report of the Secretary-General*, [A/79/88], 2024.

¹²⁹ UNIDIR, *The Weaponization of Increasingly Autonomous Technologies: Artificial Intelligence*, „UNIDIR Resources” 2018, No. 8, s. 5–9.

Ma to szczególne znaczenie wobec zwiększania tempa automatyzacji oraz skali działań ofensywnych, co zmusza państwa do inwestycji w autonomiczne systemy obrony i detekcji¹³⁰. Co więcej, AI umożliwia tworzenie nowych form ataków — od hiperrealistycznej dezinformacji po adaptacyjne botnety. Wskazuje to na potrzebę tworzenia mechanizmów regulacyjnych, transparentności algorytmów i zacieśniania współpracy międzynarodowej, by ograniczyć niekontrolowaną eskalację. Ostatecznie, rosnąca rola AI oraz automatyzacji w atakach nie jest tylko kolejnym etapem technologicznej ewolucji. To zmiana jakościowa, która wpływa zarówno na strategie wojskowe, jak również na struktury społeczne i polityczne. W odróżnieniu od wcześniejszych epok, w których przewagę dawało posiadanie bardziej zaawansowanej broni, w przyszłości przewagę dać może zdolność do projektowania i obrony złożonych systemów algorytmicznych. Sprawia to, że bezpieczeństwo w epoce cyfrowej wymaga nowego paradygmatu, którego źródła oparte mogą być na ryzyku wynikającym z nakreślonych powyżej problemów.

4.2.4. Wzrost znaczenia infrastruktury krytycznej jako celu

Jednym z najbardziej widocznych trendów epoki cyfrowej, korelującego z trendami ofensywnych cyberdziałań w czasie pokoju, jest przesunięcie akcentu z ataków na cele stricte wojskowe w stronę infrastruktury krytycznej. W odróżnieniu od tradycyjnych operacji militarnych, uderzenia w sieci energetyczne, wodociągi, systemy transportowe czy służbę zdrowia mają charakter nie tylko strategiczny, lecz przede wszystkim społeczny. Skuteczność polega na możliwości wywołania paraliżu państwa i utraty zaufania społecznego — efektów, które trudno osiągnąć klasycznym atakiem kinetycznym. Co istotne, zjawisko to nie oznacza, że tylko największe państwa będą w stanie zagrażać mniejszym. Elastyczna natura cyberprzestrzeni sprawia, że oprogramowanie opracowane i użyte do ataku przez stronę silniejszą może być przechwycone, zmodyfikowane i wykorzystane (w całości lub części) przeciwko oryginalnym twórcom¹³¹.

Ponadto wzrost przestępczości świadczonej jako usługi sprawił, że wyrządzanie poważnych szkód nie wymaga już gromadzenia zespołu specjalistów, zdolnych do opracowania zaawansowanych narzędzi¹³². Niewielkie grupy, za opłatą, zyskują dostęp do zło-

¹³⁰ J. Schneider, J. Macdonald, *Looking back to look forward: Autonomous systems, military revolutions, and the importance of cost*, „Journal of Strategic Studies” 2023, Vol. 47, No. 2, s. 163–164; H. Shengning [胡延宁], L. Bingyan [李炳彦], W. Shengliang [王圣良], *Light Warfare: The New Trend in the Global Revolution in Military Affairs* [世界军事革命新趋势], Beijing 2015, s. 65–76.

¹³¹ D. Hughes, A.M. Colarik, *Predicting the Proliferation of Cyber Weapons into Small States*, „Joint Force Quarterly” 2016, Vol. 83, No. 4, s. 21.

¹³² Europol, *Internet Organised Crime Threat Assessment 2020*, Hague 2020, s. 16, 31; P.S. Chauhan, N. Kshetri, *Ransomware as a Service Kit: A Novel Cybercrime Strategy to Monetize Victims* →195

śliwego oprogramowania, aktualizowanego o nowe funkcje, wykorzystującego najświeższe podatności i zmieniającego swe sygnatury celem ograniczenia wykrywalności. Powoduje to, że cyberoperacje podejmowane przez zespoły ekspertów oraz doświadczonych oficerów obcych wywiadów stają się obrazem co najmniej niepełnym. Najskuteczniejsze ataki ostatnich lat przeprowadzane były przez relatywnie młode osoby. Jak informuje Narodowa Agencja ds. Przestępczości Wielkiej Brytanii (NCA), aresztowani członkowie Scattered Spider, jednej z niebezpieczniejszych grup¹³³, mieli od 17 do 20 lat, natomiast w USA od 17 do 25 lat¹³⁴. Zjawisko to znajduje potwierdzenie w badaniach nad mechanizmami rekrutacji młodych ludzi do roli tzw. „money mule” — osób udostępniających swoje konta bankowe do prania pieniędzy pochodzących z cyberprzestępstw. Jak pokazuje analiza przeprowadzona wśród ponad dwóch tysięcy młodych osób w Holandii, osoby w wieku 16–25 lat są szczególnie podatne na tego typu werbunek¹³⁵. Cyberprzestępczość coraz częściej opiera się bowiem na wykorzystaniu społecznych i psychologicznych mechanizmów wpływu, a nie tylko na technicznej biegłości sprawców¹³⁶. Skutkuje to budową złożonych i rozproszonych sieci przestępczych, zwiększając możliwości ataku przy kamuflowaniu centrów decyzyjnych, co zupełnie odmienia krajobraz zagrożeń dla infrastruktury krytycznej.

Kluczowym elementem tej zmiany jest podatność architektury systemów sterowania przemysłowego (ICS) i systemów nadzoru, kontroli i akwizycji danych (SCADA). Są to rozwiązania, które powstawały w okresie, gdy ich projektanci zakładali pełną izolację od świata zewnętrznego. Bezpieczeństwo opierało się na założeniu „air gap” — fizycznego oddzielenia od sieci publicznych. Współczesna transformacja cyfrowa zburzyła to założenie. Łączenie systemów przemysłowych z sieciami korporacyjnymi, a często i z internetem, umożliwia ich zdalne monitorowanie i zarządzanie, ale równocześnie otwiera je na wektory ataku, które wcześniej nie stanowiły problemu. Niepomijalne są także błędy użytkowników, które narażają sieci odizolowane na ataki z zewnątrz, np. przez nieprawidłowe posługiwanie się nośnikami pamięci¹³⁷.

Data, „Computer” 2023, Vol. 56, s. 103–105.

¹³³ CISA i inni, *Scattered Spider*, [AA23-320A], 2025, 1–2, 5–7.

¹³⁴ US District Court For the Central District of California, *Indictment. 18 U.S.C. § 1349: Conspiracy to Commit Wire Fraud; 18 U.S.C. § 371: Conspiracy; 18 U.S.C. § 1028A(a)(1): Aggravated Identity Theft; 18 U.S.C. §§ 981, 982, 1029, 1030 and 28 U.S.C. § 2461(c): Criminal Forfeiture*, [CR No. 2:24-CR00595-JWH], 2015, s. 1–4.

¹³⁵ L. Bekkers, R. Spithoven, Y.V. Houten, E.R. Leukfeldt, *The involvement mechanisms of cybercrime: Explaining previous exposure of young people to money mule recruiters*, „European Journal of Criminology” 2025, Vol. 22, No. 4, s. 493–497.

¹³⁶ Tamże, s. 499–501.

¹³⁷ Która wiąże się też z ryzykiem i nie zapewnia pełnego bezpieczeństwa, co wykazał przypadek

Podstawowy problem architektury ICS i SCADA wynika z faktu, że nie zostały one stworzone z myślą o współcześnie rozumianym cyberbezpieczeństwie. Protokoły komunikacyjne, takie jak Modbus¹³⁸ czy DNP3¹³⁹, przez dziesięciolecia funkcjonowały bez uwierzytelniania lub szyfrowania. Oznacza to, że napastnik, który uzyska dostęp do segmentu sieci przemysłowej, może manipulować przesyłanymi danymi, zmieniać parametry pracy urządzeń, czy przejmować nad nimi pełną kontrolę. Z perspektywy taktycznej tworzy to asymetrię: obrońcy muszą chronić złożone, rozproszone i często przestarzałe systemy, podczas gdy atakującemu wystarczy znaleźć jeden słaby punkt, aby uzyskać efekt operacyjny lub nawet strategiczny. W tym kontekście szczególnie wrażliwym obszarem są tzw. punkty styku — miejsca, w których sieci przemysłowe (OT) łączą się z sieciami IT. Coraz częściej wymagania biznesowe, takie jak optymalizacja produkcji, zdalny nadzór czy integracja danych w czasie rzeczywistym, prowadzą do „spłaszczania” architektury bezpieczeństwa. Z perspektywy napastnika umożliwia to przechodzenie od systemów IT do OT, co znacząco skraca drogę do krytycznych komponentów. Wyróżnić tu należy ataki na źle zaprojektowaną infrastrukturę IT albo dostawców usług utrzymania systemów OT. Analizy przeprowadzone przez MITRE¹⁴⁰ i SANS Institute¹⁴¹ pokazują, że wiele incydentów w ICS wynikało właśnie z lateralnego ruchu w sieci — początkowa in-

Stuxnet. Zaatakowany ośrodek w Natanz był całkowicie odizolowany od sieci. Złe nawyki pracowników i podpinanie tych samych pamięci przenośnych na komputerach domowych oraz wewnątrz ośrodka „rozszerzyły tę izolację. Skala problemu była tak duża, że utworzono w ten sposób kanał względnie regularnej komunikacji między instancjami Stuxnet oraz serwerami dowodzenia i kontroli; S. Dygantowski, *Cyberbezpieczeństwo jako fundament bezpieczeństwa infrastruktury krytycznej w kontekście współczesnych zagrożeń*, „Journal of KONBiN” Vol. 50, Issue 4, s. 315–317.

¹³⁸ Modbus — protokół opracowany w 1979 roku, przeznaczony pierwotnie do komunikacji między sterownikami PLC a panelami programującymi. Opiera się na architekturze master-slave, w której tylko urządzenie nadrzędne (master) inicjuje transmisję, a urządzenia podrzędne (slave) odpowiadają. Protokół umożliwia transmisję danych w formie zapytań i odpowiedzi, działając w wielu trybach i na różnych warstwach fizycznych, co zapewnia jego uniwersalność i trwałą popularność w automatyce przemysłowej. Jednakże brak mechanizmów uwierzytelniania, szyfrowania transmisji oraz kontroli integralności danych sprawia, że jest podatny na ataki; G. Thomas, *Introduction to the Modbus Protocol*, „The Extension” 2008, Vol. 9, Issue 4, s. 1–4.

¹³⁹ DNP3 (Distributed Network Protocol) — protokół opracowany w 1991 roku, szeroko stosowany w systemach SCADA, zwłaszcza w sektorze energetycznym. Umożliwia przesyłanie danych zarówno do pojedynczych urządzeń, do wielu urządzeń jednocześnie, jak również wysyłanie informacji przez urządzenia bez wcześniejszego zapytania. Mimo swojej funkcjonalności, DNP3 nie został zaprojektowany z uwzględnieniem bezpieczeństwa. Jest podatny na podsłuch sieci, odtwarzanie odpowiedzi, wstawienie urządzenia pośredniczącego, fałszywe flagi, zmiany adresu, przepełnienie długości komunikatów, i wiele innych; S. East, J. Butts, M. Papa, S. Sheno, *A Taxonomy of Attacks on the DNP3 Protocol*, [w:] *Critical Infrastructure Protection III*, C. Palmer, S. Sheno (eds.), Hanover 2009, s. 68–79.

¹⁴⁰ O. Alexander, M. Belisle, J. Steele, *MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy*, McLean 2020, s. 2.

¹⁴¹ D. Parsons, *SANS ICS/OT Cybersecurity Survey: 2023's Challenges and Tomorrow's Defenses*, „SANS Analyst Program” 2023, Sep., s. 5–6.

fekcja w infrastrukturze IT przenosiła się stopniowo na systemy operacyjne. Wdrożenie izolacji bez odpowiedniego wykrywania ruchu lateralnego jest też jednym z istotnych zagrożeń dla systemów przemysłowych, wskazywanych przez NIST¹⁴².

Różnica w sytuacji obrońców i agresorów jest tu zasadnicza. Atakujący może działać skrycie, wybierać moment uderzenia i dopasować narzędzia do konkretnego środowiska. Obrońcy wręcz przeciwnie — muszą zapewnić ciągłość działania systemów w trybie 24/7/365, często przy ograniczonych zasobach finansowych i kadrowych. Wymusza to coraz częściej stosowanie zewnętrznych usług zespołów SOC (centrów operacji bezpieczeństwa). Wymaga to jednak ustanowienia zdalnego połączenia przez ogólny trend przechodzenia narzędzi monitorujących na rozwiązania chmurowe¹⁴³. Potencjalny problemem leży w architekturze systemów monitorujących. Pożądanym byłoby ustanowienie komunikacji jednokierunkowej. Lokalni agenci zainstalowani na urządzeniach przesyłają dane do centralnego kolektora logów. Natomiast dwukierunkowy ruch z zewnątrz jest możliwy tylko do kolektora, z którego systemy monitorujące odczytują informacje (logi) i poddają je analizie, bez możliwości wpłynięcia na infrastrukturę. Jednakże współczesne rozwiązania chmurowe wymagają bezpośredniej interpretacji danych, a zatem dwukierunkowego ruchu aż do końcowych urządzeń w sieci OT. Rozwiązanie to ma istotne zalety: pozwala na skuteczniejsze monitorowanie, zdalną aktualizację agentów i szybszą reakcję. Zarazem jednak utrudnia nawet logiczną izolację systemów wrażliwych na ataki w cyberprzestrzeni.

Kolejnym czynnikiem, który zwiększa podatność infrastruktury krytycznej, jest brak standaryzacji i silna heterogeniczność systemów¹⁴⁴. Architektura ICS i SCADA różni się między branżami, a nawet między zakładami należącymi do tej samej sieci. Powoduje to, że wdrażanie uniwersalnych zabezpieczeń jest trudne, a proces reagowania na incydenty wymaga specjalistycznej wiedzy o danym środowisku. To kolejna przewaga atakujących — mogą oni wykorzystywać specyficzne konfiguracje i luki w implementacji. Wiele elementów ICS to urządzenia działające od kilkunastu do kilkudziesięciu lat, co często prowadzi do akumulacji podatności. Modernizacja jest kosztowna i ryzykowna, ponieważ przestoje w działaniu infrastruktury krytycznej mają bezpośrednie konse-

¹⁴² K. Stouffer i inni, *Guide to Operational Technology (OT) Security*, [NIST SP 800-82r3], 2023, s. 74–77, 102–103.

¹⁴³ J.M. López Velásquez i inni, *Systematic review of SIEM technology: SIEM-SC birth*, „International Journal of Information Security” 2023, No. 22, s. 692–698.

¹⁴⁴ Heterogeniczność systemów oznacza, że w ramach jednej infrastruktury współdziałają różne technologie, urządzenia, protokoły lub systemy operacyjne. Taka różnorodność zwiększa elastyczność i funkcjonalność, ale jednocześnie komplikuje zarządzanie, integrację oraz bezpieczeństwo.

kwencje społeczne i gospodarcze. W efekcie łatwiej jest napastnikowi znaleźć lukę niż obrońcom całkowicie je wyeliminować.

Nie mniej istotnym problemem jest różnica w dynamice działania. Atakujący może planować kampanię miesiącami, badając sieć, wprowadzając złośliwe oprogramowanie i powoli budując dostęp. Tymczasem obrońcy zmuszeni są do natychmiastowej reakcji w przypadku wykrycia incydentu, pod presją zachowania ciągłości świadczonych usług. Każda pomyłka może doprowadzić do eskalacji problemu lub zatrzymania działania infrastruktury. W praktyce oznacza to, że obrona jest reaktywna i ryzykowna, a ofensywa — planowa i selektywna. Choć formułowane są stanowiska przeciwne, wskazujące na większy balans między obiema stronami, to również i te źródła wskazują na zależność od konkretnych warunków¹⁴⁵. W przypadku infrastruktury krytycznej, przewaga leży po stronie agresorów. Systemy przemysłowe, które kiedyś uważano za „odporne” dzięki izolacji, stają się podatne, ponieważ zostały włączone w globalny ekosystem cyfrowy. W kontekście wpływu środowiska sieciocentrycznego na działalność państw, modernizacja omawianego sektora i jego odpowiednie zabezpieczenie prawdopodobnie będzie jednym z ważniejszych wyzwań.

Podsumowanie

Analiza roli wykorzystania cyberprzestrzeni wskazała na niejednoznaczność prawa międzynarodowego i zobowiązań sojuszniczych, głęboka współzależność państwa z sektorem prywatnym, przyspieszenie decyzyjne wywołane AI oraz automatyzacją, jak również architektoniczne słabości ICS/SCADA infrastruktury krytycznej. Łącznie wymienione czynniki przekształcają logikę eskalacji, tworząc problem wynikowy. Próg „użycia siły” staje się ruchomy, gdyż skutki mogą materializować się na polu bezpieczeństwa publicznego, finansów lub usług społecznych, zanim pojawi się jednoznaczny sygnał militarnej agresji. Jednocześnie „czas operacyjny” ulega kompresji: cykle wykrycia-decyzji-reakcji liczy się w minutach, a nie w dniach. Skutkiem jest przesunięcie ciężaru odstraszania. Dotychczasowa prezencja kinetycznej siły militarnej, deklaracje polityczne, sankcje kierowane przeciwko innym państwom, przedsiębiorstwom, organizacjom lub pojedynczym osobom, stają się niewystarczające. Cyberprzestrzeń narzuca nowe podejście: budowę mierzalnej odporności ekosystemów ze wszystkimi tego implikacjami. Za stwierdzeniem tym kryje się bowiem złożony system zależności, holistycznego podej-

¹⁴⁵ E. Gartzke, J.R. Lindsay, *Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace*, „Security Studies” 2015, Vol. 24, No. 2, s. 343–346.

ścia do zarządzania i koordynacji działań, przy odpowiednio szybkiej wymianie informacji, pozwalającej reagować na narastające zagrożenia.

Wydać się także, że główne wektory przyszłej eskalacji będą miały charakter kumulatywny, a nie spektakularny. Operacje rozpoznania i budowania możliwie trwałych dostępu w środowiskach IT/OT staną się „tłem” rywalizacji, z którego w dowolnym momencie można wyprowadzić ograniczony efekt kinetyczny (np. zakłócenie parametrów procesowych), polityczny (wzniesienie kryzysu zaufania) lub ściśle cyfrowy. Ryzyko eskalacyjne będzie rosło zwłaszcza tam, gdzie występują sprzężenia między domenami: zakłócenia w cyberprzestrzeni generują skutki gospodarcze, te zaś presję społeczną, będącą sygnałem dla władz politycznych oraz wojskowych. W tym kontekście, problem atrybucji — naturalny w cyfrowym środowisku pośrednictwa połączeń, usług chmurowych i łańcuchów dostaw — będzie działać jak akcelerator nieporozumień i potencjalnie kolejne narzędzie wpływu. Niezrozumienie tej problematyki, przy jednoczesnym mierzeniu się z reperkusjami, skutkować może oczekiwaniem społecznymi, które nie będą zbieżne z celami strategicznymi, operacyjnymi czy taktycznymi. Dlatego poza koordynacją złożonego środowiska sieciocentrycznego, utrzymanie konwergencji celów państwa (w znaczeniu cywilnym), sił zbrojnych, sektora prywatnego i potrzeb obywateli, powinno być postrzegane jako konieczność.

Dotychczasowe instrumenty prawa międzynarodowego i doktryn sojuszniczych z trudem odwzorowują tę dynamikę. Aktualne modele odstraszania, wypracowane m.in. w reakcji na terroryzm¹⁴⁶, stają się niewystarczające wobec działań w cyberprzestrzeni. W szczególności, klasyczne podejścia oparte na „deterrence by punishment” tracą operacyjną użyteczność w środowisku, gdzie przypisanie sprawcy ataku jest nie tylko technicznie trudne, ale często politycznie nieopłacalne. Jak wskazuje literatura¹⁴⁷, skuteczność odstraszania w cyberprzestrzeni zależy nie tyle od groźby odwetu, co od zdolności systemu do absorpcji zakłóceń i kontynuacji działania mimo ich wystąpienia. W tym kontekście „deterrence by denial” również napotyka ograniczenia, zwłaszcza gdy infrastruktura krytyczna pozostaje heterogeniczna, oparta na przestarzałych protokołach komunikacyjnych i zależna od złożonych relacji z dostawcami ICT. Brak jednolitych standardów interoperacyjności, a także fragmentaryzacja odpowiedzialności między sektorami publicz-

¹⁴⁶ J. Gearson, *Detering Conventional Terrorism: From Punishment to Denial and Resilience*, „Contemporary Security Policy” 2012, Vol. 33, No. 1, s. 172–175, 177–181.

¹⁴⁷ M. Zapfe, *Deterrence from the Ground Up Understanding NATO's Enhanced Forward Presence*, „Survival” 2017, No. 59, s. 152; T. Prior, *Resilience: The 'Fifth Wave' in the Evolution of Deterrence*, [w:] *Strategic Trends 2018. Key Developments in Global Affairs*, O. Thränert, M. Zapfe (eds.), Zürich 2018, s. 68–72, 77–28; E.D. Borghard, S.W. Lonergan, *Deterrence by denial in cyberspace*, „Journal of Strategic Studies” 2023, Vol. 43, No. 3, s. 545–549.

nym i prywatnym, osłabiają zdolność do skutecznego przeciwdziałania zagrożeniom hybrydowym. W rezultacie, coraz większe znaczenie zyskuje „deterrence by resilience” jako forma odstraszania przez zdolność systemu do adaptacji, regeneracji i kontynuacji funkcji mimo zakłóceń. „Resilience” nie jest tu rozumiana jako statyczna odporność, lecz jako dynamiczna zdolność do reorganizacji i uczenia się w warunkach permanentnej niepewności. W ujęciu systemowym, działa ona jako „bufor eskalacyjny”, który redukuje presję na natychmiastową reakcję polityczną, umożliwiając zarządzanie kryzysem w sposób rozproszony, celowy i rozważny.

Kluczowa pozostaje też rola AI oraz automatyzacji. Po stronie atakującego, algorytmy będą wspierały rekonesans, eskalację uprawnień i maskowanie ruchu w czasie rzeczywistym, jak również dalsze działania w systemach. Po stronie obrony, o ile zautomatyzowana reakcja pozwoli na znaczącą poprawę czasu reakcji, to wprowadzić może nowe klasy błędów w procesach. Uogólnienia modeli, konflikty polityk między obszarami sieci informatycznych oraz przemysłowych, jak również „kolizje” autonomicznych agentów ofensywnych i defensywnych w tej samej infrastrukturze, mogą zaważyć na skuteczności AI w obronie. Problemy te tworzą bowiem scenariusze eskalacji niezamierzonej, w której łańcuch szybkich, lokalnie racjonalnych decyzji prowadzi do systemowych zakłóceń. Co więcej, same trendy architektoniczne sprzyjają przeciwnikowi. Wyzwaniem stają się: łączenie IT z OT, standaryzacja interfejsów, zdalne utrzymanie ruchu, a także konsolidacja ekosystemów wokół kilku dostawców platformowych. Każdy z tych procesów przynosi korzyści efektywnościowe, ale jednocześnie tworzy „płaskie” powierzchnie ataku i punkty koncentracji ryzyka. Rysuje to perspektywę nie „cyfrowego Pearl Harbor”, lecz długotrwałego, iteracyjnego wyniszczania: erozji niezawodności infrastruktury, wzrostu kosztów zabezpieczeń (finansowych, czasowych, społecznych), zmęczenia organizacyjnego czy politycznej polaryzacji.

Krajobraz ryzyka może kształtować także jedna z wyjątkowych cech środowiska sieciocentrycznego jako przestrzeni walki, czyli jego strukturalna asymetria (szerzej omówiona w II rozdziale). Izolowanie i zamykanie sieci na poziomie krajowym zwiększa odporność na ingerencję z zewnątrz. Nie wpływa też negatywnie na prowadzenie operacji na zewnątrz, bez symetrycznej ekspozycji na odwet. Z kolei otwartość sieci skutkuje wzrostem zależności od komercyjnych dostawców chmury, łączności i rozpoznania. Skutkować to może znacznie szybszym osiąganiem efektów, pozwalającym na skuteczną współpracę między państwami, lecz zarazem przenosi kluczowe decyzje operacyjne poza aparat państwowy.

W konsekwencji rekomendacje strategiczne powinny być ukierunkowane na spójność i tempo, przez systemowe stosowanie szeregu działań:

- a) normatywne ustalenie progów odpowiedzi i ich „mapowanie” na typy skutków (społeczne, gospodarcze, techniczne, polityczne, wojskowe);
- b) minimalne wymagania względem architektury systemów, w zakresie odporności oraz zbieżności z wymaganiami i potrzebami operacyjnymi państw;
- c) reżimy odpowiedzialności za wadliwe oprogramowanie i infrastrukturę w środowiskach krytycznych;
- d) jednolite formaty wymiany danych o zagrożeniach i automatyczną dystrybucję wskaźników;
- e) mechanizmy „cyfrowej mobilizacji”, czyli zdolność do szybkiego włączenia zasobów prywatnych w operacje obronne na mocy przejrzystych ram prawnych;
- f) budowę świadomości wśród obywateli względem ich roli w cyberprzestrzeni jako polu walki (cyber-przysposobienie obronne).

Zauważyć należy, że część tych działań wdrażana jest już dziś na wszystkich szczeblach. Firmy prywatne kierują się ochroną zysków przez zachowanie ciągłości działania, stosując uznane normy i standardy. Państwa realizują swoje potrzeby i wymagania w zakresie cyberbezpieczeństwa przez przepisy na poziomie krajowym. Z kolei ponadnarodowo ustalane są ramy współpracy, takie jak w przypadku Unii Europejskiej. Obecnie jednak koordynacja tych wysiłków wydaje się niewystarczająca, w tym również konwergencja celów. Co więcej, kształtowanie odpowiednich postaw obywatelskich w zakresie cyberbezpieczeństwa wciąż jest jednym z najsłabszych ogniw.

Rozdział V

Prognoza perspektyw i nowe ramy analizy wojen cyfrowych

Wnioski płynące z wcześniejszych rozdziałów ukazują, że hybrydowość i asymetryczność, choć stanowią użyteczne narzędzia opisu, nie wystarczają do uchwycenia specyfiki współczesnych i przyszłych konfliktów w epoce cyfrowej. Analiza wykazała, że cyberprzestrzeń nie jest już jedynie uzupełnieniem konwencjonalnych działań wojennych, lecz odrębnym środowiskiem, w którym aktorzy państwowi i pozapaństwowi prowadzą zarówno operacje militarne, jak i polityczne, psychologiczne czy ekonomiczne. Zdolność do kontroli przepływu informacji, eksploatacji podatności technicznych oraz oddziaływania na percepcję społeczną staje się kluczowym wyznacznikiem siły. W tej perspektywie prognozowanie przyszłych konfliktów w cyberprzestrzeni wymaga nowych kategorii analitycznych, wykraczających poza metafory i schematy, które dziedziczone są z historii wojen konwencjonalnych. Jednakże wiele współczesnych analiz nadal posługuje się językiem właściwym dla kinetycznego pola walki, przenosząc go niemal mechanicznie na cyberprzestrzeń. Używanie pojęć takich jak „cyfrowa linia frontu”, „teatr działań” czy „obrona terytorialna sieci” sugeruje, że cyberprzestrzeń daje się podporządkować logice fizycznej przestrzeni i zajmowania pozycji. Tworzy to iluzję kontroli, sugerując, że przestrzeń cyfrową można opisać w kategoriach terytorialnych, a następnie chronić jak obszar geograficzny. W praktyce jednak atakujący korzysta z asymetrii: działa selektywnie, punktowo i często poniżej progu wykrywalności. W tym sensie cyberprzestrzeń ujawnia nie tylko nowy wymiar operacji, lecz także problem epistemiczny: jak w ogóle formułować wiedzę o zagrożeniach. Zatem konwencjonalne metafory wojskowe nie tylko tracą charakter wyjaśniający, lecz utrudniają zrozumienie cyfrowych zjawisk i opracowanie adekwatnych strategii obrony. Z tego względu zasadnym wydaje się podjęcie próby krytycznej rewizji dotychczasowych sposobów prognozowania przyszłych konfliktów w cyberprzestrzeni. Celem stało się jednak nie tylko wskazanie ograniczeń wynikających z dziedziczenia pojęć militarnych, lecz przede wszystkim wypracowanie alternatywnego podejścia: opartego na analizie ryzyka i odporności systemowej.

Z powyższym wiąże się druga istotna trudność prognozowania: tempo innowacji technologicznej. W tradycyjnych konfliktach rozwój broni i doktryn trwał dekady, co umożliwiało relatywnie stabilne prognozy. W cyberprzestrzeni cykl życia technologii liczony jest w miesiącach¹. Sztuczna inteligencja, automatyzacja ataków czy wykorzystanie uczenia maszynowego do unikania detekcji, doprowadziły do zasadniczych zmian w dynamice starcia. Oznacza to, że każda próba przewidywania przyszłych wojen w cyberprzestrzeni musi uwzględniać nie tylko istniejące narzędzia, lecz przede wszystkim trendy innowacyjne. Choć nie zmieniają one zasadniczo struktury stosunków międzynarodowych, to mogą w krótkim czasie odwrócić relację sił. Wynika to z faktu, że tradycyjne mechanizmy balansowania wpływów są trudne do zastosowania w środowisku cyfrowym.² Wymagają raczej budowy cyfrowej odporności, zaufania pomiędzy państwami oraz wielosektorowej i ponadnarodowej współpracy.

Nie mniej istotnym pozostaje też problem atrybucji. Przenoszenie do analiz kategorii takich jak „państwo-agresor” czy „sojusznik” bywa zwodnicze. Małe grupy hakerskie mogą osiągać efekty porównywalne z działaniami państw, a państwa mogą wykorzystywać je jako „maski” dla własnych operacji. Tradycyjna typologia przeciwników staje się przez to niewystarczająca.

Wszystkie te czynniki — językowe, poznawcze i technologiczne — sprawiają, że prognozowanie konfliktów w cyberprzestrzeni wymaga porzucenia prostych analogii wojskowych. Nie oznacza to jednak rezygnacji z prób systematyzacji. Przeciwnie, konieczne staje się poszukiwanie ram analitycznych, które lepiej oddają naturę zagrożeń. Jednym z takich podejść, które wydaje się odpowiadać na potrzeby środowiska sieciocentrycznego, jest modelowanie ryzyka: nie w kategoriach linii frontu czy dominacji przestrzeni, ale w kategoriach prawdopodobieństwa, skutków i podatności systemów.

Dlatego w niniejszym rozdziale przyjęto podejście krytyczno-prognostyczne. Skonfrontowanie bieżących paradygmatów z ustaleniami z poprzednich rozdziałów zdaje się negatywnie oceniać szanse na prognozowanie przyszłych konfliktów z dużą pewnością. W zamian jednak zaproponowano podejście alternatywne, którego centralnym punktem staje się odporność systemowa i zdolność do zarządzania ryzykiem w warunkach stałej i głębokiej niepewności. Tylko takie podejście pozwala uniknąć iluzji kontroli i przygotować państwa oraz społeczeństwa na realne wyzwania przyszłych konfliktów cy-

¹ S. Saeed i inni, *Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations*, „Sensors” 2023, Vol. 23, Issue 6666, s. 11–14.

² A. Klimburg, L. Faesen, *A Balance of Power in Cyberspace*, [w:] *Governing Cyberspace Behavior, Power, and Diplomacy*, D. Broeders, B. van den Berg (eds.), Lanham-Boulder-New York-London 2020, s. 154–158.

frowych. Zarazem proponuje się zmianę podejścia do zarządzania informacją, a tym samym decyzją: z silnej hierarchii do struktury bardziej elastycznej i ramowej. Przyjęcia bardziej elastycznych narzędzi pozwoli uwzględnić złożoność cyberprzestrzeni, współzależność sektora publicznego i prywatnego oraz wielowymiarowość ryzyka.

5.1. Prognozy rozwoju wojen cyfrowych: krytyka i perspektywy

Refleksja nad przyszłością konfliktów w cyberprzestrzeni od samego początku obarczona jest napięciem między potrzebą prognoz a świadomością ograniczeń poznawczych. W literaturze strategicznej nie brakuje prób modelowania tego, jak wyglądać będą wojny nadchodzących dekad — od wizji „cyfrowych pól bitewnych”³ po scenariusze zakładające istotną lub całkowitą dominację sztucznej inteligencji⁴. Jednakże każdy z tych kierunków myślenia mierzy się z podstawowym problemem: cyberprzestrzeń, w przeciwieństwie do domen tradycyjnych, nie ma ustalonych granic ani trwałych struktur. Jej natura jest zdeterminowana przez nieustannie zmieniającą się architekturę techniczną, regulacyjną i społeczną. To sprawia, że przewidywania formułowane w jednej dekadzie bardzo szybko tracą aktualność w następnej. Doświadczenia z ostatnich trzydziestu lat wskazują, że wiele prognoz nadmiernie eksponowało czynniki technologiczne, nie doceniając dynamiki politycznej czy społecznej. W latach 90. dominującym konceptem była rewolucja w sprawach wojskowych, która miała uczynić z cyfrowych narzędzi dźwignię absolutnej przewagi operacyjnej⁵. Atak na Estonię w 2007 roku czy operacja Stuxnet w 2010 roku pokazały jednak, że cyberkonflikt rozwija się w sposób bardziej nieregularny i asymetryczny, niż zakładano. Prognozy skupione na wizjach państwowej dominacji nad sieciami okazały się nietrafionymi w obliczu wzrostu znaczenia aktorów pozapaństwowych, przestępczości zorganizowanej, czy nawet pojedynczych hakerów, którzy potrafili wywołać skutki geopolityczne niewspółmierne do własnych zasobów.

³ N. Solce, *The Battlefield of Cyberspace: The Inevitable New Military Branch — The Cyber Force*, „Albany Law Journal of Science & Technology” 2008, Vol. 18, Issue 1, 300–311; F. Douzet, A. Gery, *Cyberspace is used, first and foremost, to wage wars: proliferation, security and stability in cyberspace*, „Journal of Cyber Policy” 2021, Vol. 6, No. 1, s. 98–101

⁴ A. Husain, *AI is Shaping the Future of War*, „Prism” 2021, Vol. 9, No. 3, s. 59–60; W. Chemlal, F. Maabed, *Artificial Intelligence: The New Cognitive Terrain for World Domination*, „Aleph” 2024 Vol. 11, No. 4–2, s. 580; A. Valiaveedu, P.F. Rybinski, *The Race for Artificial Intelligence*, „Illini Journal of International Security” 2021, Vol. 8, s. 58–60.

⁵ R. Owens, *The American Revolution in Military Affairs*, „Joint Force Quarterly” 1995, No. 10, s. 37–38.

Niepomijalne pozostają też kalki pojęciowe. Terminologia zaczerpnięta z Clausewita czy koncepcji zimnowojennych, bywa adaptowana niemal mechanicznie do opisu rzeczywistości cyfrowej. Skutkiem jest iluzja, że można ją pojmować w kategoriach przestrzeni terytorialnej. W praktyce atak może zostać przeprowadzony spoza przewidywanego kierunku natarcia, a nawet z wnętrza własnych struktur, poprzez przejęcie zaufanych poświadczeń czy infiltrację łańcucha dostaw. W tym sensie cyberprzestrzeń wymyka się logice linii i granic, a próby ich wyznaczania częściej zaciemniają obraz, niż go porządkują.

Kolejnym ograniczeniem prognoz jest tempo innowacji technologicznych. W tradycyjnych konfliktach, rozwój nowych broni (od czołgów po broń jądrową) przebiegał w perspektywie dekad. To z kolei umożliwiało państwom i teoretykom wojskowości na stopniowe dostosowywanie strategii. W przypadku cyberprzestrzeni cykl innowacji liczony jest w miesiącach: od powstania nowej luki bezpieczeństwa do jej wykorzystania może minąć kilka dni. Dane za 1 kwartał 2025 ukazują, że 28,3% podatności technicznych było wykorzystywanych w atakach w mniej niż 24 godziny od upublicznienia informacji na ich temat⁶. Zarazem w ciągu ostatnich dwóch lat zaobserwowano stały (choć liniowy) wzrost liczby aktywnie wykorzystywanych podatności⁷. Zastosowanie sztucznej inteligencji do automatyzacji ataków, dynamicznego ukrywania śladów czy generowania treści dezinformacyjnych, radykalnie zmienia obraz działań w cyberprzestrzeni. Prognozowanie w horyzoncie dłuższym niż kilka lat staje się przez to obarczone błędem systemowym — opiera się bowiem na przesłankach, które mogą ulec dezaktualizacji, zanim jeszcze prognoza trafi do decydentów lub ich zbiór pozwoli utworzyć szerszy obraz.

Dlatego aktualne próby przewidywania zagrożeń w cyberprzestrzeni są raczej krótkoterminowe i opierają się na szacowaniu prawdopodobieństwa. Jedną z najnowszych propozycji jest model LEV (ang. Likely Exploited Vulnerabilities). Wykorzystuje on dane z systemu EPSS (ang. Exploit Prediction Scoring System), który codziennie prognozuje ryzyko wykorzystania podatności w ciągu 30 dni. LEV traktuje te prognozy jako minimalne wartości i sumuje je w czasie, celem szacowania prawdopodobieństwa. W przeciwieństwie do list KEV (ang. Known Exploited Vulnerabilities), które zawierają tylko potwierdzone przypadki, LEV dostarcza ciągłą miarę ryzyka, co pozwala lepiej ustalać prio-

⁶ P. Garrity, *2025 Q1 Trends in Vulnerability Exploitation*, 24 April 2025, „VulnCheck”, <https://www.vulncheck.com/blog/exploitation-trends-q1-2025> [odczyt: 03.06.2025].

⁷ S. Robinson, *Time to next exploit*, [WITH-SECURE 7/16/2025], 2025, s. 4.

rytety działań naprawczych, oceniać kompletność KEV oraz wykrywać groźne podatności pominięte w tradycyjnych rejestrach⁸.

Stały charakter zagrożeń środowiska sieciocentrycznego, z realnymi atakami na krytyczną infrastrukturę, pozwala stawiać pytanie o kategorie eskalacji i progu wojny. Szczególnie, że problem atrybucji często nie pozwala na rozróżnienie aktorów państwowych i pozapaństwowych. Czasami te same grupy działają jednocześnie w logice przestępczej, politycznej i wojskowej. Zarazem bywają finansowane lub inspirowane przez państwa, lecz zachowują strukturalną autonomię. Uwidacznia to szczególnie problem z perspektywy badań nad bezpieczeństwem. W publikacjach powtarza się pytanie, czy cyberatak o dużej skali może zostać uznany za użycie siły w rozumieniu Karty Narodów Zjednoczonych⁹. Przykłady ataków na infrastrukturę krytyczną, od sieci energetycznych po systemy wyborcze, dowodzą, nieostrości granicy między „operacją poniżej progu” oraz aktem agresji. Prognozowanie przyszłych konfliktów wymaga więc nie tylko modelowania technicznych wektorów ataku w czasie konfliktu, lecz przede wszystkim zdolności obronnych w czasie formalnego pokoju.

Wszystko to prowadzi do wniosku, że refleksja nad przyszłością wojen w cyberprzestrzeni nie może być redukowana ani do opisu technologicznych innowacji, ani do prostego transponowania terminologii militarnej. Konieczne jest bardziej złożone podejście, które uwzględni interdyscyplinarny charakter tego środowiska: sprzężenie między technologią, polityką i procesami społecznymi. Tylko wtedy możliwe będzie budowanie modeli pozwalających choćby częściowo uchwycić dynamikę przyszłych konfliktów. Należy przy tym zaakcentować, że takie modele zawsze będą miały charakter przybliżony i niepełny. Prognozowanie nie polega więc na budowaniu zamkniętej wizji przyszłości, lecz na konstruowaniu ram, które pozwalają systematyzować niepewność i wskazywać obszary szczególnie podatne na zakłócenia. W tym sensie refleksja nad przyszłością wojny w cyberprzestrzeni stanowi nie tyle projekt „przewidzenia jutra”, ile projekt porządkowania wiedzy tak, aby państwa, sojusze i organizacje mogły reagować adekwatnie na zmieniające się uwarunkowania. Wydaje się bowiem, że to właśnie ten praktyczny aspekt ma większe znaczenie niż tylko teoretyczne rozważania i próba definiowania zjawisk.

⁸ P. Mell, J. Spring, *Likely Exploited Vulnerabilities. A Proposed Metric for Vulnerability Exploitation Probability*, [NIST CSWP 41], 2025, s. 1–3, 5–8, 23.

⁹ W. Goździewicz, *From Riga to Wales. NATO's Road to Collective Cyberdefence*, [w:] *NATO Road to Cybersecurity*, J. Świątkowska (ed.), Kraków 2016, s. 12–13; S. Ducaru, M. Caradaică, A.M. Costea, *Can a Cyberattack Become an Act of War? European and Trans-Atlantic Perspectives*, „Romanian Journal of European Affairs” 2024, Vol. 24, No. 1, s. 23–24; J. Hakala, J. Melnychuk, *Russia's Strategy in Cyberspace*, Riga 2021, s. 9–10.

5.1.1. Krytyka metafor i kategorii tradycyjnej wojny w odniesieniu do cyberprzestrzeni

W literaturze i praktyce strategicznej zaobserwować można do przenoszenia pojęć i metafor z wojen konwencjonalnych na opis walk w cyberprzestrzeni. Cyberprzestrzeń przedstawiana jest jako pełnoprawny teatr działań operacyjnych, w którym dowodzenie i kontrola (C2) stanowią centralny element zdolności bojowej¹⁰. W podejściu takim dostrzega się jednak traktowanie infrastruktury cyfrowej jako pola bitwy, zamiast środowiska rozproszonego i wielowarstwowego¹¹. Próba definiowania granic w cyberprzestrzeni (np. odpowiedzialności, wpływu, czy w ujęciu terytorium państwa)¹² wykorzystywana jest jako ujęcie mające militaryzować środowisko sieciocentryczne¹³, które wymaga raczej zintegrowanego, międzysektorowego podejścia. Z tego powodu niewłaściwym wydaje się także wskazywanie linii frontu w cyberoperacjach. Z jednej strony podkreśla się, że w środowisku sieciocentrycznym są one co do zasady asymetryczne i nie mogą być stosowane zamiennie z konwencjonalnymi liniami frontu¹⁴. Z drugiej jednak spotyka się postrzeganie cyberprzestrzeni jako izolowanych zasobów, które chronione są przez logiczne podziały z użyciem fizycznej infrastruktury¹⁵. Według takiego podejścia, uzyskanie dostępu wgłąb wymaga sforsowania urządzeń sieciowych logicznie izolujących dostęp¹⁶. Tworzy to łańcuch punktów: wirtualną ścieżkę z liniami frontu, na których możliwe jest prowadzenie działań obronnych, a w razie konieczności wycofywanie się za kolejne linie. Spotkać można też określenia ogólne, przypisujące raczej funkcje linii frontu pewnym obszarom, takim jak sieci publiczne (w domyśle chroniące podsieci infrastruktury krytycznej i podsieci z informacjami niejawnymi)¹⁷, lub miejsca styku sieci publicznej z zastrzeżonymi podsieciami różnego rodzaju¹⁸.

Jednakże tak ujęte metafory terytorialne fałszują obraz faktycznego ryzyka. W wojnie kinetycznej obszar kontrolowany przez przeciwnika ma ciągłą topologię: gra-

¹⁰ J.M. Hicks, *A Theater-Level Perspective on Cyber*, „Joint Force Quarterly” 2015, No. 76, s. 59–62.

¹¹ Tamże.

¹² C.V. Greene, *Cyberwarfare and our Allies: The Importance of Theater Security Cooperation*, [OMB No. 0704-01880], 2009, s. 5–10.

¹³ Tamże, s. 2, 9–11.

¹⁴ J. Kukkola, J.P. Nikkarila, M. Ristolainen, *Asymmetric frontlines of cyber battlefields*, [referat konferencyjny] *22nd ICCRTS Proceedings. Frontiers of C2*, Los Angeles 2017, s. 3–4.

¹⁵ Tamże, s. 15–16.

¹⁶ Tamże, s. 19–20.

¹⁷ X.Y. Yang i inni, *Research on the Construction of a Novel Cyberspace Security Ecosystem*, „Engineering” 2018, Vol. 4, s. 48.

¹⁸ J.P. Nikkarila, B. Åkesson, V. Kuikka, J. Hämäläinen, *Modelling Closed National Networks—Effects in Cyber Operation Capabilities*, [w:] *Game Player. Facing the structural transformation of cyberspace*, J. Kukkola, M. Ristolainen, J.P. Nikkarila (eds.), Riihimäki 2019, s. 104.

nice, przebieg linii, punkty oporu. W środowisku sieciocentrycznym przestrzeń „kontroli” składa się z węzłów wymiany informacji, które powiązane są zależnościami technicznymi i społecznymi¹⁹. Skuteczna infiltracja jednego węzła może dać atakującemu dostęp do wielu „obszarów” równocześnie²⁰. Mówienie o liniach frontu sugestywnie implikuje, że można ją zlokalizować i utrzymać. W praktyce oznaczałoby to nieoptymalne alokowanie zasobów ochronnych — chronilibyśmy rzekome fronty, podczas gdy rzeczywiste wektory wejścia pozostawałyby nieosłonięte. Trudno bowiem mówić o froncie przebiegającym przez urządzenia brzegowe podsieci, jeżeli dostęp do niej uzyskać można przez podatności w systemach, czy bezpośrednio przez użytkowników. Z kolei włączenie w koncepcję linii frontu także pozostałych wektorów, zwłaszcza czynnika ludzkiego i negatywnego wpływu²¹, rozmyłoby ten koncept. Takie podejście prowadzić może do braku wyobraźni strategicznej w sposób podobny do zjawiska zahamowania rozwoju lotnictwa po I wojnie światowej²².

Co więcej, metafory militarne sprzyjają błędnej klasyfikacji aktorów i celów. Tradycyjne kategorie armia–cywil tracą precyzję, gdy infrastruktura krytyczna jest współdzielona między państwem a prywatnym dostawcą usług. Podobnie, doszukiwanie się wojskowej aktywności państw w cyberprzestrzeni, takich jak militarne cyberstarcia i akty wojny w środowisku sieciocentrycznym²³, pomija hybrydowość sprawstwa. Grupy przestępcze, kontraktowi operatorzy, „szare” podmioty tworzą sieć, w której tożsamość sprawcy jest często rozmyta²⁴. Utrzymanie binarnej wizji przeciwnika upośledza zarówno ocenę prawno-polityczną, jak i wybór narzędzi odpowiedzi²⁵. Gdy problem przedstawia się jako bitwy o „pozycje”, naturalną reakcją jest wzmocnienie obrony „terytorialnej” — zapory, hardening, kontrola dostępu. To ważne, lecz niewystarczające. Cyberprzestrzeń

¹⁹ M. Li, X. He, Z. Sun, Y. Wen, *A framework for social media information flow analytics in cyberspace and physical space*, „Transactions in GIS” 2022, No. 26, s. 1486–1488, 1504; L. Zhang i inni, *Research on the Cyberspace Map and Its Conceptual Model*, „ISPRS” 2023, No. 12(353), s. 7–10.

²⁰ N. Kostyuk, *Allies and diffusion of state military cybercapacity*, „Journal of Peace Research” 2024, Vol. 61, No. 1, s. 46–48.

²¹ А.В. Петров, *Глобальные социальные процессы и современные исследования социокультурных трансформаций в социологии*, [w:] *Глобальные социальные процессы 4.0: социокультурные трансформации в системе современных обществ*, А.В. Петров i inni (red.), Санкт-Петербург 2023, s. 8–10.

²² E. Cook, *The Future of the Cyber Theater of War*, „HSGC Foreign Policy & International Issues” 2023, No. 13, s. 2, 3, 6.

²³ N. Ashraf, *The Paradox of Cyber Warfare and Clausewitz’s Conception of War*, „NUST Journal of International Peace & Stability” 2025, Vol. 8, No. 1, s. 18–20, 22–23.

²⁴ А.А. Кузнецов, *Цифровая трансформация и кибербезопасность: вызовы и стратегии*, [w:] *Глобальные социальные процессы 4.0...*, s. 391–393.

²⁵ E.T. Barrett, *Warfare in New Domain: The Ethics of Military Cyber-operations*, „Journal of Military Ethics” 2013, Vol. 12, No. 1, s. 3, 7–8.

wymaga zwiększenia zdolności do wykrywania, izolowania i szybkiego odzyskiwania funkcji (celem budowania odporności)²⁶. W praktyce taka strategia nadmiernego skupienia się na zapobieganiu, czyli wzmacnianiu barier, zapór, szyfrowania i filtrów, przy jednoczesnym niedoinwestowaniu w zdolność reagowania, czyni systemy szczególnie wrażliwymi na ataki długotrwałe i trudne do wykrycia, oparte m.in. o powolną eksfiltrację danych czy ciche wykorzystywanie podatności.

Innym problemem przenoszenia terminologii wojskowej na cyberprzestrzeń pozostaje założenie, że przeciwnika można powstrzymać przez groźbę odwetu, tzw. *deterrence by punishment*. W świecie cyfrowym ta logika coraz częściej zawodzi. Przede wszystkim dlatego, że nie sposób zawsze jednoznacznie ustalić tożsamość adversarza (problem atrybucji), a wielu z nich działa w sposób rozproszony. Nie można więc skutecznie „ukarać” agresora, skoro nie da się go pewnie wskazać²⁷. Próby przeniesienia doktryn odstraszania nuklearnego czy konwencjonalnego na cyberprzestrzeń kończą się więc najczęściej na poziomie deklaratywnym — jako polityczne komunikaty bez realnych narzędzi egzekwowania. Dlatego skuteczna obrona nie może opierać się wyłącznie na odstraszaniu, ale musi łączyć prewencję z odpornością — budowaniem zdolności do szybkiego wykrycia, ograniczenia skutków i przywrócenia sprawności systemu po incydencie. Jest to odstraszanie przez odmowę (*deterrence by denial*), które polega na uczynieniu ataku nieopłacalnym nie poprzez groźbę odwetu, lecz przez uniemożliwienie osiągnięcia celu²⁸. Taka strategia pozwala zachować przewagę w warunkach, gdzie całkowite uniknięcie ataku jest nierealne.

Metafory wojenne, z których te powyżej wymienione nie tworzą katalogu zamkniętego, zdają się zubożać analizę. Prognozowanie i modelowanie wymagają operjonalizacji wskaźników ryzyka, powierzchni ataku i skutków, a klasyczna terminologia militarna nie dostarcza tych zmiennych. Zamiast budować hipotezy oparte na analogii, potrzebujemy empirycznych kategorii: prawdopodobieństwo przełamania kontroli dostępu; czas do wykrycia; zdolność do infiltracji systemu; relacja skutku do złożoności systemu czy jego zabezpieczenia. Dopiero takie parametry umożliwiają tworzenie porównywalnych scenariuszy i formułowanie wniosków dających się testować. W związku z tym ko-

²⁶ S. Pitcher, T. Andress, *Cybersecurity and Cyber Resilience Requirements Critical to Cyberspace Survivability*, „Naval Engineers Journal” 2024, Volume 136, No. 1–2, s. 205–207.

²⁷ E.D. Borghard, S.W. Lonergan, *Deterrence by denial in cyberspace*, „Journal of Strategic Studies” 2023, Vol. 46, No. 3, s. 535–537.

²⁸ Tamże, s. 545–547; E. Lonergan, M. Montgomery, *What is the Future of Cyber Deterrence?*, „SAIS Review of International Affairs” 2021, Vol. 41, No. 2, s. 64–65; E. Lilli, *Redefining deterrence in cyberspace: Private sector contribution to national strategies of cyber deterrence*, „Contemporary Security Policy” 2021, Vol. 42, No. 2, s. 170–171.

nieczne jest ograniczenie użycia metafor terytorialnych do roli ilustracyjnej, a nie analitycznej. Leksykon rozwijać należy raczej na pojęciach technicznych i systemowych, integrując analizy techniczne z socjologicznymi i prawnymi. Tylko perspektywa wielowymiarowa odda naturę zagrożeń. Powyższe ma praktyczne implikacje dla alokacji budżetów, projektów organizacyjnych jednostek odpowiedzialnych za cyberbezpieczeństwo, ćwiczeń sojusznicze i ram prawnych. Polityka bezpieczeństwa powinna bowiem mierzyć ekspozycję krytycznych usług, koncentrować się na redukcji czasu wykrycia i na mechanizmach szybkiego odtworzenia. W perspektywie ofensywnej z kolei musi opierać się na rozwijaniu zdolności państwa do prowadzenia działań ofensywnych w sposób skoordynowany między służbami, sektorem publicznym i prywatnym. Oznacza to tworzenie przejrzystych ram prawnych i decyzyjnych²⁹, które zapewniają zgodność z prawem międzynarodowym, a jednocześnie umożliwiają szybkie reakcje. Równie istotnym pozostaje inwestowanie w modelowanie, symulacje i szkolenia, które zwiększają odporność systemów i przygotowują personel³⁰ do działań szeroko rozumianych, tj. w charakterze agresora oraz obrońcy. Badawczo z kolei, priorytetem jest konstrukcja wskaźników operacyjnych i programów empirycznej oceny modeli odporności, dla celów zarówno defensywnych, jak również ofensywnych.

5.1.2. Zagrożenia dla środowiska sieciocentrycznego: ryzyko destrukcji

Destrukcję cyberprzestrzeni trzeba rozumieć szeroko: nie tylko jako wyłączenie serwerów czy kradzież danych, lecz jako każdy mechanizm, który trwale lub długotrwale uniemożliwia normalne funkcjonowanie ekosystemów informacyjnych. Wcześniej wykazano, w jak znaczący sposób asymetria strukturalna wpływa na rozważania nad sposobem prowadzenia działań w cyberprzestrzeni. Opis ten byłby jednak niepełnym bez wzięcia pod uwagę destrukcji samego środowiska, podatnego ze względu na swą syntetyczność. W praktyce obejmuje to:

- g) długotrwałe, niskośladowe kampanie utrzymania dostępu i eksfiltracji zasobów oraz negatywnego wpływu na systemy;
- h) ataki na krytyczne elementy architektury (centra danych, węzły sieciowe, podmorskie kable);
- i) fizyczne zdarzenia o skali systemowej, w tym sabotaż infrastruktury;

²⁹ G. Huskaj, *The Current State of Research in Offensive Cyberspace Operations*, [w:] *ECCWS 2019 — Proceedings of the 18th European Conference on Cyber Warfare and Security*, T. Cruz, P. Simoses (eds.), New York 2019, s. 663–664.

³⁰ Tamże, s. 664–665.

- j) prawno-polityczną destrukcję przez fragmentację sieci (tworzenie krajowych intranetów) i odcięcia prawne/administracyjne.

Każdy z powyższych wymiarów ma inną dynamikę, koszty wejścia i trudność atrybucji, a zatem inny potencjał eskalacyjny. Co do zasady wykazują się one jednak wysokim potencjałem szkodenia państwu³¹. Niepomijalne są również źródła naturalne, takie jak promieniowanie kosmiczne (o zasięgu globalnym), burze geomagnetyczne (globalnym lub regionalnym), wyładowania elektrostatyczne (regionalnym lub lokalnym)³². Ponieważ zdarzenia te mogą być niezależne od działalności ludzkiej, a przy tym trudne do przewidzenia, to wymagają inwestowania w odpowiednie mechanizmy ochrony, redundancji czy rozwiązań alternatywnych.

Mimo dużej heterogeniczności powyższych zagrożeń (pod kątem źródła, skali i oddziaływania), różnicowane mogą być także względem państw: podejścia do nich, sposobu ujęcia w strategiach obronnych, czy potencjału wykorzystania.

Stany Zjednoczone widzą zagrożenia destrukcyjne w perspektywie hybrydowej: technologiczno-kinetycznej i systemowej. Dokumenty federalne przykładają dużą wagę do budowy odporności wobec EMP³³ i innych, długotrwałych zakłóceń w funkcjonowaniu infrastruktury państwa. U podstaw legło rozporządzenie wykonawcze z 26 marca 2019 roku³⁴, który ustanawia ramy dla skoordynowanego wzmacniania odporności narodowej wobec impulsów elektromagnetycznych (EMP), zarówno naturalnych, jak również sztucznych. Dokument definiuje istotne pojęcia, wśród których wyróżnić należy:

krytyczne usługi narodowe — funkcje rządu i sektora prywatnego o tak kluczowym znaczeniu dla Stanów Zjednoczonych, że ich zakłócenie, korupcja lub dysfunkcja miałyby destrukcyjny wpływ na [szeroko rozumiane] bezpieczeństwo, bezpieczeństwo gospodarcze kraju, zdrowie publiczne lub bezpieczeństwo narodowe, lub dowolną kombinację tych czynników³⁵;

³¹ S. Ricciardi, C. Souque, *Modern Electromagnetic Spectrum Battlefield From EMS Global Supremacy to Local Superiority*, „PRISM” 2021, Vol. 9, No. 3, s. 137.

³² M.G. Figueroa, D.D.H. Acevedo, D.S. Porta, *Geomagnetic disturbances and grid vulnerability: Correlating storm intensity with power system failures*, „PLOS One” 2025, Vol. 20, No. 7, s. 2–3, 11–12; И. Хатиб, Д. Денев, *Природни източници на радиация и тяхното въздействие върху електрониката*, [w:] *Радиационната безопасност в съвременния свят. Том 2*, Н. Долчинков (ред.), Велико Търново 2025, s. 186–189; X. Yanzhao, L. Minzhou, C. Yuhao, *Electromagnetic resilience of critical national infrastructure*, „High Power Laser and Particle Beams” 2019, No. 31(070001), s. 1–6; D. Wang, Y.L.P. Dehghanian, S. Wang, *Power Grid Resilience to Electromagnetic Pulse (EMP) Disturbances: A Literature Review*, [w:] *2019 North American power symposium (NAPS)*, [edycja grupowa przez:] Institute of Electrical and Electronics Engineers, Inc., Wichita 2019, s. 3.

³³ EMP — impuls elektromagnetyczny (ang. Electromagnetic Pulse).

³⁴ *Coordinating National Resilience to Electromagnetic Pulses*, Executive Order 13865, 26 March 2019, „Federal Register”, Vol. 84, No. 61.

³⁵ Oryg. “National Critical Functions” means the functions of government and the private sector →213

kluczowe usługi narodowe — nadrzędna odpowiedzialność Rządu Federalnego za kierowanie i utrzymanie Narodu przed, w trakcie i po katastrofalnym stanie nadzwyczajnym, takim jak impuls elektromagnetyczny (EMP), który negatywnie wpływa na funkcjonowanie Rządu³⁶.

Podobny podział zastosowany został również w europejskiej dyrektywie NIS2, omawianej w rozdziale 2. Choć ta skupia się na podmiotach (kluczowych i ważnych), to definiuje je przez pryzmat samych usług i funkcji³⁷. Dostrzec w tym można dość podobne podejście państw Zachodnich do sposobów kategoryzacji i priorytetyzacji w kontekście budowy bezpieczeństwa.

Przedmiotowe rozporządzenie wykonawcze nakłada obowiązki na poszczególne agencje federalne, przede wszystkim Departamenty Obrony³⁸, Bezpieczeństwa Wewnętrznego³⁹ oraz Energii⁴⁰. Centralnym celem jest stworzenie całościowej polityki obejmującej prognozowanie, ostrzeganie, badania i rozwój technologii ochronnych, a także współpracę z sektorem prywatnym i partnerami międzynarodowymi⁴¹. Rozporządzenie przewiduje harmonogram działań: identyfikację najbardziej narażonych systemów infrastruktury, opracowanie standardów i wskaźników pomiarów, wdrożenie programów pilotażowych oraz przygotowanie planów reagowania i odbudowy⁴². Całość ma charakter systemowy, łącząc dyplomację, obronę, energetykę, naukę i komunikację, a przy tym zakłada coroczne raportowanie postępów oraz ocenę luk w zdolnościach.

Rozporządzenie to porządkowało działania podjęte wcześniej przez CISA (za pośrednictwem różnych organów rządowych i w zakresie integracji modelowania ryzyka)⁴³, DoE⁴⁴ czy DHS⁴⁵. Opracowane dokumenty rozpoznają wysokie ryzyko HEMP dla sieci

so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof; tamże, s. 12041, sec. 2(c).

³⁶ Oryg. "National Essential Functions" means the overarching responsibilities of the Federal Government to lead and sustain the Nation before, during, and in the aftermath of a catastrophic emergency, such as an EMP that adversely affects the performance of Government; tamże, s. 12041, sec. 2(d).

³⁷ NIS2, załącznik I [sektory kluczowe], załącznik II [sektory ważne].

³⁸ *Coordinating National Resilience...*, s. 12042, sec. 5(b).

³⁹ Tamże, s. 12043, sec. 5(c).

⁴⁰ Tamże, s. 12043, sec. 5(d).

⁴¹ Tamże, s. 12041–12042, sec. 3(a, b).

⁴² Tamże, s. 12044–12046, sec. 6.

⁴³ Zob. NCC, *Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment*, [NCC/NCCIC v2.2], 2019;

⁴⁴ Zob. DoE, *Geomagnetic Disturbance Monitoring Approach and Implementation Strategies*, [DoE 20585], 2019.

⁴⁵ Zob. DHS, *Strategy for Protecting and Preparing the Homeland Against Threats of Electromagnetic Pulse and Geomagnetic Disturbances*, 9 October 2018.

energetycznej i proponują środki zmniejszające skutki (hardening, plany awaryjne, koordynacja z sektorem prywatnym). Równocześnie DoD⁴⁶ i inne agencje cywilne koncentrują się na ochronie bazy przemysłu obronnego i łańcuchów dostaw oprogramowania. Odzwierciedla to przekonanie, że systemowa degradacja cyberprzestrzeni często zaczyna się od naruszeń w firmach prywatnych oraz u dostawców krytycznych komponentów.

Należy jednak podkreślić, że zarówno przytoczone rozporządzenie wykonawcze, ani dokumenty wykonawcze programów agencji rządowych, nie nakładają na sektor prywatny silnych mechanizmów nacisku. Może to skutkować niewystarczającym lub zbyt powolnym wdrażaniem zaleceń, lub ich nieskutecznością przez często ogólnikowe zapisy. Zabrakło też spójnych wskaźników na poziomie federalnym, które pozwoliłyby ocenić skuteczność rozporządzenia. Jest to jedna z zasadniczych różnic między podejściem USA i UE, która z kolei jasno definiuje obowiązki oraz reperkusje za niedostosowanie się do nich. Na pozytywną ocenę zasługuje natomiast sam sposób budowy bezpieczeństwa przez odporność infrastruktury. Akceptuje się, że zapobieganie nie jest możliwe, dlatego agencje rządowe skupiają się na inwestowaniu w szybką detekcję, automatyczne mechanizmy izolacji i plany odtworzeniowe. To podejście minimalizuje szansę, że pojedynczy atak doprowadzi do systemowej destrukcji, choć nie eliminuje ryzyka skoordynowanych akcji łączących ataki cybernetyczne, oddziaływanie EMP z uderzeniami kinetycznymi (np. równoległe uderzenie w elektrownię i jej sterowniki).

Rosyjska doktryna wojskowa od lat uwzględnia możliwość użycia EMP jako narzędzia ofensywnego (w charakterze asymetrycznego oddziaływania na przeciwnika) i w takim zakresie jest badana przez Zachód⁴⁷. Jednakże w obszarze obrony własnej infrastruktury krytycznej widoczny jest brak konsekwencji i praktycznych rozwiązań. Strategiczne dokumenty państwowe koncentrują się raczej na cyberbezpieczeństwie oraz klasycznych zagrożeniach militarnych, marginalizując problem EMP. Z jednej strony rosyjskie siły zbrojne i służby interesują się bronią elektromagnetyczną w kontekście scenariuszy degradacji systemów przeciwnika⁴⁸, lecz sektor cywilny jest pozbawiony adekwatnych ram prawnych.

Literatura rosyjska dostrzega zagrożenie ze strony EMP dla infrastruktury elektrotechnicznej, zwłaszcza w sektorze energetycznym. Odnosi się ona głównie do braków

⁴⁶ Zob. DoD, *Defense Industrial Base Cybersecurity Strategy 2024*, 21 March 2024.

⁴⁷ P.V. Pry, *RUSSIA: EMP THREAT The Russian Federation's Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack*, [EMP TFNHS Report] 2021, s. 5–19.

⁴⁸ В.А. Иванов і inni, *Роль и место электромагнитного оружия при реализации наступательной стратегии в информационной специальной операции*, „Техника средств связи” 2022, № 3(159), s. 63–70.

doktrynalnych i strategicznych w obszarze obronnym, proponując wdrożenie wymogów dotyczących odporności na EMP, jak również opracowanie dokumentów regulacyjnych, ustawodawczych i prawnych dotyczących bezpieczeństwa energetycznego⁴⁹. Warto przy tym wspomnieć, że część źródeł czyni to przez analizę podejścia amerykańskiego⁵⁰. W tym zakresie interesującą jest propozycja wykorzystania obiektów testowych Rosatomu do oceny i poprawy odporności infrastruktury cywilnej⁵¹. Niemniej, formułowane wnioski są raczej propozycjami niż opisami istniejących, kompleksowych ram polityki.

Faktyczne wdrażanie działań zmierzających do zwiększenia odporności infrastruktury rosyjskiej wciąż jest obarczone licznymi problemami. Mimo wieloletnich badań i licznych raportów, infrastruktura cywilna pozostaje w praktyce niechroniona, a próby adaptacji rozwiązań wojskowych okazują się nieskuteczne⁵². W zamian obserwować można rozwój systemów balistycznych i kontenerowych (np. LORA), które mogą być użyte do generowania EMP, co wpisuje się w szerszą doktrynę odstraszania i asymetrycznego oddziaływania na przeciwnika⁵³. Rosja traktuje EMP jako narzędzie destabilizacji infrastruktury przeciwnika, a nie jako obszar ochrony własnej infrastruktury cywilnej, ta pozostaje w dużej mierze nieprzygotowana na skutki takiego ataku.

Chińska doktryna podkreśla koncepcję suwerenności w cyberprzestrzeni i traktuje infrastrukturę ICT jako główną sferę strategiczną. Rząd chiński kładzie nacisk na ochronę narodowych zasobów informacyjnych, budowę niezależnych łańcuchów technologicznych i integrację cywilno-wojskową w celu zapewnienia zdolności reagowania⁵⁴. Oficjalne białe księgi i ustawy⁵⁵ pokazują orientację na regulowanie i kontrolę środowi-

⁴⁹ В.И. Гуревич, *Электромагнитный импульс высотного ядерного взрыва и защита электрооборудования от него*, Москва 2019, s. 80–92. Н.Н. Шве́ц і inni, *Об энергетической безопасности России в условиях воздействия электромагнитного импульса высотного ядерного взрыва*, „Национальные интересы: приоритеты и безопасность” 2020, Т. 16, № 11, s. 2038–2040, 2050–2052; А.А. Двилянский, В.А. Иванов, М.Ю. Коньшев, *Эргооптимизация системы обеспечения функциональной устойчивости объектов критической информационной инфраструктуры в условиях деструктивного электромагнитного воздействия*, „Эргодизайн” 2021, № 2, s. 120–123.

⁵⁰ Zob. Е.П. Грабчак, Е.Л. Логинов, *Противодействие угрозам воздействия электромагнитного импульса: стратегические подходы к защите критической энергетической инфраструктуры в США*, „Сложные системы: модели, анализ и управление” 2021, № 2; А.В. Копылов і inni, *Взгляды военно-политического руководства США на защиту критически важных объектов от угроз кибернетического воздействия*, „Общество: политика, экономика, право” 2024, № 9.

⁵¹ Н.Н. Шве́ц і inni, *Об энергетической безопасности России...*, s. 2039–2040.

⁵² V. Gurevich, *A New Strategy is Needed to Solve the 50-Year Old Problem - EMP Protection of Critical Civilian Infrastructure*, „International Journal of Emerging Science and Engineering” 2014, Vol. 12, Issue 2, s. 10.

⁵³ Tamże, s. 6–8.

⁵⁴ C. Cheney, *China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism*, „Issues & Insights” 2019, Vol. 18, W.P. 8, s. 13, 20

⁵⁵ Zob. *The State Council Information Office of the People's Republic of China* [中华人民共和国 → 216

ska sieciowego oraz zwiększanie odporności samej infrastruktury. Jednocześnie chińskie programy defensywne w zakresie odporności na EMP⁵⁶ pozostają mniej transparentne niż analogiczne działania USA⁵⁷. Choć Chiny budują redundancję i izolacji infrastruktury, ochrona w skali cywilnej może pozostawać fragmentaryczna⁵⁸. Silny nacisk kładziony jest na sektory wojskowe i kluczowe systemy państwowe, podczas gdy zabezpieczenia infrastruktury komunalnej lub prywatnej są mniej systematyczne.

Chińskie podejście do ofensywnego wykorzystania EMP opiera się na traktowaniu go jako narzędzia strategicznego, zdolnego do paraliżowania infrastruktury przeciwnika w kluczowych momentach konfliktu⁵⁹. Zarazem dokumenty te odnoszą się głównie do impulsu wielkoskalowego: HEMP. W otwartych źródłach odnajdujemy plany Pekinu dotyczące użycia HEMP przeciwko Tajwanowi oraz amerykańskim lotniskowcom w cieśninie tajwańskiej⁶⁰, co wpisuje się w szerszą koncepcję odstraszenia i ograniczania zdolności interwencyjnych USA. Jednocześnie bliskość potencjalnych punktów zapalnych (Korei Północnej i Tajwanu) zwiększa ryzyko niezamierzonych skutków ubocznych dla samej Chin, jeśli jej infrastruktura krytyczna pozostanie niechroniona.

Choć wiedza o chińskich działaniach obronnych jest ograniczona, źródła wskazują na rozbudowaną sieć podziemnych tuneli i stanowisk dowodzenia⁶¹. Mają one chronić przede wszystkim wojskowe zasoby, zapewniając ciągłość operacji. W efekcie obraz chińskiej strategii HEMP jest asymetryczny: rozwój zdolności ofensywnych jest dobrze udokumentowany, natomiast ochrona cywilnej infrastruktury pozostaje niejasna i prawdopodobnie niedostateczna.

Porównanie podejść mocarstw do destrukcji środowiska sieciocentrycznego przy użyciu EMP ujawnia szereg różnic. USA (oraz inne państwa zachodnie w tym UE) stawiają silny nacisk na odporność systemów, zabezpieczenie łańcuchów dostaw ICT, czy

国务院新闻办公室], *China's Law-Based Cyberspace Governance in the New Era*, L. Mo (ed.), 16 March 2023.

⁵⁶ P. Chen i inni, *Low Cost and Sustainable Test Methods to Study Vulnerabilities of Large-Scale Systems against EMP*, „Sustainability” 2023, Vol. 15(320), s. 1–2.

⁵⁷ P.V. Pry, *China: EMP Threat. The People's Republic of China Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack*, 10 June, [TFNHS Report], 2020, s. 8–9.

⁵⁸ W. Qi i inni, *Non-nuclear electromagnetic pulse threat of critical infrastructures and protection strategies*, „Strategic Study of Chinese Academy of Engineering” 2022, Vol. 24, No. 4, s. 251–255.

⁵⁹ P.V. Pry, *China: EMP Threat...*, s. 9.

⁶⁰ N. Beauchamp-Mustafaga i inni, *Denial Witout Disaster. Keeping a US-China Conflict over Taiwan Under the Nuclear Threshold*, Santa Monica 2024, s. 28–29; L.M. Wortzel, *What the Chinese People's Liberation Army Can Do to Thwart the Army's Multi-Domain Task Force*, „Land Warfare” 2019, No. 126, s. 5.

⁶¹ W. Qiu, *Development and consideration of Chinese super-large diameter shield tunne*, „Archives of Civil Engineering” 2024, Vol. 70, Issue 1, s. 475–482; L.C. Russell-Hsiao, *China's Underground 'Great Wall' and Nuclear Deterrence*, „China Brief” 2009, Vol. 9, Issue 25, s. 1–2.

też szeroko rozumianą defensywę. Zarówno Moskwa jak i Pekin kładą duży nacisk na potencjał ofensywnego wykorzystania EMP, przy czym oba te państwa wykazują się pewnymi brakami w obszarze zabezpieczenia sektora prywatnego, stojąc w opozycji do podejścia Zachodniego. O ile w przypadku Rosji dostrzec można istotne braki, podnoszone w literaturze jako problem, to w przypadku Chin trudno mieć pewność co do skali rzekomego nieprzygotowania. Informacje o wojskowych wysiłkach w zakresie ochrony przed EMP wskazują, że kluczowe usługi państwa mogą pozostawać zabezpieczone adekwatnie do realnych zagrożeń i potrzeb utrzymania instytucji.

Niezależnie od przyjętego podejścia, powyższe każe sądzić, że ewentualna destrukcja cyberprzestrzeni najczęściej będzie miała charakter selektywny, kumulatywny i wielowektorowy. Trudno mówić o całkowitym zniszczeniu środowiska sieciocentrycznego, gdyż reperkusje byłyby odczuwalne tak przez ofiarę ataku, jak również samego agresora. Nie będzie nadużyciem stwierdzenie, że obecne *status quo* względem globalnego użycia EMP podobne jest do użycia broni nuklearnej w charakterze kinetycznym. Z tego względu spodziewać się należy raczej działań lokalnych, polegających na połączeniu kampanii cybernetycznych (ataki na kluczowe węzły, wykorzystanie podatności, utrzymanie dostępu), działań informacyjnych, wywoływania awarii wybranej infrastruktury ICT oraz działań kinetycznych. Dlatego tak istotne staje się ustanawianie szeroko rozumianej odporności systemów przez ich segmentację, redundancję oraz koordynację sektorów publicznego i prywatnego.

5.1.3. Granice prognozowania: epistemiczne trudności i potrzeba nowych modeli

Prognozowanie dynamiki konfliktów w cyberprzestrzeni natrafia na kilka rodzajów granic poznawczych, tj. ograniczeń w tym, co w praktyce można wiedzieć i w jaki sposób tę wiedzę wykorzystywać. Podsumowując analizy wynikające z poprzednich części niniejszej pracy, dostrzec można wielokrotnie pojawiające się problemy. Te zarówno dostrzegane są w literaturze, jak również natrafiano na nie w czasie prowadzenia badań do niniejszej dysertacji. Uwzględniając tę powtarzalność, przyjąć można następujące kategorie przedmiotowych problemów:

- niepełność danych,
- niemożliwa pełna atrybucja tożsamości uczestników działań w cyberprzestrzeni,
- tempo zmian wyzwań i szans przewyższające możliwości analityczne (oraz wnioskowanie z danych historycznych),
- stała heterogeniczność środowiska,

- relacja społeczno-technologiczna, umożliwiająca uzyskiwanie nieproporcjonalnych efektów względem włożonych wysiłków,
- głęboka asymetria podmiotów.

Pierwsza grupa trudności dotyczy w sposób ścisły charakteru dostępnych danych. Incydenty są często niejawne, raportowane selektywnie lub w ogóle utajniane; ofiary i firmy ukrywają szczegóły z obawy przed konsekwencjami wizerunkowymi lub prawnymi⁶². Brak pełnych, wiarygodnych i porównywalnych zbiorów danych uniemożliwia budowanie długookresowych statystyk, testowanie hipotez i walidację modeli prognostycznych. W efekcie nie jest to tylko problemem praktycznym, lecz metodologicznym. Bez systematycznych danych modelowanie staje się trudne, a jego wyniki mogą być łatwo kwestionowane.

Jednym z najczęściej napotykanym ograniczeń jest problem atrybucji. Nawet tam, gdzie zdarzenie jest dobrze udokumentowane technicznie, przypisanie odpowiedzialności sprawcy bywa obarczone wielowarstwową niepewnością. Analizy znacząco komplikują pośrednicy, działania pod fałszywą flagą, użycie publicznie dostępnych narzędzi oraz wieloetapowe łańcuchy kompromitacji. Rozwój modeli sztucznej inteligencji dodatkowo utrudnia przypisywanie sprawstwa. Modele generatywne umożliwiają tworzenie coraz bardziej zaawansowanych form automatyzacji, takich jak hiperpersonalizowane kampanie phishingowe (spear-phishing)⁶³. Działania dotychczas będące domeną zorganizowanych podmiotów, głównie inspirowanych przez państwa lub będących jego instytucjami, aktualnie stają się łatwo dostępne. Jest to o tyle istotne, że współczesne, złożone ataki nie wymagają nawet adekwatnego zestawu umiejętności od atakujących. Rozwój narzędzi przestępczych w charakterze usługi znacząco przyczynił się do zwiększenia skali ataków⁶⁴. Zarazem też utrudnił odróżnienie działań państwowych aktorów APT od małych grup przestępczych, czy nawet tzw. *samotnych wilków*. W efekcie wiele decyzji politycznych — jak reakcja retorsyjna czy zastosowanie sankcji — musi być po-

⁶² M. Mott i inni, „*There was a bit of PTSD every time I walked through the office door*”: Ransomware harms and the factors that influence the victim organisation's experience, „Journal of Cybersecurity” 2024, Vol. 10, No. 1, s. 3–4, 30–32; S. Schmitz-Berndt, *Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive*, „Journal of Cybersecurity” 2023, Vol. 9, No. 1, s. 1–2, 8; S. Perera, X. Jin, A. Maurushat, D.G.J. Opoku, *Factors Affecting Reputational Damage to Organisations Due to Cyberattacks*, „Informatics” 2022, Vol. 9, No. 28, s.5–6, 12–13.

⁶³ S. Yadav, *Social automation and APT attributions in national cybersecurity*, „Journal of Cyber Security Technology” 2024, Vol. 8, No. 4 s. 293–298.

⁶⁴ O. Smirnova, T.J. Holt, *Exploring and Estimating the Revenues of Cybercrime-As-Service Providers: Analyzing Booter and Stresser Services*, „Deviant Behavior” 2025, Vol. 46, No. 10, s. 1301–1302; O. Akinsuli, *The rise of AI-enhanced ransomware-as-a-service (RaaS): A new threat frontier*, „World Journal of Advanced Engineering Technology and Sciences” 2021, Vol. 1, No. 2, s. 88–93.

dejmowanych na podstawie prawdopodobieństw, a nie całkowitej pewności. Tworzy to komplikacje nie tylko operacyjne, lecz także normatywne: prawo międzynarodowe i doktryny odstraszania były projektowane z myślą o jasnej identyfikacji podmiotu agresji⁶⁵. W warunkach rozproszonego i ukrytego sprawstwa fundament ten zostaje naruszony.

Problemem jest także dynamika rozwoju technologii. W przeciwieństwie do materiałów i systemów kinetycznych, cykle innowacji w dziedzinie oprogramowania, algorytmów oraz urządzeń są ekstremalnie szybkie. Pojawienie się nowych narzędzi wykorzystujących podatność, czy nowej techniki unikania detekcji, może zmienić krajobraz ryzyka w ciągu kilku miesięcy⁶⁶. To powoduje, że modele przewidywania oparte na historycznych trendach są narażone na nagłą zmianę warunków, po której wcześniejsze zależności tracą ważność. W praktyce prognozy muszą być więc projektowane jako adaptacyjne: nie jednorazowy produkt analityczny, lecz proces ciągłej rekalkulacji wobec nowych danych i sygnałów technologicznych⁶⁷. W tym zakresie narzędzia wykorzystujące uczenie maszynowe i modele sztucznej inteligencji wykazują się wyższą skutecznością niż klasyczne podejście do przewidywania zagrożeń⁶⁸. Z drugiej jednak strony, takie podejście wciąż pozostaje selektywne (tj. wąski sposób wdrożenia), a ponadto brakuje uniwersalnych i szerzej zaadaptowanych modeli predykcyjnych.

Czwarty problem to heterogeniczność architektur. Internet rzeczy (IoT) w dużej części indywidualnych rozwiązań, systemy SCADA w przemyśle, chmury publiczne oraz prywatne centra danych, tworzą mozaikę środowisk o odmiennych parametrach ryzyka i dynamikach awarii. Europejska ENISA, amerykańska CISA oraz inne instytucje wskazu-

⁶⁵ N. Tsagourias, *Cyber Attribution Agencies: A Sceptical View*, „QIL Zoom In” 2024, No. 106, s. 24–26, 36–37.

⁶⁶ Przykładem może być rozwój Banshee, oprogramowania wykradającego dane z urządzeń Apple, udostępnionego w formie usługi. Jednym z etapów jego dynamicznego rozwoju było przejście kryptografii Xprotect, wbudowanej w macOS platformy antywirusowej. W efekcie oprogramowanie to mogło się podszywać pod procesy systemowe i działać w sposób niezauważony. Wzrost popularności tego złośliwego oprogramowania, problemy z udostępnieniem usługi oraz rozwój o nowe możliwości kryptograficzne nastąpił w ostatnim kwartale 2024 roku. Proces był dynamiczny, a analizy powalające lepiej zrozumieć obraz zagrożenia pojawiły się dopiero w pierwszym kwartale 2025 roku; UAE Cyber Security Council, *Banshee Stealer Targets macOS Users*, [432316724], 2025, s. 1–2; A. Terefos, *Banshee: The Stealer That “Stole Code” From MacOS XProtect*, „Check Point Research” 9 January 2025, <https://research.checkpoint.com/2025/banshee-macos-stealer-that-stole-code-from-macos-xprotect/#single-post> [odczyt: 11.09.2025].

⁶⁷ R.H. Chowdhury, N.U. Prince, S.M. Abdullah, L.A. Mim, *The role of predictive analytics in cybersecurity: Detecting and preventing threats*, „World Journal of Advanced Research and Reviews” 2024, Vol. 23, No. 2, s. 1619–1620.

⁶⁸ S.R.P. Dandamudi, J. Sajja, A. Khanna, *Advancing Cybersecurity and Data Networking Through Machine Learning-Driven Prediction Models*, „International Journal of Innovative Research in Computer Science and Technology” 2025, Vol. 13, Issue 1, s. 28–29; S.I. Rishad, *Leveraging AI and Machine Learning for Predicting, Detecting, and Mitigating Cybersecurity Threats: A Comparative Study of Advanced Models*, „International Journal of Science & Information System” 2025, Vol. 10, Issue 1, s. 15–18.

ją⁶⁹, że podatności jednego obszaru (np. IoT) mogą przyspieszyć eskalację ataku, przenosząc go do warstw o większym oddziaływaniu skutków. Różnorodność ta może stanowić istotne ograniczenie dla uniwersalności modeli analitycznych. Strategia lub metodyka badań wykazująca się efektywnością w jednym kraju, sektorze czy sieci, w innym miejscu lub obszarze może okazać się mało przydatna, albo wprost myląca. Wydaje się zatem, że słuszne może być podejście modułowe lub ramowe. Pozwalałoby ono wytworzyć zestaw narzędzi i kryteriów, które następnie dawałoby się dopasować do lokalnej architektury i zagrożeń⁷⁰. Tym co odróżniałoby je od podejścia zupełnie indywidualnego, byłyby wspólne ramy, zapewniające bardziej przewidywalną metodykę, a być może względnie porównywalne pomiary.

Istotną granicą możliwości analitycznych jest interakcja między technicznym oraz społecznym wymiarem poruszanej problematyki. Skutki incydentów cybernetycznych wprost zależą od reakcji społecznej, politycznej i rynkowej. Wywołana reperkusjami dezinformacja i/lub panika, czy następcze decyzje operatorów krytycznych systemów i reakcje rządów, mogą wzmocnić lub osłabić pierwotny efekt techniczny ataku.

Ma to szczególne znaczenie w kontekście asymetrii wpływu między państwami autorytarnymi i demokratycznymi, którą omówiono we wcześniejszej części dysertacji. Wnioskiem płynącym z ustaleń było stwierdzenie, iż przez spowszechnienie ścisłego nadzoru, politycznej cenzury lub innych ograniczeń (w tym odcinania dostępów w cyberprzestrzeni), dużo trudniej jest wywierać wpływ na społeczeństwa państw takich jak Chiny czy Rosja. Z kolei wysoka wartość przypisywana szeroko rozumianej wolności w demokracjach sprawia, że wszelkie formy kontroli nad zewnętrznym wpływem mogą być postrzegane jako wrogie działania własnego państwa, tym samym tylko wzmacniając zmanipulowany przekaz. Problemy w negatywnej reakcji społecznej zwiększa również coraz powszechniejsza polaryzacja i wzrastający populizm⁷¹. Choć umożliwia on polity-

⁶⁹ ENISA, *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*, Brussels 2017, s. 36–56; C. Skouloudi, A. Malatras, R. Naydenov, G. Dede, *Guidelines for Securing the Internet of Things. Secure supply chain for IoT*, Brussels 2020, s. 18–23; CISA, FBI, *Product Security Bad Practices*, [Joint Guidance v2.0], 2025, s. 3–8; EG-CERT, NTRA [arab. الجهاز القومي لتنظيم الاتصالات], *IOT Cyber Security Framework*, [EG-CESC-OPER 100-01 DP-2210-EN], 2022, s. 11, 20–27.

⁷⁰ N. Chowdhury, S. Katsikas, V. Gkioulos, *Modeling effective cybersecurity training frameworks: A delphi method-based study*, „Computers & Security” 2022, No. 113(102551), s. 5–6.

⁷¹ T. Lochocki, *The Rise of Populism in Western Europe. A Media Analysis on Failed Political Messaging*, Berlin 2018, s. 11–12, 69–70, 149; A. Hristova, *Populism: A Basis for Polarization Processes in Society*, [w:] *Social Response to Polycrisis: The Case of Bulgaria*, A. Hristova (ed.), New York 2024, s. 88–91; F. Gonthier, *How party polarisation exacerbates the link between democratic deficit and populist voting: evidence from Europe*, „West European Politics” 2025, Vol. 49, No. 1, s. 81–84.

kom silniejsze oddziaływanie, to w dłuższej perspektywie utrudnia on skuteczną reakcję na cyberincydenty, niejako zaciągając dług.

Wykazało to m.in. badanie odporności na dezinformację online⁷². Czynnikiem znacząco zwiększającym odporność społeczną są: niski poziom populizmu oraz polaryzacji, budowanie zaufania do mediów przy silnym udziale publicznych nadawców, jak również relatywnie małe rynki medialne i mniej powszechne wykorzystanie mediów społecznościowych⁷³. Wyniki innego badania — czy komunikowanie niepewności epistemicznej co do faktów w różnych tematach, formatach i wielkościach wpływa na zaufanie publiczne⁷⁴ — uzupełniają powyższe. Wskazują m.in., że kluczowymi cechami są uczciwość oraz transparentność w komunikatach, np. względem zagrożeń hybrydowych, przy braku dowodów w danym momencie, czy wobec niepełnego obrazu sytuacji. Zarazem badanie to podkreśla, iż skuteczniejsze jest wykazywanie prawdopodobieństwa liczbowego (prezentacja konkretnych danych) niż ich lingwistyczny opis⁷⁵. Zarazem jednak nawet najbardziej przejrzyste strategie informacyjne nie będą skuteczne, jeśli instytucje nie cieszą się legitymizacją⁷⁶, szczególnie w kontekście demokracji dających przestrzeń do otwartych debat. Stąd potrzebna jest strategiczne podejście do komunikacji, tj. mające elementy dobrowolnego zaangażowania oraz bezwarunkowego przyjęcia odpowiedzialności, jak również ciągłej adaptacji i elastyczności⁷⁷. Oznacza to konieczność zastosowania zróżnicowanych, choć konwergentnych podejść, uwzględniających: monitorowanie i wczesne wykrywanie zdarzeń, koordynację szybkiej odpowiedzi oraz budowę społecznego zaufania i jedności (m.in. w zakresie komunikowania interesu narodowego)⁷⁸.

A zatem analityka i prognozowanie czysto techniczne, pozbawione modelowania reakcji społeczno-politycznych (lub choćby ich uwzględnienia) skutkować może iluzorycznymi wynikami. Sposób informowania o zdarzeniu w cyberprzestrzeni winien bowiem leżeć tak samo mocno w interesie państwa, jak technologiczno-organizacyjna re-

⁷² E. Humprecht, F. Esser, P. Van Aelst, *Resilience to Online Disinformation: A Framework for Cross-National Comparative Research*, „The International Journal of Press/Politics” 2020, Vol. 25, No. 3, s. 496–499.

⁷³ Tamże, s. 502, 505.

⁷⁴ A.M. Van der Bles i inni, *The effects of communicating uncertainty on public trust in facts and numbers*. „Proceedings of the National academy of Sciences of the USA” 2020, Vol. 117, No. 14, s. 7672.

⁷⁵ Tamże, s. 7679–7680.

⁷⁶ N. Van Raemdonck, T. Meyer, *Why Disinformation is Here to Stay. A Socio-technical Analysis of Disinformation as a Hybrid Threat*, [w:] *Addressing Hybrid Threats: European Law and Policies*, L. Lonardo (ed.), Cheltenham 2024, s. 60.

⁷⁷ E. Mârzac, *Strategic Communication as a Tool for Countering Hybrid Threats. A Focus on National Resilience and Public Trust*, „Studia Securitatis” 2024, No. 2, s. 58.

⁷⁸ Tamże, s. 58–61.

akcja⁷⁹. Oznacza to zachowanie wysokiej interdyscyplinarności w rozważaniach nad działaniami w cyberprzestrzeni oraz ich opisem, która choć jest trudna, to pozostaje niezbędną. W praktyce wymagane jest zatem łączenie inżynieryjne (np. scenariusze uszkodzeń) z modelami zachowań (np. jak operatorzy reagują na alarmy, jak media rozprzestrzeniają narracje). Taka interdyscyplinarność jest trudna, ale niezbędna.

Nie można też pominąć ograniczeń wynikających z asymetrii ekonomicznej. Ataki w cyberprzestrzeni są z reguły opłacalne przy niskim koszcie wejścia i wysokiej stopie (np. ransomware)⁸⁰. Zmienia to przewidywania prawdopodobieństwa zdarzeń: wiele incydentów wynika nie z geopolitycznej kalkulacji państw, lecz z prostych motywów zysku. Dlatego prognozy i modele⁸¹ nie mogą koncentrować się wyłącznie na scenariuszach relacji międzynarodowych, lecz integrować dane ekonomiczne i motywacyjne aktorów poza państwowymi, zarówno przestępczych, jak i ideologicznych.

Z powyższego wynikają konsekwencje metodologiczne i praktyczne. Po pierwsze: modele analizy zagrożeń w cyberprzestrzeni powinny być probabilistyczne i hierarchiczne. Rozumieć przez to należy, że wymagane jest korelowanie prawdopodobieństw i zagrożeń na różnych szczeblach istotności oraz z założeniem różnych scenariuszy reperkusji. Ponadto monitoring zdarzeń musi być heterogeniczny, łączący telemetryczne wskaźniki technologiczne, sygnały ekonomiczne, a także wskaźniki informacyjne (z silnym uwzględnieniem reakcji społecznych). Co najistotniejsze, wszelkie analizy, wynikające z nich wnioski i plany winny być możliwie stale ćwiczone i testowane na szczeblu międzypodmiotowym (między państwami, ich różnymi instytucjami, czy pomiędzy sektorem publicznym i prywatnym). Przykładem takich praktyk są podręczniki publikowane przez amerykańską CISA, łączące operacyjne procedury z danymi do walidacji reakcji⁸². Analogiczne mechanizmy powinny powstać na poziomie strategicznym.

Nieprzewidywalność nie usprawiedliwia jednak paraliżu. Przyjęcie paradygmatu stałej niepewności nie oznacza rezygnacji z działania, lecz porzucenie iluzji, że możliwe jest skuteczne przewidywanie kompleksowego stanu przyszłego. W praktyce wiąże się to

⁷⁹ P.W. Singer, A. Friedman, *Cybersecurity and Cyberwar. What everyone needs to know*, Oxford 2014, s. 15–17.

⁸⁰ M. Plachkinova, A. Vo, *A Taxonomy of Cyberattacks against Critical Infrastructure*, „Journal of Cybersecurity Education, Research and Practice” 2022, Vol. 2021, No. 2(3), s. 6–7.

⁸¹ Zob. L. González-Manzano, *Identifying Key Relationships between Nation-State Cyberattacks and Geopolitical and Economic Factors: A Model*, „Security and Communication Networks” 2022, No. 1.

⁸² Zob. CISA, *Cybersecurity Incident & Vulnerability Response Playbooks. Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems*, Rosslyn 2021; FBI, CISA, ASD, ACSC, *#StopRansomware: Play Ransomware*, [AA23-352A], 2025.

z budową elastycznych ram decyzji, definiujących jakie środki podjąć przy różnych poziomach dowodów i skutków. Przyjęcie takiego mechanizmu pozwoliłoby scalić prewencję, detekcję i odporność w spójną politykę operacyjną, zamiast koncentrować się tylko na zapobieganiu. Podkreślić należy, że warunkiem skuteczności takich rozwiązań wydają się być interoperacyjność i transparentność informacji. Wymaga to zobowiązań międzyrządowych i publiczno-prywatnych do dzielenia się danymi na temat zdarzeń i incydentów w spójnym systemie cyberbezpieczeństwa. Bez tego każdy model prognostyczny lub analityczny mierzyłby się z empirycznymi ograniczeniami.

5.2 Probabilistyczne modelowanie ryzyka w konfliktach cyfrowych

Dynamiczny charakter współczesnych i przyszłych zagrożeń cyfrowych sprawia, że tradycyjne, statyczne ujęcia ryzyka przestają być wystarczające. Rosnąca liczba nieznanymi zmiennymi, jak również powyżej wskazane problemy, wymuszają stosowanie podejść, które dają zdolność operowania w warunkach stałej niepewności. W tym kontekście probabilistyczne modelowanie ryzyka staje się narzędziem pozwalającym osadzić analizę w realistycznym, statystycznie opisanym horyzoncie możliwych scenariuszy, zamiast arbitralnych klasyfikacji ujęć determinowanych⁸³. Tego rodzaju modele teoretyczne i analityczne, jak wcześniej wskazano, często są reaktywne⁸⁴. Opierają się na obserwacji przeszłych lub względnie bieżących działań, starając się zdefiniować je, opisać i wskazać możliwe reakcje. Jednakże duża bezwładność procesu — od obserwacji, przez analizę i syntezę, po proces publikacji wyników i ich ewentualnego wdrażania — jest nieprzystająca do dynamiki cyberprzestrzeni. Z kolei proponowane ujęcie probabilistyczne umożliwia uwzględnienie zarówno zdarzeń rzadkich, jak i tych, dla których dostępne są jedynie częściowe informacje, oraz uwzględnia stopniowo aktualizowane dane empiryczne. Ocena prawdopodobieństwa najlepiej też odpowiada na wyzwania stałej niepewności⁸⁵, będącej obrazem wyłaniającym się z niniejszych badań.

⁸³ R.C. Swallow, *Considering the cost of cyber warfare: advancing cyber warfare analytics to better assess tradeoffs in system destruction warfare*, „Journal of Defense Modeling and Simulation: Applications, Methodology, Technology” 2023, Vol. 20, No. 1, s. 11–15; S.N. Hamilton, W.L. Hamilton, *Adversary Modeling and Simulation in Cyber Warfare*, [w:] *Proceedings of the IFIP TC 11 23rd International Information Security Conference*, S. Jajodia, P. Samarati, S. Cimato (eds.), Milano 2008, s. 466, 472.

⁸⁴ D. Hughes, A. Colarik, *The Hierarchy of Cyber War Definitions*, [w:] *Intelligence and Security Informatics*, G.A. Wang, M. Chau, H. Chen (eds.), Jeju 2017, s. 15–20.

⁸⁵ S. Topor, *The Future of Warfare in the Volatility, Uncertainty, Complexity and Ambiguity Context*, „Land Forces Academy Review” 2024, Vol. 29, No. 2(114), s. 230–231, 234.

Kluczową cechą proponowanej architektury jest jej rekurencyjność, dzięki której ocena ryzyka może być prowadzona jednocześnie na wielu poziomach: strategicznym, operacyjnym i taktycznym, czy w wybranych jej obszarach. Pozwala to na odwzorowanie realnej struktury bezpieczeństwa cyfrowego, gdzie każde zagrożenie przenika przez różne poziomy i części systemu, a jego ostateczny efekt wynika z kombinacji podatności na każdym z nich. Ryzyko na poziomie państwa jest zatem funkcją ryzyk częściowych i organizacyjnych, czyli ryzyk poszczególnych usług i zasobów (w tym podmiotów państwa i sektora prywatnego). Każde z tych ryzyk może być obliczane osobno, stosując spójną metodologię, lecz mniejszymi, bardziej precyzyjnymi zestawami danych. Wynik takiego obliczenia może z kolei stać się daną wejściową do modelowania na wyższym poziomie. Taka struktura tworzy model skalowalny, możliwy do aplikowania na różnych szczeblach działalności państwa.

Ważnym elementem jest również adaptacyjność — możliwość aktualizacji ocen wraz z pojawianiem się nowych obserwacji. Istotnym okazało się włączenie możliwości oceny prawdopodobieństwa wstępnego, zgodnie z podejściem Bayesa⁸⁶. Dzięki niemu możliwe staje się stałe uaktualnianie ocen w oparciu o dane telemetryczne, incydenty, sygnały wywiadowcze czy ogólny obraz cyberbezpieczeństwa. Dzięki temu model nie jest jednorazowym pomiarem, lecz procesem ciągłym, który zmienia się wraz z sytuacją strategiczną i operacyjną. Co szczególnie istotne, pozwala to uchwycić nie tylko poziom zagrożeń, ale także tempo ich ewolucji, co w środowisku cybernetycznym stanowi krytyczny parametr decyzyjny. Włączenie twierdzenia Bayesa stanowi tutaj element osadzający zaproponowany model w określonym kontekście, czyniąc potencjalną analizę mniej syntetyczną.

Ostatecznie, zaproponowana w dalszej części konstrukcja modelu ryzyka umożliwia integrację informacji jakościowych i ilościowych, tworząc przestrzeń analityczną, w której dane techniczne (np. luki bezpieczeństwa, telemetryczne sygnały ataku), operacyjne (czas reakcji, redundancja zasobów) i strategiczne (motywacje aktorów, napięcia geopolityczne, aspekty społeczne) składają się na jedną, spójną ocenę. Takie podejście pozwala na racjonalizację procesu decyzyjnego: priorytetyzację ochrony, alokację zasobów i określenie, które obszary wymagają wzmocnienia, zanim staną się celem ataku. W tym sensie model probabilistyczny nie obiecuje pełnej przewidywalności. Zamiast te-

⁸⁶ Zob. S. Mouti i inni, *Cyber Security Risk management with attack detection frameworks using multi connect variational auto-encoder with probabilistic Bayesian networks*, „Computers and Electrical Engineering” 2022, Vol. 103, s. 4–5.

go dostarcza struktury do działania w warunkach niepewności, co jest niezbędne wobec charakteru przyszłych konfliktów cyfrowych.

5.2.1. Architektura proponowanego modelu oceny ryzyka

Proponowany model opiera się na trzech fundamentach (1) analizie prawdopodobieństwa, z uwzględnieniem wstępnej jego oceny zgodnie z twierdzeniem Bayesa, (2) rekurencyjnej strukturze warstwowej oraz (3) integracji danych heterogenicznych. Jego celem jest stworzenie jednolitych ram analitycznych, które pozwalałyby obliczać ryzyko zarówno na poziomie pojedynczego systemu, jak i całego państwa, przy zachowaniu metodologicznej spójności. Architektura została zaprojektowana w sposób modułowy, aby poszczególne komponenty można było zastępować innymi, zgodnie z dostępnością danych lub specyfiką analizowanego środowiska.

Ze względu na potencjalne wykorzystanie informacji źródłowych pochodzących z systemów informatycznych lub innych modeli (w ramach działań organizacyjnych, ocen społecznych, itd.), w identyfikatorach wartości przyjęto nomenklaturę angielską.

Model posługuje się trzema podstawowymi wielkościami:

- i) Prawdopodobieństwo zagrożenia (threat, T) — oceniane jako wartość probabilistyczna $P(T)$, odnosząca się do prawdopodobieństwa wystąpienia zdarzenia powodującego zagrożenie. W uproszczonej wersji może być oceniane indywidualnie lub z uwzględnieniem bayesowskiego modułu probabilistycznego (opisanego w dalszej części).
- j) Ekspozycja (exposure, E) — poziom podatności zasobu lub systemu na skutki danego zagrożenia. Wartość ta wynika ze szczegółowych miar technicznych (np. liczba krytycznych podatności), organizacyjnych (np. procedury awaryjne, dojrzałość i stopień świadomości zagrożeń), architektonicznych (redundancja, segmentacja) oraz społecznych (kompetencje operatorów).
- k) Wartość konsekwencji (consequence impact, CI) — szacowana jako potencjalna strata (operacyjna, ekonomiczna, społeczna lub strategiczna).

Na podstawie powyższego, ryzyko definiuje się jako:

$$R = P(T) \times E \times CI$$

Jednak w odróżnieniu od klasycznych ujęć, tutaj każdy z tych elementów może być obliczany ponownie w warstwach podrzędnych, a wynik wyższej warstwy stanowi funkcję ryzyk warstw niższych. Architektura modelu zakłada trzy poziomy analityczne:

- d) Poziom taktyczny — analiza ryzyka dla pojedynczych systemów, usług, komponentów technicznych lub procesów operacyjnych. Dane wejściowe: skany podatności, analiza logów, dane telemetryczne, statystyki incydentów.
- e) Poziom operacyjny — agregacja ryzyka dla organizacji, sektora infrastruktury lub klas usług cyfrowych. Dane wejściowe: raporty, oceny audytowe, analizy sektorowe, dane o zdolności reakcji.
- f) Poziom strategiczny — ocena dla państwa, koalicji lub kluczowych domen infrastrukturalnych. Dane wejściowe: dane wywiadowcze, oceny zagrożeń państwowych, analiza geopolityki, dane makroekonomiczne.

Rekurencyjne obliczanie ryzyka wygląda następująco:

$$R_n = f(R_{n-1,1}, R_{n-1,2}, \dots, R_{n-1,k})$$

gdzie:

- e) R_n — ryzyko warstwy wyższej,
- f) $R_{n-1,i}$ — ryzyko komponentu składowego warstwy niższej,
- g) funkcja agregacji f może być sumą ważoną, medianą ważoną, maksimum znormalizowanym lub funkcją nieliniową.

W modelu rekurencyjnym funkcja agregacji f określa sposób, w jaki ryzyka niższych warstw (np. systemów, komponentów, procesów) są łączone w wynik dla warstwy wyższej (np. organizacji, sektora, państwa). Wybór ten nie może być arbitralny i musi odpowiadać strukturze zależności, charakterystyce infrastruktury oraz profilowi zagrożeń.

- d) Suma ważona — ryzyko warstwy wyższej jest sumą ryzyk elementów niższych, przemnożonych przez ich względne wag. Stosowana, gdy elementy warstwy są częściowo substytucyjne, gdy ryzyko jest rozproszone równomiernie lub gdy awaria pojedynczego elementu nie powoduje katastrofalnej utraty całej funkcji.
- e) Mediana ważona — ryzyko wyższej warstwy to wartość środkowa, po uwzględnieniu wag dla każdego elementu. Jest to funkcja odporna na wartości skrajne, stosowana, gdy zachodzi konieczność uniknięcia dominacji ekstremalnie wysokich lub niskich wartości, gdy architektura jest modularna i redundancja zmniejsza podatność na pojedynczy punkt awarii, lub w analizach strategicznych, gdzie dane są obarczone dużą niepewnością.
- f) Maksimum znormalizowane — ryzyko wyższej warstwy jest determinowane przez element o najwyższym ryzyku, po znormalizowaniu go względem jego znaczenia. Podejście to jest szczególnie przydatne, gdy architektura ma punkty kry-

tyczne (tzw. pojedyncze punkty awarii lub wąskie gardła), lub gdy nawet lokalna awaria może wywołać kaskadowy kolaps systemu (np. w sektorach ICS/SCADA).

- g) Funkcja nieliniowa — stosowana jest, gdy system ma złożone zależności (np. sieć energetyczna, łańcuchy dostaw), lub gdy istnieją silne zależności między elementami, w analizie ryzyka systemowego i kaskadowego. Sugerowane są funkcje:
- a) multiplikatywna, stosowana tam, gdzie ryzyka wzmacniają się wzajemnie (kumulacja z efektem synergii),
 - b) logistyczna, wykorzystywana do modelowania efektów progowych,
 - c) kaskadowa, opisująca prawdopodobieństwo przejścia z fazy stabilnej do niestabilnej.

Funkcja agregacji f nie jest jedynie operacją matematyczną, lecz stanowi odzwierciedlenie struktury logicznej i technicznej analizowanego systemu. To właśnie dobór odpowiedniej funkcji pozwala utrzymać zgodność modelu z realnym charakterem badanej infrastruktury i uniknąć uproszczeń, które zniekształcają wynik.

5.2.2. Moduł probabilistyczny — osadzenie analizy w kontekście sytuacji bieżącej

Moduł probabilistyczny jest centralnym elementem proponowanego modelu, ponieważ pozwala przekształcić dane jakościowe, ilościowe oraz niepełne w spójną strukturę oceny ryzyka. W przeciwieństwie do klasycznych metod punktowych, które traktują ryzyko jako czystą funkcję *prawdopodobieństwo* $\times$ *skutek*, moduł ten pracuje na rozkładach prawdopodobieństwa, aktualizowanych wraz z napływem danych. Moduł ten pełni w modelu trzy funkcje, umożliwiając: skuteczniejsze szacowanie, ciągłą aktualizację oraz fuzję probabilistyczną.

Prawdopodobieństwo wstępne $P(H)$, będące kluczowym elementem przedmiotowego modułu, odzwierciedla stan wiedzy o zagrożeniu *przed* obserwacją bieżących sygnałów. W kontekście działań w cyberprzestrzeni nie jest to jedynie historycznym uśrednieniem zdarzeń, lecz obejmuje:

- g) statystyki incydentów z wielu lat (np. dane ENISA, CISA),
- h) sygnalizowane kierunki działań przeciwników (raporty służb wywiadowczych, raporty NSA/CISA/FBI, dane z zespołów CERT i CSIRT),
- i) wiedzę ekspercką,
- j) parametry kontekstowe, takie jak: globalne napięcia geopolityczne, sezonowość ataków, czy sektor działalności.

Uwzględnienie wszystkich tych czynników pozwala minimalizować szum informacyjny, szczególnie w środowisku sieciocentrycznym, mierzącym się z problemem fał-

szywych alarmów, utrudnionej atrybucji, błędów systemowych i konfiguracyjnych, dających fałszywe objawy ataków czy ataków niewykrytych. W praktyce oznacza to, że Po zaobserwowaniu sygnału diagnostycznego D (np. wzrostu wrogich działań) prawdopodobieństwo wstępne aktualizuje się zgodnie z twierdzeniem Bayesa:

$$P(H \vee D) = \frac{P(D/H) \times P(H)}{P(D)}$$

gdzie:

- $P(H \vee D)$ — prawdopodobieństwo warunkowe, czyli prawdopodobieństwo zajścia zdarzenia H , jeżeli zachodzi zdarzenie D ,
- $P(H)$ — prawdopodobieństwo wstępne, że zagrożenie H jest aktywne,
- $P(D \vee H)$ — prawdopodobieństwo zaobserwowania sygnału D , jeśli H faktycznie zachodzi (np. jak często grupa APT przed atakiem wykonuje rekonesans),
- $P(D)$ — normalizator, uwzględniający wszystkie możliwe scenariusze generujące obserwację.

W praktyce zatem najpierw należy ustalić prawdopodobieństwo wstępne, np. na podstawie raportów *threat intelligence*, raportów aktywności z systemów, kontekstu geopolitycznego i atrakcyjności celu dla grup przestępczych. Przyjmijmy, że w przykładzie istnieje 10% szans, że grupy APT prowadzi przygotowania do operacji dla mierzonego obszaru, co jest wypadkową trendów i wzorców aktywności takich grup. Zatem $P(H)=0.10$. Obserwujemy jednak sygnał mogący świadczyć o działalności grupy, np. wykryto skany portów pochodzące z infrastruktury, która we wcześniejszych kampaniach była celem działań grup APT. W takich wypadkach często trudno jest odróżnić faktyczny atak od ruchu automatycznego, czy skryptów botnetów, a zatem jest to *sygnał niejednoznaczny*. Przy użyciu analizy TTP⁸⁷ ustalamy, że jeżeli grupa APT faktycznie przygotowuje operację, to takie sygnały obserwujemy w 70% przypadków, a zatem $P(D \vee H)=0.70$. Zarazem warto też oszacować wysokość prawdopodobieństwa, że skany portów wystąpią nawet jeśli APT nie przygotowuje operacji, gdyż infrastruktura w internecie jest skanowana niemalże w sposób stały. Dlatego założmy, że na podstawie telmetrii danych systemów, prawdopodobieństwo, że dla sygnału D , H nie jest działaniem

⁸⁷ Analiza Tactics, Techniques and Procedures (TTP) — systematyczne badanie wzorców działań przeciwnika, obejmujących taktyki (ogólne sposoby prowadzenia operacji), techniki (konkretne metody realizacji zadań) oraz procedury (utrwalone sekwencje czynności). Celem tej analizy jest identyfikacja powtarzalnych schematów, które umożliwiają przewidywanie zachowań, ocenę zdolności operacyjnych oraz opracowanie skutecznych środków przeciwdziałania; zob. G. Leigh, *Cyber Security Operations: Tactics, Techniques, and Procedures*, [w:] *The Handbook of Homeland Security*, S.N. Romaniuk, M.S. Catino, C.A. Martin (eds.), Milton 2023.

grupy APT (oznaczane jako $\neg H$) wynosi 15%, a zatem $P(D \vee \neg H) = 0.15$. Zgodnie z przyjętym modelem, będzie to:

$$P(H \vee D) = \frac{P(D \vee H) \times P(H)}{P(D \vee H) \times P(H) + P(D \vee \neg H)(1 - P(H))}$$

Podstawiając powyższe wartości, uzyskujemy:

$$P(H \vee D) = \frac{0.70 \times 0.10}{0.70 \times 0.1 + 0.15 \times 0.9} = \frac{0.07}{0.07 + 0.135} = \frac{0.07}{0.205} \approx 0.341$$

A zatem prawdopodobieństwo faktycznego ataku grupy APT wynosi 34%, gdzie informacja płynąca z samego sygnału, bez uwzględnienia prawdopodobieństwa wstępnego, wynosiłaby 70%, lecz zarazem jest to wartość ok. trzykrotnie wyższa niż przyjęte prawdopodobieństwo wstępne. Wynikiem jest stwierdzenie, iż zdarzenie to nie przesądza o ataku, lecz wskazuje na wzrost możliwego zagrożenia. Dzięki temu obliczone prawdopodobieństwo końcowe (34%) może stać się nowym prawdopodobieństwem wstępnym, osadzając reakcję na kolejne incydenty w nowym, zaktualizowanym kontekście.

5.2.3. Zmienne, metryki i skalowanie ryzyka w proponowanym modelu

Kluczowym elementem proponowanego modelu jest precyzyjne zdefiniowanie zmiennych wejściowych, ich relacji oraz sposobu kwantyfikacji. Dlatego każdy z proponowanych czynników głównego wzoru ($R = P(T) \times E \times CI$) podzielono na zestaw mierzalnych zmiennych, których wartości są skalowane w przedziale 0–1.

Składnik prawdopodobieństwa zdarzenia $P(T)$ powinien być obliczany modelem probabilistycznym. Szacowanie prawdopodobieństwa wstępnego powinno się odbywać przez ocenę: intencji (intent — I), zdolności (capability — C) oraz możliwości (opportunity — O). Dalej w modelu probabilistycznym wykorzystać można zbiór danych obserwowanych (technicznych i kontekstowych — D). Zarazem w modelu uwzględniono opcjonalne wagi w_x , pozwalające odzwierciedlić hierarchię czynników i dynamicznie kalibrować model do zastanej sytuacji, przy czym $w_1 + w_2 + w_3 = 1$.

$$P(T) = f(I, C, O \vee D)$$

Wskaźnik intencji, świadczący o motywacji do ataku, określa się jako:

- I_1 — interes strategiczny (0–1),
- I_2 — skala intensyfikacji działań (0–1),
- I_3 — zgodność z wcześniej obserwowanymi działaniami (0–1),

co agreguje się do:

$$I = w_1 I_1 + w_2 I_2 + w_3 I_3.$$

Wskaźnik zdolności, odzwierciedlający faktyczne możliwości przeprowadzenia operacji, definiowany jest jako:

- C_1 — zasoby techniczne i organizacyjne (na podstawie analiz otwartoźródłowych, danych wywiadowczych),
- C_2 — przygotowanie infrastruktury do przeprowadzenia ataku,
- C_3 — podobieństwo sekwencji działań do wcześniejszych operacji,

co agreguje się do:

$$C = w_1 C_1 + w_2 C_2 + w_3 C_3.$$

Wskaźnik możliwości (operacyjnych), rozumiany winien być jako realna możliwość przeprowadzenia ataku, gdzie:

- O_1 — istnienie okna operacyjnego,
- O_2 — poziom podatności technicznych, społecznych lub organizacyjnych po stronie celu, albo wypadkowa nich wszystkich,
- O_3 — poziom skuteczności zabezpieczeń oraz odporności po stronie obrońcy,

co agreguje się do:

$$O = w_1 O_1 + w_2 O_2 + w_3 O_3.$$

Co istotne, sama funkcja $P(T) = f(I, C, O)$ może być liczona jako suma ważona, znormalizowane maksimum, funkcja logistyczna lub nieliniowa, zgodnie z wcześniejszymi kryteriami wyboru.

Składnik ekspozycji E odzwierciedla szansę powodzenia działań skierowanych przeciwko broniącemu się podmiotowi i składa się z:

- technologicznego wskaźnika powierzchni ataku E_1 , rozumianego jako zbiór podatności technicznych, otwartych punktów ataku, oraz możliwych kanałów dostępu do systemu, wspólnie określanymi jako:

$$E_1 = \frac{\text{otwarte punkty ataku}}{\text{wszystkie punkty ataku}},$$

- społecznego wskaźnika powierzchni ataku E_2 , będącego zbiorem podatności wynikających z czynnika ludzkiego, zarówno w zakresie błędów organizacyjnych, jak również podatności społeczeństwa na negatywny wpływ zewnętrzny, określanego jako:

$$E_2 = \frac{\text{podatny odsetek społeczeństwa } \vee \text{ organizacji}}{\text{ogół społeczeństwa } \vee \text{ organizacji}},$$

- wskaźnika poziomu zdolności obronnych E_3 , rozumianego jako ocena stref, obszarów lub systemów, do których możliwe jest uzyskanie dostępu, będącego:

$$E_3 = \frac{\text{przekraczalne strefy o możliwym dostępie}}{\text{strefy istniejące}},$$

co agreguje się do:

$$E = w_1 E_1 + w_2 E_2 + w_3 E_3.$$

Składnik konsekwencji incydentu CI służy oszacowaniu maksymalnej szkody, którą można ponieść w analizowanym obszarze. Składa się z:

- wskaźnika wpływu operacyjnego CI_1 , czyli potencjalnej utraty usług, niedostępności systemów, wyłączenia infrastruktury krytycznej, rozumianych jako:

$$CI_1 = \frac{\text{czas przestoju (wstrzymania usług)}}{\text{maksymalny dopuszczalny czas}},$$

- wskaźnika wpływu ekonomicznego CI_2 , wnoszącego szacunki finansowej opłacalności poniesienia incydentu względem możliwego do przeznaczenia budżetu operacyjnego, gdzie:

$$CI_2 = \frac{\text{koszt incydentu}}{\text{budżet operacyjny}},$$

- wskaźnika wpływu strategicznego CI_3 , określającego zagrożenie dla suwerenności, wpływ na procesy decyzyjne, utratę zaufania do państwa lub ich połączenia, będącego metryką ekspercką (*analiza jakościowa + praktyka operacyjna*) w skali 0–1,

co agreguje się do:

$$CI = w_1 CI_1 + w_2 CI_2 + w_3 CI_3.$$

Wynikiem każdorazowej oceny według $P(T) \times E \times CI$ będzie uzyskanie wartości ryzyka (R) w skali 0–1. Na podstawie potrzeb i możliwości organizacyjnych, strategicznych, politycznych lub innych ocen wyzwań oraz szans, należy ustalić właściwe progi reakcji. Winny być one adekwatne dla danego poziomu oceny (strategicznego, operacyjnego lub taktycznego), przy czym różnić się mogą między poszczególnymi poziomami, jeżeli zachodzi taka potrzeba. Dzięki tak określonym progom, wynik oceny ryzyka powinien wszczynać określone działanie, po którym przewidziano sprzężenie zwrotne w zakresie:

- oceny stosowanych zabezpieczeń celem zmniejszenia ryzyka,
- oceny możliwych zagrożeń i ich potencjalnego wpływu na ryzyko,
- oceny skuteczności przyjętych progów celem ich ewentualnej rewizji,
- oceny istotności wag celem kalibracji modelu.

Zaletą tak przyjętego podejścia jest jego rekurencyjność, tj. możliwość wykorzystania tego samego wzoru na poziomie strategicznym, operacyjnym i taktycznym. CI

w ujęciu taktycznym może wiązać się z uszkodzeniem jednego systemu. Z kolei na poziomie strategicznym *CI* oznaczać będzie paraliż istotnych struktur państwowych, mający wpływ na znaczącą część prowadzących działań. Struktura zmiennych pozostaje ta sama, lecz różna jest skala i typ danych. Pozostaje jednak możliwe powiązanie danych wyjściowych szczebla niższego z wejściowymi wyższego.

5.2.4. Dalsza kalibracja modelu i integracja z procesami decyzyjnymi

Skuteczność zaproponowanego modelu oceny ryzyka zależy od jego zakorzenienia zarówno w realnych danych, jak i w cyklu decyzyjnym organizacji lub państwa. Kalibracja służy temu, aby parametry modelu — wagi przypisywane zmiennym, wartości prawdopodobieństw wstępnych, progi reakcji i funkcje agregacji — odpowiadały rzeczywistemu zachowaniu adwersarzy oraz stanowi strony broniącej się. Integracja z procesem decyzyjnym zapewnia z kolei, że model nie pozostanie abstrakcyjną konstrukcją, lecz będzie mógł wpływać na realne wybory na poziomie strategicznym, operacyjnym i taktycznym. Te dwa wątki nie są rozdzielne: model nie może być użyteczny bez kalibracji, a kalibracja nie ma sensu bez jasnej ścieżki wykorzystania wyników w praktyce⁸⁸.

Pierwszym z procesów kalibracyjnych jest analiza historyczna, tj. testowanie modelu na znanych przypadkach. Pozwala to określić, czy zmienne tworzą realistyczny obraz rzeczywistości. Dobrze skalibrowany model powinien wykazywać rosnące prawdopodobieństwo $P(T \vee D)$ w okresie poprzedzającym incydenty, w których obserwowano charakterystyczne wzorce. Przykład mogą stanowić narastające anomalie telemetryczne, nietypowe aktywności wykrywane przez zautomatyzowane systemy monitorowania lub korelacje z wydarzeniami politycznymi poprzedzającymi działania ofensywne. Ocena czy model odpowiednio reagowałby na takie sygnały, pozwala doprecyzować wagi modułów *I*, *C* i *O*, a także wartości *E* i kontekstu *CI*. Co istotne, analiza historyczna ujawnia zarówno przeszacowania, jak i niedoszacowania⁸⁹ — umożliwiając korektę parametrów i wzmocnienie tych elementów formuły, które dotąd nie miały odpowiedniej mocy predykcyjnej.

Uzupełnieniem mogą być symulacje scenariuszowe. W przeciwieństwie do metod analizujących dane historyczne, ich celem nie jest rekonstrukcja przeszłości, lecz weryfikacja zachowania modelu w warunkach hipotetycznych, zwłaszcza tam, gdzie brakuje

⁸⁸ M. Dekker, L. Alevizos, *A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making*, „Security and Privacy” 2024, Vol. 7, No. 1(e333), s. 2–3.

⁸⁹ F. Sufi, M. Alsulami, *Mathematical Modeling and Clustering Framework for Cyber Threat Analysis Across Industries*, „Mathematics” 2025, Vol. 13(655), s. 22.

empirycznych danych⁹⁰. W symulacjach takich analizuje się zachowanie modelu w obliczu skoordynowanych kampanii wieloetapowych, ataków w infrastrukturze dostawców usług i rozwiązań, albo skomplikowanych operacji informacyjnych i technicznych. Umożliwia to stwierdzenie czy model jest czuły na istotne zmienne oraz czy jego zachowanie pozostaje stabilne przy radykalnie odmiennych zestawach warunków. Umożliwiają też ocenę na ile relacja między modulem probabilistycznym oraz wskaźnikami I , C , O jest prawidłowa, jak również czy nie dochodzi do zbyt gwałtownych skoków wartości $P(T \vee D)$, prowadzących do nieuzasadnionych decyzji⁹¹.

Szczególnie przydatna może być także analiza Monte Carlo, czyli metoda symulacyjna polegająca na wielokrotnym losowym próbkowaniu wartości wejściowych w celu uzyskania rozkładu możliwych wyników dla badanego modelu lub procesu⁹². Jej istotą jest wykorzystanie generatorów liczb losowych do tworzenia tysięcy, a nawet milionów scenariuszy, które odzwierciedlają różnorodność warunków i niepewności obecnych w rzeczywistych systemach⁹³. Analiza ta, stosowana jako narzędzie kalibracyjne, nabiera szczególnego znaczenia w sytuacjach, gdy model obciążony jest wysoką niepewnością oraz wieloma zależnościami warunkowymi⁹⁴. Poprzez wykorzystanie szerokiego spektrum kombinacji parametrów — od wariantów prawdopodobieństw wstępnych, przez różne konfiguracje wag modułów, aż po wartości wskaźników E i CI — uzyskujemy nie tylko rozkłady prawdopodobieństw, ale także bogaty obraz wariacji wyników. Dzięki temu możliwe staje się uchwycenie subtelnych różnic w zachowaniu modelu⁹⁵, wskazanie zmiennych krytycznych, które w największym stopniu wpływają na stabilność prognoz. Przede wszystkim powinno to pozwolić rozróżnić ryzyka centralne, mających charakter systemowy, od ryzyk brzegowych, które ujawniają się jedynie w ekstremalnych konfiguracjach. Co więcej, Monte Carlo potencjalnie stanowi krytyczną przeciwwagę dla pozornej pewności, która mogłaby wynikać z proponowanego modelu. W ten sposób analiza ta nie tylko wspiera proces kalibracji, lecz także chroni przed nadmiernym zaufaniem do

⁹⁰ S.H. Oh, J. Kim, J.H. Nah, J. Park, *Employing Deep Reinforcement Learning to Cyber-Attack Simulation for Enhancing Cybersecurity*, „Electronics” 2024, Vol. 13(555), s. 2–4.

⁹¹ L.V. Montiel, J.E. Bickel, *Simulation-Based Approach to Decision Making with Partial Information*, „Decision Analysis” 2012, Vol. 9, No. 4, s. 334–335, 343.

⁹² C.Z. Mooney, *Monte carlo simulation*, London-New Delhi 1997, s. 4–6.

⁹³ Tamże, s. 7–10.

⁹⁴ J.L.A. Cox, *Game Theory and Risk Analysis*, „Risk Analysis” 2009, Vol. 29, No. 8, s. 1062–1068.

⁹⁵ T. Fagade, K. Maraslis, T. Tryfonas, *Towards effective cybersecurity resource allocation: the Monte Carlo predictive modelling approach*, „International Journal of Critical Infrastructures” 2017, Vol. 13, No. 2–3, s. 9–10.

pozornie stabilnych rezultatów, które w rzeczywistości mogą być produktem przypadkowych zbieżności.

Równie istotna z powyższymi działaniami pozostaje integracja proponowanego modelu z procesami decyzyjnymi. Na poziomie strategicznym model pełnić może funkcję narzędzia priorytetyzacji, czyli kształtowania polityk bezpieczeństwa, kierunków inwestycji, strategii ochrony infrastruktury krytycznej oraz planów rozwoju zdolności państwa. Model pozwala wskazać sektory infrastruktury, w których skumulowane prawdopodobieństwo zagrożenia ($P(T)$) jest wysokie, a jednocześnie ekspozycja (E) oraz konsekwencje (CI) powodują, że potencjalna skala skutków jest nieakceptowalna. Dzięki temu decyzje strategiczne stają się oparte na porównywalnych danych. W praktyce oznacza to np. możliwość wykazania, że pewne obszary wymagają wzmocnienia nie ze względu na ogólne trendy czy społeczną lub polityczną presję⁹⁶, lecz dlatego, że ich ryzyko systemowe jest mierzalnie większe.

Na poziomie operacyjnym model wspiera zarządzanie sytuacją bieżącą. Tutaj kluczowa może się okazać zdolność do szybkiego aktualizowania prawdopodobieństwa wstępnego po pojawieniu się nowych obserwacji. Dynamicznie wyznaczane $P(T \vee D)$ umożliwia szybkie przejście z poziomu normalnego na podwyższony poziom czujności, aktywację dodatkowego środków technicznych, zwiększenie zasobów osobowych lub uruchomienie innych, zdefiniowanych progów reakcji. Warto podkreślić, że zaproponowany model nie daje instrukcji co należy zrobić, gdyż nie taki był jego cel. W zamian wskazuje, kiedy działania operacyjne nabierają racjonalnych podstaw i jak zmienia się prawdopodobieństwo scenariusza w czasie.

Najniższym poziomem integracji jest szczebel taktyczny, obejmujący bezpośrednie działania reagowania i wykrywania. Tutaj model stanowi wsparcie dla analityków pracujących w warunkach niepewności oraz presji czasu. Dynamiczne przeliczanie prawdopodobieństwa, nawet gdy wartości pozostają niskie, pozwalać może na śledzenie subtelnych zmian. To z kolei potencjalnie umożliwia identyfikację zjawisk będących wczesnymi sygnałami wystąpienia faktycznego zagrożenia. W tym sensie model umożliwia zarządzanie ryzykiem przy niepełnych danych. Jak ustalono wcześniej, taka stała niepewność jest charakterystyczną cechą środowiska cybernetycznego. Stąd wydaje się, że podejście oparte na analizie prawdopodobieństwa wykazuje się przewagą nad klasycznymi metodami opartymi o progi jakościowe.

⁹⁶ D. Belkheir, *Pressure Groups and Their Impact on Government Decision-Making Processes*, „Russian Law Journal” 2024, Vol. 12, Issue 1, s. 1418–1420; T. Bekefi, M.J. Epstein, *Integrating Social and Political Risk Into Management Decision-Making*, Toronto 2006, s. 10.

Całość prowadzi do spójnego sprzężenia zwrotnego: kalibracja umożliwia rzetelny pomiar, a integracja pozwala przekładać ten pomiar na decyzje. Dzięki temu proponowany model stać się może narzędziem o praktycznej wartości. Jednocześnie procesy te pozwalają systematycznie redukować przedmiotową niepewność — nie poprzez eliminację ryzyka, lecz poprzez zarządzanie wynikającą z niego nieprzewidywalnością.

5.2.5. Przyszłe kierunki rozwoju proponowanego modelu na przykładzie praktycznych implementacji

Dalsze doskonalenie probabilistycznego, rekurencyjnego modelu oceny ryzyka wymaga uwzględnienia zarówno zmian technologicznych, jak również ewolucji praktyki operacyjnej przeciwnika. W miarę jak cyberprzestrzeń w coraz większym stopniu kształtuje przebieg konfliktów, model musi rozszerzać swoje możliwości przewidywania, adaptacji oraz analizy zależności międzydomenowych. Stąd zidentyfikowano potrzebę wskazania kierunków rozwoju o charakterze systemowym, które zilustrowano poprzez konkretne przypadki. Dowodzą one, że zaproponowany model może zwiększyć precyzję oceny ryzyka i skrócić cykl decyzyjny: od wykrycia sygnału, przez jego interpretację, po adekwatne działanie.

Pierwszym i najbardziej naturalnym kierunkiem rozwoju modelu jest integracja z systemami uczenia maszynowego. Obecna wersja modelu opiera się na definiowaniu prawdopodobieństwa wstępnego oraz zestawach zmiennych I , C i O . Szacowanie z ich użyciem prostych algorytmów, wymagałoby dużych nakładów pracy analityków. Instancje sztucznej inteligencji potencjalnie mogłyby znacząco usprawnić i zautomatyzować proces⁹⁷, a przy tym wykrywać anomalie nieprzewidziane lub niedające się opisać prostymi regułami.

Niech zestaw danych D obejmuje zbiory niezwykle wysokiej szczegółowości: ruch sieciowy, metadane DNS, zmiany w konfiguracji systemów, aktywność procesów, logi warstwy aplikacyjnej i sygnały zewnętrzne (np. aktywność podmiotów w ekosystemach ransomware jako usługi). Modele klastrowania (DBSCAN, HDBSCAN)⁹⁸ oraz auto-

⁹⁷ T.T. Nguyen, V.J. Reddi, *Deep Reinforcement Learning for Cyber Security*, „Transactions on Neural Networks and Learning Systems” 2021, Vol. 34, Issue 8, s. 3779–3780.

⁹⁸ DBSCAN to metoda grupowania danych, która pozwala wykrywać skupiska elementów w dużych zbiorach informacji oraz odróżniać je od przypadkowych, odosobnionych obserwacji. W praktyce oznacza to, że algorytm potrafi wskazać, gdzie występują „gęste” obszary danych — na przykład regiony o wysokiej aktywności zagrożeń — i oddzielić je od pojedynczych incydentów, które nie tworzą większego wzorca. HDBSCAN rozwija tę koncepcję, dodając możliwość budowania hierarchii takich skupisk i lepszego rozróżniania obszarów o różnej intensywności. Dzięki temu narzędzie jest szczególnie użyteczne w analizie bezpieczeństwa, gdzie istotne jest nie tylko wykrycie głównych ognisk ryzyka, lecz także zrozumienie ich wewnętrznej struktury oraz odróżnienie zagrożeń systemowych od incydentalnych; R.J.G.B. Campello, D. Moulavi, J. Sander, *Density-Based Clustering Based on Hierarchical Density Estimates*, [w:] *Advances in Knowledge* →236

enkodery⁹⁹ mogą wykrywać odchylenia w tych danych, a następnie generować zbiory sygnałów S . W takim wypadku ocena prawdopodobieństwa wstępnego przyjmuje postać:

$$P(T \vee S_t) = \alpha \times P(T) + (1 - \alpha) \times g(S_t),$$

gdzie g jest funkcją podobieństwa obserwowanych sygnałów do historycznych wzorców przygotowania operacji, α jest parametrem określającym stopień zaufania do prawdopodobieństwa wstępnego względem nowych danych, a indeks S_t wskazuje potencjalną zmianę sygnału w czasie.

Na przykład w działalności związanej z rosyjskim GRU grupy Sandworm, badania Mandiant¹⁰⁰ i Dragos¹⁰¹ wykazały, że na kilka tygodni przed właściwymi atakami w sieciach ofiar pojawiały się subtelne, powtarzalne sygnały. Były to m.in. skany portów ICS, zmiany w konfiguracji PLC i krótkotrwałe połączenia z domenami C2 o charakterystycznych parametrach. Model uczenia maszynowego identyfikowałby te sygnały jako odchylenie od dotychczasowego profilu ruchu i aktualizował $P(T)$, nawet przy braku bezpośrednich wskaźników kampanii. Potencjalnie pozwalałoby to wykryć etap rekonesansu, zanim przeciwnik przystąpiłby do modyfikacji logiki sterowników.

Drugim kierunkiem rozwoju modelu jest systemowe ujęcie zależności między domenami: cywilną, wojskową, gospodarczą i informacyjną. Operacje cybernetyczne rzadko stanowią izolowane wydarzenia; ich skutki przenikają przez granice organizacyjne i funkcjonalne. Do modelu wprowadzić więc można wektor domen, by oszacować specyficzne dla nich ryzyko:

$$X = \{ X_{cyber}, X_{civ}, X_{log}, X_{fin}, X_{info}, X_{mil} \},$$

gdzie każde z X_{domena} jest odrębnym obliczeniem ryzyka (R_{domena}), a całościowe X jest zbiorem ryzyk domenowych, które mogą stanowić podstawę dalszych analiz, lub zostać usójnzione według wzoru:

$$R = \sum_i w_i \times R_i,$$

gdzie:

Discovery and Data Mining. Part II, J. Pei i inni (eds.), Berlin 2013, s. 160–165.

⁹⁹ Autoenkodery to sieci neuronowe uczące się uproszczonej reprezentacji danych poprzez ich kompresję i rekonstrukcję. Dzięki temu potrafią wykrywać anomalie: jeśli dane odbiegają od wyuczonego wzorca, ich odtworzenie jest mniej dokładne, co sygnalizuje nietypowe zachowanie systemu; W.H.L. Pinaya, S. Vieira, R. Garcia-Dias, A. Mechelli, *Autoencoders*, [w:] *Machine Learning*, A. Mechelli, S. Vieira (eds.), London-San Diego-Cambridge-Kidlington 2020, s. 194–196.

¹⁰⁰ K. Proska i inni, *Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology*, 9 November 2023, „Mandiant”, <https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/> [odczyt: 05.11.2025].

¹⁰¹ M. Pollard, *A Case Study of Russian Cyber-Attacks on the Ukrainian Power Grid: Implications and Best Practices for the United States*, „Pepperdine Policy Review” 2024, Vol. 166, Art. 1, s. 14–15.

- R — łączna ocena ryzyka dla całego badanego systemu,
- i — przyjęty numer domeny (np. 1=cyber, 2=logistyka, itp.),
- R_i — ryzyko w konkretnej domenie obliczone według głównego wzoru

$$R_i = P(T_i) \times E_i \times CI_i,$$
- w_i — waga domeny określająca jej znaczenie dla badanego systemu, przy czym suma wszystkich wag =1.

Sumaryczne ryzyko nie jest średnią, lecz ważoną sumą, ponieważ domeny mają różną wagę dla strategicznego funkcjonowania. Dzięki takiemu rozszerzeniu, model staje się narzędziem do badania efektów kaskadowych: uszkodzenie systemu logistycznego może podnieść ryzyko operacji o charakterze wojskowym, nawet jeśli w warstwie cyfrowej poziom zagrożenia pozostaje umiarkowany.

Jak wskazują analizy¹⁰², strategiczne zdolności państw w dotychczasowych konfliktach zależały od dostępności określonych podzespołów elektronicznych. Model systemowy mógłby oszacować, jak cyberoperacja wymierzona w łańcuch dostaw (np. atak na centra logistyczne w krajach trzecich) może zwiększyć ryzyko dla domeny wojskowej R_{mil} , nawet przy niskiej bezpośredniej aktywności agresora w sieciach wojskowych. Tego rodzaju integracja może być istotna z punktu widzenia planowania strategicznego.

Jeszcze innym kierunkiem rozwoju może być dążenie do ulepszenia odporności decyzyjnej i adaptacyjnych progów alarmowych. Aktualna praktyka w cyberbezpieczeństwie — zarówno państw, jak i podmiotów prywatnych — często opiera się na statycznych progach decyzyjnych (eskalacyjnych). Tymczasem proponowany model powinien rozwijać się w stronę logicznie spójnych progów adaptacyjnych, gdyż inaczej taka reakcja prawie zawsze będzie spóźniona. W związku z tym wprowadzić można funkcję:

$$\theta_{t+1} = \theta_t + \beta \times (R_t - \theta_t),$$

gdzie;

- θ_t — obecny próg reakcji, czyli poziom ryzyka, powyżej którego organizacja powinna działać, w tym przypadku adaptacyjny,
- β — współczynnik adaptacji ($0 < \beta < 1$), czyli najważniejszy parametr określający prędkość dostosowania progu do zmian ryzyka; wysoki β oznacza sektor reagują-

¹⁰² Z. Wolford i inni, *Scoping the future Improving Ukrainels awareness of future technologies*, Cambridge 2025, s. 16–17; E.A. Solomennikova, L.I. Lugacheva, M.M. Musatova, *The Strengthening of Economic Position of Russian Electronics: Mechanisms and Capabilities*, „Журнал Сибирского федерального университета. Гуманитарные науки” 2020, № 13(11), s. 1844, 1848; E. Zavhorodnya, A. Mazarak, T. Melnyk, *ICT sector competitiveness: A comparative analysis of Ukraine and other 7 eastern european countries*, „Regional and Sectoral Economic Studies” 2024, Vol. 24, No. 2, s. 91, 94.

cy szybko (np. wojskowy), a niski sektor unikający gwałtownych zmian (np. medyczny),

- R_t — bieżące ryzyko z głównego modelu, wyliczone dla chwili t .

W równaniu ocenić można zależności między ryzykiem i progiem, tj., jeżeli $R_t > \theta_t$, to próg rośnie (system adaptuje się do poziomu zagrożeń), a jeśli $R_t < \theta_t$, to system wraca do normalnego stanu. Oznacza to, że kiedy zagrożenie rośnie stopniowo, system sam zaczyna reagować wcześniej, a gdy sytuacja się stabilizuje to system obniża gotowość, lecz nie natychmiast. To kluczowa różnica wobec statycznych progów. Formalnie więc model ryzyka ocenia *stan*, a model progu ocenia *potrzebę działania*. Oddziela ewaluację sytuacji od decyzji, co jest fundamentalną zasadą w systemach adaptacyjnych¹⁰³.

Przykładem zastosowania powyższej propozycji mogą być zakłócenia łączności lub systemów funkcjonujących w cyberprzestrzeni, poprzedzających operacje kinetyczne. Dotychczas reagowanie odbywa się na podstawie manualnej analizy¹⁰⁴, która może być nieodpowiednia do dynamiki zdarzeń. Adaptacyjne progi bazujące na dynamicznej ocenie ryzyka w danym czasie (R_t) pozwalają na natychmiastowe przełączenie na kanały alternatywne.

Proponowane kierunki rozwoju modelu, min. integracji z uczeniem maszynowym, rozszerzenie na domeny pozacyfrowe, czy adaptacyjnych progów decyzyjnych, pokazują potencjał proponowanego narzędzia do decyzji na poziomach strategicznym, operacyjnym i taktycznym. Jednak każdy z tych kierunków wymaga ostrożności. Wykorzystanie algorytmów AI w generowaniu sygnałów ryzyka skutkować może błędami systematycznymi oraz wpływem nieobiektywności modeli AI¹⁰⁵ na wyniki. Podobnie rozszerzenie modelu na wiele domen zwiększa jego użyteczność, ale wprowadza również złożoność, która może utrudnić ocenę i kalibrację. Z kolei niewłaściwe dostosowanie analizy do potrzeb (np. w zakresie zmiany wartości wag), może negatywnie oddziaływać na progi decyzyjne. W tym sensie powyższy model nie jest gotowym rozwiązaniem, lecz rama-

¹⁰³ J. Rasmussen, *Risk management in a dynamic society: a modelling problem*, „Safety Science” 1997, Vol. 27, Issue 2–3, s. 190, 203, 206.

¹⁰⁴ R. Müller, B. Graf, T. Ellwart, C.H. Antoni, *How Software Agents Can Help to Coordinate Emergency Response Teams: Adaptive Team Performance Comparing Manual and Automated Team Communication*, „Journal of Business and Psychology” 2023, Vol. 38, s. 1124, 1132; J. Sehgal, *Enhancing Site Reliability Engineering: Scalable Strategies for Automated Incident Response and System Resilience*, „Journal of Artificial Intelligence, Machine Learning and Data Science” Vol. 2, Issue 4, s. 3–4.

¹⁰⁵ A.S. Tejani, Y.S. Ng, Y. Xi, J.C. Rayan, *Understanding and Mitigating Bias in Imaging Artificial Intelligence*, „Informatics” 2024, Vol. 44, No. 5, s. 2–3; R. Srinivasan, C. Ajay, *Biases in AI systems*, „Communications of the ACM” 2021, Vol. 64, No. 8, s. 46–48.

mi analitycznymi, które wymagają dostosowania do specyficznych potrzeb. Alternatywnie, stanowić może dane wejściowe dla innych ram teoretycznych.

Drugim ograniczeniem jest to, że każdy model probabilistyczny opisuje rzeczywistość tylko w pewnym zakresie, ale jej nie zastępuje. Ryzyko fundamentalne, wynikające z nowych technik ataku, ukrytych przygotowań czy decyzji politycznych, nie zawsze da się ująć w schemacie oceny prawdopodobieństwa. Adaptacyjne progi alarmowe, choć zmniejszają wpływ arbitralnych decyzji, mogą rodzić inne trudności: nadmierną wrażliwość systemu, zbyt szybkie zmiany stanów czy reakcje oparte na szumie zamiast sygnału. Dlatego model powinien być traktowany jako narzędzie wspierające ocenę ryzyka, a nie jako mechanizm decydujący. Jego zadaniem jest raczej porządkowanie niepewnej i niepełnej wiedzy niż jej rozstrzyganie. Każdy kierunek rozwoju należy więc postrzegać nie jako etap końcowy, lecz jako otwarte pole badań, wymagające dalszych prac teoretycznych, empirycznych i technicznych.

Podsumowanie

Wobec niejednorodnego postrzegania cech działań w cyberprzestrzeni, koniecznością okazała się krytyka części dotychczasowych podejść teoretycznych, jak również zarysowanie realistycznych perspektyw analitycznych. Wynika to z faktu, iż w warunkach gwałtownych zmian technologicznych, ograniczonej widoczności działań przeciwnika w środowisku sieciocentrycznym, jak również rosnącej roli aktorów niepaństwowych, tradycyjne opisy konfliktów cyfrowych stają się coraz mniej adekwatne. Odpowiedzią może być ich rekonstrukcja w oparciu o paradygmat stałej niepewności oraz narzędzia probabilistyczne dostosowane do tej logiki.

Część współczesnej literatury wojskowej i strategicznej powiela kalki pojęciowe wywodzące się z wojen konwencjonalnych, co prowadzi do błędnych diagnoz i nieadekwatnych schematów planowania. Krytyka takich pojęć, jak „cyfrowe linie frontu”, „cyberprzestrzeń jako teatr działań”, czy analogii logistycznych, wykazała zasadniczy problem podobnych ujęć. Przenoszenie prostych kategorii na nieliniową, silnie zdecentralizowaną sferę informacyjną, fałszuje obraz zjawisk. Cyberataki często omijają klasycznie rozumiane „linie styczności”, wykorzystując wektory boczne, socjotechnikę, infiltrację dostawców usług lub podatności w systemach. Oznacza to, że militarne metafory, opisujące cyberprzestrzeń jako terytorium z wyznaczalną przestrzenią operacyjną, przestają cokolwiek objaśniać, a za to generują złudzenie kontroli i przewidywalności.

Próby przewidywania przyszłych konfliktów cyfrowych cierpią z braku danych empirycznych, trudności w atrybucji oraz przede wszystkim wysokiej dynamiki rozwoju technologii: AI, automatyzacji ataków, a w dalszej perspektywie również technologii kwantowych¹⁰⁶. To właśnie te czynniki uzasadniają przyjęcie paradygmatu stałej niepewności: co do intencji przeciwników, ich zdolności technicznych, wewnętrznej architektury systemów chronionych, kierunków działań ofensywnych i metod ataków w przestrzeni cyfrowej. Podkreślić bowiem należy, że przyszłe konflikty w cyberprzestrzeni, poza zwiększoną intensywnością, niekoniecznie różnić się muszą od wyzwań, z jakimi państwa będą się mierzyć w czasie pokoju. W toku badań wykazano, że działania aktorów państwowych niewiele się różnią od ataków prowadzonych przez grupy przestępcze różnej wielkości. Sprawia to, iż zagrożenie w środowisku sieciocentrycznym istnieje zawsze, a odpowiedzią na taki stan rzeczy jest zarządzanie ryzykiem.

W badaniach uwzględniono także asymetrię strukturalną oraz możliwość celowej lub niezamierzonej destrukcji znacznych fragmentów cyberprzestrzeni. Szczególnie interesującymi były wyniki postrzegania wpływu impulsów elektromagnetycznych przez państwa. Gdy USA włączają tę kategorię zagrożeń do swoich doktryn budowy odporności infrastruktury i jej ochrony, to Rosja oraz Chiny traktują ją jako opcję eskalacyjną służącą odstraszeniu. W każdym z tych przypadków decydująca jest jednak obserwacja, że gwałtowne przerwanie ciągłości działania infrastruktury informacyjnej może wywołać efekty kaskadowe, które znacząco komplikują działania zarówno agresorów, jak również obrońców. Stąd ewentualne wykorzystanie EMP w kontekście cyberprzestrzeni porównać można do roli potencjału nuklearnego w walce kinetycznej.

Dotychczasowe modele myślenia o przyszłych wojnach cyfrowych oparte na stabilnych doktrynach, twardych założeniach i schematach binarnych (atak–obrona, penetracja–blokada, intruz–ochrona) są zbyt sztywne, aby operować w środowisku o wysokiej zmienności i niskiej widoczności. Prognoza musi zatem opierać się na uznaniu braku pełnej wiedzy, a także na narzędziach, które potrafią działać przy niekompletnych informacjach. Z tego względu zaproponowano probabilistyczny model oceny ryzyka jako próbę przezwyciężenia ograniczeń wcześniejszych ujęć. Kluczowym założeniem jest tu rozdzielenie problemu na trzy niezależne zmienne: intencje (*I*), kompetencje techniczne i zasoby, czyli zdolności (*C*), jak również możliwości operacyjne (*O*). Osadzono je w oce-

¹⁰⁶ A.S. Vance, *Cybersecurity risks and opportunities in the quantum computing age: A study*, „Quantum Journal of Engineering, Science and Technology” 2024, Vol. 5, No. 3, s. 36–37; P. Radanliev, *Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing*, „Journal of Cyber Security Technology” 2024, Vol. 9, No. 1, s. 33–35.

nie prawdopodobieństwa wstępnego, pozwalającej na aktualizację oceny zagrożenia w czasie rzeczywistym, a przy tym osadzenie analizy w konkretnym kontekście. Model ten nie zakłada pewności co do zachowania przeciwnika, lecz umożliwia realistyczną ocenę ryzyka przy każdorazowym napływie nowych danych. Model uwzględnia także różne domeny ryzyka (cywilną, militarną, finansową, logistyczną i informacyjną), co z jednej strony pozwala uchwycić efekty kaskadowe, a z drugiej rozszerzyć go na zagrożenia np. dla samej cyberprzestrzeni. Co istotne, model jest rekurencyjny: jego wyjścia mogą stanowić wejścia w analizie kolejnych warstw decyzyjnych, jak również stanowić sprzężenie zwrotne. Pozwala to na budowanie spójnych i skalowalnych mechanizmów oceny ryzyka w sposób systemowy.

Rekapitulując, przyszłe konflikty w cyberprzestrzeni nie będą toczyły się według schematów znanych z przeszłości. Będą chaotyczne, nieprzejrzyste, często pozbawione jednoznacznych wskaźników eskalacji. Spodziewać się można także łączenia ich z procesami gospodarczymi, społecznymi i technologicznymi. Kluczowe znaczenie będzie miała nie tyle zdolność do przewidywania konkretnych scenariuszy, co zdolność do realistycznego zarządzania niepewnością: elastyczność, szybka aktualizacja priorytetów, zdolność do operowania na danych niepełnych i adaptacja działań ochronnych do zmieniającej się sytuacji. Aby taka reakcja była skuteczna, rozważyć należy zwiększanie autonomii niższych szczebli decyzyjnych w ramach przyjętych ram. Rozumieć przez to należy wyznaczanie granic, w ramach których działania taktyczne mogą być prowadzone w sposób niezależny, bez konsultacji ze szczeblem operacyjnym.

Zakończenie

I. Usystematyzowanie kontekstu badań i podstaw teoretycznych podejmowanej problematyki

Wojna od zawsze łączyła w sobie zmienność i stały rdzeń, który sprawia, iż do dziś dzieła Sun Tzu oraz Clausewitza są obowiązkową lekturą dla studiów polemologicznych. Właściwie w każdym konflikcie obserwowano te same elementy: kontynuację polityki szczególnymi środkami, w oparciu o przemoc, lecz przy uzyskiwaniu przewagi przez wywiad, adaptację czy wykorzystywanie zaskoczenia. Nierozłącznie wiązało się to z niepewnością, chaosem i szeroko rozumianą „mgłą wojny”. Pomimo zmian technologicznych towarzyszących rozwojowi ludzkości — gdzie niejednokrotnie to walka indukowała postawianie nowych wynalazków — rdzeń konfliktów pozostawał ten sam. W efekcie uzyskiwano kolejne dowody na to, że postęp jest wykładnikiem siły, lecz zasadnicze równanie wojny pozostaje niezmiennie.

Upřednio zmiany następowały na przestrzeni tysiącleci, wieków albo przynajmniej wielu dekad. Jednak niespotykana wcześniej skala wojen światowych rozwinęła sposób prowadzenia walki w sposób bardziej radykalny. Dalsza budowa arsenału nuklearnego oraz ambitnych projektów inżynieryjnych sprawiły natomiast, że środki walki uchodzące za nowoczesne, zaczęły szybko się przedawniać.

Prawdziwą rewolucję przyniósł rozwój technologii komputerowej, a przez to także komunikacji czy możliwości rozwoju technicznego i kryptograficznego. Jak tylko cyfrowe urządzenia opuściły laboratoria oraz ośrodki badawcze, zostały natychmiast zaadaptowane przez instytucje państwowe i korporacje. Wkrótce, wraz ze stopniowym zmniejszaniem kosztów, nowoczesna technologia przyjęła się szeroko w społeczeństwie, prowadząc do fundamentalnych zmian. Różnice między pokoleniami nie przejawiały się już przez artykułowanie innych potrzeb lub różne postrzeganie spraw politycznych. Wraz z komputeryzacją nastąpiło rozwarstwienie w oparciu o cyfrowe nieprzystosowanie. Starsze pokolenia przestały rozumieć technologię młodszych, a ci przynajmniej częściowo utracili możliwość oparcia się na doświadczeniu i poradach swoich poprzedników. Tak zasadnicze zmiany, w kontekście wyścigu kosmicznego, przełamywania kolej-

nych barier technologicznych i bicia rekordów w rywalizacji między mocarstwami, skłaniały autorów do przemyśleń na temat wojny. Część z nich wskazywała, że również i walka musi zmienić się równie znacząco.

Zmiany rzeczywiście zaszły, co można było obserwować już podczas konfliktu w byłej Jugosławii. Technologiczna dominacja w powietrzu, komunikacji czy pozyskiwaniu oraz analizie danych wywiadowczych, zaczęła redefiniować sposób prowadzenia walki. W sytuacji, w której aktorowi brakowało porównywalnego potencjału, powstawała potrzeba równoważenia asymetrii przez zastosowanie innych form działań bojowych. Na znaczeniu zyskało łączenie starć konwencjonalnych z partyzanckimi, uderzaniem tam, gdzie przeciwnik się tego nie spodziewa, wykorzystywaniem jego słabości, czy użyciem samego społeczeństwa (jego morale i emocji). Jednakże nie było to tak naprawdę nic nowego. Wpisuje się to tak samo w dialektykę Sun Tzu, jak również reguły Clausewitza i jego triady lud-armia-rząd.

Tym, co rzeczywiście zaczęło odmieniać pole walki, była kontrola nad informacją. Dawniej scentralizowana, wykorzystywana była jako narzędzie prowadzenia polityki wewnętrznej i międzynarodowej, czasem przybierając formę propagandy na szeroką skalę. Państwo dysponowało licznymi narzędziami: zarówno wywierania wpływu na społeczeństwa, jak również uciszania głosów przeciwnych racji stanu. Przy tym zastosowane metody różniły zarówno na przestrzeni wieków, jak również systemów politycznych. O ile przypadki cenzury były szeroko znane przez swoją jaskrawość i poziom oddziaływania, to podejście miękkie, kierowane interesem narodowym, było powszechne. Przykład może stanowić instrukcja O.T.¹, stosowana w II Rzeczypospolitej w ochronie tajemnic wojskowych. W rozdziale II regulowała ona udział wojska w działalności prasy i wydawnictw², także w zakresie publikowania informacji szczytkowych, które mogłyby być wykorzystane przez przeciwnika do złożenia pełniejszego obrazu przez wywiad otwartoźródłowy³.

Rozpowszechnienie się medium telewizji umożliwiło wojsku zarządzanie informacją w wojnie oraz dominację przekazu. Systemy akredytacyjne, a w efekcie reglamentacja dostępu mediów do pola walki, budowanie określonego przekazu i oficjalne briefingi, pozwalały budować obraz nowoczesnych, precyzyjnych armii. W efekcie ataków

¹ Centralne Archiwum Wojskowe Samodzielny Referat Informacyjny Dowództwa Okręgu Korpusu nr IX, sygn. I.371.9A.22, *Instrukcja o ochronie tajemnicy wojskowej*, Warszawa 1932.

² Tamże, s. 7–8.

³ Instrukcja O.T.1 miała charakter ramowy i wprowadzała zasady ogólne. Jej zapisy precyzowane były w dokumentach wykonawczych, np. *Prasa i jej stosunek do pracy O.II. przy ochronie tajemnic wojskowych i zwalczaniu szpiegostwa. Instrukcja dla D.O.K.*, Nr 16862/II Inf.III.Z.W.I., 1923.

z 11 września, relacjonowana w trybie 24/7 globalna wojna z terroryzmem umożliwiła trwałą rozbudowę reżimów prawnych i technologicznych. Wojsko uzyskało nadzór i militaryzację walki informacyjnej, włączając ją stały komponent operacji prowadzonych w Afganistanie oraz Iraku. Doprowadziło to do wytworzenia spektaklu (często inscenizowanego), synchronizującego ofensywę wizualną z tempem nowoczesnych działań. Dzięki temu armia była nadawcą aktywnie wpływającym na percepcję społeczeństw, a nie tylko nadzorcą informacji.

Wraz z rozpowszechnieniem Internetu i dywersyfikacją źródeł informacji, ten syntetyczny obraz działań wojskowych zaczął ulegać postępującej erozji. Blogi, fora oraz treści produkowane oddolnie obnażyły brutalność wojny. Zamiast precyzyjnych uderzeń ograniczających ofiary cywilne, do powszechnej świadomości trafiły obrazy zrujnowanych domów i obiektów użyteczności publicznej, czy nagrania tortur. Późniejsze masowe wycieki niejawnych informacji wojskowych (np. Wikileaks) dodatkowo zwiększyły transparentność wojny, ze wszystkimi tego reperkusjami dla dawnego monopolu państwowego. Finalnie fabryki treści (np. ISIS), czy praca wolontariuszy OSINT, przekształciły dawnych obserwatorów w aktorów działań wojskowych i politycznych.

Od tamtej pory obserwować można tworzenie się nowego układu sił: wzrostu znaczenia asymetrycznych aktorów w środowisku sieciocentrycznym. Istotnym jest jednak, że oddolne działania informacyjne były nie tylko sposobem na zniszczenie poprzedniej dominacji państw w tym obszarze, lecz zapowiedzą głębszych przemian. Przestrzeń cyfrowa zniosła monopol tak w budowaniu wizji świata (a w tym działań wojskowych), jak również w samym sposobie prowadzenia walki.

Coraz większe znaczenie zyskiwali mniejsi aktorzy, zdolni do prowadzenia własnych operacji skierowanych przeciwko pojedynczym użytkownikom sieci, międzynarodowym korporacjom czy instytucjom państwowym. Przypadek wykorzystania Stuxnet w 2010 roku nie był zapowiedzią nowej ery walki między armiami. Stanowił raczej odosobnioną operację na przełomie dawnego i współczesnego status quo. Był pierwszym przypadkiem wykorzystania czegoś, co nazwać można było cyberbronią, a zarazem ostatnim przejawem wyłączności państw w tego rodzaju operacjach. Kolejne lata przyniosły szybki rozwój ofensywnych cyberaktywności — przestępczości, terroryzmu i dywersji. O ile inspiracja przez służby państwowe wciąż odgrywa istotną rolę, to na znaczeniu zyskały powody ideologiczne, finansowe, wizerunkowe i inne. Zamiast cyfrowego starcia państw, kierujących się przynajmniej częściowo przewidywalną racją stanu, obserwujemy działalność grup hakerskich, skierowaną także przeciwko krytycznej infrastrukturze. Są to aktorzy zróżnicowani, często niedający rękojmi racjonalności, co utrudnia lub unie-

możliwia ewentualne prowadzenie negocjacji. Co więcej, jeszcze większym problemem jest działalność tzw. samotnych wilków, zupełnie nieprzewidywalnych, trudnych w namierzeniu, a wciąż mogących wyrządzać państwu realne szkody. Skutkuje to powstaniem stanu częściowej anarchii, w której dominuje siła przejawiająca się w cyfrowej ofensywie i defensywie.

Wobec tego rodzaju zagrożeń, klasyczne podejście do odstraszania traci swoją funkcjonalność. Poprzednie doktryny budowano na założeniu, że przeciwnik jest rozpoznawalny, jego interesy relatywnie stabilne, a koszty narzucone represją (militarną czy ekonomiczną), będą przez niego czytelnie interpretowane. Aktorzy w cyberprzestrzeni nie spełniają jednak tych warunków. Problem atrybucji tworzy próżnię decyzyjną: reakcja wymierzona w niewłaściwy podmiot może eskalować konflikt, podczas gdy brak reakcji wzmacnia zachętę do kolejnych operacji. Co więcej, wielu aktorów pozostałoby odpornych na tradycyjne represje nawet wtedy, gdyby udało się ich jednoznacznie powiązać z atakiem. W efekcie odstraszanie represjami (*deterrence by punishment*) staje się mechanizmem ograniczonej przydatności, a jego skuteczność maleje wraz z nieustannie rosnącą decentralizacją sprawczości w cyberprzestrzeni.

Równie problematyczne okazuje się odstraszanie przez odmowę (*deterrence by denial*), czyli uniemożliwianie agresorowi uzyskania zamierzonego efektu. W przestrzeni cyfrowej całkowita blokada wejścia przeciwnika pozostaje nieosiągalna. Powody są strukturalne: złożoność systemów, ich wzajemna zależność, niski poziom odporności łańcuchów dostaw oraz nieusuwalna rola czynnika ludzkiego sprawiają, że całkowite uszczelnienie powierzchni ataku jest fikcją. Każde nowe ogniwo infrastruktury tworzy potencjalną lukę. Co więcej, nawet państwa o najbardziej rozwiniętych zdolnościach obronnych nie są w stanie zapewnić odporności swoich ekosystemów cyfrowych bez istotnego udziału sektora prywatnego, a to dodatkowo komplikuje kwestię odpowiedzialności i jasnych sygnałów odstraszających.

W świetle powyższego staje się jasne, że logika odstraszania, jeden ze znaczących filarów stabilności strategicznej, przestaje pełnić tę rolę w cyberprzestrzeni. Choć nie zanika całkowicie, to staje się mechanizmem fragmentarycznym. W konsekwencji państwa muszą budować bezpieczeństwo na innych fundamentach: odporności systemowej, zdolności szybkiego wykrywania i neutralizacji szkód, elastycznym zarządzaniu ryzykiem oraz nowych metodach skoordynowanej reakcji. Przejście to nie oznacza rezygnacji z odstraszania jako elementu polityki bezpieczeństwa, ale jego przesunięcie na dalszy plan. Zarazem wymaga to uznania, że stabilność w cyberprzestrzeni osiąga się nie przez

strach przeciwnika, lecz przez własną zdolność przetrwania, rekonfiguracji i odzyskiwania sprawności w warunkach permanentnej niepewności.

Podejmując próby opisanie nowych oraz przyszłych konfliktów, autorzy proponowali liczne definicje, które skupiały się na analizie przez pryzmat nieregularności, złożoności, niekonwencjonalności i podobnych. Zdecydowanie najczęściej pisano o wojnie hybrydowej. Choć próby jej usystematyzowania sięgają lat 90 XX wieku, to dopiero definicja Franka Hoffmana z 2007 roku zyskała na znaczeniu — i to także nie od razu. Znaczącą popularność pojęcie to zyskało podczas aneksji ukraińskiego Krymu przez Rosję w 2014 roku. Źródła naukowe często traktowały hybrydowość sceptycznie, wskazując zarówno na problemy samego pojęcia, jak i na nieprzystawanie do faktycznej strategii Moskwy. Rzekoma „doktryna Gierasimowa” nigdy nie istniała, a największe poparcie dla wojny hybrydowej dostrzec można było u autorów, którzy zachodnio-centryczne podejście do współczesnej walki próbowali aplikować do źródeł rosyjskich. Te rzeczywiście często poruszały hybrydowość (choć często nie dosłownie), lecz głównie jako pogłębioną analizę spojrzenia amerykańskiego. Zdarzało się jednak, że taka praca badawcza odczytywana była jako przyjęcie koncepcji zachodnich. Skutkiem było niezrozumienie rzeczywistego sposobu postrzegania współczesnego pola walki przez Rosję, a przynajmniej w istotnej części.

Mimo to, hybrydowość została szeroko zaadaptowana. Kiedy kolejni autorzy dowodzili jej niskiej przydatności metodologicznej i badawczej, stała się pojęciem politycznym — do czego nadawała się doskonale. Zbyt duża pojemność definicji, nieostrość, brak solidnych podstaw strategicznych oraz doktrynalnych, czyli największe zarzuty naukowe, zaważyły nad jej sukcesem w debacie publicznej. Wynikało to właśnie z tego, jak wiele można było nią wytłumaczyć, jak nośnym pojęciem się stała i jak trudno było w merytoryczny sposób wykazać brak podstaw do jej stosowania. Z koncepcji sposobu prowadzenia współczesnych konfliktów, wojna hybrydowa stała się elementem dyskursu politycznego oraz legitymizacją działania państwa przed jego własnym społeczeństwem. Nazwanie wydarzeń mianem wojny hybrydowej często wiąże się z brakiem konieczności podania dodatkowego uzasadnienia dla wybranej reakcji, niezależnie od jej adekwatności, etyki czy legalności. Z tego względu uzasadnionym wydaje się stwierdzenie, że hybrydowość już teraz utraciła naukowe znaczenie, a w kolejnych latach obserwować będziemy dalszą jej erozję w tym zakresie.

Z podobnymi problemami mierzyła się asymetryczność. Jak wykazano w pierwszych dwóch rozdziałach, zarówno ona, jak i łączenie wielu rodzajów działań do osiągnięcia zamierzonego celu (a zatem domniemana hybrydowość), były stałą konfliktów

w przeszłości. Te same mechanizmy towarzyszyły nam od starożytności po współczesność. Przyznać należy, iż zmieniała się intensywność ich wykorzystania, choć w toku przeprowadzonych badań także i do tego stwierdzenia zachowano krytyczne podejście. Jak wykazano, źródła historyczne miały określoną narrację, osadzoną silnie w kulturowym kontekście danego okresu i miejsca. W efekcie działania dziś nazywane asymetrycznymi lub hybrydowymi mogły być postrzegane jako niegodne, niehonorowe, lub niewpisujące się w pożądaną wizerunek państwa oraz jego sił. Zakładać należy zatem, że część takich metod prowadzenia walki nie miała wystarczającej reprezentacji w źródłach, co może zaburzać finalny obraz. Niemniej, wraz ze wzrostem złożoności relacji międzynarodowych, zmieniali się także aktorzy zyskujący na znaczeniu. Stąd dostrzec można, iż rola podmiotów asymetrycznych względem ich adwersarzy zaczęła zyskiwać na znaczeniu, a zmiana tych proporcji przyspieszyła w ciągu ostatnich kilku dekad.

Uwagę zwrócić należy na skalę operacji prowadzonych przez aktorów niepaństwowych, którzy wykorzystywali słabości Zachodu nie tylko militarnie, lecz przede wszystkim informacyjnie i psychologicznie. Przykładem są operacje Al-Kaidy z końca lat 90., w tym zamachy na ambasady USA w Nairobi i Dar es Salaam w 1998 roku oraz późniejsze ataki z 11 września 2001 roku. Choć były to działania kinetyczne, to asymetryczny wpływ uzyskano przez dominację informacyjną, czyli natychmiastową globalizację przekazu oraz umiejętne wykorzystania mediów do własnych celów. Siłę potencjałów wojskowych zamieniono na uzyskiwanie efektów strategicznych za pomocą minimalnych środków i z wykorzystaniem podatności przeciwnika, w tym społecznych. Operacje te ukazały, że państwa o największych możliwościach konwencjonalnych są szczególnie podatne na działania podważające ich pętlę decyzyjną, wrażliwość opinii publicznej oraz wewnętrzne mechanizmy polityczne.

Równolegle, na przełomie XX i XXI wieku ujawniły się pierwsze symptomy asymetrii o charakterze stricte cyfrowym, wskazujące na rosnącą rolę aktorów, którzy nie dysponowali ani przewagą technologiczną, ani zapleczem państwowym. Wystarczy przywołać kampanie prowadzone przez aktywistów w czasie konfliktu w Kosowie w latach 1998–1999, ataki na estońską infrastrukturę sieciową w 2007 roku, czy późniejsze operacje grup powiązanych luźno z interesami politycznymi państw, lecz formalnie działających poza ich strukturami. W każdym przypadku efekt strategiczny wykraczał poza skalę samego ataku lub działania informacyjnego. To właśnie tutaj ujawniła się kluczowa cecha asymetrii w epoce globalnej sieci: możliwość eskalacji efektów przy minimalnym nakładzie środków. Przewagę uzyskiwał nie ten, kto miał więcej zasobów, lecz aktor potrafiący lepiej wykorzystać słabości przeciwnika. I choć samo w sobie jest to podejście

równie stare co traktat Sun Tzu, to współczesna technologia nadała mu o wiele większego znaczenia. Tym co rzeczywiście odróżnia działania współczesne od historycznych jest nie tylko intensyfikacja technik asymetrycznych, lecz możliwość rzeczywistego i skutecznego prowadzenia działań wyłącznie przy ich użyciu.

II. Odpowiedź na pytania badawcze

Takie przedstawienie wyzwań dla państw pozwala udzielić odpowiedzi na zasadnicze pytanie badawcze. To właśnie cyberprzestrzeń umożliwiła tak radykalne zmiany w prowadzeniu działań i sprawiła, że przymiotnik asymetryczności zyskał na tak dużym znaczeniu. Środowisko sieciocentryczne dało mniejszym aktorom możliwość oddziaływania na niespotykaną dotychczas skalę, przez prowadzenie operacji w niemal dowolnym miejscu i o globalnym zasięgu. Zarazem próg wejścia został znacząco obniżony, czego dowodzą przykłady aresztowań członków grup hakerskich wyrządzających najpoważniejsze szkody. Za atakami na infrastrukturę krytyczną, największe korporacje ze sztabami profesjonalistów czy instytucje państwowe nadzorowane przez służby, stoją często osoby w wieku 16–25 lat. Podkreślić jednak należy, że to nie przesądza o demografii cyberprzestępców. Słusznym byłoby stwierdzenie, iż ze względu na niższe doświadczenie i poziom wiedzy, to raczej najmłodsi członkowie popełnią błędy pozwalające ich zidentyfikować. Nie podważa to jednak sedna problemu: łatwości, z jaką można osiągać rezultaty wcześniej zarezerwowane dla służb specjalnych lub operacji wojskowych. A zatem cyberprzestrzeń bezpośrednio przyczyniła się do znaczącego rozszerzenia katalogu aktorów, będących potencjalnym zagrożeniem dla państw.

Również dostępność narzędzi, od serwisów społecznościowych i platform komunikacyjnych, po złośliwe oprogramowanie w formie usługi, odegrały istotną rolę. Opisana wcześniej utrata monopolu kontroli nad informacją, na rzecz budowania nowego układu sił, była też zapowiedzią szerszego trendu (podobnych zmian w innych obszarach). Sama możliwość oddziaływania na inne podmioty — w dowolnym miejscu i przy niskim progu wejścia — jest tylko składową problemu. Istotne są bowiem potencjalne skutki prowadzonych działań. Stale rosnąca złożoność systemów, a także zależność nawet najbardziej zaawansowanych państw od sektora prywatnego, otworzyły nowe perspektywy działań. Nie wystarczy już zabezpieczać się przed klasycznymi atakami hakerskimi, wymierzonymi bezpośrednio w cel. Na znaczeniu zyskują łańcuchy dostawców systemów ICT, zależności oprogramowania od zewnętrznych bibliotek i zasobów, czy heterogeniczność infrastruktury oraz wykorzystywanych technologii. Wszystko to znacząco zwiększa po-

wierzchnię ataku, skutkując znaczącą asymetrią między broniącym się i atakującym. Obrońca musi bowiem stale dbać o zabezpieczenia, bez przestrzeni do popełnienia błędu. Z kolei agresor nie tylko dysponuje potencjalnie większą liczbą szans, lecz także wykorzystać może problem atrybucji. Ukrywając własną tożsamość, podejmuje działania do skutku, często bez żadnych konsekwencji. A zatem cyberprzestrzeń nie tylko zrównuje w cyfrowej walce aktorów zdecydowanie silniejszych (jak państwa, międzynarodowe korporacje) z mniejszymi grupami, lecz tworzy środowisko dla nich niesprzyjające.

Mimo to, wojna w Ukrainie, która toczy się od 2022 roku, ukazuje raczej ograniczone wykorzystanie środowiska sieciocentrycznego. Przyczyny tego są złożone. Przede wszystkim: sposób postrzegania potencjału Federacji Rosyjskiej w prowadzeniu walki cyfrowej okazał się nieadekwatny. Mimo bardzo wczesnych deklaracji militaryzowania cyberprzestrzeni (bo na przełomie mileniów), kiedy inne państwa postrzegały ją raczej jako przedmiot zainteresowania służb specjalnych, nie zaobserwowano przełomowych metod walki. Przeciwnie, działania wymierzone głównie w infrastrukturę krytyczną Ukrainy okazały się nie różnić od metod stosowanych przez grupy przestępcze. Podobne są zarówno techniki, jak również wykorzystywane oprogramowanie, a nawet skala osiągniętych rezultatów. Tu podkreślić należy, iż ze względu na wciąż toczące się starcia, nie jest to czas na retrospektywną ocenę wojny, lecz w dużej mierze bieżące reagowanie. Istnieje więc szansa, iż w przyszłości ujawnione mogą zostać nieznane dotychczas sposoby cyberwalki, czy wykorzystania cyberbroni na miarę Stuxnet — choć nie obserwuje się przesłanek ku temu. Zarazem nawet w przypadku stwierdzenia takiej operacji, nie będzie mieć ona przełomowego znaczenia, gdyż nie obserwujemy adekwatnych skutków. Co więcej, Rosja sama padała ofiarą podobnych ataków ze strony różnych aktorów. Przykładem może być działania skierowane przeciwko Aerofłotowi oraz usługom państwowym (w tym pocztom), czy wyciek danych z NTC Vulkan.

Co oczywiste, cyberprzestrzeń nie pozwala na realne zajmowanie terytorium. Jednakże wojna w Ukrainie pokazała, że integracja cyberoperacji z walką kinetyczną wciąż stanowi duże wyzwanie. W efekcie, wykorzystanie dronów wywarło dużo większy wpływ na sposób prowadzenia walki niż którekolwiek z działań w środowisku sieciocentrycznym. Poddaje to w wątpliwość jego wpływ na sposób prowadzenia przyszłych wojen. Nie pomaga również fakt, że nowoczesne rozwiązania technologiczne są drogie. Przy wciąż ograniczonym ich wpływie oraz dużym koszcie, państwa mogą osiągać większe efekty przez alokację zasobów w klasycznych formach zwiększania potencjału. Dużo prościej jest przeprowadzić dodatkowy pobór niż opracować zaawansowaną cyberkampanię, która miałaby wymierzyć przeciwnikowi porównywalne straty. Dlatego futurystyczne wi-

zje argumentowanych żołnierzy i wielkiej liczby zaawansowanych sprzętów, w których możliwe staje się równoległe walczenie z nimi w przestrzeni logicznej, pozostają tylko fikcją. Rola cyberprzestrzeni rozwija się aktualnie w dwóch kierunkach: stałej niepewności poza konfliktami oraz uzyskiwania i wykorzystywania przewagi informacyjnej w czasie prowadzenia działań wojennych.

Wraz z niewielkim wpływem walki cyfrowej na wojnę w Ukrainie, w tym samym czasie cyberzagrożenia dla innych państw wciąż rosły, stając się przedmiotem pilnie wprowadzanych zmian prawnych. Aktorzy w środowisku sieciocentrycznym mierzą się bowiem ze stałym zagrożeniem. Wykorzystanie tych samych cybertechnik w czasie pokoju (w ujęciu ogólnym), jak również między dwoma państwami w stanie konfliktu (wojna w Ukrainie) ukazuje istotną implikację. W cyberprzestrzeni rozróżnienie na stan pokoju i wojny rozmywa się w praktyce. Choć zmieniać się może intensyfikacja działań, na podstawie potencjalnych korzyści materialnych, przyczyn społecznych i ideologicznych, czy wreszcie geopolitycznych i strategicznych, to co do zasady są one podobne. Nie sposób więc mówić o przygotowaniu się do wojny cyfrowej, kiedy rzeczywistość najlepiej oddaje koncepcja stałego zagrożenia.

Środowisko cyfrowe wykorzystywane też może być nie jako element walki kinetycznej, lecz główne jej wsparcie. Proponowane głównie przez Chiny użycie uczenia maszynowego i złożonych algorytmów, w połączeniu z licznymi punktami zbioru danych, pozwoliłoby odmienić sposób dowodzenia walką. Systemy takie, jako doskonały doradca sztabowy, umożliwiłyby szybszą i skuteczniejszą reakcję na zastaną sytuację. Podkreślić należy, że wiąże się to z ryzykiem eksfiltracji takich danych przez przeciwnika, czy też innych ataków na infrastrukturę takiego systemu. Jednak przyjęcie perspektywy stałej niepewności i zagrożenia sprawia, że niezależnie od rodzaju cyfrowej działalności państwa, może być ono obiektem wrogich działań, tak w czasie pokoju, jak również wojny. Skoro więc ryzyko istnieje, a potencjalnie można nim zarządzać, to racjonalnym wydaje się jego minimalizowanie i akceptacja tam, gdzie to możliwe, a w zamian przyjęcie szans, jakie daje cyberprzestrzeń.

Perspektywa ta nie jest wyłącznie chińską. Inne państwa również rozwijają systemy agregowania oraz przetwarzania dużej ilości danych, także w celu potencjalnego wykorzystania do autonomizacji pola walki czy wsparcia procesów decyzyjnych. Pytaniem otwartym pozostaje jednak stan działań. Stworzenie skutecznie działającego rozwiązania wymaga technologii, infrastruktury, środków oraz wiedzy, jak również wielu testów połączonych z procesem ciągłego doskonalenia. Porównanie systemów państwowych zajmujących się ściśle analizą informacji, niezależnie od ich przeznaczenia, wydaje się skłaniać

ku tezie, że to Chiny wysuwają się na prowadzenie w tym wyścigu. Dla państw demokratycznych, w których indywidualizm i ochrona prywatności są istotne dla obywateli, oznacza to potencjalnie trudną do zmniejszenia różnicę potencjałów. Trudno będzie bowiem wykorzystać chińskie mechanizmy nabywania doświadczenia w takiej analizie danych, bez jednoczesnego naruszenia kluczowych wartości (liberalnych, wolnościowych) wyznawanych przez społeczeństwo. To także buduje niepomijalną asymetrię, lecz zarazem stanowi interesujący przypadek badawczy dla przyszłych analiz.

Ponadto w toku badań ustalono, że współczesne rozumienie cyberprzestrzeni wymaga odejścia od intuicji scentralizowanej infrastruktury kontrolowanej przez państwa. Nie jest ona przestrzenią terytorialną, lecz dynamicznym układem relacji, w którym splatają się warstwy techniczne, informacyjne, organizacyjne i społeczne. Jej przedmiotem są procesy przetwarzania, przechowywania i przesyłania informacji, a podmiotowość obejmuje państwa, korporacje, grupy przestępcze, hakerów i użytkowników końcowych. W praktyce oznacza to zerwanie z klasycznym podziałem na aktora i środowisko: działania aktorów współtworzą ekosystem, generując nowe poziomy złożoności i nieprzewidywalności.

Wprawdzie możliwe jest ingerowanie w samo środowisko przez asymetrię strukturalną, np. izolując sieć na poziomie państwa, lecz nie jest to rozwiązanie odporne na próby obejścia. Podobnie, samo niszczenie infrastruktury utrzymującej przestrzeń cyfrową, np. przy użyciu impulsów EMP/HEMP stanowi pewną możliwość, lecz praktycznie mało przydatną na dużą skalę. Wykazano, że jest to odpowiednikiem impasu nuklearnego, choć dostrzec w nim można pewne różnice. O ile Zachód skupia się na budowaniu odporności w przypadku użycia takich impulsów (lub zagrożeń środowiskowych o podobnej skali), to Rosja i Chiny koncentrują się na odstraszeniu przez potencjał EMP/HEMP. Przy obecnym rozwoju technologii nie jest to jednak problem najistotniejszy, gdyż nie pozwala na łatwe generowanie tego rodzaju impulsów w skali mającej istotne znaczenie. Głównym źródłem EMP/HEMP mogłaby być broń nuklearna, detonowana na dystansie ok. 30 km powyżej powierzchni planety⁴. To z kolei jest przedmiotem samego impasu atomowego, a w przypadku użycia mogłoby się wiązać z trudnymi do przewidzenia konsekwencjami dla każdej ze stron. Wydaje się jednak, że nawet brak zagrożenia konfliktem nuklearnym o dużej skali, nie spowodowałby powszechnego wykorzystania EMP/HEMP. Wynika to z ekonomii konfliktu: cyberprzestrzeń jest zbyt cenna, by ją niszczyć, ale wystarczająco krucha, by stać się celem presji operacyjnej. Dlatego można

⁴ P.V. Pry, *Russia: EMP Threat*, [AD1123491] 2025, s. 4.

spodziewać się selektywnych uderzeń w krytyczne punkty celem obniżenia zdolności przeciwnika, a nie globalnego niszczenia środowiska sieciocentrycznego.

Cyberprzestrzeń powoli staje się ukrytą architekturą pola walki, czego przykładem są zarówno pomniejsze działania przestępcze, jak i złożone operacje APT. Pytanie o przyszłość nie brzmi „czy domeny będą się przenikać?”, lecz „jak szybko i z jakimi konsekwencjami?”. Operacje kinetyczne wymagają zaplecza informacyjnego, a cyfrowe dążą do efektów politycznych, gospodarczych czy militarnych, mogąc indukować lub po prostu poprzedzać użycie konwencjonalnej siły. Co więcej, architektura ta sprzyja odhumanizowaniu działań. Wobec coraz szerszej adaptacji sztucznej inteligencji, wykorzystania dronów oraz systemów asystowania w prowadzeniu walki, rozpowszechnienie większej autonomii urządzeń wydaje się być kwestią czasu. W cyberprzestrzeni takie zjawiska obserwowane są już dzisiaj. Odnotowano przypadki złośliwego oprogramowania, które samoczynnie dostosowuje się do zastanego systemu i bez udziału człowieka sporządza kod pozwalający lepiej realizować założone cele. Po stronie obrońców funkcjonują z kolei zaawansowane mechanizmy analizy, które gromadzą informacje z wielu urządzeń, by wykrywać anomalie i aktywnie na nie reagować.

W konsekwencji klasyczne paradygmaty wojny — definiowanie podmiotów, przewidywanie celów czy oddzielanie działań kinetycznych od informacyjnych — w środowisku sieciocentrycznym tracą użyteczność. Ich miejsce zajmuje logika zmienności, niepewności i adaptacji. Przyszłość konfliktów w cyberprzestrzeni polegać będzie bowiem nie na przewidywaniu konkretnych wojen, lecz na działaniu w warunkach stałego zagrożenia: budowaniu odporności i elastycznych ram decyzyjnych. Cyberprzestrzeń jawi się jako środowisko współtworzone, przenikające domeny konfliktu, podatne na zakłócenia, lecz jednocześnie umożliwiające nowe formy projekcji siły. To właśnie jej złożoność, wielopodmiotowość i pewna kruchość zdają się być determinantami jej roli w przyszłych konfliktach, a przez to cechami wymagającymi dalszej analizy.

III. Weryfikacja hipotezy badawczej

Sformułowana we wstępie hipoteza zasadniczo znajduje potwierdzenie w przeprowadzonych analizach. Cyberprzestrzeń nie funkcjonuje już jako odrębna domena, lecz przenika strukturalnie inne obszary działań, prowadząc do bezprecedensowego sprzężenia informacji, infrastruktury i operacji. Ścisłe powiązanie środowiska sieciocentrycznego z innymi domenami wzmacnia asymetrię oraz nieregularność konfliktów. Otwiera to pole działania dla nowych aktorów pozapaństwowych (niehierarchicznych

i o trudnym do przewidzenia sposobie działania). Ustalono też, że państwa w reakcji na rosnącą złożoność dążą do częściowej „decyfryzacji” (funkcjonalnej), wdrażając izolowane podsieci i systemy, kierując się budowaniem odporności.

Wnioski te pozostają zgodne z ustaleniami wcześniejszych rozdziałów: analizą strukturalnych przemian w konfliktach (2.2, 4.2), wskazaniem podatności infrastruktury krytycznej (4.2.4), rozważaniami nad destrukcją cyberprzestrzeni poprzez scenariusze EMP/HEMP (5.1.2), a także paradygmatem stałej niepewności i degradacji sieci (5.1.4). Ujęcie probabilistyczne (5.2) dodatkowo podkreśla, że przyszłość sporów w cyberprzestrzeni nie polega na przewidywaniu ich jednoznacznego kształtu, lecz na adaptacji do warunków nieprzewidywalności. W konsekwencji hipoteza wskazuje na trzy kluczowe cechy przyszłych konfliktów: strukturalne przenikanie domen, wzrost asymetrii oraz dążenia państw do budowy odporności cyfrowej na zakłócenia.

Cyberprzestrzeń z jednej strony stała się obszarem działań obok lądu, morza, powietrza i kosmosu. Zarazem jednak przenika każde z pozostałych środowisk, mając przy tym własne, niepowtarzalne cechy, m.in. możliwości wpłynięcia na samą strukturę przestrzeni cyfrowej. Wynika z tego, że to nie cyberprzestrzeń indukuje konflikty, przy okazji częściowo przenosząc je w nią samą, lecz to konflikt korzysta z cyberprzestrzeni. Elementy zarządzania informacją i infrastrukturą są jednymi z głównych celów, a środowisko sieciocentryczne pozwala osiągać rezultaty w sposób najskuteczniejszy. To wskazuje, że rola cyberprzestrzeni nie jest ontologicznie odrębna, lecz funkcjonalna — i dlatego jej przenikalność jest tak istotna.

Wskazano także, iż środowisko cyfrowe rzeczywiście nasiliło problemy wynikające przede wszystkim z asymetryczności, lecz także hybrydowości i nieregularności — przyjmując szeroki zakres definicji tych pojęć. Technologia zawsze była mnożnikiem siły, lecz w przypadku cyberprzestrzeni tempo, zakres podmiotów, niskie koszty wejścia, efekty kaskadowe i możliwość działania bez geograficznego kontaktu, łącznie skutkowały rewolucją. Asymetria nie zyskała jednak na znaczeniu „sama w sobie”, lecz doszło do zmiany krajobrazu operacyjnego, który gwałtownie zwiększył potencjał asymetrycznych aktorów przez wyżej opisane cechy cyberprzestrzeni.

Analizowany materiał wskazał także, że państwa będą ograniczać zależność kluczowych sfer od problemów wytwarzanych przez samo środowisko sieciocentryczne i jego cechy, przez stosowanie rozwiązań uodpornionych na jej wyłączenie. Wyróżnić tu należy utrzymanie zdolności operacyjnych NATO (ang. *mission assurance*), zachodnie (w szerokim rozumieniu) uwzględnianie odporności systemów cyfrowych na etapie projektowania (ang. *resilience-by-design*), chińską informatyzację pod warunkami zakłóceń,

czy rosyjskie próby izolacji segmentów sieci przez budowę RuNet. Wnioski z badań wskazują jednak, że decyfryzacja na dużą skalę nie jest możliwa. O ile wysiłki na poziomie operacyjnym są uzasadnione i wydają się być skuteczne, to strategicznie nie mają zastosowania. Gospodarka, logistyka, prace rozwojowe (R&D) stały się nieodłącznie cyfrowe, a rosnąca zależność od sektora prywatnego (dla której nie ma praktycznej alternatywy) dodatkowo wzmacnia ten efekt.

IV. Wnioski

Syntezyując powyższe ustalenia, stwierdzić należy, iż asymetryczność i hybrydowość konfliktów są historycznie trwałymi cechami, lecz ich współczesna dynamika została radykalnie przekształcona przez cyfryzację, która zwiększyła skalę, tempo i wielowarstwowość działań. Rewolucja informacyjna przyspieszyła obieg danych, obniżyła próg wejścia dla aktorów niepaństwowych i umożliwiła prowadzenie operacji poniżej progu wojny. Zatarło to granicę między pokojem oraz konfliktem, czyniąc cyberprzestrzeń środowiskiem stałej presji strategicznej. Od lat 90. informacja stała się głównym polem rywalizacji, a operacje cyfrowe zaczęły bezpośrednio oddziaływać na działania kinetyczne, zmieniając architekturę walki poprzez upadek monopolu informacyjnego i wzrost roli podmiotów pozapaństwowych. Współczesne konflikty — od Bliskiego Wschodu, przez Ukrainę, po globalną cyberprzestrzeń — pokazują, że przewaga informacyjna opiera się na zdolności do utrzymania przepływu danych, ich ochrony oraz zakłócania wrogich systemów, a asymetria została spotęgowana przez łatwość zadawania uderzeń o dużym efekcie przy minimalnym ryzyku. Wielość aktorów sprawia natomiast, że klasyczne teorie odstraszania tracą skuteczność, a bezpieczeństwo wymaga nowych ram strategicznych.

Z tego względu kluczowym wnioskiem niniejszej pracy jest to, że współczesna cyberprzestrzeń wymusza przyjęcie paradygmatu stałej niepewności. Niepewność ta ma charakter epistemiczny (brak pełnej obserwowalności), ontologiczny (ciągłe zmiany cyberprzestrzeni i jej podmiotów), operacyjny (niejednoznaczna atrybucja) i strategiczny (wielowarstwowość aktorów). Wykazano, że żadna koncepcja wojny hybrydowej czy asymetrycznej nie jest w stanie wyczerpać tej dynamiki, jeśli pozostaje zakorzeniona w taksonomiach oraz metaforach właściwych konfliktom konwencjonalnym. Przeciwnie, zacierają one realny charakter ryzyka. Cyberprzestrzeń nie operuje bowiem liniowością, lecz rozproszonymi zależnościami, które wymagają zupełnie innego języka i podejścia analitycznego.

Uzasadnia to także brak możliwości skutecznego przewidzenia kierunku rozwoju obecnych technologii, a co dopiero prognozowania powstania przyszłych. Generatywna sztuczna inteligencja, automatyzacja operacji ofensywnych (zwłaszcza prowadzonych wyłącznie w cyberprzestrzeni), walka radioelektroniczna i scenariusze naruszeń struktury samego środowiska sieciocentrycznego, wskazały na konieczność odszukania elementu wspólnego. Jest nim szeroko rozumiane ryzyko, które cechuje się dostateczną uniwersalnością. W przeciwieństwie jednak do koncepcji choćby wojny hybrydowej, podejście oparte na ryzyku możliwe jest do skutecznego zastosowania w każdym sektorze dotkniętym przez cyfryzację. Wnosi także aparat analityczny, który może być dostosowany do potrzeb państwa i stosowany w sposób dostatecznie spójny. I choć podkreślić należy, że efektem takiego podejścia nie będzie spójny opis rzeczywistości (w rozumieniu gotowej teorii), to możliwe jest uzyskanie pragmatycznie przydatnych wyników. Te mogą dalej służyć do adekwatnego reagowania — zarówno w sferze faktycznych działań (przez instytucje i służby państwa oraz sektor prywatny), jak również w zakresie doskonalenia doktryn, strategii oraz planowania.

Zaproponowano zastosowanie podejścia opartego na probabilistycznym, rekurencyjnym modelu oceny zagrożeń. Jego intencją było umożliwienie integrowania danych z wielu domen, przy stałej aktualizacji oceny ryzyka w świetle nowych obserwacji (tj. osadzenie w konkretnym kontekście środowiska). Model ten może być zastosowany do poziomu strategicznego, operacyjnego i taktycznego — tak, że dane wyjściowe z jednego szczebla stają się wejściowymi dla innego, a możliwa jest także analiza kaskadowych skutków między różnymi domenami (np. cyberprzestrzenią, wojskiem, zarządzaniem informacją). Nie jest to zatem narzędzie przewidywania konkretnych scenariuszy, lecz utrzymywania stabilności decyzyjnej w warunkach permanentnej niepewności. W takim ujęciu przewaga strategiczna wynika nie ze zdolności do pełnej kontroli (w cyberprzestrzeni i tak niemożliwej), lecz z kompetencji w utrzymywaniu odporności będącej fundamentem dla innych działań, w tym ofensywnych.

Należy podkreślić, że same modele analizy ryzyka muszą być przedmiotem stałej weryfikacji przydatności i kalibracji. Trudności w testowaniu na danych historycznych, czy pozyskaniu reprezentatywnych informacji wejściowych, mogą skutkować iluzją precyzji. Zaproponowane w niniejszej dysertacji rozwiązanie nie jest wyczerpujące i wymaga dalszego doskonalenia. W przypadku niezastosowania zaproponowanej metodyki szacowania ryzyka, jej elementy (wraz z kontekstem badań niniejszej dysertacji) mogą zostać wykorzystane w charakterze usystematyzowanych parametrów na rzecz tworzenia przyszłych modeli.

Powyższe ograniczenie wynika ze złożoności przedmiotu badań, przede wszystkim jego interdyscyplinarnego charakteru. Łączy on bowiem analizy działalności wewnętrznej państw oraz relacji międzynarodowych, strategii i doktryn ze zmieniającymi się potrzebami operacyjnymi oraz taktycznymi, jak również relacji sektora publicznego z prywatnym. Wymaga też uwzględnienia potencjału przemian technologicznych oraz ich oddziaływania na otoczenie. Wreszcie: sama cyberprzestrzeń gromadzi powyższe wraz z wyzwaniem współczesnej walki informacyjnej, problemami asymetrii (w tym strukturalnej) oraz czynnika ludzkiego. Analizując źródła można dojść do wniosku, że próby definiowania roli środowiska sieciocentrycznego z perspektywy politycznej, wojskowej, technologicznej lub społecznej są liczne. Mogą być jednak niewystarczające, jeżeli nie zostaną adekwatnie uzupełnione badaniem mniejszych grup i psychologii jednostki. Podatność przeciętnego obywatela, adekwatność umiejętności zespołów reagujących na cyberincydenty, czy wpływ sztucznej inteligencji na człowieka, mogą być wartościowymi oraz interesującymi kierunkami badań. Szczególnie, że skala długofalowego wpływu cyfryzacji i wynikłego z niej stałego zagrożenia (także dla pojedynczych osób) jest nieznana, a wciąż może mieć istotny, oddolny wpływ na pozostałe perspektywy.

Wyzwaniem mogą być także analizy prawne. Autonomiczność decyzji wciąż pozostaje problemem, zarówno względem działań w cyberprzestrzeni, jak również w walce kinetycznej, wykorzystującej nowoczesne rozwiązania technologiczne. Problem atrybucji zdaje się wymagać rewizji przydatności aktualnych mechanizmów legalnych reakcji państw, w sposób który będzie balansować między wolnościami obywatelskimi i skutecznością. Wiąże się to nierozdzielnie z pytaniami natury etycznej, w tym oceny samych aktorów w cyberprzestrzeni. Nielegalna cyberaktywność jest postrzegana jako oczywista konsekwencja środowiska sieciocentrycznego. Ważnym jest jednak pytanie o status osób się jej dopuszczających w czasie wojny. To czy i kiedy mogą stać się uczestnikami walki, a zatem utracić ochronę przynależną cywilom, pozostaje kwestią otwartą.

Jednakże największą niepewnością, a zarazem potencjałem badawczym, wydaje się cechować sztuczna inteligencja. Przemiany, które zaszły wraz z popularyzacją Internetu, postrzegane były jako rewolucyjne, gdyż w relatywnie krótkim czasie odmieniły właściwie każdą domenę codzienności — tak dla państw, jak i jego obywateli. Jednakże jest to perspektywa wielokrotnie dłuższa niż czas popularyzacji AI. Niezwykle szybkie tempo rozwoju, coraz szersza implementacja, a także również rosnąca złożoność poszczególnych instancji, generują adekwatnie dużą potrzebę zrozumienia wpływu AI na współczesny świat, w tym także przedmiot niniejszych badań.

Podsumowując, cyberprzestrzeń nie tylko stała się równa innym domenom prowadzenia działań, takim jak ląd, woda, powietrze i kosmos, lecz przenika każdą z nich w sposób wyjątkowy. Tym samym w każdym miejscu, które zmienia się przez procesy cyfryzacji, wnosi równie unikatowe problemy. Niespotykana nigdzie indziej skala asymetrii, złożoności aktorów i działań (w ujęciu szeroko rozumianej hybrydowości) oraz tempa rozwoju sprawia, że jest to środowisko permanentnie trudne w przewidywaniu. Wynikające z tego nieustanne ryzyko tworzy stałą niepewność, która wymaga odpowiedzi na każdym szczeblu: od środowiska międzynarodowego i innych państw, do postaw pojedynczych osób. Skutkuje to pesymistyczną wizją wykorzystania cyberprzestrzeni w przyszłych konfliktach. Postrzeganie jej jako alternatywy dla przelewu krwi, na rzecz prowadzenia cyberwojen, wydaje się błędne. Przeciwnie, daje ona przestrzeń do rozwoju brutalizacji kinetycznego pola walki, a w sferze cyfrowej — poza ryzykiem i pewnymi szansami — wnosi pogłębiającą się dehumanizację.

Wykaz rysunków i tabel

- Rysunek 1.** Poziomy planowania i prowadzenia działań, z uwzględnieniem integracji międzydomenowej, kontekstu oraz fundamentu s. 116.
- Rysunek 2.** System współpracy NATO-UE, opracowany w ramach kompleksowego podejścia do zagrożeń hybrydowych s. 124.
- Tabela 1.** Wybrane wydarzenia reprezentatywne dla okresów „nowych wojen” (ery cyfrowej) s. 163–166.

Wykaz skrótów

A2 lub AD	Anti-Access/Area Denial , strategia wojskowa polegająca na wykorzystaniu systemów obronnych i środków rażenia w celu uniemożliwienia przeciwnikowi wejścia do określonego obszaru operacyjnego oraz ograniczenia jego swobody działania w tym rejonie.
APT	Advanced Persistent Threat , długotrwała, ukierunkowana kampania cyberataków prowadzona przez zorganizowanego przeciwnika.
ASD	Australian Signals Directorate , australijska Wojskowa Służba Wywiadu Elektronicznego.
C2 lub C&C	Command & Control , infrastruktura i mechanizmy komunikacyjne wykorzystywane przez atakujących do zdalnego zarządzania zainfekowanymi systemami, koordynowania działań złośliwego oprogramowania oraz utrzymywania kontroli nad siecią ofiar.
C4	Command, Control, Communication, Computers , zintegrowany system dowodzenia i zarządzania, obejmujący procesy kierowania siłami zbrojnymi, utrzymywania łączności, wymiany informacji oraz wykorzystania technologii komputerowych do koordynacji działań operacyjnych i strategicznych.
CERT	Computer Emergency Response Team , zespół reagowania na incydenty bezpieczeństwa komputerowego, zwykle o szerszym zakresie działań niż CSIRT. W pracy występuje z wyróżnikiem krajowym (np. CERT-UA) lub wskazaniem afiliacji (np. CERT NASK). <i>Zob. CSIRT.</i>
CIA	Central Intelligence Agency , amerykańska Centralna Agencja Wywiadowcza.
CISA	Cybersecurity and Infrastructure Security Agency , amerykańska Agencja ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury, podlegająca pod Departament Bezpieczeństwa Krajowego USA.
CNMF	Cyber National Mission Forces , amerykańskie Wspólne Siły Cybernetyczne, wspierające Dowództwo Cybernetyczne Stanów Zjednoczonych (USCYBERCOM, United States Cyber Command).
CSIRT	Computer Security Incident Response Team , zespół reagowania na incydenty bezpieczeństwa komputerowego, zwykle o węższym zakresie

działań niż CERT. Jeżeli nie wskazano wyróżnika krajowego, wówczas przyjąć należy, że jest to zespół polski (np. CSIRT GOV). *Zob. CERT.*

CVE	Common Vulnerabilities and Exposures , publiczny system identyfikacji i katalogowania luk w zabezpieczeniach oprogramowania i sprzętu, ułatwiający ich jednoznaczne oznaczanie, śledzenie oraz wymianę informacji między społecznością bezpieczeństwa. Prowadzony jest przez różne instytucje. <i>Zob. KEV.</i>
DHS	Department of Homeland Security , Departament Bezpieczeństwa Krajowego Stanów Zjednoczonych.
DoD	Department of Defense , Departament Obrony Stanów Zjednoczonych (od 5 września 2025 Departament Wojny, DoW, Department of War, jednak w niniejszej pracy zachowano uprzednią nazwę celem zachowania spójności ze źródłami).
DoE	Department of Energy , Departament Energii Stanów Zjednoczonych.
DoS	Denial of Service , blokada działania usługi, najczęściej w wyniku przeciążenia serwera nadmiarem zapytań (choć nie tylko). W przypadku ataku wykorzystującego koordynowaną infrastrukturę rozproszoną, stosowany jest skrót DDoS.
EDR	Endpoint Detection and Response , system monitorowania urządzeń końcowych, wykrywające podejrzane aktywności oraz umożliwiające szybką reakcję na zagrożenia. <i>Zob. XDR.</i>
EEAS	European External Action Service , Służby Działań Zewnętrznych Unii Europejskiej.
EMP	Electromagnetic Pulse , impuls elektromagnetyczny, zdolny zakłócić lub zniszczyć systemy elektroniczne, co do zasady w małej skali <i>Zob. HEMP.</i>
ENISA	European Union Agency for Cybersecurity , Agencja Unii Europejskiej ds. Cyberbezpieczeństwa.
EU INTCEN	EU Intelligence and Situation Centre , Centrum Wywiadu i Sytuacji Unii Europejskiej.
FBI	Federal Bureau of Investigation , amerykańskie Federalne Biuro Śledcze.
FLN	Front de Liberation Nationale , algierski Front Wyzwolenia Narodowego.
GRU	Главное разведывательное управление , ГРУ, rosyjski Główny Zarząd Wywiadowczy (wywiad wojskowy).
HC3	Health Sector Cybersecurity Coordination Center , amerykańskie Centrum Koordynacji Cyberbezpieczeństwa Sektoru Zdrowia, podległe

pod Departament Zdrowia i Pomocy Humanitarnej (HHS, Department of Health and Human Services).

HEMP	High-altitude Electromagnetic Pulse , impuls elektromagnetyczny powstający w wyniku wybuchu jądrowego na dużej wysokości, zdolny zakłócić lub zniszczyć systemy elektroniczne i sieci energetyczne na dużą skalę. <i>Zob. EMP.</i>
HTTP	Hypertext Transfer Protocol , protokół komunikacyjny warstwy aplikacji, służący do przesyłania dokumentów hipertekstowych (np. stron WWW) między serwerem a przeglądarką. W wersji szyfrowanej oznaczany jako HTTPS.
ICS	Industrial Control Systems , ogólna kategoria urządzeń elektronicznych, sterujących kujących infrastrukturą przemysłową lub automatyzujących ją.
ICT	Information and Communication Technology , zbiór technologii obejmujących przetwarzanie, gromadzenie, przesyłanie i udostępnianie informacji za pomocą systemów komputerowych, sieci telekomunikacyjnych oraz narzędzi cyfrowych.
IoC	Indicators of Compromise , ślady lub artefakty wskazujące na potencjalne naruszenie bezpieczeństwa systemu lub sieci.
IoT	Internet of Things , Internet rzeczy, tj. sieć połączonych urządzeń i obiektów wyposażonych w czujniki, oprogramowanie oraz mechanizmy komunikacji.
IT	Information Technology , technologie cyfrowe służące do przetwarzania i zarządzania informacją w systemach. <i>Zob. OT.</i>
KEV	Known Exploited Vulnerabilities , katalog podatności w oprogramowaniu, co do których wiadomo, że są wykorzystywane w atakach. Prowadzony jest przez amerykańską CISA wraz z Narodowym Instytutem Standardów i Technologii (NIST, National Institute of Standards and Technology) oraz organizacją non-profit MITRE Corporation. <i>Zob. CVE.</i>
LAWS	Lethal Autonomous Weapon Systems , autonomiczne systemy uzbrojenia, mogące samodzielnie identyfikować, wybierać i atakować cele, bez bezpośredniej kontroli człowieka.
NCA	National Crime Agency , brytyjska Narodowa Agencja ds. Przestępczości.
NCSC	National Cyber Security Centre , brytyjskie Narodowe Centrum Cyberbezpieczeństwa, podlegające pod Centralę Łączności Rządowej (GCHQ, Government Communications Headquarters).

NIST	National Institute of Standards and Technology , amerykański Narodowy Instytut Standardów i Technologii.
NSA	National Security Agency , amerykańska Agencja Bezpieczeństwa Narodowego.
NTRA	National Telecom Regulatory Authority , egipska instytucja nadzorująca sektor telekomunikacji.
OODA	Observe, Orient, Decide, Act , cykliczny proces podejmowania decyzji w dynamicznych warunkach: obserwacja otoczenia, orientacja w sytuacji, wybór działania i jego realizacja.
OT	Operational Technology , technologie sterujące fizycznymi procesami i urządzeniami, często integrowane z IT dla zapewnienia bezpieczeństwa i efektywności. <i>Zob. IT, SCADA.</i>
RMA	Revolution in Military Affairs , koncepcja opisująca zasadnicze zmiany w sposobie prowadzenia działań wojennych, wynikające z przełomowych innowacji technologicznych, organizacyjnych i doktrynalnych, które radykalnie zwiększają skuteczność sił zbrojnych i zmieniają charakter konfliktu.
SCADA	Supervisory Control And Data Acquisition , system nadzorowania i sterowania procesami technologicznymi lub produkcyjnymi. <i>Zob. OT.</i>
SIEM	Security Information and Event Management , system zbierający i analizujący logi oraz zdarzenia z różnych źródeł w sieci, aby wykrywać incydenty bezpieczeństwa i wspierać reakcję na nie.
SKW	polska Służba Kontrwywiadu Wojskowego .
SOC	Security Operations Center , centrum operacji (cyber)bezpieczeństwa.
SWR	Служба Внешней Разведки, СВР , rosyjska Służba Wywiadu Zagranicznego.
TCP	Transmission Control Protocol , protokół komunikacyjny warstwy transportowej, przesyłający dane między urządzeniami w sieci z zachowaniem kontroli kolejności i integralności pakietów.
XDR	Extended Detection and Response , rozszerzony EDR, integrujący dane z wielu obszarów (urządzenia, sieć, poczta, chmura), aby zapewnić szerszy i bardziej skoordynowany obraz zagrożeń oraz skuteczniejszą reakcję. <i>Zob. EDR.</i>

Bibliografia

Akty prawne, regulacyjne

Charter of The United Nations and Statute of the International Court of Justice, San Francisco 1945.

Cybersecurity Law of the People's Republic of China [中华人民共和国网络安全法], [promulgated by the Standing Committee of the National People's Congress, Nov. 7, 2016, effective Jun. 1, 2017].

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. 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, Eur-lex L 333/80, [NIS2].

Ocena skutków regulacji, 3 października 2024, [projekt UC32]: Załącznik nr 4 do OSR: podsumowanie wydatków dla poszczególnych części budżetowych w zł.

Protokół dodatkowy do konwencji genewskich z 12 sierpnia 1949 r., dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych, [Dz. U. z 1992 r., nr 41, poz. 175, załącznik].

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011, Eur. Lex. PE/41/2022/INIT [DORA].

Rozporządzenie Wykonawcze Rady (UE) 2020/1125 z dnia 30 lipca 2020 r. wykonujące rozporządzenie (UE) 2019/796 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim, Eur. Lex. L 246/4.

Ustawa z dnia (...) 2025 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, projekt z dnia 7 lutego 2025 r. [projekt UC32].

Volumina legum. Tom III, Petersburg 1859.

Źródła publikowane

Alexander O., Belisle M., Steele J., *MITRE ATTE&CK® for Industrial Control Systems: Design and Philosophy*, McLean 2020.

Anderson K., *Rise of the Drones: Unmanned Systems and the Future of War*, Subcommittee on National Security and Foreign Affairs, Committee on Oversight and Government Reform, US House of Representatives, 23 March, [11th Congress, 2nd Session] 2010.

Bayley H., *A citizen's guide to NATO's priorities after the Wales Summit*, Brussels 2014.

Beauchamp-Mustafaga N. i inni, *Deciphering Chinese Deterrence Signalling in the New Era: An Analytic Framework and Seven Case Studies*, [RR-A1074-1], Santa Monica 2021.

Bejar A., *Balancing Social Media with Operations Security (OPSEC) in the 5a. CONTRACT NUMBER 21st Century*, [OMB No. 0704-0188], 2010.

Broeders D., Adamson L., Creemers C., *A coalition of the unwilling? Chinese and Russian perspectives on cyberspace*, [The Hague Program For Cyber Norms Policy Brief], Leiden 2019.

Brussels Summit Communiqué, 14 June, [NATO Press Release (o86)], 2021.

Brussels Summit Declaration, 11 July, [NATO Press Release (brak numeru)], 2018.

Buckley G., Caulfield T., Becker I., *“It May Be a Pain in the Backside but...” Insights into the Resilience of Business after GDPR*, [referat konferencyjny] *New Security Paradigms Workshop*, North Conway, 2022.

Burdette Z. i inni, *An AI Revolution in Military Affairs? How Artificial Intelligence Could Reshape Future Warfare*, [WR-A4004-1], 2025.

Calha J.M., *Hybrid warfare? NATO’s new strategic challenge*, NATO Parliamentary Assembly Defence and Security Committee General Report, 10 October [166 DSC 15 E bis], 2015.

Centralne Archiwum Wojskowe Samodzielny Referat Informacyjny Dowództwa Okręgu Korpusu nr IX, sygn. I.371.9A.22, *Instrukcja o ochronie tajemnicy wojskowej*, Warszawa 1932.

CERT NASK, NCSC, FBI, CISA, NSA, SKW, *Russian Foreign Intelligence Service (SVR) Cyber Actors Use JetBrains TeamCity CVE in Global Targeting*, [1.0] 2023.

Cheng D., *China’s Active Defense Strategy and Its Regional Impact*, 27 January, [U.S.-China Economic and Security Review Commission Hearing], 2011.

Choudhury M.R., *Letter dated 8 March 2021 from the Panel of Experts on Libya established pursuant to resolution 1973 (2011) addressed to the President of the Security Council*, [S/2021/229], 2021.

CIA, *Statement of Work for Asymmetric Warfare Threats to US Interests: Expert Panel Support*, Washington 1998.

CISA i inni, *Mitigating Log4Shell and Other Log4j-Related Vulnerabilities*, [AA21-356A], 2021.

CISA i inni, *Scattered Spider*, [AA23-320A], 2025.

CISA, *Cyber-Attack Against Ukrainian Critical Infrastructure*, [IR-ALERT-H-16-056-01], 2021.

CISA, *Cybersecurity Incident & Vulnerability Response Playbooks. Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems*, Rosslyn 2021.

CISA, *DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*, [AA21-131A], 2021.

CISA, FBI, *Product Security Bad Practices*, [Joint Guidance v2.0], 2025.

CNMF i inni, *North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime’s Military and Nuclear Programs*, [AA24-207A], 2024.

Coordinating National Resilience to Electromagnetic Pulses, Executive Order 13865, 26 March 2019, „Federal Register”, Vol. 84, No. 61.

Countering Hybrid Threats. Working document of the European External Action Service, 13 May, [EEAS (2015) 731], 2015.

CTA, *Year 7 Report*, [b.m.w.] 2025.

Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation, 12 May, [DPC ref. IN-20-8-1] 2023.

Department of Defense, *Strategy for Operating in Cyberspace*, Arlington 2011.

Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China* 2020, Virginia 2020.

Department of Defense, *Cyber Strategy*, 2018.

Department of Defense. Defense Communications Agency, White House Audio Recordings 1961–1963, Access No. WH-103-001, ID JFKWHA-103-001, J.F. Kennedy, *Remarks to the Graduating Class of the U.S. Military Academy*, West Point-New York 1962, 8:22–8:48 [audio].

DHS, *Strategy for Protecting and Preparing the Homeland Against Threats of Electromagnetic Pulse and Geomagnetic Disturbances*, 9 October 2018.

Director of Net Assessment, 22 August, [DoDD 5111.11], 2001.

DoD, *Defense Industrial Base Cybersecurity Strategy* 2024, 21 March 2024.

DoE, *Geomagnetic Disturbance Monitoring Approach and Implementation Strategies*, [DoE 20585], 2019.

EG-CERT, NTRA [arab. الجهاز القومي لتنظيم الاتصالات], *IOT Cyber Security Framework*, [EG-CESC-OPER 100-01 DP-2210-EN], 2022.

ENISA, *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*, Brussels 2017.

ENISA, *Technical Implementation Guidance On Commission Implementing Regulation (EU) 2024/2690 laying down rules for the application of NIS2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures*, Luxembourg 2025.

ENISA, *Technical Implementation Guidance*, Luxembourg 2025.

ESET Research, *APT Activity Report*, [OCT24-MAR25] 2025.

EU strategic communication to counteract anti-EU propaganda by third parties, 21 November, [P8_TA (2016) 0441], 2016.

European Council meeting (19 and 20 March 2015) — *Conclusions*, 20 March, [Cover note EUCO 11/15], 2015.

Europol, *Facing reality? Law enforcement and the challenge of deepfakes, an observatory report from the Europol Innovation Lab*, Luxembourg 2022.

Europol, *Internet Organised Crime Threat Assessment* 2020, Hague 2020.

F. Lieber, *Instructions for the Government of Armies of The United States in the Field*, Washington 1898. J.P. Eckert,

FBI, CISA, ASD, ACSC, #StopRansomware: *Play Ransomware*, [AA23-352A], 2025.

FBI, CISA, NSA i inni, *Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure*, [AA24-249A] 2024.

Final Joint Framework on countering hybrid threats. A European Union response, 6 April, [Joint communication JOIN(2016)18 | CELEX: 52016JCO018], 2016.

Greene C.V., *Cyberwarfare and our Allies: The Importance of Theater Security Cooperation*, [OMB No. 0704-01880], 2009.

HC3, *Threat Profile: China-Based Threat Actors*, [202308161700], 2023.

HM GOV, *National Cyber Strategy 2022. Pioneering a cyber future with the whole of the UK*, London 2022.

Horvath M.D., *Wikileaks.org—An Online Reference to Foreign Intelligence Services, Insurgents, or Terrorist Groups?*, [NGIC-2381-0617-08], 2008.

Insikt Group, *Ghostwriter in the Shell: Expanding on Mandiant's Attribution of UNC1151 to Belarus*, [CTA-2022-0318], 2022.

Institute of Electrical and Electronics Engineers, Inc., *2019 North American power symposium (NAPS)*, Wichita 2019.

J.W. Mauchly, *Electronic numerical integrator and computer*, (Patent US3120606A), filed 26.06.1947, issued 04.02.1964.

Jinping X., *Speech at the Work Conference for Cybersecurity and Informatization [在网络安全和信息化工作座谈会上的讲话]*, 19 April 2016, The State Council PRC [中华人民共和国中央人民政府].

Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, 8 July, [NATO Press Release (119)], 2016.

Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, 8 July, [PR: (2016) 119], 2016.

Joint Declaration on EU-NATO Cooperation, by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, 10 July, [PR: (2018) 095], 2018.

Joint Staff Working Document. EU operational protocol for countering hybrid threats, 5 July, [SWD (2016) 227 z późn. zm. — wersja finalna], 2016.

Joint Warfare of the Armed Forces of the United States [Joint Pub. 1], Washington 1995.

Karásková I., Běrziņa-Čerenkova U.A., Němečková K., *Foreign Electoral Interference Affecting EU Democratic Processes*, [study requested by the Authority for European Political Parties and European Political Foundations], 2023.

Kofman M. i inni, *Russian Military Strategy: Core Tenets and Operational Concepts*, [DRM-2021-U-029755], 2021.

Komitet Regionów UE, *Zwalczanie analfabetyzmu funkcjonalnego – Opracowanie ambitnej europejskiej strategii przeciwdziałania wykluczeniu i wspierania rozwoju osobistego*, 1 slipca, [2010/C 175/07], 2010.

Kristi R., Järvenpää P., *A New Era of EU-NATO Cooperation: How to Make the Best of a Marriage of Necessity*, Tallinn 2017.

Kukkola J., Nikkarila J.P., Ristolainen M., *Asymmetric frontlines of cyber battlefields*, [referat konferencyjny] 22nd ICCRTS Proceedings. *Frontiers of C2*, Los Angeles 2017.

Langø H.I., *Slaying Cyber Dragons: Competing Academic Approaches to Cyber Security*, [NUPI-WP 820], Oslo 2013.

Lehman J.H., *Military Engagement with Social Media*, [OMB No. 0704-0188], 2011.

Marczak B. i inni, *An Analysis of China's "Great Cannon"*, [referat konferencyjny] 5th USENIX Workshop on Free and Open Communications on the Internet, Washington 2015.

Marshall A.W., *Some Thoughts on Military Revolutions*, Memorandum Office of Net Assessment, 29.08.1993.

Mell P., Spring J., *Likely Exploited Vulnerabilities. A Proposed Metric for Vulnerability Exploitation Probability*, [NIST CSWP 41], 2025.

Microsoft, *Defending Ukraine: Early Lessons from the Cyber War*, [Report 22.06], 2022.

Narayanan V., Howard P.N., Kollanyi B., Elswah M., *Russian Involvement and Junk News during Brexit*, [COMPROP D.M.2017.10], 2017.

National Military Strategy of the United States of America. *A Strategy of Flexible and Selective Engagement*, Washington 1995.

NATO 2022 Strategic Concept, Madrid 2022.

NCC, *Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment*, [NCC/NCCIC v2.2], 2019.

NCSC, CISA, FBI, NSA, Advisory. *Further TTPs associated with SVR cyber actors*, [1.0], 2021.

Next Steps in NATO's Transformation: *To the Warsaw Summit and Beyond*, [White Paper — NATO Transformation Seminar], Washington 2015.

NSA i inni, *Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System*, [U/OO/198904-25, PP-25-3703], 2025.

NSA i inni, *Russian GRU Targeting Western Logistics Entities and Technology Companies*, [U/OO/157019-25, PP-25-2107], 2025.

NSA, CISA, FBI, *Chinese State-Sponsored Cyber Operations: Observed TTPs*, [U/OO/163624-21, PP-21-0971] 2021.

NSA, CISA, FBI, NCSC, *Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments*, [U/OO/158036-21, PP-21-0782], 2021.

NSA, CISA, FBI, *Russian SVR Targets U.S. and Allied Networks*, [U/OO/132340-21, PP-21-0292], 2021.

NSA, FBI, NCSC i inni, *Russian GRU Targeting Western Logistics Entities and Technology Companies*, [U/OO/157019-25, PP-25-2107] 2025.

NSA, FBI, *Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware*, [U/OO/160679-20, PP-20-0714], 2020.

Nye Jr. J.S., *Cyber Power*, [OMB No. 0704-0188], 2010.

Peixi X., *A Chinese Perspective on the Future of Cyberspace*, [Cyberstability Paper Series, GCSC, HCSS], 2021.

Pintat X., *NATO's Readiness Action Plan: Assurance and Deterrence for the post-2014 Security Environment*, NATO Parliamentary Assembly Defence and Security Committee Report, 10 October, [167 DSCFC 15 E bis], 2015.

PLA Academy of Military Science, Military Strategy Department [军事科学院战略研究部] — S. Zhaoli (ed.), *Science of Military Strategy* [战略学], Beijing 2013.

Prasa i jej stosunek do pracy O.II. przy ochronie tajemnic wojskowych i zwalczaniu szpiegostwa. *Instrukcja dla D.O.K.*, Nr 16862/II Inf.III.Z.W.I., 1923.

Program for Joint Education (PJE), [U.S. Army War College Documentation], Carlisle Barracks 1996.

Pry P.V., *China: EMP Threat. The People's Republic of China Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack*, 10 June, [TFNHS Report], 2020.

Pry P.V., *Russia: EMP Threat*, [AD1123491] 2025.

Pry P.V., *RUSSIA: EMP THREAT The Russian Federation's Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack*, [TFNHS Report], 2021.

Quadrennial Defense Review Report, D. Rumsfeld (ed.), Washington D.C. 2006.

Remarks to the United States Attorneys Conference, „Weekly Compilation of Presidential Documents” [Ro4], 2001, Vol. 37, No. 48.

Revolution in Military Affairs. A selected Bibliography, [U.S. Army War College Documentation], Carlisle Barracks 1996.

Robinson S., *Time to next exploit*, [WITH-SECURE 7/16/2025], 2025.

Seagroatt S.B., *Persistent Engagement and Defend Forward: the United States' Critical Role in Cyberspace*, [OMB 0704-0188] 2021.

Sipri Yearbook 2001, Stockholm 2001.

Sitek M., Prokopek A., Penszko P., Chyl K., Haman J., *Główne wyniki międzynarodowego badania umiejętności dorosłych PIAAC 2023*, Warszawa 2024.

Siukonen V., Ristolainen M., Nikkarila J.P., Kukkola J., *Are We There Yet?: Monitoring the Technical Deployment of the National Segments of the Internet*, [referat konferencyjny] MILCOM 2019–2019 IEEE Military Communications Conference (MILCOM), Norfolk 2020.

Skouloudi C., Malatras A., Naydenov R., Dede G., *Guidelines for Securing the Internet of Things. Secure supply chain for IoT*, Brussels 2020.

Słownik terminów i definicji NATO, [AAP-6], 2017.

State Council Information Office of the People's Republic of China [中华人民共和国国务院新闻办公室], *White Paper: China's Law-Based Cyberspace Governance in the New Era* [新时代的中国网络法治建设], Beijing 2023.

State Council Information Office of the People's Republic of China [中华人民共和国国务院新闻办公室], *White Paper: China's Military Strategy* [中国的军事战略], Beijing: 2015.

State Council Information Office of the People's Republic of China [中华人民共和国国务院新闻办公室], *White Paper: The Diversified Employment of China's Armed Forces* [中国武装力量的多样化运用], Beijing 2013.

Stouffer K. i inni, *Guide to Operational Technology (OT) Security*, [NIST SP 800-82r3], 2023.

ThaiCERT, *“PromptLock”: First-Ever Ransomware Leveraging AI for File Encryption Discovered*, [311/68], 2025.

Thales P.T. i inni, *Towards an Active, Autonomous and Intelligent Cyber Defense of Military Systems: the NATO AICA Reference Architecture*, [IST-152-RTG], 2018.

The White House, *National Security Strategy*, Washington 2022.

Trimintzios P. i inni, *Cybersecurity in the EU Common Security and Defence Policy (CSDP) Challenges and risks for the EU*, [EPRS/STOA/SER/16/214N], 2017.

UAE Cyber Security Council, *Banshee Stealer Targets macOS Users*, [432316724], 2025.

UN General Assembly, *Lethal autonomous weapons systems. Report of the Secretary-General*, [A/79/88], 2024.

UNIDIR, *The Weaponization of Increasingly Autonomous Technologies: Artificial Intelligence*, „UNIDIR Resources” 2018, No. 8.

Unit42, *2022 Ransomware Threat Report*, Santa Clara 2022.

US District Court For the Central District of California, *Indictment. 18 U.S.C. § 1349: Conspiracy to Commit Wire Fraud; 18 U.S.C. § 371: Conspiracy; 18 U.S.C. § 1028A(a)(1): Aggravated Identity Theft; 18 U.S.C. §§ 981, 982, 1029, 1030 and 28 U.S.C. § 2461(c): Criminal Forfeiture*, [CR No. 2:24-CR00595-JWH], 2015.

USA-GOV, *Humanitarian benefits of emerging technologies in the area of lethal autonomous weapon systems*, [CCW/GGE.1/2018/WP.4], 2018.

Wales Summit Declaration, 5 September, [NATO Press Release (120)], 2014.

Warsaw Summit Communiqué. *Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016*, [PR (2016) 100], 2016.

Williams P., Fiddner D. (eds.), *Cyberspace: Malevolent Actors, Criminal Opportunities and Strategic Competition*, [AD1014198] 2016.

Wood P., *2015 Internet Security Threat Report*, [04/15 21347933, Vol. 20], 2015.

Wspólny komunikat do Parlamentu Europejskiego i Rady: *Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym*, 6 April, [JOIN (2016) 018], 2016.

Zettl-Schabath K., Bund J., Gschwend T., Borrett C., *Advanced Threat Profile. APT29 — Stealth at Scale*, „European Repository of Cyber Incidents” 2023, 23 February.

Военная доктрина Российской Федерации, 25 декабря, Москва 2014.

Доктрина информационной безопасности Российской Федерации, [утверждена Указом Президента РФ № 646 от 5 декабря 2016], Москва 2016.

Концепция национальной безопасности Российской Федерации, [в редакции Указа Президента Российской Федерации от 10 января 2000], Москва 2000.

Министерство Обороны Российской Федерации, *Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве*, Москва 2011.

Стратегия национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 2 июля 2021 г. № 400.

Monografie

Abu Rumman M., Abu Hanieh H., *Infatuated with martyrdom: female jihadism from Al Qaeda to the “Islamic State”*, Amman 2017.

Al Kahtani AM., *The Performance of the Saudi Arabian Press During the Gulf Conflict, 1990-1991*, Leeds 1999.

Amstutz J.B., *Afghanistan: The First Five Years of Soviet Occupation*, Washington 1994.

- Anderson E., *State-Specific Vulnerabilities to Russian Influence: A Case Study of Montenegro*, Brno 2019.
- Arif K.M., *Khaki Shadows: Pakistan 1947–1997*, Oxford 2001.
- Arkin W.M., *Divining Victory Airpower in the 2006 Israel-Hezbollah War*, Maxwell AFB 2007.
- Assmann A., Conrad S. (eds.), *Memory in a Global Age. Discourses, Practices and Trajectories*, New York 2010.
- Atkinson R.J., *NATO Cyber Defence, 2000–2022*, Londyn (Canada) 2023.
- Bania R., Zdulski K. (red.), *Bezpieczeństwo narodowe i międzynarodowe w regionie Bliskiego Wschodu i Północnej Afryki (MENA) u progu XXI wieku*, Łódź 2012.
- Baran P., *On Distributed Communications. Networks*, Santa Monica 1962.
- Beauchamp-Mustafaga N. i inni, *Denial Witout Disaster. Keeping a US-China Conflict over Taiwan Under the Nuclear Threshold*, Santa Monica 2024.
- Bekefi T., Epstein M.J., *Integrating Social and Political Risk Into Management Decision-Making*, Toronto 2006.
- Bekesiene S., Hoskova-Mayerova S. (eds.), *Challenges to National Defence in Contemporary Geopolitical Situation*, Wilno 2022.
- Bilski R., *Kocioł Bałkański*, Warszawa 2000.
- Black J. i inni, *Strategic competition in the age of AI Emerging risks and opportunities from military use of artificial intelligence*, Santa Monica-Cambridge 2024.
- Blumenthal M., *The 51 Day War: Resistance and Ruin in Gaza*, London 2015.
- Braithwaite R., *Afgantsy: The Russians in Afghanistan 1979–89*, New York 2011.
- Brangetto P., Maybaum M., Stinissen J. (eds.), *2014 6th International Conference on Cyber Conflict*, Tallin 2014.
- Broeders D., Berg B. (eds.), *Governing Cyberspace Behavior, Power, and Diplomacy*, Lanham-Boulder-New York-London 2020.
- Brown A., *The Gorbachev Factor*, Oxford 1997.
- Browne M.W., *The New Face of War*, New York 1965.
- Bures O., Carrapicio H. (eds.), *Security Privatization How Non-security-related Private Businesses Shape Security Governance*, [b.m.w.] 2018.
- Burke E.J., Gunness K., Cooper C.A., Cozad M., *People's Liberation Army Operational Concepts*, Santa Monica 2020.
- Campbell-Kelly M., Aspray W., *Computer: A History of the Information Machine*, New York 1996.
- Cavelty M.D., Mauer V. (eds.), *The Routledge Handbook of Security Studies*, Abingdon-New York 2010.
- Chalk F.R., Jonassohn K., *The History and Sociology of Genocide: Analyses and Case Studies*, New Haven 1990.
- Chao F., *Sunzi's Art of War: A Structural Analysis*, Beijing 2010.
- Cheng D., *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, California 2017.

- Choucri N., *Cyberpolitics in International Relations*, Cambridge 2012.
- Cîrciumaru F., Cojocaru I. (eds.), *The Complex and Dynamic Nature of the Security Environment*, Bucharest 2024.
- Civikov G., *Proces Miloszewicia. Relacja obserwatora*, Warszawa 2009.
- Čížik T. (ed.), *Information Warfare — New Security Challenge for Europe*, Bratislava 2017.
- Clarke R.A., Knake R., *Cyber War: The Next Threat to National Security and What to Do About It*, [b.m.w] 2010.
- Clausewitz C., *O wojnie*, Warszawa 2010.
- Claverie B., Prébot B., Buchler N., Du Cluzel F. (eds.), *Cognitive Warfare*, Neuilly 2022.
- Conlin D., *Pirates of the Atlantic: robbery, murder and mayhem off the Canadian East Coast*, Halifax 2009.
- Cosentino G., *Social Media and the Post-Truth World Order The Global Dynamics of Disinformation*, Cham 2020.
- Craig D.W., *Asymmetrical Warfare and the Transnational Threat: Relearning the Lessons from Vietnam*, North York 1998.
- Crile G., *Charlie Wilson's War: The Extraordinary Story of the Largest Covert Operation in History*, New York 2003.
- Cruz T., Simoses P. (eds.), *ECCWS 2019 — Proceedings of the 18th European Conference on Cyber Warfare and Security*, New York 2019.
- Cusumano E., Corbe M. (eds.), *A Civil-Military Response to Hybrid Threats*, London 2018.
- Слипченко В.И., *Война будущего (прогностический анализ)*, Москва 1999.
- Слипченко В.И., *Войны нового поколения: дистанционные бесконтактные*, Москва 2004.
- Darczewska J., *Diabeł tkwi w szczegółach. Wojna informacyjna w świetle doktryny wojennej Rosji*, Warszawa 2015.
- Davies B.J. (ed.), *Warfare in the Eastern Europe, 1500–1800*, Leiden 2012.
- Davies C.C., *Warren Hastings, and Oudh*, Oxford 1939.
- Deibert R., Palfrey J., Rohozinski R., Zittrain J. (eds.), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, Cambridge 2010.
- Dembołęcki W., *Pamiętniki o Lisowczykach, czyli przewagi elearów polskich. 1619–1623*, Kraków 1859.
- Dick C.J., *Mujahideen Tactics in the Soviet-Afghan War*, Camberley 2002.
- Dmochowski A., *Wietnam: wojna bez zwycięzców*, Kraków 1991.
- Dočkal J., Jirsa M., Kaderka J. (eds.), *Proceedings of Conference SPI 2017: Security and Protection of Information*, Brno 2017.
- Earle E.M., *Makers of Modern Strategy from Machiavelli to Hitler*, Princeton 1943.
- Easton D., *A framework for political analysis*, New York 1965.
- Easton D., *The Political System. An Inquiry into the State of Political Science*, New York 1966.

- Ellerby C.R., *British Interests in the Falkland Islands: Economic Development, The Falkland Lobby and the Sovereignty Dispute. 1945 to 1989*, Oxford 1990.
- Engel D., Fischer M. (eds.), *Proceedings of the 17th International Conference on Availability, Reliability and Security*, Vienna 2022.
- Ertan A., Floyd K., Pernik P., Stevens T. (eds.), *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, Tallin 2020.
- Ertan A., Floyd K., Pernik P., Stevens T. (eds.), *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, Tallinn 2020.
- Fall B.B., *Street Without Joy: The French Debacle in Indochina*, Mechanicsburg 1994.
- Fang I., *A History of Mass Communication Six Information Revolutions*, New York 1997.
- Ferguson N., *The Ascent of Money: A Financial History of the World*, New York 2008.
- Flower K., *Medieval Mercenaries volume 1. The Great Companies*, Oxford 2000.
- Fong B.C.H., Wu J., Nathan A.J. (eds.), *China's Influence and the Center-periphery Tug of War in Hong Kong, Taiwan and Indo-Pacific*, London 2020.
- Foran J., *Taking Power: On the Origins of Third World Revolutions*, New York 2005.
- Forbes A.D.W., *Warlords and Muslims in Chinese Central Asia: a political history of Republican Sinkiang 1911–1949*, Cambridge 1986.
- Ford M., Hoskins A., *Radical War. Data, Attention and Control in the Twenty-First Century*, Oxford 2022.
- Forstreuter K., *Die deutsche Sprache im auswärtigen Schriftverkehr des Ordenslandes und Herzogtums Preußen*, Königsberg 1933.
- Foucault M., "Society must be defended". *Lectures at the Collège de France*, Macey D. (trans.), London 2003.
- Freedman F., *Przyszła Wojna*, tłum. W. Jeżewski, Ożarów Mazowiecki 2019.
- Fronza M.P., *Between Rome and Carthage. Southern Italy during the Second Punic War*, Cambridge 2010.
- Gaddis J.L., *Zimna Wojna. Historia podzielonego świata*, Kraków 2007.
- Gardner H., *Crimea, Global Rivalry, and the Vengeance of History*, New York 2015.
- Gareyev M.A., *If War Comes Tomorrow? The Contours of Future Armed Conflict*, Fomenko Y.V. (trans.), Kipp J.W. (ed.), London 1998.
- Garnett J.C., *Commonsense and the Theory of International Politics*, London 1984.
- Garver J.W., *Protracted Contest: Sino-Indian Rivalry in the Twentieth Century*, Washington 2001.
- Gazzini T., *The Changing Rules on the Use of Force in International Law*, Manchester 2005.
- Gibas-Krzak D., *Asymetryczne Bałkany*, Częstochowa 2015.
- Giles J.A., *Roger of Wendover's Flowers of History: Comprising the History of England from the Descent of the Saxons to A.D. 1235. Volume II*, London 1849.
- Gill B. i inni (eds.), *SIPRI Yearbook 2010. Armaments, Disarmament and International Security*, Oxford 2010.

- Gobodo-Madikizela P. (ed.), *Breaking Intergenerational Cycles of Repetition A Global Dialogue on Historical Trauma and Memory*, Opladen-Berlin-Toronto 2016.
- Goldsworthy A., *The Fall of Carthage: The Punic Wars 265–146 BC*, London 2006.
- Gooch J. (ed.), *The Boer War. Distraction, Experience and Image*, London-New York 2013.
- Gray C.S., *Categorical Confusion? The Strategic Implications of Recognizing Challenges Either as Irregular or Traditional*, Carlisle 2012.
- Gray C.S., *The Future of Strategy*, London 2015.
- Gray C.S., *The Strategy Bridge: Theory for Practice*, New York 2010.
- Grey C.S., *Modern Strategy*, Oxford 1999.
- Grey C.S., *Strategic Studies: A Critical Assessment*, Westport 1982.
- H. Johnston, B. Klandermans (eds.), *Social Movements and Culture. Volume 4*, Minneapolis 1995
- Hakala J., Melnychuk J., *Russia's Strategy in Cyberspace*, Riga 2021.
- Hall E.T., *Beyond culture*, New York 1989.
- Hanson V.D., *A War Like No Other: How the Athenians and Spartans Fought the Peloponnesian War*, New York 2006.
- Hart B.L., *Strategy: The Indirect Approach*, London 1967.
- Hart B.L., *Strategy. Second revised edition*, London 1991.
- Harvey D., *Justice, Nature and the Geography of Difference*, Cambridge 1996.
- Haug K.E., Maaø O.J. (eds.), *Conceptualising Modern War*, London 2011.
- Head T., Landes R. (eds.), *The Peace of God: Social Violence and Religious Response in France around the Year 1000*, Ithaca-London 1992.
- Heap B., Hansen P., Gill M., *Strategic Communications Hybrid Threats Toolkit* *Strategic Communications Hybrid Threats Toolkit*, Riga 2021.
- Heim M. (ed.), *The Metaphysics of Virtual Reality*, Oxford 1993.
- Hellige H.D. (hg.), *Geschichten der Informatik. Visionen, Paradigmen, Leitmotive*, Berlin 2004.
- Herman E.S., Hammond P. (eds.), *Degraded Capability: The Media and the Kosovo Crisis*, London 2000.
- Hoffman F., *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington 2007.
- Holmes D. (ed.), *Virtual Politics: Identity and Community in Cyberspace*, London-Thousand Oaks-New Delhi 1997.
- Hoskins A., O'Loughlin B., *War and Media. The Emergence of Diffused War*, Cambridge 2010.
- Hristova A. (ed.), *Social Response to Polycrisis: The Case of Bulgaria*, New York 2024.
- Huber T.M. (ed.), *Compound Warfare: The Fatal Knot*, Fort Leavenworth 2002.
- Huntington S.P., *Zderzenie cywilizacji i nowy kształt ładu światowego*, Warszawa 2011.
- Ivanov H., *Inside Propaganda Serbian Media in the Yugoslav Wars 1991–1995*, London 2021.

- Jajodia S., Samarati P., Cimoto S. (eds.), *Proceedings of the IFIP TC 11 23rd International Information Security Conference*, Milano 2008.
- Jalali A.A., Grau L.W., *The Other Side of the Mountain: Mujahideen Tactics in the Soviet-Afghan War*, Quantico 2002.
- Jančárková T., Lindström L., Signoretti M., Tolga I., Visky G. (eds.), *12th International Conference on Cyber Conflict. 20/20 Vision: The Next Decade. Proceedings 2020*, Tallin 2020.
- Janczewski L.J., Wolfe H.B., Sheno S. (eds.), *Security and Privacy Protection in Information Processing Systems*, Auckland 2013.
- Janijić J., Pesić M. (eds.), *History and Cultural Memory*, Belgrade 2024.
- Jinn G.W., *China's Development of Asymmetric Warfare Capabilities and the Security of Taiwan*, Monterey 2004.
- Johnson D.E., *Hard Fighting: Israel in Lebanon and Gaza*, Santa Monica-Arlington-Pittsburgh 2011.
- Johnson O., *The Russian Understanding of War: Blurring the Lines between War and Peace*, Washington 2019.
- Jun M., *Ma Jun Explains Sunzi's Art of War*, Beijing 2008.
- Jureńczyk Ł., Sadowski S., Jastrzębski M., Waskan J. (red.), *Czynnik wojskowy w środowisku międzynarodowym na przełomie XX i XXI wieku*, Bydgoszcz 2016.
- Kaldor M., *New and Old Wars: Organized Violence in a Global Era*, Cambridge 2012.
- Kania E.B., *Battlefield singularity. Artificial intelligence, military revolution, and china's future military power*, Washington 2017.
- King G., Keohane R.O., Verba S., *Designing Social Inquiry*, Princeton 1994.
- Kiss A.P. (ed.), *Conflicts in the Gray Zone A Challenge to Adapt*, Budapest 2017.
- Kortüm H.H. (ed.), *Transcultural Wars. From the Middle Ages to the 21st Century*, Berlin 2006.
- Kowalski M., *Prawo do samoobrony jako środek zwalczania terroryzmu międzynarodowego*, Warszawa 2013.
- Krekel S.B., *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, McLean 2009.
- Kukkola J., Ristolainen M., Nikkarila J.P. (eds.), *Game Player. Facing the structural transformation of cyberspace*, Riihimäki 2019.
- Kukkola J., Ristolainen M., Nikkarila J.P. (eds.), *Game Changer: Structural transformation of cyberspace*, Riihimäki 2017.
- Kulesza R., *Wojna peloponeska*, Warszawa 2006.
- Kurz H.R., *Schweizerschlachten*, Bern 1962.
- Kuźniar R. (red.), *Porządek międzynarodowy u progu XXI wieku*, Warszawa 2005.
- Lamb Sr. M.W., *Operation Allied Force. Golden Nuggets for Future Campaigns*, Alabama 2002.
- Lasica D.T., *Strategic Implications of Hybrid War: A Theory of Victory*, Fort Leavenworth 2009.

- Lee R.M., Assante M.J., Conway T., *Analysis of the Cyber Attack on the Ukrainian Power Grid*, Washington 2016.
- Leighton G., *Ideology and Holy Landscape in the Baltic Crusades*, Leeds 2022.
- Lewis J.A., *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Washington 2002.
- Li R., *Lectures on Sunzi's Art of War*, Beijing 2013.
- Liang Q., Xiangsui W., *Unrestricted Warfare (超限战) 2nd ed.*, Wuhan, 2011.
- Libicki M.C., *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge 2007.
- Licklider J.C.R., *Man-Computer Symbiosis*, Cambridge 1960.
- Lieber F., *Guerrilla parties: considered with reference to the laws and usages of war*, New York 1862.
- Liere L., Sremac S. (eds.), *Trauma and Nostalgia. Practices in Memory and Identity*, Amsterdam 2024.
- Lindstrom G., Tardy T. (eds.), *The EU and NATO: The Essential partners*, Paris 2019.
- Livius T., *Books XXVI-XXVII With An English Translation*, W. Heinemann (ed.), Cambridge 1943.
- Lochocki T., *The Rise of Populism in Western Europe. A Media Analysis on Failed Political Messaging*, Berlin 2018.
- Lonardo L. (ed.), *Addressing Hybrid Threats: European Law and Policies*, Cheltenham 2024.
- Luttwak E.N., *Strategy: The Logic of War and Peace*, Cambridge 1987.
- M. Kaldor, *New and Old Wars. Organized violence in a Global Era*, Cambridge 2012.
- Macdonald J., Hackett J.W., Malczyk M., *Wielkie Bitwy Historii*, Warszawa 1994.
- Mallory K., *New Challenges in Cross-Domain Deterrence*, Santa Monica 2018.
- Manwaring M.G., *The Complexity of Modern Asymmetric Warfare*, Oklahoma 2012.
- Markiewicz S. (red.), *Rosyjska wizja prowadzenia operacji militarnych*, Warszawa 2018.
- Matuszek K.C., *Systemy wojenne: współczesne wojny w perspektywie teorii Niklasa Luhmanna*, Kraków 2010.
- McCartney S., *ENIAC, the triumphs and tragedies of the world's first computer*, New York 1999.
- McKenzie, Jr. K.F., *The Revenge of the Melians: Asymmetric Threats and the Next QDR*, Washington 2000.
- Mechelli A., Vieira S. (eds.), *Machine Learning*, London-San Diego-Cambridge-Kidlington 2020.
- Merom G., *How Democracies Lose Small Wars State, Society, and the Failures of France in Algeria, Israel in Lebanon, and the United States in Vietnam*, Cambridge 2003.
- Miles F.B., *Asymmetric Warfare: an Historical Perspective*, Carlisle 1999.
- Militzer K., *Historia zakonu krzyżackiego*, Kraków 2007.

- Misra B.B., *The Central Administration of the East India Company, 1773–1834*, Manchester 1959.
- Mooney C.Z., *Monte carlo simulation*, London-New Delhi 1997.
- Morgan K.E., Mueller K.P., Medeiros E.S., Pollpeter K.L., Cliff R., *Dangerous Thresholds: Managing Escalation in the 21st Century*, Santa Monica 2008.
- Morris J.E., *The Welsh Wars of Edward I*, Oxford 1901.
- Moser C., Blockans S., *The extent of the European Parliament's competence in Common Security and Defence Policy*, Brussels 2022.
- Mountel R.A., *Indo-China in retrospect: The Communist Insurgency*, Carlisle 1973.
- Münkler H., *The New Wars*, Cambridge–Malden 2005.
- Murray W., Mansoor P.R. (eds.), *Hybrid Warfare Fighting Complex Opponents from the Ancient World to the Present*, Cambridge 2012.
- Murray W., Mansoor P.R. (eds.), *Hybrid Warfare in History*, New York 2012.
- Negroponte N., *Being Digital*, New York 1995.
- Nahm A.C., *A panorama of 5000 years: Korean history*, Seoul. 1989.
- Nemeth W.J., *Future War and Chechnya: A Case for Hybrid Warfare*, Monterey 2002.
- Nye Jr. J.S., *Cyber Power*, Cambridge 2010.
- O'Conner L. (ed.), *2021 IEEE Symposium on Security and Privacy (SP)*, Los Alamitos 2021.
- O'Hanlon M.E., *Technological Change and the Future of Warfare*, Washington 2000.
- Oleński J., *Ekonomika informacji*, Warszawa 2001.
- Oman C., *A History of the Art of War in the Middle Ages. Volume I*, London 1991.
- Orme A., *A History of the Military Transactions of the British Nation in Indostan: from the Year 1745. Vol. 2*, Norderstedt 2020.
- Osinga F.P.B., *Science, Strategy and War*, London 2006.
- Palmer C., Sheno S. (eds.), *Critical Infrastructure Protection III*, Hanover 2009.
- Palmer J.T., Fullenkamp L.J., *Battle Command in the 1864 Campaign for Atlanta: the emergence of William Tecumseh Sherman as a Strategic Leader*, Carlisle Barracks 1996.
- Paul T.V., *Asymmetric Conflicts: War Initiation by Weaker Powers*, Cambridge 1994.
- Pegg M.G., *A Most Holy War. The Albigensian Crusade and the Battle for Christendom*, New York 2008.
- Pei J. i inni (eds.), *Advances in Knowledge Discovery and Data Mining. Part II*, Berlin 2013.
- Penney H.R., *The Future of Fighter Force Our Nation Requires: Building a Bridge*, Arlington 2021.
- Pieke F.N., Iwabushi K. (eds.), *The Global Square*, Berkeley 2021.
- Pikulicka-Wilczewska A., Sakwa R. (ed.), *Ukraine and Russia: People, Politics, Propaganda and Perspectives*, Bristol 2015.
- Pikulska-Radomska A., *Fiscus non erubescit. O niektórych włoskich podatkach rzymskiego pryncypatu*, Łódź 2003.
- Plutarch, *Lives, volume III, Pericles and Fabius Maximus. Nicias and Crassus*, B. Perrin (ed.), Cambridge 1916.

- Plutarch, *Żywoty sławnych mężów (Perykles)*, M. Brożek (tłum. i red.), Wrocław 1956.
- Polibius, *The Histories, volume I*, W.R. Paton (ed. & trans.), Cambridge 1922.
- Polibius, *The Histories, volume IV*, W.R. Paton (ed. & trans.), Cambridge 1925.
- Politkovskaya A., *A Dirty War: A Russian Reporter in Chechnya*, New York 2001.
- Pollpeter K.L., Chase M.S., Heginbotham E., *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations*, Santa Monica 2017.
- Proceedings of the International Scientific Conference Strategies XXI. The Complex And Circummaru F., Ioniță C.C. (eds.), Dynamic Nature of The Security Environment*, Bucharest 2021.
- Pucelj M. (ed.), *The impact of COVID-19 crisis on diverse democratic perspectives through gender perspective*, Novo Mesto 2024.
- R. Lemkin, *Lemkin on Genocide*, Plymouth 2012.
- Rashid A., *Taliban: Militant Islam, Oil and Fundamentalism in Central Asia*, New Haven 2000.
- Regina-Zacharski J., *Wojna w świecie współczesnym. Uczestnicy — cele — Modele — Teorie*, Łódź 2014.
- Rhodes R., *Dark Sun: The Making of the Hydrogen Bomb*, New York 1995.
- Rice H.G., *Unconventional Cyber Warfare: Creating a Cyber Resistance in the Private Sector*, Quantico 2019.
- Rojas R., Hashagen U. (eds.), *The First Computers: History and Architecture*, Cambridge 2000.
- Romaniuk S.N., Catino M.S., Martin C.A. (eds.), *The Handbook of Homeland Security*, Milton 2023.
- Rotaru V., Troncotă M. (eds.), *Russia and the former Soviet space. Instrumentalizing Security, Legitimizing Intervention*, Cambridge 2017.
- Russel F. H., *The Just War in the Middle Ages*, Cambridge 1975.
- Sarnicki S., *Księgi hetmańskie*, Kraków 2015.
- Schelling T., *The Strategy of Conflict*, Cambridge 1980.
- Schmitt C., *Theorie des Partisanen: Zwischenbemerkung zum Begriff des Politischen*, Berlin, 1975.
- Schmitt M.N. (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge 2013.
- Serafinelli E. (ed.), *Drones in Society. New Visual Aesthetics*, Cham 2024.
- Shats D., *Chinese Views of Effective Control: Theory and Action*, Montgomery 2022.
- Shengning H. [胡延宁], Bingyan L. [李炳彦], Shengliang W. [王圣良], *Light Warfare: The New Trend in the Global Revolution in Military Affairs [世界军事革命新趋势]*, Beijing 2015.
- Sikora R., *Wojskowość polska w dobie wojny polsko-szwedzkiej 1626–1629. Kryzys mocarstwa*, Poznań 2005.
- Silova I. (ed.), *Post-Socialism is not Dead: (Re)Reading the Global in Comparative Education*, Bingley 2010.

- Singer P.W., Brooking E.T., *Like War: The Weaponization of Social Media*, Boston 2018.
- Singer P.W., Friedman A., *Cybersecurity and Cyberwar. What everyone needs to know*, Oxford 2014.
- Singleton C. i inni, *X-Force Threat Intelligence Index 2021*, Armonk 2021.
- Smeliansky R. (ed.), 2020 *International Scientific and Technical Conference Modern Computer Network Technologies*, Moscow 2020.
- Stein B., *A History of India*, Oxford 2010.
- Stenslie S., Haugom L., Vaage B.H. (eds.), *Intelligence Analysis in the Digital Age*, New York 2021.
- Strachan H., *The Direction of War: Contemporary Strategy in Historical Perspective*, Cambridge 2013.
- Sturken M., *Tangled Memories: The Vietnam War, the AIDS Epidemic, and the Politics of Remembering*, Berkeley-LosAngeles-London 1994.
- Summers H.G., *On Strategy: A Critical Analysis of the Vietnam War*, New York 1995.
- Sun Tzu, *Sun Tzu on the Art of War: The Oldest Military Treatise in the World*, Leicester 2000.
- Sun Tzu, *Sztuka wojny*, Warszawa 1994.
- Sun Tzu, *The Art of War*, S.B. Griffith (ed. & trans.), Oxford 1971.
- Sweeney M.S., *The Military and the Press: An Uneasy Truce*, Evanston 2006.
- Świątkowska J. (ed.), *NATO Road to Cybersecurity*, Kraków 2016.
- Thränert O., Zapfe M. (eds.), *Strategic Trends 2018. Key Developments in Global Affairs*, Zürich 2018.
- Tilford E.H., *The Revolution in Military Affairs: Prospects and Cautions*, Carlisle Barracks 1995.
- Tingguang R., Weiguo L., *Sun Tzu's Art of War: Collected Expositions*, Beijing 2013.
- Tsai W.H., *An Analysis of China's Information Technology Strategies and their Implication for US National Security*, Monterey 2006.
- Tukidydes, *Wojna peloponeska*, K. Kumaniecki (tłum. i red.), Warszawa 1957.
- Urban W., *Średniowieczni Najemnicy*, Warszawa 2008.
- Urban W., Terry J., *Medieval Mercenaries. The Business of War*, London 2006.
- Vaudenay S. (ed.), *Progress in Cryptology — AfricaCrypt*, Casablanca 2008.
- Vegetius, *Epitome of Military Science*, Milner N.P. (ed. & trans.), Liverpool 1996, Book 3.
- Verbruggen J.F., *The Art of Warfare in Western Europe during the Middle Ages*, Woodbridge 1997.
- Waldenberg M., *Rozbicie Jugosławii: jugosłowiańskie lustro międzynarodowej polityki*, Warszawa 2005.
- Walker R.G., *Spec Fi: The U.S. Marine Corps and Special Operations*, Monterey 1998.
- Wallace C.D., *Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis*, Tallin 2018.

- Wallerstein I., *The modern World System I: Capitalist Agriculture and the Origins of the European World-Economy in the Sixteenth Century*, New York 1974.
- Wang G.A., Chau M., Chen H. (eds.), *Intelligence and Security Informatics*, Jeju 2017.
- Watson G. R., *The Roman Soldier*, Ithaca 1969.
- Weissmann M, Nilsson N, Palmertz B, Thunholm P. (eds.), *Hybrid Warfare. Security and Asymmetric Conflict in International Relations*, London 2021.
- Wickremesekera C., *Best Black Troops in the World': British Perceptions and the Making of the Sepoy 1746-1805*, New Delhi-Manohar 2002.
- Wilson R.L., Curran B. (ed.), *Proceedings of the 18th International Conference on Cyber Warfare and Security*, Reading 2023.
- Wojciechowski S., Fiedler R. (red.), *Zagrożenia asymetryczne współczesnego świata*, Poznań 2009.
- Wolford Z. i inni, *Scoping the future Improving Ukrainels awareness of future technologies*, Cambridge 2025.
- Wortzel L.M., *The Chinese People's Liberation Army and Information Warfare*, Carlisle Barracks 2014.
- Wrightt Q., *A Study of War*, Chicago 1965.
- Wu M., *Intelligent Warfare: Prospects of Military Development in the Age of AI*, New York 2022.
- Wurzel D. J., McGruther K. R., Murray W. R., *A Survey of Unclassified Literature on the Subject of Asymmetric Warfare*, Sherman Oaks 1998.
- Yarger H.R., *Strategic Theory of for the 21 st Century: The Little Book on Big Strategy*, Carlisle 2006.
- Yoshihara T., *Chinese Information Warfare: A Phantom Menace Or Emerging Threat?*, Carlisle 2001.
- Yulian Z., *The Science of Campaigns [战役学]*, Beijing 2006.
- Zięba R. (red.), *Bezpieczeństwo międzynarodowe po zimnej wojnie*, Warszawa 2008.
- Żakowski K. (ed.), *New Dynamics in Asia*, Łódź 2020.
- Бочарников И.В., Лемешев С.В., Люткине Г.В., *Современные концепции войн и практика военного строительства*, Москва 2013.
- Гуревич В.И., *Электромагнитный импульс высотного ядерного взрыва и защита электрооборудования от него*, Москва 2019.
- Долчинков Н. (ред.), *Радиационната безопасност в съвременния свят. Том 2, Велико Търново* 2025.
- Марченкова В.И., *Хочешь мира, победи мятежевойну! Творческое наследие Е. Э. Месснера*, Москва 2005.
- Огарков Н.В., *Всегда в готовности к защите отечества*, Москва 1982.
- Петров А.В. i inni (ред.), *Глобальные социальные процессы 4.0: социокультурные трансформации в системе современных обществ*, Санкт-Петербург 2023.
- Слипченко В.И., *Войны шестого поколения. Оружие и военное искусство будущего*, Москва 2002.

Шевелев Э.Г., *Введение в военную системологию*. Москва 1993.

Artykuły w czasopismach naukowych

Abels J., *Private infrastructure in geopolitical conflicts: the case of Starlink and the war in Ukraine*, „European Journal of International Relations” 2024, Vol. 30, No. 4.

Abraham S., *Chechnya: Between War and Peace*, „Human Rights Brief” 2001, Vol. 8, Issue 2.

Achen C.H., *Realism and Rationality*, „Critical Review” 2024, Vol. 35, No. 4.

Akinsuli O., *The rise of AI-enhanced ransomware-as-a-service (RaaS): A new threat frontier*. „World Journal of Advanced Engineering Technology and Sciences” 2021, Vol. 1, No. 2.

Alexander M., Keiger J.F.V., *France and the Algerian War: strategy, operations and diplomacy*, „Journal of Strategic Studies” 2002, Vol. 25, No. 2.

Allan P., Stahel A.A., *Tribal Guerrilla Warfare against a Colonial Power: Analyzing the War in Afghanistan*, „The Journal of Conflict Resolution” 1983, Vol. 27, No. 4.

Allen M., *What was Web 2.0? Versions as the dominant mode of internet history*, „New Media & Society” 2012, Vol. 15, No. 2.

Andén-Papadopoulos K., *The Abu Ghraib torture photographs: News frames, visual culture, and the power of images*, „Journalism” 2008, Vol. 9, No. 1.

Anderson G.M., McCormick R.E., Tollison R.D., *The economic organization of the English East India Company*, „Journal of Economic Behavior & Organization” 1983, No. 4 (2–3).

Anghel I., *Social Media as Hybrid Warfare Tool – Putting Russia’s Informational Strategy in Context*, „Romanian Military Thinking” 2020, No. 1.

Apel D., *Torture Culture: Lynching Photographs and the Images of Abu Ghraib*, „Art Journal” 2005, Vol. 64, No. 2.

Araujo L., Spring M., *Services, products, and the institutional structure of production*, „Industrial Marketing Management” 2006, Vol. 35, No. 7.

Arnold J.M., *NATO’s Readiness Action Plan: Strategic Benefits and Outstanding Challenges*, „Strategic Studies Quarterly” 2016, Vol. 10, No. 1.

Arreguín-Toft I., *How the Weak Win Wars: A Theory of Asymmetric Conflict*, „International Security” 2001, Vol. 26, No. 1.

Aryal K., *The Gulf War as Simulacra: An Analysis of Vishwa Ghatana [World Affairs] on Nepal Television*, „Journal of Arts & Humanities” 2023, Vol. 5, No. 1.

Ashraf N., *The Paradox of Cyber Warfare and Clausewitz’s Conception of War*, „NUST Journal of International Peace & Stability” 2025, Vol. 8, No. 1.

Asmolov G., Kolozaridi P., *The imaginaries of RuNet: the change of the elites and the construction of online space*, „Russian Politics” 2017, Vol. 2, No. 1.

Ayalon A., Popovich E., Yarchi M., *From Warfare to Imagefare: How States Should Manage Asymmetric Conflicts With Extensive Media Coverage*, „Terrorism and Political Violence” 2016, No. 28.

Babic M., Fichtner J., Heemskerk E.M., *States versus Corporations: Rethinking the Power of Business in International Politics*, „The International Spectator” 2017, Vol. 52, No. 4.

- Barrett E.T., *Warfare in New Domain: The Ethics of Military Cyber-operations*, „Journal of Military Ethics” 2013, Vol. 12, No. 1.
- Barrow C.W., *There are Better Alternatives than Easton: A Critical Rejoinder to William J. Kelleher*, „New Political Science” 2018, Vol. 40, Issue 1.
- Bartles C.K., *Getting Gerasimov Right*, „Military Review” 2016, Vol. 96, No. 1.
- Bathelt H., Glückler J., *Resources in Economic Geography: From Substantive Concepts towards a Relational Perspective*, „Environment and Planning A: Economy and Space” 2005, Vol. 37, Issue 9.
- Batyuk V.I., *The US Concept and Practice of Hybrid Warfare*, „Strategic Analysis” 2017, Vol. 41, Issue 5.
- Behrendt P., *San Zhong Zhanfa or Three Warfares. Chinese Hybrid Warfare* „Kwartalnik Boyma” 2022, nr 1 (11).
- Bekkers L., Spithoven R., Houten Y.V., Leukfeldt E.R., *The involvement mechanisms of cybercrime: Explaining previous exposure of young people to money mule recruiters*, „European Journal of Criminology” 2025, Vol. 22, No. 4.
- Belkheir D., *Pressure Groups and Their Impact on Governemnt Decision-Making Processes*, „Russian Law Journal” 2024, Vol. 12, Issue 1.
- Bell C., *Hybrid warfare and its metaphors*, „Humanity: An International Journal of Human Rights, Humanitarianism, and Development” 2012, Vol. 3 (2).
- Benkler Y., *A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate*, „Harvard Civil Liberties Law Review” 2011, Vol. 46, Rev. 311.
- Bērziņš J., *A New Generation of Warfare*, „Per Concordiam” 2015, Vol. 6, No. 3.
- Betts R.K., *The Concept of Deterrence in the Postwar Era*. „Security Studies” 1991, Vol. 1, No. 1.
- Betts R.K., *The Soft Underbelly of American Primacy: Tactical Advantages of Terror*, „Political Science Quarterly” 2002, Vol. 117, No. 1.
- Bialuschewski A., *Between Newfoundland and the Malacca Strait: a Survey of the Golden Age of Piracy, 1695-1725*, „The Mariner's Mirror” 2004, Vol. 90, Issue 2.
- Biddle S., *Back in the Trenches: Why New Technology Hasn't Revolutionized Warfare in Ukraine*, „Foreign Affairs” 2023, No. 102.
- Birithriya S.K., Ahlawat P., Jain A.K., *Detection and prevention of spear phishing attacks: A comprehensive survey*, „Computers & Security” 2025, No. 151.
- Biuchak O, Hoskins A., *My war: participation in warfare*, „Digital War” 2022, No. 3.
- Boldyrew A., Łopatecki K., *Polish Way: The Light Cossack Cavalry in the Era of Military Revolution*, „Вестник СПбГУ. История” 2020, Т. 65. Вып. 3.
- Boothby W.H., *Methods and Means of Cyber Warfare*, „International Law Studies” 2013, Vol. 83.
- Borghard E.D., Lonergan S.W., *Deterrence by denial in cyberspace*, „Journal of Strategic Studies” 2023, Vol. 46, No. 3.
- Bowen J., *Managing Service Organizations: Does Having a “Thing” Make a Difference?*, „Journal of Management” 2002, Vol. 28, No. 3.

- Bradley L.P., *Was the Colonial Cyberattack the First Act of Cyberwar Against the U.S.? Finding the Threshold of War for Ransomware Attacks*, „St. John's Law Review” 2022, Vol. 96, No. 2.
- Breen M., Geltzer J.A., *Asymmetric Strategies as Strategies of the Strong*, „Parameters” 2011, Vol. 41, No. 1.
- Brizhinev D., Ryan N., Bradbury R., *Modelling Hegemonic Power Transition in Cyberspace*, „Complexity” 2018, Vol 2018, Art. ID: 9306128.
- Bryant G.J., *Asymmetric Warfare: The British Experience in Eighteenth-Century India*, „The Journal of Military History” 2004, Vol. 68, No. 2.
- Bryczek-Wróbel P., Moszczyński M., *The evolution of the concept of information warfare in the modern information society of the post-truth era*, „Defence Science Review” 2022, No. 13.
- Buffaloe D.F., *Defining Asymmetric Warfare*, „The Land Warfare Papers” 2006, No. 58.
- Buhnia S., Blackert M., Deal H., DePero A., Patra A., *Analyzing the 2021 Kaseya Ransomware Attack: Combined Spearphishing Through SonicWall SSLVPN Vulnerability*, „IET Information Security” 2025, Issue 1.
- Burkholder R., *Tackling Russian Gray Zone Approaches in the Post-Cold War Era*, „Journal of Advanced Military Studies” 2023, Vol. 14, No. 2.
- Burton J., *The Future of Cyber Conflict Studies*, „The Cyber Defense Review” 2022, Vol. 7, No. 3.
- Calcara A., Gilli A., Gilli M., Marchetti R., Zaccagnini I., *Why Drones Have Not Revolutionized War. The Enduring Hider-Finder Competition in Air Warfare*, „International Security” 2022, Vol. 46, No. 4.
- Calcara A., Marchetti R., *State-industry relations and cybersecurity governance in Europe*, „Review of International Political Economy” 2021, Vol. 29, No. 4.
- Caliskan M., Liégeois M., *The concept of 'hybrid warfare' undermines NATO's strategic thinking: insights from interviews with NATO officials*, „Small Wars & Insurgencies” 2020, Vol. 32, No. 2.
- Caliskan M., *Hybrid warfare through the lens of strategic theory*, „Defense & Security Analysis” 2019, Vol. 35, No. 1.
- Chace J.G., *Defining Asymmetric Warfare: A Losing Proposition*, „Joint Force Quarterly” 2011, No. 61.
- Chancellor N.H.M., *Mysore: The Making and Unmaking of a Model State*, „South Asian Studies” 2010, No. 13.
- Chansoria M., *Defying Borders in Future Conflict in Eas Asia: Chinese Capabilities in the Realm of Information Warfare and Cyber Space*, „Journal of East Asian Affairs” 2012, Vol. 26, No. 1.
- Chauhan P.S., Kshetri N., *Ransomware as a Service Kit: A Novel Cybercrime Strategy to Monetize Victims' Data*, „Computer” 2023, Vol. 56.
- Chávez K., Swed O., *Emulating underdogs: Tactical drones in the Russia-Ukraine war*, „Contemporary Security Policy” 2023, Vol. 44, No. 4.
- Chemlal W., Maabed F., *Artificial Intelligence: The New Cognitive Terrain for World Domination*, „Aleph” 2024 Vol. 11, No. 4–2.

- Chen P. i inni, *Low Cost and Sustainable Test Methods to Study Vulnerabilities of Large-Scale Systems against EMP*, „Sustainability” 2023, Vol. 15(320).
- Cheney C., *China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism*, „Issues & Insights” 2019, Vol. 18, W.P. 8.
- Cheng D., *Unrestricted Warfare: Review Essay II*, „Small Wars and Insurgencies” 2000, No. 11(1).
- Cheng J., Zeng J., „Digital Silk Road” as a Slogan Instead of a Grand Strategy, „Journal of Contemporary China” 2024, Vol. 33, No. 149.
- Cheng J.W., Mitomo H., Otsuka T., Jeon S.Y., *Cultivation effects of mass and social media on perceptions and behavioural intentions in post-disaster recovery – The case of the 2011 Great East Japan Earthquake*, „Temeatics and Informatics” 2016, Vol. 33, Issue 3.
- Cheng J.Y.M., *The Challenges Taiwan Faces in Cognitive Warfare and Its Impact on US–Taiwan Relations*, „Journal of Indo-Pacific Affairs” 2025, Vol. 8, No. 1.
- Chinwe E.E., Alozie C.E., *Adversarial Tactics, Techniques, and Procedures (TTPs): A Deep Dive into Modern Cyber Attacks*, „IRE Journals” Vol. 8, Issue 7.
- Chircop L., *A due diligence standard of attribution in cyberspace*, „International & Comparative Law Quarterly” 2018, Vol. 67, No. 3.
- Cho Y., Chung J., *Bring the State Back In: Conflict and Cooperation Among States in Cybersecurity*, „Pacific Focus” 2017, Vol. 32, No. 2.
- Chowdhury N., Katsikas S., Gkioulos V., *Modeling effective cybersecurity training frameworks: A delphi method-based study*, „Computers & Security” 2022, No. 113(102551).
- Chowdhury R.H., Prince N.U., Abdullah S.M., Mim L.A., *The role of predictive analytics in cybersecurity: Detecting and preventing threats*, „World Journal of Advanced Research and Reviews” 2024, Vol. 23, No. 2.
- Cohen E.A., *A Revolution in Warfare*, „Foreign Affairs” 1996, Vol. 75, No. 2.
- Cohen J.E., *Cyberspace as/and Space*, „Georgetown Law Faculty Publications and Other Works” 2007, 107 Colum. L. Rev. 210-256.
- Connelly M., *Rethinking the Cold War and Decolonization: The Grand Strategy of the Algerian War for Independence*, „International Journal of Middle East Studies” 2001, Vol. 33, No. 2.
- Cook E., *The Future of the Cyber Theater of War*, „HSGC Foreign Policy & International Issues” 2023, No. 13.
- Cooper R.G.S., *Culture, Combat, and Colonialism in Eighteenth-and Nineteenth-Century India*, „The International History Review” 2005, Vo. 27, No. 3.
- Costa M., *Exploring Hacktivism: The Role and Impact of Social Media*, „Advanced Research on Information Systems Security” 2025, Vol. 5, No. 1.
- Cox D.G., Bruscano T., Ryan A., *Why Hybrid Warfare Is Tactics Not Strategy: A Rejoinder to “Future Threats and Strategic Thinking”*, „Infinity Journal” 2012, Vol. 2, No. 2.
- Cox J.L.A., *Game Theory and Risk Analysis*, „Risk Analysis” 2009, Vol. 29, No. 8.
- Cox R., *Asymmetric warfare and military conduct in the Middle Ages*, „Journal of Medieval History” 2012, Vol. 38, No. 1.
- Cześnik M., Miśta R., Żerkowska-Balas M., *Uczestnictwo i mobilizacja w wyborach parlamentarnych 2019 roku*, „Studia Socjologiczne” 2020, nr 4.

- Czetwertyński S., *Tragedia zasobów niczych a gospodarka internetowa*, „Rynek Społeczeństwo Kultura”, nr 3(7).
- Слипченко В.И., *К какой войне должны готовиться вооружённые силы*, „Отечественные записки” 2002, № 8(9).
- Dandamudi S.R.P., Sajja J., Khanna A., *Advancing Cybersecurity and Data Networking Through Machine Learning-Driven Prediction Models*, „International Journal of Innovative Research in Computer Science and Technology” 2025, Vol. 13, Issue 1.
- Davies D.W., *An Historical Study of the Beginnings of Packet Switching*, „British Computer Society Journal” 2001, Vol. 44, No. 3.
- Dekker M., Alevizos L., *A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making*, „Security and Privacy” 2024, Vol. 7, No. 1(e333).
- Demir K., Güraksın G.E., *Determining middle school students' perceptions of the concept of artificial intelligence: A metaphor analysis*, „Participatory Educational Research”, Vol. 9, No. 2.
- Denby B. i inni, *Silent speech interfaces*, „Speech Communication” 2009, No. 52.
- Douzet F., Gery A., *Cyberspace is used, first and foremost, to wage wars: proliferation, security and stability in cyberspace*, „Journal of Cyber Policy” 2021, Vol. 6, No. 1.
- Druckman J.N., Kifer M.J., Parkin M., *Timeless Strategy Meets New Medium: Going Negative on Congressional Campaign Web Sites, 2002–2006*, „Political Communication” 2010, Vol. 27, Issue 1.
- Ducaru S., Caradaică M., Costea A.M., *Can a Cyberattack Become an Act of War? European and Trans-Atlantic Perspectives*, „Romanian Journal of European Affairs” 2024, Vol. 24, No. 1.
- Dygantowski S., *Cyberbezpieczeństwo jako fundament bezpieczeństwa infrastruktury krytycznej w kontekście współczesnych zagrożeń*, „Journal of KONBiN” Vol. 50, Issue 4.
- Dylevsky I.N., Komov S.A., Korotkov S.V., Petruinn A.N., *Operations in Cyberspace: Theory, Politics, Law*, „Military Thought” 2011, Vol. 20, No. 3.
- Dyner A.M., *Strategia bezpieczeństwa narodowego Rosji*, „Biuletyn PISM” 2021, Nr 131 (2329).
- Dziwisz D., *Rethinking Future Conflicts: The Cyber Grey Zone From the Russian Perspective*, „Politeja” 2024, nr 5 (92).
- Easton D., *An Approach to the Analysis of Political Systems*, „World Politics” 1957, Vol. 9, No. 3.
- Ensafi R., Winter P., Mueen A., Crandall J.R., *Analyzing the Great Firewall of China Over Space and Time*, „Proceedings on Privacy Enhancing Technologies” 2015, No. 1.
- Erie M.S., Streinz T., *The Beijing Effect: China's Digital Silk Road as Transnational Data Governance*, „Journal of International Law and Politics” 2021, Vol. 54, No. 1.
- Evans M., *Elegant Irrelevance Revisited: A Critique of Fourth-Generation Warfare*, „Contemporary Security Policy” 2005, Vol. 26, Issue 2.
- Ewing R.D., *Hu Jintao: The Making of a Chinese General Secretary*, „The China Quarterly” 2003, Vol. 173.

- Fagade T., Maraslis K., Tryfonas T., *Towards effective cybersecurity resource allocation: the Monte Carlo predictive modelling approach*, „International Journal of Critical Infrastructures” 2017, Vol. 13, No. 2–3.
- Farwell J.P., Rohozinski R., *Stuxnet and the Future of Cyber War*, „Survival: Global Politics and Strategy” 2011, Vol. 53, No. 1.
- Farwell J.P., *Industry’s Vital Role in National Cyber Security*, „Strategic Studies Quarterly” 2012, Vol. 6, No. 4.
- Farwell J.P., Rohozinski R., *Stuxnet and the Future of Cyberwar*, „Survival” 2011, Vol. 53, No. 1.
- Fenster M., *Disclosure’s Effects: WikiLeaks and Transparency*, „UF Law Scholarship Repository” 2012, No. 97, Rev. 753.
- Figueroa M.G., Acevedo D.D.H., Porta D.S., *Geomagnetic disturbances and grid vulnerability: Correlating storm intensity with power system failures*, „PLoS One” 2025, Vol. 20, No. 7.
- Fikry A., *Defining the Beauty of Cyber Hygiene: A Retrospective Look*, „Engineering Management Review” 2024, Vol. 52, Issue 2.
- Finkelstein D. i inni, *Information manipulation on TikTok and its relation to American users’ beliefs about China*, „Frontiers in Social Psychology” 2024, Vol. 2.
- Finlayson K., *The 1960s: A Decade of Revolution*, „Veritas” 2008, Vol. 4, No. 4.
- Firdman O., *Hybrid Warfare or Gibridnaya Voyna? Similar, But Different*, „The RUSI Journal” 2017, Vol. 162, No. 1.
- Fischerkeller M.P., *David versus Goliath: Cultural judgments in asymmetric wars*, „Security Studies” 1998, Vol. 7 No. 4.
- Fitzsimmons S., *Evaluating the Masters of Strategy: A Comparative Analysis of Clausewitz, Sun Tzu, Mahan, and Corbett*, „Innovations: A Journal of Politics” 2007, Vol. 7.
- Flis J., *Wojna hybrydowa — zjawisko nowe czy ewolucja starego?*, „Ante Portas — Studia nad Bezpieczeństwem” 2018, Nr 2 (11).
- Flockhart T., *The problem of change in constructivist theory: ontological security seeking and agent motivation*, „Review of international studies” 2016, No. 42 (5).
- Flockhart T., *Towards a strong NATO narrative: from a “practice of talking” to a “practice of doing”*, „International politics” 2012, No. 49 (1).
- Floridi L., *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, „Philosophy & Technology” 2020, No. 33.
- Frenznick D.A., *First Amendment on the Battlefield: A Constitutional Analysis of Press Access to Military Operations in Grenada, Panama and the Persian Gulf*, „McGeorge Law Review” 1991, Vol. 23, Issue 2.
- Fridman O., *On the “Gerasimov Doctrine”. Why the West Fails to Beat Russia to the Punch*, „PRISM” 2019, Vol. 8, No. 2.
- Fridman O., *Memories of the 1999 NATO Bombing in Belgrade, Serbia*, „Südosteuropa” 2016, Vol. 64, No. 4.
- Galeotti M., *The mythical ‘Gerasimov Doctrine’ and the language of threat*, „Critical Studies on Security” 2019, Vol. 7, No. 2.

- Gartzke E., Lindsay J.R., *Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace*, „Security Studies” 2015, Vol. 24, No. 2.
- Gartzke E., *The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth*, „International Security” 2013, Vol. 38, No. 2.
- Gearson J., *Deterring Conventional Terrorism: From Punishment to Denial and Resilience*, „Contemporary Security Policy” 2012, Vol. 33, No. 1.
- Gelgi M. i inni, *Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques*, „Sensors” 2024, No. 24, Issue 11.
- Gentile G.P., *The imperative for an American general purpose army that can fight*, „Orbis” 2009, No. 3.
- Gibson R, Lusoli W, Ward S., *The Australian public and politics on-line: Reinforcing or re-inventing representation?*, „Australian Journal of Political Science” 2008, Vol. 43, Issue 1.
- Gilady L., MacKay J., *Bringing the Insurgents Back In: Early Wars in British India*, „Terrorism and Political Violence” 2015, Vol. 25, Issue 5.
- Gilli A., Gilli M., *The diffusion of drone warfare? Industrial, organizational, and infra-structural constraints*. „Security Studies” 2016, Vol. 25, No. 1.
- Givens A.D., Gorbachevsky M., Biernat A.C., *How Putin's Cyberwar Failed in Ukraine*, „Journal of Strategic Security” 2023, Vol. 16, No. 2.
- Gliwa A., *The Tatar Military Art of War in the Early Modern Period: An Example of Asymmetric Warfare*, „Acta Poloniae Historica” 2016, nr 114.
- Gonthier F., *How party polarisation exacerbates the link between democratic deficit and populist voting: evidence from Europe*, „West European Politics” 2025, Vol. 49, No. 1.
- González-Manzano L., *Identifying Key Relationships between Nation-State Cyberattacks and Geopolitical and Economic Factors: A Model*, „Security and Communication Networks” 2022, No. 1.
- Goodman W., *Cyber Deterrence: Tougher in Theory than in Practice?*, „Strategic Studies Quarterly” 2010, Vol. 4, No. 3.
- Gorzkowicz A., *Wojna hybrydowa na Ukrainie jako przykład współczesnych konfliktów zbrojnych*, „Roczniki Studenckie Akademii Wojsk Lądowych” 2017, nr 1.
- Górka S.P., *Wpływ kolejnych rewolucji w sprawach wojskowych na przyszłe wojny*, „Kultura i polityka” 2014, Nr 16.
- Grabowski T., *Metody walki informacyjnej w mediach elektronicznych na przykładzie konfliktu rosyjsko ukraińskiego (2014–2016)*, „Horyzonty Polityki” 2016, Nr 7 (20).
- Graham M., Khosravi S., *Reordering Public and Private in Iranian Cyberspace: Identity, Politics, and Mobilization*, „Global Studies in Culture and Power”, Vol. 9, No. 2.
- Greenfield P., Beagles-Roos J., *Radio vs. Television: Their Cognitive Impact on Children of Different Socioeconomic and Ethnic Groups*, „Journal of Communication” 1988, Vol 38, No. 2.
- Gridina I., Bulyk M., *Russian-ukrainian war: the way how the "Gray war" in the east of Ukraine turned into a large-scale "black" one*, „Sci. J. Cahul St. U. Bogdan Petriceicu Hasdeu” 2022, No. 1 (15).
- Gryglewski K., *Przyczyny rozwoju wojsk najemnych i zaciężnych w Europie od XIV do XVI wieku*, „Kurier Instytutu Historii” 2017, nr 5–6 (102–103), R. XI.

Guerra J.M., *An Introduction to Clausewitzian Strategic Theory: General Theory, Strategy, and Their Relevance for Today*, „Infinity Journal” 2012, Vol. 2, Issue 3.

Güler M.Ç., Shakirova A., *Deciphering Russia's 2021 National Security Strategy Document*, „SETA | Perspective” 2021, No. 67.

Gurevich V., *A New Strategy is Needed to Solve the 50-Year Old Problem - EMP Protection of Critical Civilian Infrastructure*, „International Journal of Emerging Science and Engineering” 2014, Vol. 12, Issue 2.

Haataja S., *The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach*, „Law, Innovation and Technology” 2017, No. 9(2).

Hammond P., *Reporting "Humanitarian" Warfare: propaganda, moralism and NATO's Kosovo war*, „Journalism Studies” 2000, Vol. 1, No. 3.

Hare F.B., *Private Sector Contributions to National Cyber Security: A Preliminary Analysis*, „Journal of Homeland Security and Emergency Management” 2009, Vol. 6, No. 1.

Haroon S., *The Rise of Deobandi Islam in the North-West Frontier Province and Its Implications in Colonial India and Pakistan 1914-1996*, „Journal of the Royal Asiatic Society” 2008, No. 18 (1).

Hashemi S.A., Sahrapeyma M., *Proxy Wars and US's Smart-Power Strategy (the Case of Syria, 2011-2016)*, „The Quarterly Journal of Political Studies of Islamic World” 2018, Vol. 6, No. 24.

Havercroft J., Prichard A., *Anarchy and International Relations theory: A reconsideration*, „Journal of International Political Theory” 2017, Vol. 13, No. 3.

Heinegg W.H., *Asymmetric Warfare: How to Respond?*, „U.S. Naval War College, International Law Studies” 2011, Vol. 87.

Herring G.C., *Reflecting the Last War: the Persian Gulf and the „Vietnam Syndrome”*, „Journal of Third World Studies” 1993, Vol. 10, No. 1.

Herzog S., *Ten Years after the Estonian Cyberattacks. Defense and Adaptation in the Age of Digital Insecurity*, „Georgetown Journal of International Affairs”, 2017, Vol. 18, No. 3.

Heupel M., Zangl B., *Von 'alten' und 'neuen' Kriegen. Zum Gestaltwandel kriegerischer Gewalt*. „Politische Vierteljahresschrift” 2004, No. 45.

Heyningen E.V., *The Concentration Camps of the South African (Anglo-Boer) War, 1900-1902*, „History Compass” 2009, Vol. 7, No. 1.

Hicks J.M., *A Theater-Level Perspective on Cyber*, „Joint Force Quarterly” 2015, No. 76.

Hiesgen R., Nawrocki M., Schmidt T.C., Wählisch M., *The Log4j Incident: A Comprehensive Measurement Study of a Critical Vulnerability*, „Transactions on Network and Service Management” 2024, Vol. 21, No. 6.

Hill P., *Intangibles and Services: A New Taxonomy for the Classification of Output*, „The Canadian Journal of Economics” 1999, Vol. 32, No. 2.

Hiller J.S., Russell R.S., *The challenge and imperative of private sector cybersecurity: An international comparison*, „Computer Law & Security Review” 2013, No. 29.

Hoffman F.G., *Hybrid Warfare and Challenges*, „Joint Force Quarterly” 2009, Issue 52 (1st quarter).

Hoffman F.G., *Hybrid Warfare and Challenges*, „Joint Force Quarterly” 2009, Issue 52.

- Hofmokl J., *Rozwój pola organizacyjnego Internetu — dominacja sieciowej formy porządku społecznego*, „Studia Socjologiczne” 2002, Nr 4 (167).
- Horváth T., Szatai J.Z., *History of detection of explosive devices 2.(1951 to the present)*, „Land Forces Academy Review” 2020, Vol. XXV, No. 4(100).
- Hughes D., Colarik A.M., *Predicting the Proliferation of Cyber Weapons into Small States*, „Joint Force Quarterly” 2016, Vol. 83, No. 4.
- Hughes G., *The Soviet–Afghan War, 1978–1989: An Overview*, „Defence Studies” 2008, Vol. 8, No. 3.
- Hulvey R.A., *Cyber Sovereignty: How China is Changing the Rules of Internet Freedom*, „IGCC” 2021, No. 2.
- Humprecht E., Esser F., Van Aelst P., *Resilience to Online Disinformation: A Framework for Cross-National Comparative Research*, „The International Journal of Press/Politics” 2020, Vol. 25, No. 3.
- Husain A., *AI is Shaping the Future of War*, „Prism” 2021, Vol. 9, No. 3.
- Iamandi L., Virgolici I.V., Ioniță A.M., A. Drăgănescu, *Malicious Cyber Attacks*, „Journal of Danubian Studies and Research” 2022, Vol. 12, No. 1.
- Jai B.R., Shih M.F., *Technology: Limited or Infinite?*, „Emerging Media” 2024, Vol. 2, Issue 1.
- Jansen S.C., Martin B., *The Streisand Effect and Censorship Backfire*, „International Journal of Communication” 2015, No. 9.
- Jash A., *Fight and Win Without Waging a War: How China Fights Hybrid Warfare*, „CLAWS Journal” 2019, Vol. 12, No. 2.
- Jewell J.R., *Using barbaric methods in South Africa: The British concentration camp policy during the Anglo-Boer War*, „Scientia Militaria — South African Journal of Military Studies” 2012, Vol. 31, No. 1.
- Ji Y., *The Revolution in Military Affairs and the Evolution of China’s Strategic Thinking*, „Contemporary Southeast Asia” 1999, Vol. 21, No. 3.
- Johnson D., *Darwinian selection in asymmetric warfare: the natural advantage of insurgents and terrorists*, „2010 Journal of the Washington Academy of Sciences” 2010, Vol. 95, No. 3.
- Johnson R., *Hybrid War and Its Countermeasures: A Critique of the Literature*, „Small Wars & Insurgencies” 2018, Vol. 29, Issue 1.
- Jones L., *The Future of Warfare Is Irregular*, „Fletcher Forum of World Affairs” 2022, Vol. 46, No. 2.
- Kaldor M., *In defence of new wars*, „Stability: International Journal of Security and Development” No. 2 (1).
- Kamionka M., *Rosyjska wojna hybrydowa w mediach społecznościowych na przykładzie portalu Facebook*, „Wiedza Obronna” 2023, t. 282, nr 1.
- Kania E.B., *Artificial intelligence in China’s revolution in military affairs*, „Journal of Strategic Studies”, 2021, Vol. 44, No. 4.
- Kania E.B., *The PLA’s Latest Thinking on the Three Warfares*, „China Brief” 2016, Vol. 16, No. 13.

- Katagiri N., Two explanations for the paucity of cyber-military, cross-domain operations, „Journal of Cybersecurity” 2022, Vol. 1, Issue 10.
- Kaukiainen Y., *Shrinking the world: Improvements in the speed of information transmission, c. 1820-1870*, „European Review of Economic History” 2001, Vol. 5, No. 1.
- Keating V.C., O. Schmitt, *Ideology and influence in the debate over Russian election interference*, „International Politics” 2021, Vol. 58, No. 5.
- Kesan J.P., Hayes C.M., *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, „Harvard Journal of Law & Technology” 2012, Vol. 25, No. 2.
- Kim J., Tucker S.C., Kim G.H., *How did the Weaker Actor Defeat the Stronger Actor? Koguryō's War with Sui (612–614) Revisited*, „Sungkyun Journal of East Asian Studies” 2018, Vol. 18, No. 2.
- Kiper J., *Remembering the Causes of Collective Violence and the Role of Propaganda in the Yugoslav Wars*, „Nationalities Papers” 2024, Vol. 52, No. 1.
- Kittel W.J., *Koncepcja pętli decyzyjnej Johna Richarda Boyda – „OODA Loop”*, „Kwartalnik Bellona” 2022, nr 4.
- Kobayashi B.H., *An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and other Public Security Goods*, „Supreme Court Economic Review” 2006, Vol. 14.
- Kofman M., Rojansky M., *A Closer look at Russia's 'Hybrid War'*, „Kennan Cable” 2015, No. 7.
- Kolodiziev O. i inni, *Digital transformation as a tool for creating an inclusive economy in Ukraine during wartime*, „Problems and Perspectives in Management”, Vol. 22, No. 3.
- Kostyuk N., *Allies and diffusion of state military cybercapacity*, „Journal of Peace Research” 2024, Vol. 61, No. 1.
- Kostyuk N., Gartzke E., *Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine*, „Texas National Security Review” 2022, Vol. 5, No. 3.
- Kraj K., *Wojny asymetryczne czy miatężewojna Jewgienija Messnera zagrożeniem dla bezpieczeństwa w XXI wieku*, „Bezpieczeństwo. Teoria i Praktyka” 2012, Nr 3.
- Krzak A., *Wojny przyszłości po rosyjsku — wojna hybrydowa, informacyjna i psychologiczna na tle konfliktu ukraińskiego*, „Przegląd Bezpieczeństwa Wewnętrznego” 2018, Nr 18 (10).
- Kubicek P., *The Commonwealth of Independent States: an example of failed regionalism?*, „Review of International Studies” 2009, No. 35.
- Kuzlu M., Fair C., Guler O., *Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity*, „Discover” 2021, Vol. 1.
- Kuźnicka-Błaszowska D., Kostyuk N., *Emerging need to regulate deepfakes in international law: the Russo-Ukrainian war as an example*, „Journal of Cybersecurity” 2025, Vol. 11, Issue 1.
- La Bruyère E., *The Network Great-Power Strategy: A Blueprint for China's Digital Ambitions*, „Asia Policy” 2021, Vol. 16, No. 2.
- Lallie H.S. i inni, *Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic*, „Computers and Security” 2021, No. 105.
- Lambakis S., Kiras J., Kolet K., *Understanding „Asymmetric” Threats to the United States*, „Comparative Strategy” 2002, Vol. 21, No. 4.

- Lambi A., Vijayaraghvan V., *Cross-Domain Deterrence in the Cyber World*, „International Journal for Research in Applied Science & Engineering Technology” 2022, Vol. 10, Issue IX.
- Lane J.F., *Ferhat Abbas, Vichy's National Revolution, and the Memory of the Royaume arabe*, „L'Esprit créateur” 2007, Vol. 47.
- Lane K., *Punishing the sea wolf: corsairs and cannibals in the early modern Caribbean*, „Nieuwe West-Indische Gids” 2003, No. 3(4).
- Lee S., *China's 'Three Warfares': Origins, Applications, and Organizations*, „Journal of Strategic Studies” 2014, Vol. 37, No. 2.
- Legucka A., *Wojna w sieci. Polityka Rosji w zakresie międzynarodowego bezpieczeństwa informacyjnego*, „Biuletyn PISM” 2021, nr 111 (2309).
- Lele A., *Asymmetric Warfare: A State vs Non-State Conflict*, „OASIS” 2014, No. 20.
- Leslie P., *General Theory in Political Science: A Critique of Easton's Systems Analysis*, „British Journal of Political Science” 1972, Vol. 2, Issue 2.
- Lewandowski P., Orgmasz Ł., *Racja stanu Polski w cyberprzestrzeni i cyberbezpieczeństwie*, „De Securitate Et Defensione. O Bezpieczeństwie I Obronności” 2022, Nr 8 (1).
- Lewis D., *China's Global Internet Ambitions: Finding Roots in ASEAN*, „ICS” 2017, No. 14.
- Li M., He X., Sun Z., Wen Y., *A framework for social media information flow analytics in cyberspace and physical space*, „Transactions in GIS” 2022, No. 26.
- Liao C.H., *Exploring the Influence of Public Perception of Mass Media Usage and Attitudes towards Mass Media News on Altruistic Behavior*, „Behavioral Sciences” 2023, Vol. 13, No. 621.
- Libiseller C., *'Hybrid warfare' as an academic fashion*, „Journal of Strategic Studies” 2023, 21 Feb [wydane poza numerem].
- Light M., *In search of an identity: Russian foreign policy and the end of ideology*, „Journal of Communist Studies and Transition Politics” 2003, Vol. 19, Issue 3.
- Lilli E., *Redefining deterrence in cyberspace: Private sector contribution to national strategies of cyber deterrence*, „Contemporary Security Policy” 2021, Vol. 42, No. 2.
- Lindroos S., Hakkala A., Virtanen S., *The COVID-19 pandemic and remote working did not improve WLAN security*, „Procedia Computer Science” 2022, No. 201.
- Liu H., Miao C., *Digital Geopolitics in a VUCA World: China Encounters a New Global Order*, „Global Policy” 2024, Vol. 15, Issue 56.
- Lobastova S., *Geopolitics of Cyberspace and Virtual Power*, „Journal of Liberal Arts and Humanities” 2020, Vol. 1, No. 3.
- Lonergan E., Montgomery M., *What is the Future of Cyber Deterrence?*, „SAIS Review of International Affairs” 2021, Vol. 41, No. 2.
- Loringhoven A.F., *Adapting NATO Intelligence in Support of "One NATO"*, „Gandirea Militara Romaneasca” 2017, Issue 3(4).
- López Velásquez J.M. i inni, *Systematic review of SIEM technology: SIEM-SC birth*, „International Journal of Information Security” 2023, No. 22.
- Luna E., Calderón J., Cataña P., Ponce M., *Advances in Technologies for the Soldiers of the Future*, „Revista Athenea” 2025, Vol. 6, Issue 20.

- Mack A., *Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict*, World Politics 1975, Vol. 27, No. 2.
- Malarczyk J., *Myśliciele włoskiego Renesansu o potrzebie rewolucyjnego przewrotu w Italii*, „Czasopismo prawno-historyczne” 1985, t. XXXVII, z. 1.
- Mälksoo M., *Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO*, „European Security” 2018, Vol. 27, No. 3.
- Manantan M.B., *The People’s Republic of China’s Cyber Coercion: Taiwan, Hong Kong, and the South China Sea*, „Issues & Studies: A Social Science Quarterly on China, Taiwan, and East Asian Affairs” 2020, Vol. 56, No. 3.
- Mandelbaum M., *The Television War*, „Daedalus” 1982, Vol. 111.
- Marjanović A, Smiljanić D., *Cognitive warfare—the human mind as the new battlefield*, „Proceedings of the Defence and Security Conference” 2025, Vol. 1, No. 1.
- Markovits C, *The Political Economy of Opium Smuggling in Early Nineteenth Century India: Leakage or Resistance?*, „Modern Asian Studies” 2009, Vol. 43, No. 1.
- Martinez J., Durian J.M., *Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds’ Case Study*, „International Journal of Safety and Security Engineering” 2021, Vol. 11, No. 5.
- Mârzac E., *Strategic Communication as a Tool for Countering Hybrid Threats. A Focus on National Resilience and Public Trust*, „Studia Securitatis” 2024, No. 2.
- Maynard J.L., *Ideology and armed conflict*, „Journal of Peace Research” 2019, Vol. 56, No. 5.
- Mączka K., *Dyrektywa NIS2 jako wytyczna do wdrożenia systemu zarządzania bezpieczeństwem informacji w organizacji*, „Ochrona Ludności i Dziedzictwa Kulturowego” 2024, nr 5.
- McDermott R.N., *Does Russia Have a Gerasimov Doctrine?*, „The US Army War College Quarterly: Parameters” 2016, Vol. 46, No. 1.
- Melella C., Ferazza F., Mersinas K., *Disjointed Cyber Warfare: Internal Conflicts among Russian Intelligence Agencies*, „ACIG” 2024, Vol. 4, No. 2.
- Mickiewicz P., Kasprzycki D.D., *Od „konfliktu hybrydowego” do działań konwencjonalnych? Koncepcja oddziaływania militarnego Rosji, ze szczególnym uwzględnieniem zmian po 2018 roku*, „Przegląd Bezpieczeństwa Wewnętrznego” 2021, Nr 25 (13).
- Mihaljinac N., Vujošević A., *The Representation of the NATO Bombing of Yugoslavia in Foreign Artistic and Mass Media Texts: Unjustified War or Justified Intervention?*, „TEME: Časopis za društvene nauke” 2021, Vol. XLV, No 2.
- Min K.S., Chai S.W., Han M., *An International Comparative Study on Cyber Security Strategy*, „International Journal of Security and Its Applications” 2015, Vol. 9, No. 2.
- Minasyan S., *“Hybrid” vs. “Compound” War: Lessons From The Ukraine Conflict*, „PON-ARS Eurasia Policy Memo” 2015, No. 401.
- Mitzen J., *Ontological security in world politics: state identity and the security dilemma*, „European Journal of International Relations” 2006, No. 12 (3).
- Mollaefar M., Ranise S., *Identifying and quantifying trade-offs in multi-stakeholder risk evaluation with applications to the data protection impact assessment of the GDPR*, „Computers & Security” 2023, Vol. 129.

- Montiel L.V., Bickel J.E., *Simulation-Based Approach to Decision Making with Partial Information* „Decision Analysis” 2012, Vol. 9, No. 4.
- Moore G.J., *Huawei, Cyber-Sovereignty and Liberal Norms: China's Challenge to the West/Democracies*, „Journal of Chinese Political Science” 2023, Vol. 28.
- Morgan K.O., *The Boer War and the Media (1899–1902)*, „Twentieth Century British History” 2002, Vol. 13, No. 1.
- Moruzi K., *Feminine Bravery: The Girl's Realm (1898–1915) and the Second Boer War*, „Children's Literature Association Quarterly” 2009, Vol. 34, No. 3.
- Mott M.i inni, *“There was a bit of PTSD every time I walked through the office door”: Ransomware harms and the factors that influence the victim organisation's experience*, „Journal of Cybersecurity” 2024, Vol. 10, No. 1.
- Mould D.H., *Press pools and military-media relations in the Gulf War: a case study of the battle of Khaffi, January 1991*, „Historical Journal of Film, Radio and Television” 1996, Vol. 16, No. 2.
- Mouti S. i inni, *Cyber Security Risk management with attack detection frameworks using multi connect variational auto-encoder with probabilistic Bayesian networks*, „Computers and Electrical Engineering” 2022, Vol. 103.
- Mroccka K., Żarna K., Nowakowski M., *Wykorzystanie algorytmów i narzędzi sztucznej inteligencji w kampanii wyborczej w Rzeczypospolitej Polskiej i Republice Słowacji — analiza case studies*, „Studia politologiczne” 2024, nr 72.
- Müller R., Graf B., Ellwart T., Antoni C.H., *How Software Agents Can Help to Coordinate Emergency Response Teams: Adaptive Team Performance Comparing Manual and Automated Team Communication*, „Journal of Business and Psychology” 2023, Vol. 38.
- Nalbandov R., *Irrational Rationality of Terrorism*, „Journal of Strategic Security” 2013, Vol. 6, No. 4.
- Nalewaj K., *Rosyjska ingerencja w wybory prezydenckie w USA w 2016 r.*, „Com.press” 2024, nr 1.
- Nassauer O., Plesch D., *NATO Strategy Review: Out of Step with Events*, „Armed Forces Journal International” 1999, No. Oct.
- Natter III W.H., Brooks J. (eds.), *American Strategy and Purpose: Reflections on Foreign Policy and National Security in an Era of Change*, Lexington 2014.
- Neculcea C., *China's Three Warfare Strategy. Origins, evolution, applicability*, „Journal of Defense Resources Management” 2023, Issue 1.
- Nedzinskaitė-Mitkė V., *Modern National Identity and Patriotism*, „Filosofija. Sociologija” 2022, Issue 3.
- Neer T., O'Toole M.E., *The Violence of the Islamic State of Syria (ISIS): A Behavioral Perspective*, „Violence and Gender” 2014, Vol. 1, No. 4.
- Newman E., *Conflict Research and the 'Decline' of Civil War*, „Civil Wars” 2009, Vol. 11, No. 3.
- Nguyen T.T., Reddi V.J., *Deep Reinforcement Learning for Cyber Security*, „Transactions on Neural Networks and Learning Systems” 2021, Vol. 34, Issue 8.
- Nie N.H., Miller III D.W., Golde S., Butler D.M., Winneg K. *The World Wide Web and the U.S. Political News Market*, „American Journal of Political Science” 2010, Vol. 54, No. 2.

- Nikitina Y., *The "Color Revolutions" and "Arab Spring" in Russian Official Discourse*, „Connections” 2014, Vol. 14, No. 1.
- Nourian A., Madnick S., *A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet*, „IEEE Transactions on Dependable and Secure Computing” 2018, Vol. 15, Issue 1.
- Nowak Z., *Akt rozpoczynający „Wielką Wojnę”. List wypowiedni wielkiego mistrza Ulryka von Jungingen z 6 sierpnia 1409 roku*, „Komunikaty Mazursko-Warmińskie” 1976, nr 1.
- Nutting P.B., *The Madagascar Connection: Parliament and Piracy, 1690-1701*, „The American Journal of Legal History” 1978, Vol. 22, No. 3.
- Nye J.S., *Deterrence and Dissuasion in Cyberspace*, „International Security” 2017, Vol. 41, No. 3.
- Nye Jr. J.S., *Nuclear Lessons for Cyber Security?*, „Strategic Studies Quarterly” 2011, Vol. 5, No. 4.
- Nye Jr. J.S., *Soft Power — the Means to Success in World Politics*, New York 2004; R.K. Betts, *The Lost Logic of Deterrence. What the Strategy That Won the Cold War Can—and Can't—Do Now*, „Foreign Affairs” 2013, Vol. 92, No. 2.
- O'Loughlin J., Witmer F.D.W., Linke A.M., Thorwardson N., *Peering into the Fog of War: The Geography of the WikiLeaks Afghanistan War Logs, 2004–2009*, „Eurasian Geography and Economics” 2010, Vol. 51, No. 4.
- Oates S., *War Propaganda and the Patriotic Model of the News in the 21st Century*, „Journalism & Communication Monographs” 2021, Vol. 23(4).
- Ochmann P., Wojas J., *Wojna hybrydowa jako przykład umiędzynarodowionego konfliktu wewnętrznego*, „Studia Prawa Publicznego” 2018, nr 2 (22).
- Oh S.H., Kim J., Nah J.H., Park J., *Employing Deep Reinforcement Learning to Cyber-Attack Simulation for Enhancing Cybersecurity*, „Electronics” 2024, Vol. 13(555).
- Ojdana-Kościuszko M., *Ewolucja i wyzwania polskiego systemu cyberbezpieczeństwa*, „De Securitate et Defensione” 2024, nr 1.
- Ojiako U., Liu Y., Johnson J., *Eastern promises: a philosophical exploration of decision making under 'unconventional' and asymmetric competition*, „International Journal of Business Environment), Vol. 5, No. 1.
- Ornatowski C., *Retoryka uzbrojona: walka o świadomość we współczesnej przestrzeni medialnej*, „Res Rethorica” 2021, Nr 8(4).
- Owen C., *Participatory authoritarianism: From bureaucratic transformation to civic participation in Russia and China*, „Review of International Studies” 2020, Vol. 46, Issue 4.
- Owens R., *The American Revolution in Military Affairs*, „Joint Force Quarterly” 1995, No. 10.
- Paavola S. i inni, *Transformed knowledge work infrastructures in times of forced remote work*, „Information and Organization” 2025, No. 35.
- Palmer R.K., *Critical Infrastructure: Legislative Factors for Preventing a Cyber-Pearl Harbor*, „Virginia Journal of Law & Technology” 2014, Vol. 18, No. 3.
- Pan D., *Storing data on the margins: making state and infrastructure in Southwest China*, „Information, Communication & Society” 2022, Vol. 25, Issue 16.
- Pardesi M.S., *Explaining the asymmetry in the Sino-Indian Strategic Rivalry*, „Australian Journal of International Affairs” 2021, Vol. 75, No. 3.

- Parks W.H., *The Gulf War: A Practitioner's View*, „Penn State International Law Review-Penn State International Law Review” 1992, Vol. 10(3).
- Parsons D., *SANS ICS/OT Cybersecurity Survey: 2023's Challenges and Tomorrow's Defenses*, „Sans Analyst Program” 2023, Sep.
- Patrikarakos D., *Web 2.0: The New Battleground*, „Armed Conflict Survey” 2018, Vol. 4, No. 1.
- Pauwels E., *Preparing for next-generation information warfare with generative AI*, „CIGI Papers” 2024, No. 310.
- Payne K.B., *On Deterrence, Defense and Arm Control: In Honor of Colin S. Gray*, „NIFPP Information Series”, 2020, No. 461.
- Pazdej M., *Recepcja wojny zaprezentowana w traktatach Sun Tzu i Carla von Clausewitza oraz możliwość ich wykorzystania do metodologicznego określenia nowoczesnych konfliktów asymetrycznych*, „Świat Idei i Polityki” 2014, t. 13(14).
- Perera S., Jin X., Maurushat A., Opoku D.G.J., *Factors Affecting Reputational Damage to Organisations Due to Cyberattacks*, „Informatics” 2022, Vol. 9, No. 28.
- Phole J., Thiel T., *Digital sovereignty*, „Internet Policy Review” 2020, Vol. 9, Issue 4.
- Piątkowski K., *Wojna nowego typu?*, „Polska w Europie” 2002, nr 1.
- Pijpers P., Arnold K., *Rethinking Cyber Deterrence*, „Journal of Strategic Security” 2025, Vol. 18, No. 1.
- Pincus R.W., *Press access to military operations: Grenada and the need for a new analytical framework*, „University of Pennsylvania Law Review” 1987, Vol. 135(813).
- Pitcher S., Andress T., *Cybersecurity and Cyber Resilience Requirements Critical to Cyberspace Survivability*, „Naval Engineers Journal” 2024, Volume 136, No. 1–2.
- Plachkinova M., Vo A., *A Taxonomy of Cyberattacks against Critical Infrastructure*, „Journal of Cybersecurity Education, Research and Practice” 2022, Vol. 2021, No. 2(3).
- Polegkyi O., *Russian disinformation and propaganda before and after the invasion of Ukraine*, „Rocznik Instytutu Europy Środkowo-Wschodniej” 2023, nr 21, z. 1.
- Pollard M., *A Case Study of Russian Cyber-Attacks on the Ukrainian Power Grid: Implications and Best Practices for the United States*, „Pepperdine Policy Review” 2024, Vol. 166, Art. 1.
- Poltavtseva M. A., *Formation of Data Structures in the Problems of Active Security Monitoring*, „Automatic Control and Computer Sciences” 2021, Vol. 57, Issue 2.
- Porter P., *Shadow Wars: Asymmetric Warfare in the Past and Future*, „Security Dialogue” 2006, Vol. 37, No. 4.
- Price N.S., *The Vikings in Brittany*. „Saga Book” 1986–1989, Vol. 22.
- Puchala D.J., *Of Pirates and Terrorists: What Experience and History Teach*, „Contemporary Security Policy” 2005, Vol. 26, No. 1.
- Purhonen S., *Generations on paper: Bourdieu and the critique of 'generationalism'*, „Social Science Information” 2016, Vol. 55 (1).
- Qi Q., Wang Z., Xu Y., Fang Y., Wang C., *Enhancing Phishing Email Detection through Ensemble Learning and Undersampling*, „Applied Sciences” 2023, No. 13.

- Qi W. i inni, *Non-nuclear electromagnetic pulse threat of critical infrastructures and protection strategies*, „Strategic Study of Chinese Academy of Engineering” 2022, Vol. 24, No. 4.
- Qiu W., *Development and consideration of Chinese super-large diameter shield tunne*, „Archives of Civil Engineering” 2024, Vol. 70, Issue 1.
- Radanliev P., *Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing*, „Journal of Cyber Security Technology” 2024, Vol. 9, No. 1.
- Radnitz S., *Solidarity through Cynicism? The Influence of Russian Conspiracy Narratives Abroad*, „International Studies Quarterly” 2022, No. 66.
- Ramet S.P., *The denial syndrome and its consequences: Serbian political culture since 2000*, „Communist and Post-Communist Studies” 2007, No. 40.
- Rasmussen J/, *Risk management in a dynamic society: a modelling problem*, „Safety Science” 1997, Vol. 27, Issue 2–3.
- Redeer J.R., Hall T., *Cybersecurity’s Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack*, „Cyber Defense Review” 2021, Vol. 6, No. 1.
- Regina-Zacharski J., *Ukraina 2014–2015: wojna (nie)hybrydowa*, „Zeszyty Naukowe AON” 2015, nr 3(100).
- Reichborn-Kjennerud E., Cullen P., *What is Hybrid Warfare?*, „Policy Biref” 2016, No. 1.
- Reis F., Grzybowski J., *Moving ‘redlines’: The Russian–Ukrainian war and the pragmatic (mis-)use of international law*, „Global Constitutionalism” 2024, Vol. 13 No. 2.
- Ren H., *Network Warfare and Information Communication: the role and Challenge of New Media in the conflict in Ukraine*, „International Journal of Social Sciences and Economic Management” 2024, Vol. 5, Issue 2.
- Renz B., *Russia and ‘hybrid warfare’*, „Contemporary Politics” 2016, Vol. 22, No. 3.
- Renz B., Smith H., *Russia and Hybrid warfare—going beyond the label*, „Aleksanteri Papers” 2016, No. 1.
- Ricciardi S., Souque C., *Modern Electromagnetic Spectrum Battlefield From EMS Global Supremacy to Local Superiority*, „PRISM” 2021, Vol. 9, No. 3.
- Richter J., Hatch W.F., *Organizing Civil Society in Russia and China: A Comparative Approach*, „International Journal of Politics, Culture, and Society” 2013, Vol. 26.
- Rid T., Buchanan B, *Attributing Cyber Attacks*, „Journal of Strategic Studies” 2015, Vol. 38, No. 1–2.
- Rid T., *More Attacks, Less Violence*, „Journal of Strategic Studies” 2013, Vol. 36, No. 1.
- Rishad S.I., *Leveraging AI and Machine Learning for Predicting, Detecting, and Mitigating Cybersecurity Threats: A Comparative Study of Advanced Models*, „International Journal of Science & Information System” 2025, Vol. 10, Issue 1.
- Roberts A., *WikiLeaks: the illusion of transparency*, „International Review of Administrative Sciences” 2012, Vol. 78, No. 1.
- Roberts H., *North African Islamism in the Blinding Light of 9-11*, „Crisis States Programme” 2003, No. 34.
- Rollins P.C., *The Vietnam War: Perceptions Through Literature, Film, and Television*, „American Quarterly”, 1984, Vol. 36, No. 3.

- Romański R., *Mechanisms of Disinformation Amplification in Hybrid Warfare: The Case of the Conflict in Ukraine*, „Bulletin of Carol I National Defence University” 2025, No. 2.
- Roscbwalb S.A., *The Hill & Knowlton Cases: A Brief on the Controversy*, „Public Relations Review” 1994, Vol. 20, No. 3.
- Rowse A.E., *How to Build Support for War*, „Columbia Journalism Review” 1992, No. 31.
- Russell-Hsiao L.C., *China's Underground 'Great Wall' and Nuclear Deterrence*, „China Brief” 2009, Vol. 9, Issue 25.
- Saeed S. i inni, *Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations*, „Sensors” 2023, Vol. 23, Issue 6666.
- Savelyev Y., *Untruthful claims, real war, dire consequences: understanding the narrative of the Russian invasion of Ukraine*, „Journal of Contemporary Central and Eastern Europe” 2023, Vol. 31, No. 2.
- Schmidt N., *Neither Conventional War, nor a Cyber War, but a Long-Lasting and Silent Hybrid War*, „Obrana a strategie” 2014, Vol. 14 No. 2.
- Schmitz-Berndt S., *Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive*, „Journal of Cybersecurity” 2023, Vol. 9, No. 1.
- Schneider J., Macdonald J., *Looking back to look forward: Autonomous systems, military revolutions, and the importance of cost*, „Journal of Strategic Studies” 2023, Vol. 47, No. 2.
- Schroefl J., Kaufman S.J., *Hybrid Actors, Tactical Variety: Rethinking Asymmetric and Hybrid War*, „Studies in Conflict & Terrorism” 2014, Vol. 37, Issue 10.
- Schwartz P.M., *Global Data Privacy: The EU Way*, „New York University Law Review” 2019, Vol. 94, Rev. 771.
- Sehgal J., *Enhancing Site Reliability Engineering: Scalable Strategies for Automated Incident Response and System Resilience*, „Journal of Artificial Intelligence, Machine Learning and Data Science” Vol. 2, Issue 4.
- Shea G.W., *Justinian's North African Strategy in the Johannis of Corippus*, „Byzantine Studies” 1983, t. 10.
- Shea J., *How is NATO Meeting the Challenge of Cyberspace?*, „PRISM” 2017, Vol. 7, No. 2.
- Shirin S.S., Bogolubova N.M., Nikolaeva J.V., *Application of David Easton's Model of Political System to the World Wide Web*, „World Applied Sciences Journal” 2014, Vol. 30, No. 8.
- Shorer M., *Mobilization of Women to Terrorism: Tools and Methods of ISIS*, „International Annals of Criminology” 2018, No. 56.
- Singh A., *China's 'Three Warfares' and India*, „Journal of Defence Studies” 2013, Vol. 7, No. 4.
- Singsank R., *Skepticism and Exposure: Television Coverage of the Vietnam*, „Armstrong Undergraduate Journal of History” 2020, Vol. 10: Issue 2.
- Sisoyan A., *New cybersecurity challenges: digital transformation and the political implications of their implementation*, „Journal of Political Science: Bulletin of Yerevan University” 2025, Vol. 4, No. 1 (10).
- Sithole T.O., *The use of digital platforms by citizen aid actors during the Ukraine humanitarian crisis*, „Frontiers in Human Dynamics” 2024, Vol. 6.

- Small G., *The Rogue Private Company and National Defense Emergencies*, „Duke Journal of Constitutional Law & Public Policy” 2025, Vol. 20.
- Smirnova O., Holt T.J., *Exploring and Estimating the Revenues of Cybercrime-As-Service Providers: Analyzing Booter and Stresser Services*, „Deviant Behavior” 2025, Vol. 46, No. 10.
- Smith M.L.R., Stone J., *Explaining Strategic Theory*, „Infinity Journal” 2011, Vol. 1, No. 4.
- Solce N., *The Battlefield of Cyberspace: The Inevitable New Military Branch — The Cyber Force*, „Albany Law Journal of Science & Technology” 2008, Vol. 18, Issue 1.
- Solomennikova E.A., Lugacheva L.I., Musatova M.M., *The Strengthening of Economic Position of Russian Electronics: Mechanisms and Capabilities*, „Журнал Сибирского федерального университета. Гуманитарные науки” 2020, № 13(11).
- Srinivasan R., Ajay C., *Biases in AI systems*, „Communications of the ACM” 2021, Vol. 64, No. 8.
- Srogosz T., *Między mitem sublimacji a mitem apokalipsy wojennej w badaniu historii wojskowości XVII wieku*, „Acta Universitatis Lodzianis. Folia Historica” 2024, nr 117.
- Stachura M., *Wojna Justyniana z Maurami — przykład konfliktu asymetrycznego?*, „Prace Historyczne” 2016, nr 4.
- Stachura M., *Żołnierze Justyniana w Afryce — okupanci czy wyzwoliciele?*, „Przegląd Historyczno-Wojskowy” 2022, nr 4.
- Steingartner W., Galinec D., Kozina A., *Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model*, „MDPI Symmetry”, 2021, No. 13.
- Steven R.C., Murdoch S.J., Watson R.N.M., *Ignoring the Great Firewall of China*, „Journal of Law and Policy for the Information Society” 2007, Vol. 3, No. 2.
- Stevens C., *Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet*, „Contemporary Security Policy” 2020, Vol. 41, No. 1.
- Stouraitis I., *‘Just War’ and ‘Holy War’ in the Middle Ages*, „Jahrbuch der Österreichischen Byzantinistik” 2012, T. 62.
- Strachan H., *On War, Joint Warfare*, „The RUSI Journal” 2009, Vol. 154, No. 4.
- Street E., Chen S.S., *Teamwork from the Golden-Age Pirates: Could this Strategy Work in Today’s Contemporary Sports Setting?*, „Missouri Journal HPERD” 2018, vol. 28.
- Stroker D., Whiteside C., *Blurred Lines: Gray-Zone Conflict and Hybrid War — Two Failures of American Strategic Thinking*, „Naval War College Review” 2020, Vol. 73, No. 1.
- Subramanian L., *Banias and the British: The Role of Indigenous Credit in the Process of Imperial Expansion in Western India in the Second Half of the Eighteenth Century*, „Modern Asian Studies” 1987, Vol. 21, No. 3.
- Sufi F., Alsulami M., *Mathematical Modeling and Clustering Framework for Cyber Threat Analysis Across Industries*, „Mathematics” 2025, Vol. 13(655).
- Sullivan G.R., Dubik J.M., *War in the information age*, „Strategic Studies Institute” 1994, Vol. 94, No. 4.
- Svobodová M., *Russia’s approach to arms control: caught between asymmetry and the desire for strategic stability*, „European Security” 2023, Vol. 33, Issue 1.

- Swallow R.C., *Considering the cost of cyber warfare: advancing cyber warfare analytics to better assess tradeoffs in system destruction warfare*, „Journal of Defense Modeling and Simulation: Applications, Methodology, Technology” 2023, Vol. 20, No. 1.
- Szpak A., *Status „małych zielonych ludzików” w konflikcie zbrojnym na Ukrainie*, „Stosunki Międzynarodowe” 2016, Tom 52, Nr 1.
- Śliwa Z., *The Synergy Between Technology and Soldiers in Warfare–The Russian Armed Forces Image During the War in Ukraine*, „Wiedza obronna”, t. 281, nr 4.
- Tejani A.S., Ng Y.S., Xi Y., Rayan J.C., *Understanding and Mitigating Bias in Imaging Artificial Intelligence*, „Informatics” 2024, Vol. 44, No. 5.
- Tenenbaum E., *Le piège de la guerre hybride*, „Focus stratégique” 2105, No. 63.
- Terlikowski M., *Cyber attacks on Estonia. Implications for International and Polish Security*, „Polish Quarterly of International Affairs” 2007, Vol. 16, No. 3.
- Thomas G., *Introduction to the Modbus Protocol*, „The Extension” 2008, Vol. 9, Issue 4.
- Thornton R., *The Changing Nature of Modern Warfare. Responding to Russian Information Warfare*, „The RUSI Journal” 2015, Vol. 160, No. 4.
- Thussu D.K., *Legitimizing Humanitarian Intervention? CNN, NATO and the Kosovo Crisis*, „European Journal of Communication” 2000, Vol. 15, No. 3.
- Tidy J., *Visual regimes and the politics of war experience: Rewriting war ‘from above’ in WikiLeaks’ ‘Collateral Murder’*, „Review of International Studies” 2016, Vol. 43.
- Tielidze G., *Russia’s Changed Attack Tactics and Vectors in Cyberspace*, „Rondeli Foundation Expert Opinion” 2021, No. 171.
- Tona P.S., *An Overview of China’s Development in Cyberspace*, „International Journal of Cyber Diplomacy” 2024, Vol. 5.
- Topor S., *The Future of Warfare in the Volatility, Uncertainty, Complexity and Ambiguity Context*, „Land Forces Academy Review” 2024, Vol. 29, No. 2(114).
- Tor U., *‘Cumulative Deterrence’ as a New Paradigm for Cyber Deterrence*, „Journal of Strategic Studies” 2017, Vol. 40, No. 1–2.
- Trbojević D., *Unearthing memories: 1999 bombing of FR Yugoslavia between crisis, trauma and nostalgia*, „Ethnologia Slovaca et Slavica” 2024, T. 45.
- Tsagourias N., *Cyber Attribution Agencies: A Sceptical View*, „QIL Zoom In” 2024, No. 106.
- Tsantikidou K., Sklavos N., *Threats, Attacks, and Cryptography Frameworks of Cybersecurity in Critical Infrastructures*, „Cryptography” 2024, Vol. 8, No. 7.
- Val O.O. i inni, *Strengthening Cybersecurity Measures for the Defense of Critical Infrastructure in the United States*, „Asian Journal of Research in Computer Science” 2024, Vol. 17, No. 11.
- Valiaveedu A., Rybinski P.F., *The Race for Artificial Intelligence*, „Illini Journal of International Security” 2021, Vol. 8.
- Van der Bles A.M. i inni, *The effects of communicating uncertainty on public trust in facts and numbers*. „Proceedings of the National academy of Sciences of the USA” 2020, Vol. 117, No. 14.
- Vance A.S., *Cybersecurity risks and opportunities in the quantum computing age: A study*, „Quantum Journal of Engineering, Science and Technology” 2024, Vol. 5, No. 3.

- Vartavarian M., *An Open Military Economy: The British Conquest of South India Reconsidered, 1780-1799*, „Journal of the Economic and Social History of the Orient” 2014, No. 57 (4).
- Venable J., *Expensive F-15EX Does Not Deliver: Congress Should Nix Its Purchase*, „Issue Brief: Center for National Defense” 2020, No. 6009.
- Vishwanath A. i inni, *Cyber hygiene: The concept, its measure, and its initial tests*, „Decision Support Systems” 2020, No. 128.
- Vitale H.M., Keagle J.M., *A Time to Tweet, as Well as a Time to Kill: ISIS's Projection of Power in Iraq and Syria*, „Defense Horizons” 2014, No. 77.
- Vlad R.O., *The perils of presidential openness: strikes, secrecy and performative opacity*, „Intelligence and National Security” 2023, Vol. 38, No. 6.
- Wachowicz M.J., *Ujęcie teoretyczne pojęcia dezinformacji*, „Wiedza Obronna” 2019, nr 1–2.
- Waldron A., *China's New Remembering of World War II: The Case of Zhang Zizhong*, „Modern Asian Studies” 1996, Vol. 30, No. 4.
- Walton D., *Appeal to Pity: A Case Study of the Argumentum Ad Misericordiam*, „Argumentation” Vol. 9, No. 5.
- Wang X., Liu C., Wei Y., Feng S., Sun D., Cheng H., *Three-dimensional transistors and integration based on low-dimensional materials for the post-Moore's law era*, „Materials Today” 2023, Vol. 63.
- Warden J.A., *The Enemy as a System*, „Airpower Journal” 1995, Vol. 9, No. 1.
- Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego”, 2013, nr 9.
- Weber V., *The Worldwide Web of Chinese and Russian Information Controls*, „Centre for Technology and Global Affairs: Working Paper Series” 2019, No. 11.
- Wheeler N.J., *Dying for 'Enduring Freedom': Accepting responsibility for civilian casualties in the war against terrorism*, „International Relations” 2002, Vol. 16, No. 2.
- Wilczyński M., *Wojna bizantyńsko-wandalska 533—53*, „Rocznik Naukowo Dydaktyczny/Prace Historyczne XII” 1987, nr 109.
- Winkler A., *The Swabian War of 1499: 500 Years Since Switzerland's Last War of Independence of Independence*, „Swiss American Historical Society Review” 1999, Vol. 35, No. 3.
- Winkler A., *The Swiss in the Swabian War of 1499: An Analysis of the Swiss Military at the End of the Fifteenth Century. Military at the End of the Fifteenth Century*, „Swiss American Historical Society Review” 2020, Vol. 56, No 3.
- Wirtz J.J., *The Cyber Pearl Harbor*, „Intelligence and National Security” 2017, Vol. 32, No. 6.
- Wither J.K., *Making Sense of Hybrid Warfare*, „Connections: The Quarterly Journal” 2016, No. 2.
- Wojanowski M., *Mit „wojny hybrydowej”. Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku*, „Przegląd Bezpieczeństwa Wewnętrznego 2015”, wyd. spec. „Wojna hybrydowa”.
- Wojanowski M., *Koncepcja „wojny nowej generacji” w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego” 2015, Nr 7 (13).

Wortzel L.M., *What the Chinese People's Liberation Army Can Do to Thwart the Army's Multi-Domain Task Force*, „Land Warfare” 2019, No. 126.

Xiong W., Wu D.D., Yeung J.H.Y., *Semiconductor supply chain resilience and disruption: insights, mitigation, and future directions*, „International Journal of Production Research” 2024, Vol. 63, No. 9.

Yadav S., *Social automation and APT attributions in national cybersecurity*, „Journal of Cyber Security Technology” 2024, Vol. 8, No. 4.

Yang X.Y. i inni, *Research on the Construction of a Novel Cyberspace Security Ecosystem*, „Engineering” 2018, Vol. 4.

Yanzhao X., Minzhou L., Yuhao C., *Electromagnetic resilience of critical national infrastructure*, „High Power Laser and Particle Beams” 2019, No. 31(070001).

Yoo C.S., Baran P., *Network Theory, and the Past, Present, and Future of Internet*, „Penn Law: Legal Scholarship Repository” 2018, pos. 2040.

Zapfe M., *Deterrence from the Ground Up Understanding NATO's Enhanced Forward Presence*, „Survival” 2017, No. 59.

Zarembo K, Knodt J., Kachel J., *Smartphone resilience: ICT in Ukrainian civic response to the Russian full-scale invasion*, „Media, War & Conflict” 2025, Vol. 18, No. 3.

Zavorodnya E., Mazaraki A., Melnyk T., *ICT sector competitiveness: A comparative analysis of Ukraine and other 7 eastern european countries*, „Regional and Sectoral Economic Studies” 2024, Vol. 24, No. 2.

Zegzhda D., Lavrova D., Pavlenko E., Shtyrkina A., *Cyber Attack Prevention Based on Evolutionary Cybernetics Approach*, „Symmetry” 2020, Vol. 12, Issue 11.

Zhang L. i inni, *Research on the Cyberspace Map and Its Conceptual Model*, „ISPRS” 2023, No. 12(353).

Zheng F., Di G., *Global Cyber Governance in China: Towards Building a Community of Shared Future in Cyberspace*, „Science, Technology and Society” 2022, Vol. 27, Issue 3.

Zinovyeva E., *U.S. Digital Diplomacy: Impact on International Security and Opportunities for Russia*, „Security Index: A Russian Journal on International Security” 2013, Vol. 19, No. 2.

Арбатов А.Г., *Украинский кризис и стратегическая стабильность*. „Полис. Политические исследования” 2022, № 4.

Булва В., *Международная информационная безопасность: от классической к сетевой дипломатии России*. „Вестник Санкт-Петербургского университета. Международные отношения” 2024, № 17(3).

Васильевич Т.О., *Теория и практика «гибридного» противоборства: обзор конфликтов с XV века до наших дней*, „Конфликтология” 2021, № 2.

Герасимов В., *Ценность науки в предвидении*, „Военно-промышленный курьер” 2013, № 8 (476).

Горбунов В.Н., Богданов С.А., *О характере вооруженной борьбы в XXI веке*, „Военная мысль” 2009, № 3.

Горбунов В.Н., Богданов С.А., *Природа и содержание войны нового поколения*, „Военная мысль” 2013, № 4.

Грабчак Е.П., Логинов Е.Л., *Противодействие угрозам воздействия электромагнитного импульса: стратегические подходы к защите критической*

энергетической инфраструктуры в США, „Сложные системы: модели, анализ и управление” 2021, № 2.

Двилянский А.А., Иванов В.А., Конышев М.Ю., *Эргооптимизация системы обеспечения функциональной устойчивости объектов критической информационной инфраструктуры в условиях деструктивного электромагнитного воздействия*, „Эргодизайн” 2021, № 2.

Иванов В.А. i inni, *Роль и место электромагнитного оружия при реализации наступательной стратегии в информационной специальной операции*, „Техника средств связи” 2022, № 3(159).

Комлева Н.А., *Гибридная война: сущность и специфика*, „Известия Уральского федерального университета. Серия 3: Общественные науки” 2017, т. 12, № 3 (167).

Копылов А.В. i inni, *Взгляды военно-политического руководства США на защиту критически важных объектов от угроз кибернетического воздействия*, „Общество: политика, экономика, право” 2024, № 9.

Михайловна К.В. (ред.), *Актуальные проблемы международных отношений в условиях формирования мультиполярного мира*, Курск 2019.

Огарков Н.В., *Военная наука и защита социалистического Отечества*, „Коммунист” 1978, № 7.

Чекинов С.Г., Богданов С.А., *Влияние непрямых действий на характер современной войны*, „Военная мысль” 2011, № 6.

Чекинов С.Г., Богданов С.А., *Асимметричные действия по обеспечению военной безопасности России*, „Военная Мысль” 2010, № 3.

Чекинов С.Г., Богданов С.А., *Влияние непрямых действий на характер современной войны*, „Военная мысль” 2011, № 6.

Черноперов В.Л., Сулейманова У.И., *Гибридная война: предпосылки появления, концепции, сущность, цели, инструментарий, правовые вопросы, риски*, „Ноосферные исследования” 2021, Вып. 3.

Швец Н.Н. i inni, *Об энергетической безопасности России в условиях воздействия электромагнитного импульса высотного ядерного взрыва*, „Национальные интересы: приоритеты и безопасность” 2020, Т. 16, № 11.

Шевелев Э.Г., *Системология национальной безопасности на рубеже веков: состояние и перспективы развития*, „Вестник Самарского государственного аэрокосмического университета” 2004, № 2.

Шилов Н.И., *Афганистан 30 лет спустя: последствия ввода советских войск в ДРА для страны и региона*, „Вестник МГИМО” 2010, №2.

Rozdziały w monografiach i publikacjach zbiorowych

Albustanji H., *COVID-19 Pandemic Impact on Cyber Threats*, [w:] *The impact of COVID-19 crisis on diverse democratic perspectives through gender perspective*, Pucelj M. (ed.), Novo Mesto 2024.

Alqurashi E., Wills G., Gilbert L., *A Viable System Model for Information Security Governance: Establishing a Baseline of the Current Information Security Operations System*, [w:] *Security and Privacy Protection in Information Processing Systems*, Janczewski L.J., Wolfe H.B., Sheno S. (eds.), Auckland 2013.

- Ångström J., *Evaluating Rivalling Interpretations of Asymmetric War and Warfare*, [w:] *Conceptualising Modern War*, Haug K.E., Maaø O.J. (eds.), London 2011.
- Arav D., *Trauma and Nostalgia in the Israeli Televised Memory of the First Gulf War*, [w:] *Trauma and Nostalgia. Practices in Memory and Identity*, Liere L., Sremac S. (eds.), Amsterdam 2024.
- Bania R., *Wojny w cyberprzestrzeni — przypadek Iranu* [w:] *Bezpieczeństwo narodowe i międzynarodowe w regionie Bliskiego Wschodu i Północnej Afryki (MENA) u progu XXI wieku*, Bania R., Zdulski K. (red.), Łódź 2012.
- Barr-Smith F., Ugarte-Pedrero X., Graziano M., Spolaor R., Martinovic I., *Survivalism: Systematic Analysis of Windows Malware Living-Off-The-Land*, [w:] *2021 IEEE Symposium on Security and Privacy (SP)*, O'Conner L. (ed.), Los Alamitos 2021.
- Bellasio J., Silfversten E., *The Impact of New and Emerging Technologies on the Cyber Threat Landscape and Their Implications for NATO* [w:] *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, Ertan A., Floyd K., Pernik P., Stevens T. (eds.), Tallinn 2020.
- Bender H., Kanderske M., *Consumer Drone Warfare: Practices, Aesthetics and Discourses of Consumer Drones in the Russo-Ukrainian War*, [w:] *Drones in Society. New Visual Aesthetics*, Serafinelli E. (ed.), Cham 2024.
- Bjorge G.J., *Compound Warfare in the Military Thought and Practice of Mao Zedong and the Chinese People's Liberation Army's Huai Hai Campagin (November 1948 — January 1949)* [w:] *Compound Warfare: The Fatal Knot*, T.M. Huber (ed.), Fort Leavenworth 2002.
- Bures O., *Contributions of Private Businesses to the Provision of Security in the EU: Beyond Public-Private Partnerships*, [w:] *Security Privatization How Non-security-related Private Businesses Shape Security Governance*, Bures O., Carrapicio H. (eds.), [b.m.w.] 2018.
- Campello R.J.G.B., Moulavi D., Sander J., *Density-Based Clustering Based on Hierarchical Density Estimates*, [w:] *Advances in Knowledge Discovery and Data Mining. Part II*, Pei J. i inni (eds.), Berlin 2013.
- Chesher C., *The Ontology of Digital Domains*, [w:] *Virtual Politics: Identity and Community in Cyberspace*, Holmes D. (ed.), London-Thousand Oaks-New Delhi 1997.
- Choucri N., *Emerging Trends in Cyberspace: Dimensions and Dilemmas*, [w:] *Cyberspace: Malevolent Actors, Criminal Opportunities and Strategic Competition*, Williams P., Fiddner D. (eds.), [AD1014198] 2016.
- Ciborek P., *Political and Economic Activities of the PRC on the Balkan Peninsula Romania: A Case Study*, [w:] *New Dynamics in Asia*, Żakowski K. (ed.), Łódź 2020.
- Claverie B., Du Cluzel F., *"Cognitive Warfare": The Advent of the Concept of "Cognitics" in the Field of Warfare* [w:] *Cognitive Warfare*, Claverie B., Prébot B., Buchler N., Du Cluzel F. (eds.), Neuilly 2022.
- Colom-Piella G., *Cyber activities in the grey zone: an overview of the Russian and Chinese approaches*, [w:] *The Complex and Dynamic Nature of the Security Environment*, Cîrcimaru F., Cojocaru I. (eds.), Bucharest 2024.
- Creemers R.J.E.H., Pieke F.N., Iwabushi K., *Common destiny in cyberspace: China's cyber diplomacy*, [w:] *The Global Square*, Pieke F.N., Iwabushi K. (eds.), Berkeley 2021.

Cullen P., *A perspective on EU hybrid threat early warning efforts*, [w:] *Hybrid Warfare. Security and Asymmetric Conflict in International Relations*, Weissmann M, Nilsson N, Palmertz B, Thunholm P. (eds.), London 2021.

Cullen P., Wegge N., *Warning of hybrid threats*, [w:] *Intelligence Analysis in the Digital Age*, Stenslie S., Haugom L., Vaage B.H. (eds.), New York 2021.

Deibert R., Rohozinski R., *Control and Subversion in Russian Cyberspace*, [w:] *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, Deibert R., Palfrey J., Rohozinski R., Zittrain J. (eds.), Cambridge 2010.

Dejneka D., *Siły Zbrojne Federacji Rosyjskiej w operacjach XXI wieku*, [w:] *Rosyjska wizja prowadzenia operacji militarnych*, Markiewicz S. (red.), Warszawa 2018.

Dewar R.S.S., *The "Triptych of Cyber Security": A Classification of Active Cyber Defence*, [w:] *2014 6th International Conference on Cyber Conflict*, Brangetto P, Maybaum M., Stinissen J. (eds.), Tallin 2014.

East S., Butts J., Papa M., Sheno S., *A Taxonomy of Attacks on the DNP3 Protocol*, [w:] *Critical Infrastructure Protection III*, Palmer C., Sheno S. (eds.), Hanover 2009.

Fantasia R., Hirsch E.L., *Culture in rebellion: The appropriation and transformation of the veil in the Algerian revolution*, [w:] *Social Movements and Culture. Volume 4*, H. Johnston, B. Klandermans (eds.), Minneapolis 1995.

Ferris J., *Small Wars and Great Games: The British Empire and Hybrid Warfare, 1700–1970* [w:] *Hybrid Warfare Fighting Complex Opponents from the Ancient World to the Present*, Murray W., Mansoor P.R. (eds.), Cambridge 2012.

Fridman O., *Old Wine in a New Bottle: The Cold-War Origins of the Concept of Gibrid-naya Voyna*, [w:] *Russia and the former societ space. Instrumentalizing Security, Legitimizing Intervention*, Rotaru V., Troncotă M. (eds.), Cambridge 2017.

Galeotti M., *'Hybrid War' and 'Little Green Men': How It Works, and How It Doesn't*, [w:] *Ukraine and Russia: People, Politics, Propaganda and Perspectives*, Pikulicka-Wilczewska A., Sakwa R. (ed.), Bristol 2015.

Goździewicz W., *From Riga to Wales. NATO's Road to Collective Cyberdefence*, [w:] *NATO Road to Cybersecurity*, Świątkowska J. (ed.), Kraków 2016.

Gross M., *Rewriting the nation: World War II narratives in Polish history textbooks*, [w:] *Post-Socialism is not Dead: (Re)Reading the Global in Comparative Education*, Silova I. (ed.), Bingley 2010.

Gulyás A., *„Lazarus” The North Korean Hacker Group*, [w:] *Proceedings of the International Scientific Conference Strategies XXI. The Complex And Dynamic Nature of The Security Enviornment*, Cîrciumaru F., Ioniță C.C. (eds.), Bucharest 2021.

Gvineria S., *Information Warfare as Russia's Hybrid Warfare Tool*, [w:] *Information Warfare — New Security Challenge for Europe*, Čížik T. (ed.), Bratislava 2017.

Hamilton S.N., Hamilton W.L., *Adversary Modeling and Simulation in Cyber Warfare*, [w:] *Proceedings of the IFIP TC 11 23rd International Information Security Conference*, Jajodia S., Samarati P., Cimito S. (eds.), Milano 2008.

Hammond P., Nizamova L., Savelieva I., *Consensus and Conflict in the Russian Press*, [w:] *Degraded Capability: The Media and the Kosovo Crisis*, Herman E.S., Hammond P. (eds.), London 2000.

Harrison G.A., *Overlord: A classic Joint and Combined Operation*, [w:] *Joint Warfare of the Armed Forces of the United States [Joint Pub. 1]*, Washington 1995.

- Heim M., *The Erotic Ontology of Cyberspace*, [w:] *The Metaphysics of Virtual Reality*, Heim M. (ed.), Oxford 1993.
- Hristova A., *Populism: A Basis for Polarization Processes in Society*, [w:] *Social Response to Polycrisis: The Case of Bulgaria*, Hristova A. (ed.), New York 2024.
- Huber T.M., *Compound Warfare: A Conceptual Framework* [w:] *Compound Warfare. That Fatal Knot*, Huber T.M. (ed.), Fort Leavenworth 2002.
- Hughes D., Colarik A., *The Hierarchy of Cyber War Definitions*, [w:] *Intelligence and Security Informatics*, Wang G.A., Chau M., Chen H. (eds.), Jeju 2017.
- Huskaj G., *The Current State of Research in Offensive Cyberspace Operations*, [w:] *EC-CWS 2019 — Proceedings of the 18th European Conference on Cyber Warfare and Security*, Cruz T., Simoses P. (eds.), New York 2019.
- Jórárt K, Rácz A., *Contemporary Russian Military Thinking on Conflicts of the 21st Century: Beyond the 'Gerasimov Doctrine'*, [w:] *Conflicts in the Gray Zone A Challenge to Adapt*, Kiss A.P. (ed.), Budapest 2017.
- Keinonen M., *Using Military Cyber Operations as a Deterrent*, [w:] *Proceedings of the 18th International Conference on Cyber Warfare and Security*, Wilson R.L., Curran B. (eds.), Reading 2023.
- Khoury J., Pour M.S., Bou-Harb E., *A Near Real-Time Scheme for Collecting and Analyzing IoT Malware Artifacts at Scale*, [w:] *Proceedings of the 17th International Conference on Availability, Reliability and Security*, Engel D., Fischer M. (eds.), Vienna 2022.
- Klimburg A., Faesen L., *A Balance of Power in Cyberspace*, [w:] *Governing Cyberspace Behavior, Power, and Diplomacy*, Broeders D., Berg B. (eds.), Lanham-Boulder-New York-London 2020.
- Kukkola J., *Cyber asymmetry — Towards new strategic thinking?*, [w:] *Game Changer: Structural transformation of cyberspace*, Kukkola J., Ristolainen M., Nikkarila J.P. (eds), Riihimäki 2017.
- Kukkola J., *The Russian National Segment of the Internet as a Source of Structural Cyber Asymmetry*, [w:] *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, Ertan A., Floyd K., Pernik P., Stevens T. (eds.), Tallinn 2020.
- Kushwaha N., Roguski P., Watson B.W., *Up in the Air: Ensuring Government Data Sovereignty in the Cloud*, [w:] *12th International Conference on Cyber Conflict. 20/20 Vision: The Next Decade. Proceedings 2020*, Jančárková T., Lindström L., Signoretti M., Tolga I., Visky G. (eds.), Tallin 2020.
- Leigh G., *Cyber Security Operations: Tactics, Techniques, and Procedures*, [w:] *The Handbook of Homeland Security*, Romaniuk S.N., Catino M.S., Martin C.A. (eds.), Milton 2023.
- Lim J-H, *Victimhood Nationalism in Contested Memories: National Mourning and Global Accountability*, [w:] *Memory in a Global Age. Discourses, Practices and Trajectories*, Assmann A., Conrad S. (eds.), New York 2010.
- Madej M., *Terroryzm i inne zagrożenia asymetryczne w świetle współczesnego pojmowania bezpieczeństwa narodowego i międzynarodowego — próba teoretycznej konceptualizacji*, [w:] *Porządek międzynarodowy u progu XXI wieku*, Kuźniar R. (red.), Warszawa 2005.
- Mansi, *Sacrorum Conciliorum Nova, et Amplissima Collectio*, Head T. (trans.), [w:] *The Peace of God: Social Violence and Religious Response in France around the Year 1000*, Head T., Landes R. (eds.), Ithaca-London 1992.

Mansoor P.R., *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, [w:] *Hybrid Warfare in History*, W. Murray, P.R. Mansoor (eds.), New York 2012.

Mastro O.S., *China's Anti-access-Area Denial (A₂/AD) Capabilities: Is American Rebalancing Enough?*, [w:] *American Strategy and Purpose: Reflections on Foreign Policy and National Security in an Era of Change*, Natter III W.H., Brooks J. (eds.), Lexington 2014.

McCulloh T., *The Inadequacy of Definition and the Utility of a Theory of Hybrid Conflict: Is the "Hybrid Threat" New?* [w:] *Hybrid Warfare. JSOU Report 13-4*, McCulloh T., Johnson R. (eds.), Florida 2013.

Mitić A., *Reflection of the 1999 NATO Agression in the Strategic Narratives of Global Powers and the Context of Multipolarity*, [w:] *History and Cultural Memory*, Janijić J., Pesić M. (eds.), Belgrade 2024.

Münkler H., *Old and new wars* [w:] *The Routledge Handbook of Security Studies*, Cavelti M.D., Mauer V. (eds.), Abingdon-New York 2010.

Nikkarila J.P., Åkesson B., Kuikka V., Hämäläinen J., *Modelling Closed National Networks —Effects in Cyber Operation Capabilities*, [w:] *Game Player. Facing the structural transformation of cyberspace*, Kukkola J., Ristolainen M., Nikkarila J.P. (eds.), Riihimäki 2019.

Ostapchuk V., *Crimean Tatar long-range campaigns: The view from Remmal Khoja's History of Sahib Gerey Khan*, [w:] *Warfare in the Eastern Europe, 1500–1800*, Davies B.J. (ed.), Leiden 2012.

Perlo-Freeman S., Ismail O., Solmirano C., Sköns E., Solmirano C., *Military expenditure*, [w:] *SIPRI Yearbook 2010. Armaments, Disarmament and International Security*, Gill B. i inni (eds.), Oxford 2010.

Pinaya W.H.L., Vieira S., Garcia-Dias R., A. Mechelli, *Autoencoders*, [w:] *Machine Learning*, Mechelli A., Vieira S. (eds.), London-San Diego-Cambridge-Kidlington 2020.

Prestwich M., *Transcultural Warfare — the Later Middle Ages*, [w:] *Transcultural Wars. From the Middle Ages to the 21st Century*, Kortüm H.H. (ed.), Berlin 2006.

Prior T., *Resilience: The 'Fifth Wave' in the Evolution of Deterrence*, [w:] *Strategic Trends 2018. Key Developments in Global Affairs*, Thränert O., Zapfe M. (eds.), Zürich 2018.

Rinelli S., Duyvesteyn I., *The Missing Link: Civil-Military Cooperation and Hybrid Wars*, [w:] *A Civil-Military Response to Hybrid Threats*, Cusumano E., Corbe M. (eds.), London 2018.

Sale T., *The Colossus of Bletchley Park — The German Cipher System*, [w:] *The First Computers: History and Architecture*, Rojas R., Hashagen U. (eds.), Cambridge 2000.

Scheiner B., *The Psychology of Security*, [w:] *Progress in Cryptology — AfricaCrypt*, Vaudenay S. (ed.), Casablanca 2008.

Schmitt M.N., *States and cyberspace*, [w:] *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Schmitt M.N. (ed.), Cambridge 2013.

Sköns E., Loose-Weintraub E., Omitoogun W., Stålenheim P., Weidacher R., *Military expenditure and arms production*, [w:] *Sipri Yearbook 2001*, Stockholm 2001.

Smith H., *Countering Hybrid Threats*, [w:] *The EU and NATO: The Essential partners*, Lindstrom G., Tardy T. (eds.), Paris 2019.

- Solovey R., *Game-Theoretic Approach to Self-Regulation of Dynamic Network Infrastructure to Protect Against Cyber Attacks*, [w:] *2020 International Scientific and Technical Conference Modern Computer Network Technologies*, Smeliansky R. (ed.), Moscow 2020.
- Špaček S., Čeleda P., Drašar M., Vizváry M., *Analyzing an Off-the-Shelf Surveillance Software: Hacking Team Case Study*, [w:] *Proceedings of Conference SPI 2017: Security and Protection of Information*, Dočkal J., Jirsa M., Kaderka J. (eds.), Brno 2017.
- Steele D., *Sailsbury and the Soldiers*, [w:] *The Boer War. Distraction, Experience and Image*, Gooch J. (ed.), London-New York 2013.
- Tarnawski M., *Rosyjska koncepcja konfliktu nieliniarnego*, [w:] *Czynnik wojskowy w środowisku międzynarodowym na przełomie XX i XXI wieku*, Jureńczyk Ł., Sadowski S., Jastrzębski M., Waskan J. (red.), Bydgoszcz 2016.
- Van Raemdonck N., Meyer T., *Why Disinformation is Here to Stay. A Socio-technical Analysis of Disinformation as a Hybrid Threat*, [w:] *Addressing Hybrid Threats: European Law and Policies*, Lonardo L. (ed.), Cheltenham 2024.
- Wang D., Dehghanian Y.L.P., Wang S., *Power Grid Resilience to Electromagnetic Pulse (EMP) Disturbances: A Literature Review*, [w:] *2019 North American power symposium (NAPS)*, [edycja grupowa przez:] Institute of Electrical and Electronics Engineers, Inc., Wichita 2019.
- Weissinger L.B., *The Challenge of Networked Complexity to NATO's Digital Security*, [w:] *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, Ertan A., Floyd K., Pernik P., Stevens T. (eds.), Tallin 2020.
- Wejksznier A., *Wojny XXI wieku. Istota współczesnych konfliktów asymetrycznych*, [w:] *Zagrożenia asymetryczne współczesnego świata*, Wojciechowski S., Fiedler R. (red.), Poznań 2009.
- Wessels A., *The Anglo-Boer War (1899–1902) and its traumatic consequences*, [w:] *Breaking Intergenerational Cycles of Repetition A Global Dialogue on Historical Trauma and Memory*, Gobodo-Madikizela P. (ed.), Opladen-Berlin-Toronto 2016.
- Whang C., *Refocusing Export Control Regimes to Effectively Address Cyber Security Concerns*, [w:] *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, Ertan A., Floyd K., Pernik P., Stevens T. (eds.), Tallin 2020.
- Wu J., *More than sharp power. Chinese influence operations in Taiwan, Hong Kong and beyond*, [w:] *China's Influence and the Center-periphery Tug of War in Hong Kong, Taiwan and Indo-Pacific*, Fong B.C.H., Wu J., Nathan A.J. (eds.), London 2020.
- Zhen Z., *Guanyu wojun zhanyi lilun de jige wenti* [Kilka pytań dotyczących teorii kampanii ALW], [w:] *Tongxiang shengli de tansou* [Odkrywając drogi do zwycięstwa], Editorial Group (ed.), Pekin 1987.
- Zieliński T., *Drones in Military Conflicts. Are Unmanned Aircraft Systems the Future of Wars?*, [w:] *Challenges to National Defence in Contemporary Geopolitical Situation*, Bekesiene S., Hoskova-Mayerova S. (eds.), Wilno 2022.
- Zięba R., *Pozimnowojenny paradygmat bezpieczeństwa*, [w:] *Bezpieczeństwo międzynarodowe po zimnej wojnie*, Zięba R. (red.), Warszawa 2008.
- Zuse K., *Frühe Gedanken zur Auswirkung des Computers auf die Gesellschaft*, [w:] *Geschichten der Informatik. Visionen, Paradigmen, Leitmotive*, Hellige H.D. (hg.), Berlin 2004.

Бугорская Е.Н., Емельянова О.В., *"Гибридная война" как новый тип войны в 21 веке*, [w:] *Актуальные проблемы международных отношений в условиях формирования мультиполярного мира*, Михайловна К.В. (ред.), Курск 2019.

Кузнецов А.А., *Цифровая трансформация и кибербезопасность: вызовы и стратегии*, [w:] *Глобальные социальные процессы 4.0: социокультурные трансформации в системе современных обществ*, Петров А.В. i inni (ред.), Санкт-Петербург 2023.

Петров А.В., *Глобальные социальные процессы и современные исследования социокультурных трансформаций в социологии*, [w:] *Глобальные социальные процессы 4.0: социокультурные трансформации в системе современных обществ*, Петров А.В. i inni (ред.), Санкт-Петербург 2023.

Хатиб И., Денев Д., *Природни източници на радиация и тяхното въздействие върху електрониката*, [w:] *Радиационната безопасност в съвременния свят. Том 2*, Долчинков Н. (ред.), Велико Търново 2025.

Artykuły prasowe

Grimes W., *Thomas C. Schelling Dies at 95; Used Game Theory to Explain Nuclear Strategy*, „New York Times” 2016, December 14.

Źródła internetowe

Bilal A., *Hybrid Warfare — New Threats, Complexity, and ‘Trust’ as the Antidote*, „NATO Review”, 30 November 2021, <https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html>.

Commission calls on 19 Member states to fully transpose the NIS2 Directive, 7 May 2025, „European Commission”, <https://digital-strategy.ec.europa.eu/en/news/commission-calls-19-member-states-fully-transpose-nis2-directive>.

Creemers R., *Xi Jinping’s Speech at the National Cybersecurity and Informatization Work Conference*, 22 April 2018, „Digichina — Stanford Cyber Policy Center”, <https://digichina.stanford.edu/work/xi-jinpings-speech-at-the-national-cybersecurity-and-informatization-work-conference/>.

Garrity P., *2025 Q1 Trends in Vulnerability Exploitation*, 24 April 2025, „Vuln Check” <https://www.vulncheck.com/blog/exploitation-trends-q1-2025>.

Garrity P., *2025 Q1 Trends in Vulnerability Exploitation*, 24 April 2025, „VulnCheck”, <https://www.vulncheck.com/blog/exploitation-trends-q1-2025> [odczyt: 03.06.2025].

Hagelstam A., Narinen K., *Cooperating to counter hybrid threats*, „NATO Review”, 23.11.2018, <https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html>.

How Microsoft names threat actors, 31 July 2025, „Microsoft”, <https://learn.microsoft.com/en-us/unified-secops-platform/microsoft-threat-actor-naming>.

Liczba operatorów usług kluczowych (OUK) z podziałem na sektory, 7 lipca 2025, „Serwis Rzeczypospolitej Polskiej”, https://dane.gov.pl/pl/dataset/3409,liczba-operatorow-uslug-kuczowych-z-podzialem-na-sektory/resource/68232/table?page=1&per_page=50&q=&sort=.

Munzinger Archiv GmbH, Internationales Biographisches Archiv, 16/2020 vom 14. April 2020 (la), Eintrag „Eppler, Erhard”, <https://www.munzinger.de/search/go/document.jsp?id=00000012072>.

Munzinger Archiv GmbH, Internationales Biographisches Archiv, 19/2021 vom 11. Mai 2021 (bo), Eintrag „Münkler, Herfried“, <https://www.munzinger.de/search/go/document.jsp?id=00000024700>.

NIS2, czyli nowe wymogi dotyczące cyberbezpieczeństwa, 25.07.2025, „PwC”, <https://www.pwc.pl/pl/uslugi/nis2-nowe-wymogi-dotyczace-cyberbezpieczenstwa.html>.

Proska K. i inni, *Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology*, 9 November 2023, „Mandiant”, <https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/>.

Putin V., *Statement by Vladimir Putin on additional steps to de-escalate the situation in Europe after the termination of the Intermediate-Range Nuclear Forces Treaty (INF Treaty)*, 26 October 2020, „President of Russia”, <http://en.kremlin.ru/events/president/news/64270>.

Questions and Answers about the East StratCom Task Force, „The Diplomatic Service of the European Union”, 27.10.2021, https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11235.

Terefos A., *Banshee: The Stealer That “Stole Code” From MacOS XProtect*, „Check Point Research” 9 January 2025, <https://research.checkpoint.com/2025/banshee-macos-stealer-that-stole-code-from-macos-xprotect/#single-post>.

The Balkans: quo vadis? Jamie Shea: Kosowo – wówczas i obecnie, 25 August 2008, „NATO Review”, <https://www.nato.int/docu/review/pl/articles/2008/08/25/jamie-shea-kosowo-wowczas-i-obecnie/index.html>.

Unit42, *Russia-Ukraine Cyberattacks (Updated): How to Protect Against Related Cyberthreats Including DDoS, HermeticWiper, Gamaredon, Website Defacement, Phishing and Scams*, 22 February 2022, „Paloalto Networks”, <https://unit42.paloaltonetworks.com/preparing-for-cyber-impact-russia-ukraine-crisis/>.

Кібератака на сайти державних органів, 14 січня 2022, „CERT-UA”, <https://cert.gov.ua/article/17899>.

СБУ: Наразі відновлено роботу 95% сайтів, що постраждали від кібератаки на державні ресурси; 17 січня 2022, „Служба безпеки України”, <https://ssu.gov.ua/novyny/sbu-narazi-vidnovleno-robotu-95-saitiv-shcho-postrazhdaly-vid-kiberataky-na-derzhavni-resursy>.

Шевелев Эдуард Геннадьевич, „Центр военно-политических исследований”, <http://eurasian-defence.ru/?q=node/22749>.