Terroryzm – studia, analizy, prewencja, 2025, wydanie specjalne: 13–34

https://doi.org/10.4467/27204383TER.25.001.21504

Artykuł

Infrastruktura krytyczna jako cel działań hybrydowych. Studia przypadków ataków na obiekty i systemy IK

Critical infrastructure as a target for hybrid operations.
Case studies of attacks against the facilities and systems of CI

WITOLD SKOMRA https://orcid.org/0000-0002-2625-6683

Wydział Zarządzania, Politechnika Warszawska
Rządowe Centrum Bezpieczeństwa

KAROLINA WOJTASIK https://orcid.org/0000-0002-1215-5005

Stałe Przedstawicielstwo RP przy Unii Europejskiej
Rządowe Centrum Bezpieczeństwa

Abstrakt

Artykuł przedstawia analizę infrastruktury krytycznej (IK) jako celu ataku w operacjach hybrydowych, które łączą różne formy działań – od konwencjonalnych po terrorystyczne. Autorzy wskazują przyczyny atakowania IK. Podstawę rozważań stanowi teoria 5 pierścieni Wardena. W artykule omówiono operację Allied Force, kampanie dezinformacyjne poprzedzające synchronizację sieci energetycznych państw bałtyckich oraz atak na Colonial Pipeline. Autorzy przeprowadzają analizę porównawczą rozwiązań dotyczących budowania odporności IK wynikających z dyrektyw CER i NIS 2 Parlamentu Europejskiego i Rady Unii Europejskiej.

Słowa kluczowe

infrastruktura krytyczna, ochrona infrastruktury krytycznej, działania hybrydowe, zagrożenia hybrydowe, wojna hybrydowa, dyrektywa CER, dyrektywa NIS 2

Abstract

The article presents an analysis of critical infrastructure (CI) as a target for attack in hybrid operations, which combine various forms of action – from conventional to terrorist. The authors identify the reasons for attacking CI. The considerations are based on Warden's 5 rings theory. The article discusses Operation Allied Force, disinformation campaigns prior to the synchronisation of the Baltic states' energy networks, and the attack on the Colonial Pipeline. The authors conduct a comparative analysis of solutions for building CI resilience derived from the CER and NIS2 Directives of the European Parliament and the Council of the European Union.

Keywords

critical infrastructure, critical infrastructure protection, hybrid operations, hybrid threats, hybrid warfare, CER Directive, NIS 2 Directive

Wprowadzenie

Obecny poziom rozwoju cywilizacyjnego charakteryzuje się uzależnieniem społeczeństw od systemów i usług, które są związane z szeroko pojętą infrastrukturą krytyczną (IK). Prawodawstwo państw członkowskich Unii Europejskiej może różnić się w szczegółach dotyczących liczby systemów zaliczanych do IK, kryteriów uznawania podmiotu czy usługi za kluczowe czy progu zakłócenia takiej usługi, ale żadne nie kwestionuje znaczenia tej infrastruktury w funkcjonowaniu państwa i społeczeństwa. W artykule omówiono, w jaki sposób IK była i jest celem ataków hybrydowych. Ponadto autorzy pokazują, na ile zapisy *Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE* (dalej: dyrektywa CER) oraz *Dyrektywy 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 (dalej: dyrektywa NIS 2) wpływają na wzmocnienie odporności IK na te zagrożenia. Podstawę rozważań stanowi teoria 5 pierścieni Wardena[1] oraz pojęcie wojny hybrydowej rozumianej jako konflikt, w którym przeciwnik stosuje kombinację środków konwencjonalnych, nieregularnych, terrorystycznych i przestępczych w celu osiągnięcia swoich celów politycznych. Jednak najważniejszym elementem wojny hybrydowej jest – zdaniem Franka Hoffmana – wpływanie na społeczeństwo przeciwnika w taki sposób, aby wywarło presję na rząd i wymusiło określone działania lub ustępstwa[2].

Infrastruktura krytyczna jako cel ataku hybrydowego

Infrastruktura krytyczna stanowi podstawę funkcjonowania każdego państwa, a jej znaczenie sprawia, że jest szczególnie narażona na działania destabilizacyjne. Istnieje kilka powodów, dla których to właśnie IK jest priorytetowym celem ataków hybrydowych.

Ataki na IK mogą sparaliżować całe państwo. W przeciwieństwie do tradycyjnych operacji militarnych, które koncentrują się na siłach zbrojnych i infrastrukturze wojskowej, ataki hybrydowe na IK uderzają w systemy (np. sieci elektroenergetycznej), od których zależy życie codzienne obywateli i funkcjonowanie gospodarki. W przypadku skoordynowanego ataku na kilka sektorów, np. energetykę, transport i telekomunikację, przeprowadzonego bez użycia konwencjonalnej siły militarnej skutki mogą być porównywalne do działań wojennych.

Najlepiej obrazuje to blackout, do którego doszło w Nowym Jorku 13 lipca 1977 r. W ciągu kilku minut całe miasto zostało pozbawione prądu, co wywołało chaos i falę przestępczości, jakiej nie widziano tam od lat. Do stopniowego przeciążenia systemu elektroenergetycznego doprowadziły uderzenia piorunów w linie przesyłowe. Około godz. 21.27 pierwsze wyładowania atmosferyczne uszkodziły linię przesyłową w hrabstwie Westchester, co spowodowało automatyczne przeniesienie obciążenia na inne części sieci.

[1] G.M. Jackson, *Warden's five-ring system theory: legitimate wartime military targeting or an increased potential to violate the law and norms of expected behavior?,* Alabama 2000, https://apps.dtic.mil/sti/pdfs/ADA425331.pdf [dostęp: 20.02.2025].

[2] F.G. Hoffman, *Conflict in the 21'st Century: The Rise of Hybrid Wars*, Virginia 2007, https://www.comw.org/qdr/fulltext/0712hoffman.pdf, s. 14 [dostęp: 20.02.2025].

Kolejne uderzenie o 21.29 doprowadziło do dalszych zakłóceń, a trzecie o 21.34 unieruchomiło najważniejsze stacje przesyłowe i wywołało efekt domina.

W odróżnieniu od wcześniejszego blackoutu z 1965 r., który przebiegł stosunkowo spokojnie, ten incydent stał się katalizatorem masowych zamieszek, rabunków i aktów przemocy. W ciągu jednej nocy zgłoszono 1809 aktów grabieży i podpaleń, wybuchło 1037 pożarów, aresztowano 2931 osób[3]. Blackout pogłębił napięcia społeczne oraz kryzys gospodarczy, z jakim zmagał się ówczesny 12-milionowy Nowy Jork. Ta amerykańska metropolia w latach 70. XX w. przeżywała recesję związaną z deindustrializacją, rosnącym bezrobociem i wysokim poziomem przestępczości. Deficyt budżetowy miasta, który sięgał miliardów dolarów, doprowadził do cięć w administracji publicznej, w tym ograniczenia liczby policjantów i strażaków. Policja nie była w stanie powstrzymać zamieszek. W wielu miejscach funkcjonariusze unikali konfrontacji i pozwali ludziom na swobodne grabieże. Złodzieje wynosili towary ze sklepów, a nawet wyprowadzali samochody z salonów. Transport publiczny został sparaliżowany, a mieszkańcy, którzy byli poza domem, musieli wracać pieszo przez pogrążone w chaosie ulice. Prąd zaczęto przywracać stopniowo rankiem 14 lipca, a pełne zasilanie przywrócono w całym mieście ok. godz. 10.39. Skutki wydarzenia były odczuwane przez następne miesiące. Wiele małych biznesów nie podniosło się po rabunkach, co jeszcze bardziej pogłębiło kryzys gospodarczy. Wzrosły poczucie zagrożenia i nieufność wobec władz, które nie zdołały zapobiec eskalacji przemocy. Straty materialne oszacowano na ok. 300 mln dolarów[4], co w przeliczeniu na dzisiejsze pieniądze stanowi równowartość ok. 1,5 mld dolarów.

Infrastruktura niezbędna do utrzymania funkcjonowania współczesnego państwa i społeczeństwa składa się z powiązanych ze sobą elementów lub samodzielnych systemów. Stanowi to dodatkową trudność przy ich zabezpieczaniu, ponieważ zarówno w ramach ich elementów składowych, jak i połączeń między nimi wykorzystuje się różne technologie. Mogą to być technologie cyfrowe, oddziaływania i przepływy fizyczne, a także automatyzacja procesów. Wiele sektorów, takich jak sieci elektroenergetyczne czy systemy transportowe, opiera się na skomplikowanych zależnościach. Awaria jednego elementu może wywołać efekt domina, np. atak na system sterowania ruchem kolejowym czy lotniczym może sparaliżować transport krajowy.

[3] *Impact Assessment of the 1977 New York City Blackout*, lipiec 1978, https://www.ferc.gov/sites/default/files/2020-05/impact-77.pdf, s. 23 [dostęp: 23.03.2025].

[4] Tamże, s. 11.

Ponadto podstawą wielu systemów są technologie projektowane przed rozpowszechnieniem internetu, co czyni je podatnymi na ataki hakerskie.

Skala i charakter ataków hybrydowych nie pozwalają na uznanie zdarzenia za konflikt zbrojny, tzn. są to działania poniżej progu wojny. Takie ataki, zwłaszcza prowadzone w sferze cyfrowej, są trudne do atrybucji. Sprawcy często wykorzystują sieci pośredników, botnety lub fałszywe ślady, co niemal uniemożliwia wskazanie atakującego. W przypadku aktów fizycznego sabotażu, takich jak uszkodzenie kabli podmorskich czy rurociągów, sprawcy mogą upozorować niewyjaśnioną awarię czy działania grup terrorystycznych. To sprawia, że zaatakowane państwo ma ograniczone możliwości reakcji. Prześladowca prowadzi działania destabilizujące i unika oficjalnej konfrontacji zbrojnej.

Działania hybrydowe (np. atak ransomware lub sabotaż przemysłowy) charakteryzuje relatywnie niski koszt ataku przy wysokich kosztach odbudowy dla zaatakowanego podmiotu. Przeprowadzenie skutecznego cyberataku na sieć elektroenergetyczną, system bankowy czy transportowy wymaga znacznie mniejszych nakładów finansowych niż klasyczne operacje wojskowe. Przykładem jest atak na Colonial Pipeline w 2021 r., o czym szerzej w dalszej części artykułu.

Jednym z powodów dużej skuteczności ataków hybrydowych jest ich multiwektorowość, czyli możliwość łączenia różnych form ataku. Przykładowy scenariusz ataku na IK może obejmować jednocześnie:

- cyberatak na sieci przesyłowe, który wywołuje przerwy w dostawie prądu;
- sabotaż, np. podłożenie ładunku wybuchowego na ważnym węźle infrastrukturalnym;
- kampanię dezinformacyjną, w której sugeruje się, że awaria to wynik korupcji lub nieudolności rządu;
- spekulacje finansowe, które uderzają w wartość waluty krajowej i destabilizują gospodarkę.

Tego typu działania, jeśli są dobrze skoordynowane, mogą wywołać chaos o skali porównywalnej do konfliktu zbrojnego. Ataki na IK często mają na celu nie tylko fizyczne uszkodzenie infrastruktury, lecz także wywołanie efektu psychologicznego. W społeczeństwach, które tracą dostęp do podstawowych usług, rośnie niezadowolenie, pojawiają się teorie spiskowe i spada zaufanie do rządu oraz instytucji publicznych. W sytuacji kryzysowej mogą się pojawić zamieszki, masowe protesty, a w konsekwencji – destabilizacja polityczna.

Niezależnie od wspomnianej destabilizacji atak na IK może być elementem wojny gospodarczej i narzędziem politycznego szantażu. Współczesna rywalizacja między państwami coraz częściej przenosi się na poziom infrastrukturalny. Blokowanie głównych tras transportowych, niszczenie rurociągów czy zakłócanie pracy systemów bankowych to działania mogące wymusić ustępstwa polityczne. Przykładem jest sabotaż gazociągów Nord Stream w 2022 r., który miał wymiar zarówno ekonomiczny, jak i polityczny, a jednocześnie wpłynął na bezpieczeństwo energetyczne Europy.

Dodatkowym problemem związanym z ochroną IK jest fakt, że często obejmuje ona zarówno elementy publiczne, jak i prywatne. W wielu krajach sieci energetyczne są zarządzane przez firmy prywatne, które realizują cele przede wszystkim biznesowe, a zapewnienie społeczeństwu dostępu do usługi nie jest dla nich priorytetem.

Cyberataki to jeden z głównych wektorów ataków hybrydowych na IK. Narzędzia takie jak ransomware, malware czy ataki DDoS mogą być używane do destabilizacji sieci elektroenergetycznych, systemów finansowych czy łańcuchów logistycznych. Cyberprzestrzeń umożliwia przeprowadzenie ataku z dowolnego miejsca na świecie, co utrudnia identyfikację sprawców. Tak było w 2015 r. w przypadku cyberataku na ukraińską sieć elektroenergetyczną. Hakerzy wykorzystali wówczas złośliwe oprogramowanie Black Energy do przejęcia kontroli nad systemami sterowania i wyłączenia podstacji energetycznych, co spowodowało masowe przerwy w dostawie prądu. Podejrzewano, że ataku dokonały rosyjskie grupy hakerskie, ale nie znaleziono na to dowodów[5].

Ataki, takie jak sabotaż gazociągów, podmorskich kabli telekomunikacyjnych czy istotnych węzłów infrastruktury transportowej, mogą być przedstawiane jako wypadek lub awaria techniczna. Tak było w przypadku wspomnianego uszkodzenia gazociągów Nord Stream. Wiele państw uznało to zdarzenie za sabotaż, ale brakowało jednoznacznych dowodów pozwalających na wskazanie zleceniodawcy[6]. Podobnie było w 2019 r. w Arabii Saudyjskiej, gdzie przeprowadzono atak dronowy na instalacje naftowe

[5] K. Gapiński, *Blackout w zachodniej Ukrainie – cyberatak o wymiarze międzynarodowym*, Fundacja im. Kazimierza Pułaskiego, 20.01.2016, https://pulaski.pl/komentarz-blackout-w-zachodniej-ukrainie-cyber-atak-o-wymiarze-miedzynarodowym/ [dostęp: 23.03.2025].

[6] Zob. np. S. Kardaś, A. Łoskot-Strachota, *Dywersja na gazociągach Nord Stream 1 i Nord Stream 2*, Ośrodek Studiów Wschodnich, 29.09.2022, https://www.osw.waw.pl/pl/publikacje/analizy/2022-09-29/dywersja-na-gazociagach-nord-stream-1-i-nord-stream-2 [dostęp: 23.03.2025].

Aramco. Doprowadziło to do czasowego wstrzymania produkcji ropy naftowej, co wpłynęło na światowe ceny surowca[7]. Choć do ataku przyznała się grupa jemeńskich rebeliantów Huti, to w wielu analizach sugerowano, że operacja mogła być wspierana przez Iran[8].

Ataki na IK często są łączone z działaniami dezinformacyjnymi. Po cyberataku na systemy bankowe lub infrastrukturę energetyczną mogą się pojawiać w sieci zmanipulowane informacje, że władze nie radzą sobie z sytuacją lub że awaria była wynikiem wewnętrznych problemów, np. korupcji czy słabości rządu. Tego typu kampanie mają na celu osłabienie zaufania społeczeństwa do instytucji państwowych i wywołanie paniki.

Cybernetyczny atak na IK trudno jednoznacznie sklasyfikować jako akt wojny, co z perspektywy sprawcy jest największą zaletą. O ile bezpośredni atak militarny na IK mógłby spotkać się z reakcją zbrojną, o tyle atak przeprowadzony przez sieć internetową czy sabotaż mogą zostać uznane za działania o niejasnym charakterze. Jeśli nie można jednoznacznie wskazać sprawcy, trudno podjąć działania odwetowe i zaangażować w nie sojuszników. Nawet jeśli istnieją podejrzenia w kwestii odpowiedzialności określonego kraju, to wątpliwości co do dowodów mogą sprawić, że możliwości dyplomatycznej lub militarnej odpowiedzi będą ograniczone. Ataki na IK są skuteczne nie tylko dlatego, że powodują ogromne straty, lecz także dlatego, że sprawcy mogą działać anonimowo i bezkarnie.

Teoretyczne ramy odniesienia

Podstawy teorii 5 pierścieni Wardena można wywodzić z dzieła Carla von Clausewitza pt. *O wojnie*[9]. Clausewitz zauważa, że aby skutecznie pokonać przeciwnika, państwo powinno skierować wszystkie swoje wysiłki

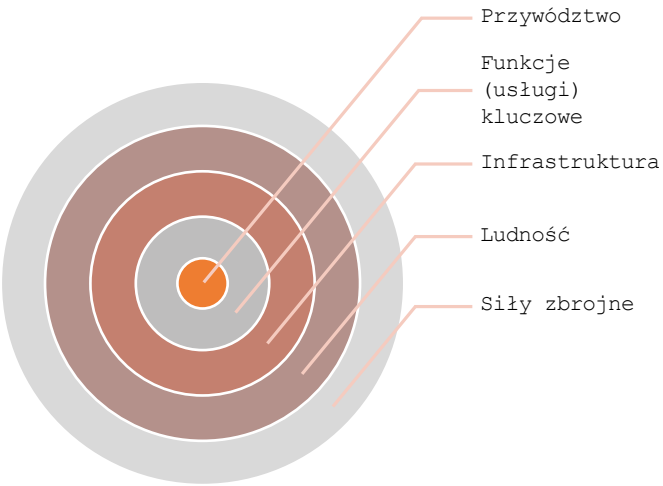
[7] A. Polus, *Atak na rafinerię w Arabii Saudyjskiej i jego konsekwencje dla Afryki*, Polskie Centrum Studiów Afrykanistycznych, 18.09.2019, https://pcsa.org.pl/atak-na-rafinerie-w-arabii-saudyjskiej-i-konsekwencje-dla-afryki/ [dostęp: 23.03.2025].

[8] Zob. np. G. Psujek, *Tajemnica ataku na saudyjską rafinerię*, Rzeczpospolita, 22.09.2019, https://radar.rp.pl/przemysl-obronny/art17499861-tajemnica-ataku-na-saudyjska-rafinerie [dostęp: 23.03.2025]; R. Muczyński, *Atak na saudyjskie rafinerie*, Milmag, 16.09.2019, https://milmag.pl/atak-na-saudyjskie-rafinerie/ [dostęp: 23.03.2025]; *CNN: Według ekspertów atak na Aramco nastąpił z Iranu*, Interia Wydarzenia, 18.09.2019, https://wydarzenia.interia.pl/zagranica/news-cnn-wedlug-ekspertow-atak-na-aramco-nastapil-z-iranu,nId,3209902 [dostęp: 23.03.2025].

[9] C. von Clausewitz, *O wojnie*, Warszawa 2022.

przeciwko tzw. punktom ciężkości, od których zależy istnienie wrogiego państwa. John Ashley Warden III[10] rozwinął tę zasadę, tworząc koncepcję ukierunkowaną na wybór celów w czasie wojny. Teoria 5 pierścieni Wardena służy do identyfikacji i hierarchizacji celów wojennych. Zakłada ona, że państwo można przedstawić jako system składający się z 5 koncentrycznych pierścieni (kręgów), z których każdy reprezentuje inny poziom strategicznego znaczenia. Są to przedstawione na rysunku 1:

1) przywództwo (władze państwowe i wojskowe),
2) zasoby systemowe niezbędne do funkcjonowania państwa i prowadzenia wojny,
3) infrastruktura, która łączy wszystkie elementy systemu,
4) ludność (cywile),
5) siły zbrojne (wojsko i sprzęt wojskowy).



Rysunek 1. Teoria 5 pierścieni Wardena.

Źródło: opracowanie własne na podstawie: G.M. Jackson, *Warden's five-ring system theory: legitimate wartime military targeting or an increased potential to violate the law and norms of expected behavior?*, Alabama 2000, https://apps.dtic.mil/sti/pdfs/ADA425331.pdf, s. 4 [dostęp: 20.02.2025].

[10] John Ashley Warden III – urodzony w 1943 r. amerykański strateg wojskowy z United States Air Force. Podczas wojny w Zatoce Perskiej (1990–1991) stworzył teorię 5 pierścieni, w której określił środki ciężkości (najbardziej wrażliwe elementy struktury państwa) i jednocześnie wskazał lotnictwo jako jedyną formację, która może zaatakować wnętrze każdego pierścienia bez przebijania się przez pozostałe.

Zaatakowanie wewnętrznych kręgów (przywództwo, niezbędne zasoby systemowe) wywołuje szybki paraliż i zakończenie konfliktu. Atakowanie zewnętrznych kręgów (ludność, siły zbrojne) jest mniej efektywne i może przedłużać wojnę.

Jeśli nie uda się skutecznie zaatakować przywództwa, Warden wskazuje następny cel, którym są zasoby systemowe (funkcje, usługi) niezbędne dla przeciwnika, m.in.: zaopatrzenie w energię elektryczną, ropę naftową, żywność i finanse. Ich zniszczenie może pozbawić państwo zdolności do prowadzenia działań wojennych, ale jednocześnie może zagrozić przetrwaniu ludności cywilnej. Według Wardena IK to elementy, takie jak drogi, lotniska, fabryki i inne, które umożliwiają funkcjonowanie państwa jako całości.

Teoria Wardena służyła ustalaniu priorytetów dla lotnictwa wykorzystywanego we współczesnej wojnie. Jednak płynące z niej wnioski mają szersze znaczenie. Kolejne poziomy (pierścienie) wskazują na ważność danego elementu dla funkcjonowania państwa. Warto zwrócić uwagę, że według tej teorii wojna XXI w. polega na tym, że siły zbrojne są atakowane na końcu lub wcale. Cele polityczne mają być osiągane przez eliminację przywództwa, blokadę najważniejszych funkcji państwa i zniszczenie infrastruktury, która tym funkcjom służy. Nadzwyczaj dobrze koresponduje to z rozważaniami o wojnie hybrydowej.

Wykorzystanie infrastruktury krytycznej w konfliktach hybrydowych

Realizacja celów politycznych bez udziału sił zbrojnych

Szczególnym przypadkiem osiągania celów politycznych przez oddziaływanie na IK była operacja Allied Force, czyli kampania bombardowań przeprowadzona przez wojska Sojuszu Północnoatlantyckiego przeciwko Jugosławii (Serbii i Czarnogórze) podczas wojny w Kosowie w 1999 r. W ten sposób chciano zmusić reżim Slobodana Miloševicia do zakończenia czystek etnicznych w Kosowie.

Bombardowania koncentrowały się początkowo na obiektach wojskowych, ale później rozszerzono je na ważną dla funkcjonowania państwa infrastrukturę, taką jak mosty (np. na Dunaju w Nowym Sadzie, którego zniszczenie miało sparaliżować transport), drogi i linie kolejowe (w tym atak na pociąg pasażerski na moście w Grdelicy), infrastrukturę lotniczą (lotnisko w Podgoricy), stacje telewizyjne i radiowe (np. atak na siedzibę

serbskiej telewizji RTS w Belgradzie, w wyniku którego zginęło 16 cywilów), zakłady przemysłowe (rafinerie, fabryki) oraz energetyczne (np. elektrownie, których bombardowanie doprowadziło do masowych przerw w dostawie prądu). Serbia poniosła ogromne straty gospodarcze, koszty odbudowy po nalotach szacowano na ok. 30–100 mld dolarów[11]. Zniszczenie obiektów cywilnych spotkało się z międzynarodową krytyką, ponieważ spowodowało ogromne problemy dla ludności. Operacja Allied Force wywołała także kontrowersje prawne, ponieważ zgodnie z prawem międzynarodowym (m.in. Protokołem I do Konwencji genewskich z 12 sierpnia 1949 r. dotyczącym ochrony ofiar międzynarodowych konfliktów zbrojnych[12]) atakowanie obiektów niezbędnych do przetrwania ludności cywilnej jest zabronione. Dowództwo NATO argumentowało jednak, że ta infrastruktura miała znaczenie również militarne, np. mosty wykorzystywano do transportu wojskowego. Allied Force była pierwszą w historii interwencją NATO bez mandatu Organizacji Narodów Zjednoczonych, co do dziś pozostaje przedmiotem debat prawnych i politycznych. Niezależnie od tych kontrowersji cele polityczne zostały osiągnięte bez wprowadzania żołnierzy na teren wrogiego państwa.

Oddziaływanie na społeczeństwo

Przytoczona na początku artykułu definicja wojny hybrydowej Hoffmana podkreśla oddziaływanie na społeczeństwo jako najważniejszy element strategii przeciwnika. Podobne podejście można znaleźć w koncepcji wojny nielinearnej Walerija Gierasimowa[13], gdzie głównymi narzędziami są manipulacja informacyjna, dezinformacja i działania psychologiczne,

[11] N. Stawarz, *„Nielegalne, ale moralne"? Operacja „Allied Force": przyczyny i konsekwencje*, Histmag.org, 24.03.2019, https://histmag.org/Nielegalne-ale-moralne-Operacja-Allied-Force-przyczyny-i-konsekwencje-18428? [dostęp: 23.03.2025]; R. Górski, *Specjalna operacja wojskowa NATO: bombardowanie Jugosławii*, Instytut Spraw Obywatelskich, 24.03.2023, https://instytutsprawobywatelskich.pl/specjalna-operacja-wojskowa-nato-bombardowanie-jugoslawii/ [dostęp: 23.03.2025].

[12] *Protokoły dodatkowe do Konwencji genewskich z 12 sierpnia 1949 r., dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych (Protokół I) oraz dotyczący ochrony ofiar niemiędzynarodowych konfliktów zbrojnych (Protokół II), sporządzone w Genewie dnia 8 czerwca 1977 r.*

[13] M.K. McKew, *The Gerasimov Doctrine. It's Russia's new chaos theory of political warfare. And it's probably being used on you*, Politico, wrzesień/październik 2017, https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/ [dostęp: 23.03.2025].

które mają doprowadzić do destabilizacji społecznej i zmiany decyzji politycznych rządu pod presją własnych obywateli.

Szerzenie dezinformacji, propagandy oraz manipulowanie informacjami prowadzi do erozji zaufania publicznego, podważania autorytetu instytucji państwowych i międzynarodowych, a w konsekwencji – fundamentów demokracji. Osłabia to również pozycję państwa na arenie międzynarodowej. Aby wywołać niepokoje społeczne, protesty oraz podziały wewnętrzne, atakujący wykorzystują różne środki, takie jak media społecznościowe, fałszywe wiadomości czy cyberataki. Wysokie ceny energii elektrycznej, strach przed technologią 5G czy elektrownią jądrową to przykłady zagadnień, wokół których buduje się narrację dezinformacyjną. W tych działaniach szczególną rolę odgrywa IK.

Przed synchronizacją sieci energetycznych krajów bałtyckich z europejskim systemem elektroenergetycznym, do której doszło w lutym 2025 r., odnotowano nasilenie kampanii dezinformacyjnych na Litwie, Łotwie i w Estonii. Działania te były szczególnie intensywne w okresie poprzedzającym odłączenie od rosyjskiego systemu BRELL i przyłączenie do europejskiej sieci. Główne wątki dezinformacyjne koncentrowały się na kilku zagadnieniach. Po pierwsze – groźba przerw w dostawach prądu. Rozpowszechniano informacje sugerujące, że synchronizacja z europejskim systemem doprowadzi do długotrwałych blackoutów. W Estonii takie doniesienia spowodowały wzrost sprzedaży generatorów prądu, gdyż mieszkańcy obawiali się nawet trzydniowych przerw w dostawie energii[14]. Po drugie – wzrost cen energii. Pojawiały się pogłoski, że przyłączenie do europejskiej sieci wywoła znaczny wzrost cen prądu dla konsumentów, a co za tym idzie – wzrost cen podstawowych produktów i w efekcie ubożenie społeczeństwa. Litewski minister do spraw energii Žygimantas Vaičiūnas ostrzegał przed takimi dezinformacjami oraz zapewniał o stabilności systemu i braku podstaw do obaw o wzrost cen[15]. Po trzecie – niewydolność nowego systemu. Propagowano tezy o rzekomej zawodności europejskiego

[14] *Rosyjski atak dezinformacją ws. energetyki. Estończycy wykupują generatory, służby w stanie gotowości*, Polskie Radio 24, 6.02.2025, https://polskieradio24.pl/artykul/3480519,rosyjski-atak-dezinformacja-ws-energetyki-estonczycy-wykupuja-generatory-sluzby-w-stanie-gotowosci [dostęp: 20.02.2025].

[15] *Minister ostrzega mieszkańców przed możliwą dezinformacją*, Made in Vilnius, 4.02.2025, https://madeinvilnius.lt/pl/Aktualno%C5%9Bci/Lietuvos-naujienos/Minister-ostrzega-mieszka%C5%84c%C3%B3w-przed-mo%C5%BCliw%C4%85-dezinformacj%C4%85/ [dostęp: 20.02.2025].

systemu elektroenergetycznego i sugerowano, że kraje bałtyckie mogą doświadczyć problemów technicznych po odłączeniu od rosyjskiej sieci[16]. Ta kampania dezinformacyjna nasiliła się, zwłaszcza ze strony rosyjskich mediów, po synchronizacji sieci. Badania przeprowadzone przez litewską firmę Mediaskopas wykazały, że po odłączeniu się krajów bałtyckich od poradzieckiego systemu i przyłączeniu do europejskiego systemu przesyłowego CESA liczba artykułów na ten temat w rosyjskich mediach wzrosła z 3650 do ponad 8000. Przedstawiano w nich apokaliptyczne scenariusze, w których sugerowano, że kraje bałtyckie stoją w obliczu kryzysu energetycznego z powodu porzucenia współpracy z Rosją[17]. Władze oraz eksperci ds. energetyki tych krajów regularnie dementują te informacje. Zapewniają o stabilności i bezpieczeństwie nowego systemu. Aby podważyć te zapewnienia, przecięto jeden z podmorskich kabli elektroenergetycznych. Chodzi o kabel EstLink 2 łączący Finlandię z Estonią, o przepustowości 650 MW i długości 170 km, w tym 145 km pod dnem Zatoki Fińskiej. Dnia 25 grudnia 2024 r. ok. południa doszło do przerwania tego połączenia, będącego ważnym elementem infrastruktury energetycznej między krajami bałtyckimi. Operator sieci, firma Fingrid, poinformował o zakłóceniach w przesyle prądu i wszczął dochodzenie w celu ustalenia przyczyn awarii. Fińskie władze zatrzymały podejrzewany o spowodowanie uszkodzenia tankowiec Eagle S – statek pływający pod banderą Wysp Cooka, który przewoził benzynę bezołowiową z rosyjskich portów. Domniemano, że należał on do rosyjskiej tzw. floty cieni. Wstępne ustalenia sugerowały, że przecięcie kabla mogło być spowodowane przez kotwicę statku[18]. Skomplikowana i kosztowna naprawa EstLink 2 potrwa prawdopodobnie do 1 sierpnia 2025 r. i pochłonie dziesiątki milionów euro. Mimo awarii dostawy energii elektrycznej dla fińskich odbiorców pozostały niezakłócone. Jednak brak tego połączenia ograniczył eksport energii z Finlandii i w efekcie średnia cena energii w Estonii wzrosła od stycznia do lutego 2025 r. niemal

[16] *Przed synchronizacją z Europą służby ostrzegają przed dezinformacją*, TVP Wilno, 3.02.2025, https://wilno.tvp.pl/84820950/przed-synchronizacja-z-europa-sluzby-ostrzegaja-przed-dezinformacja [dostęp: 20.02.2025].

[17] *Po synchronizacji sieci energetycznych krajów bałtyckich z Europą zaktywizowała się propaganda Kremla*, Polska Agencja Prasowa, 20.02.2025, https://www.pap.pl/aktualnosci/po-synchronizacji-sieci-energetycznych-krajow-baltyckich-z-europa-zaktywizowala-sie [dostęp: 20.02.2025].

[18] *Awaria kabla EstLink 2. Rosyjski tankowiec podejrzany o akt sabotażu*, PolskieRadio.pl, 26.12.2024, https://www.polskieradio.pl/399/7977/artykul/3463666%2Cawaria-ka%20bla-estlink-2-rosyjski-tankowiec-podejrzany-o-akt-sabotazu? [dostęp: 20.02.2025].

dwukrotnie i wyniosła 184 EUR/MWh. Dla porównania, w lutym poprzedniego roku ta cena wynosiła 75,5 EUR/MWh[19]. Po uszkodzeniu kabla średnia hurtowa cena energii elektrycznej na Litwie wzrosła w ciągu tygodnia o 41% z 56 EUR/MWh do 79 EUR/MWh[20]. Incydent związany z uszkodzeniem EstLink 2 wywołał niepokój wśród mieszkańców krajów bałtyckich dotyczący stabilności dostaw energii oraz potencjalnych dalszych wzrostów cen. Cele atakującego zostały osiągnięte.

Warto zauważyć, że podobne kampanie dezinformacyjne były obserwowane w innych krajach UE. Próbowano w nich obarczać UE odpowiedzialnością za podwyżki cen energii.

Oddziaływanie na rząd

Dnia 7 maja 2021 r. doszło do jednego z najpoważniejszych cyberataków na IK w Stanach Zjednoczonych. Celem był Colonial Pipeline[21], największy system rurociągowy na Wschodnim Wybrzeżu USA, który transportuje ok. 45% dostaw paliwa w tym regionie. Hakerzy wykorzystali oprogramowanie ransomware, zaszyfrowali dane firmowe i zażądali okupu. W wyniku ataku rurociąg wstrzymał działalność, co doprowadziło do poważnych zakłóceń w dostawach paliwa. Władze zareagowały natychmiast. Administracja prezydenta USA Joe Bidena ogłosiła stan wyjątkowy, aby umożliwić transport paliwa alternatywnymi środkami. Właściciel Colonial Pipeline, który chciał jak najszybciej przywrócić funkcjonowanie systemu, zapłacił hakerom okup w wysokości 4,4 mln dolarów w bitcoinach[22]. Przywrócenie pełnej działalności rurociągu zajęło jednak kilka dni. W tym czasie na Wschodnim Wybrzeżu USA zaczęło brakować paliwa. To wywołało

[19] *Jak uszkodzenie Estlink 2 wpływa na ceny energii w Estonii*, Czas Wschodni, 14.02.2025, https://czaswschodni.pl/art/wiadomosci/jak-uszkodzenie-estlink-2-wplywa-na-ceny-energii-w-estonii_116f1090-c456-4bb7-abc1-c340f6da6cf5 [dostęp: 20.02.2025].

[20] *Uszkodzenie kabla EstLink 2 podniosło ceny energii w krajach bałtyckich*, BalticWind.EU, 3.01.2025, https://balticwind.eu/pl/uszkodzenie-kabla-estlink-2-podnioslo-ceny-energii-w-krajach-baltyckich/ [dostęp: 20.02.2025].

[21] M. Perzyński, *Raport: O Colonial Pipline i zimnej wojnie w energetyce*, Biznesalert, 15.05.2021, https://biznesalert.pl/raport-colonial-pipeline-cyberatak-usa-rosja-energetyka/ [dostęp: 23.03.2025].

[22] *Prezes Colonial Pipeline potwierdza: zapłaciliśmy okup hakerom*, CyberDefence24, 20.05.2021, https://cyberdefence24.pl/biznes-i-finanse/prezes-colonial-pipeline-potwierdza-zaplacilismy-okup-hakerom [dostęp: 23.03.2025]; W. Urbanek, *Colonial Pipeline: niepożądana sława*, CRN, 24.06.2021, https://crn.pl/artykuly/colonial-pipeline-niepozadana-slawa/ [dostęp: 23.03.2025].

panikę wśród konsumentów, którzy masowo wykupywali benzynę i w ten sposób kryzys się pogłębiał. W niektórych stanach, np. w Karolinie Północnej, ponad 70% stacji benzynowych zgłaszało problemy z zaopatrzeniem. Za atak odpowiadała grupa hakerska DarkSide, działająca z Rosji. Atak na Colonial Pipeline ujawnił podatność amerykańskiej IK na cyberataki, co skłoniło administrację Bidena do zaostrzenia regulacji w zakresie cyberbezpieczeństwa dla sektora energetycznego[23]. Wprowadzono nowe wymogi dla operatorów IK, zobowiązujące ich do podjęcia dodatkowych środków ochrony przed atakami ransomware. Incydent nasilił napięcia między Waszyngtonem a Moskwą. Prezydent Biden zwrócił uwagę, że Kreml ponosi odpowiedzialność za egzekwowanie kontroli nad grupami cyberprzestępczymi działającymi w granicach Rosji, a DarkSide działało z terytorium tego kraju. Warto zauważyć, że wiosną 2021 r. USA i Niemcy prowadziły intensywne rozmowy dotyczące ukończenia gazociągu Nord Stream 2, który miał dostarczać rosyjski gaz bezpośrednio do Niemiec, z ominięciem Ukrainy i Polski. Administracja Bidena wyrażała obawy, że projekt zwiększy zależność Europy od rosyjskiego gazu i osłabi bezpieczeństwo energetyczne regionu. Mimo sprzeciwu wobec Nord Stream 2 amerykański rząd nie nałożył bezpośrednich sankcji na Nord Stream 2 AG – główną spółkę odpowiedzialną za budowę gazociągu – oraz jej prezesa Matthiasa Warniga[24]. Zamiast tego USA skupiły się na wypracowaniu porozumienia z Niemcami, które uwzględniałoby obawy dotyczące bezpieczeństwa energetycznego Europy Środkowo-Wschodniej. W lipcu 2021 r. USA i Niemcy zakończyły negocjacje. Berlin zobowiązał się do podjęcia działań w przypadku, gdyby Rosja próbowała użyć energii jako broni przeciwko Ukrainie lub innym krajom regionu, a także do wykorzystania wszelkich dostępnych środków nacisku w celu przedłużenia o 10 lat umowy tranzytowej między Rosją a Ukrainą, która wygasała w 2024 r. Ponadto Niemcy zgodziły się na utworzenie funduszu o wartości co najmniej 175 mln dolarów na wspieranie transformacji energetycznej i poprawę bezpieczeństwa energetycznego

[23] *Statement from CISA Acting Director Wales on Executive Order to Improve the Nation's Cybersecurity and Protect Federal Networks*, America's Cyber Defense Agency, 13.05.2021, https://www.cisa.gov/news-events/news/statement-cisa-acting-director-wales-executive-order-improve-nations-cybersecurity-and-protect [dostęp: 20.02.2025].

[24] W. Jakóbik, *USA mogą na dniach zadać nowy cios Nord Stream 2, ale unikają deklaracji*, Biznes Alert, 14.05.2021, https://biznesalert.pl/nord-stream-2-sankcje-usa-poszerzone-energetyka-gaz/ [dostęp: 20.02.2025].

Ukrainy[25]. Nie znaleziono bezpośrednich powiązań grupy hakerskiej z rosyjskimi służbami. Można zaryzykować jednak tezę, że cyberatak na ważne ogniwo amerykańskiego systemu energetycznego miał uzmysłowić administracji Joe Bidena, że działania na szkodę Federacji Rosyjskiej mogą się spotkać ze zdecydowaną, choć niebezpośrednią reakcją.

Postrzeganie działań hybrydowych w horyzoncie czasowym

Horyzont czasowy jest ważnym zagadnieniem, które należy brać pod uwagę przy rozważaniach na temat wykorzystywania IK w wojnie hybrydowej. Pierwszy jego wymiar to efekt zaskoczenia, czyli znalezienie takiej podatności lub wymyślenie takiego scenariusza ataku, który nie był dotąd rozpatrywany. Jest to atak, który nie spowoduje natychmiastowej reakcji, ponieważ nie istnieją odpowiednie ramy prawne, zarówno w kontekście procedury reagowania, wyznaczonego organu odpowiedzialnego za bezpieczeństwo IK, jak i sankcji karnej. Drugi wymiar dotyczy tego, że ograniczona możliwość przeprowadzenia analizy ryzyka pod kątem podatności na atak hybrydowy znacznie utrudnia zapewnienie ochrony IK. Trudno przewidzieć, czy dany obiekt będzie potencjalnym celem ataku hybrydowego. Jego typowe parametry (rodzaj produkcji, współzależności, potencjalne straty, liczba ludności, na którą oddziałuje itp.) i scenariusze ataku mogą mieć odmienne znaczenie dla użytkownika obiektu i dla atakującego. Na przykład dużym zainteresowaniem grup hakerskich cieszą się lokalne obiekty wodno-kanalizacyjne, które z punktu widzenia państwa mają niewielkie znaczenie[26]. Atak na tego rodzaju miejsce, nawet jeśli będzie dotkliwy dla społeczności lokalnej, nie wywoła kryzysu w kraju, chyba że agresor zdecyduje się na jednoczesny atak na więcej słabo zabezpieczonych instalacji. Efekt skali może wtedy spowodować reakcję mediów podobną do tej, jaka następuje po ataku na jedną dużą instalację. Trzeci wymiar horyzontu

[25] S. Lewis, A. Shalal, *U.S., Germany strike Nord Stream 2 pipeline deal to push back on Russian 'aggression'*, Reuters, 22.07.2021, https://www.reuters.com/business/energy/us-germany-deal-nord-stream-2-pipeline-draws-ire-lawmakers-both-countries-2021-07-21/ [dostęp: 20.02.2025].

[26] Zob. np. *Doniesienia o rosyjskim cyberataku. Pojawił się polski wątek*, Wirtualna Polska, 17.04.2024, https://wiadomosci.wp.pl/rosyjski-cyberatak-na-polska-infrastrukture-ofiara-oczyszczalnia-sciekow-7017937180834752a [dostęp: 20.02.2025]; *Atak hakerski na oczyszczalnię ścieków*, iSokolka.eu, 8.10.2024, https://isokolka.eu/kuznica/59444-atak-hakerski-na-oczyszczalnie-sciekow [dostęp: 20.02.2025].

czasowego to pozyskiwanie informacji, które mogą mieć militarne czy dezinformacyjne znaczenie w długiej perspektywie czasowej. Operacje hybrydowe niejednokrotnie są planowane na lata. Obiekt, który dziś nie ma strategicznego znaczenia, może w przyszłości pełnić ważną funkcję, np. jako część jakiegoś sytemu.

Budowanie odporności infrastruktury krytycznej na przykładzie dyrektyw: CER i NIS 2

Dyrektywa CER ma doprowadzić do osiągnięcia takiego poziomu odporności IK, aby zapobiegać skutkom zakłócenia usług kluczowych realizowanych za jej pomocą. Zgodnie z założeniami tej dyrektywy państwa członkowskie są zobowiązane do ustalenia listy tych usług oraz wskazania podmiotów krytycznych odpowiedzialnych za ich świadczenie. Każdy z tych podmiotów, aby przeciwdziałać skutkom zakłóceń, musi spełniać wymagania dotyczące odporności (art. 6 ust. 1 i 2 dyrektywy CER). Krajowe strategie odporności podmiotów krytycznych muszą obejmować identyfikację zagrożeń, ocenę ryzyka oraz wypracowanie środków zapobiegawczych, w tym ochronę przed zagrożeniami hybrydowymi (art. 5 ust. 1). Ponadto w dyrektywie CER zidentyfikowano wyzwania, które wynikają z coraz bardziej złożonych łańcuchów dostaw między podmiotami. Dlatego muszą one oceniać ryzyko związane z zależnościami w łańcuchu dostaw oraz stosować odpowiednie środki w celu zapewnienia ciągłości działania. W związku z tym w dyrektywie CER wskazano konieczność ustalenia alternatywnych dostawców i planów awaryjnych (art. 12 ust. 2). Podmioty są zobowiązane do utrzymywania zdolności operacyjnych w sytuacjach kryzysowych, z uwzględnieniem współzależności między różnymi podmiotami i sektorem krytycznym (art. 11 ust. 2). Dyrektywa wymaga analizy ryzyka i planów awaryjnych (art. 12 ust. 1), ale brakuje w niej wytycznych do przewidywania działań adwersarza oraz skutecznego zarządzania ryzykiem w złożonych strukturach organizacyjnych. Dyrektywa nakłada obowiązek ciągłego monitorowania i oceny zagrożeń, ale nie przewiduje mechanizmów, które mogłyby uwzględniać nieoczywiste cele ataków hybrydowych. Nie można, jak dowiedziono, przewidzieć, co będzie ważne dla przeciwnika. Tym samym podmioty, które nie zostały zidentyfikowane jako kluczowe, mogą z jakiegoś nieznanego obecnie powodu zostać zaatakowane, co będzie łatwiejsze ze względu na niższy – niż w przypadku

podmiotów realizujących usługi kluczowe – poziom ich ochrony. Należy przypomnieć, że operatorzy i instytucje zarządzające usługą kluczową nie są samowystarczalni, tzn. wykorzystują podwykonawców (często słabiej zabezpieczonych), realizują wspólne procesy, używają wspólnej infrastruktury (np. serwerowni), są zależni od globalnego łańcucha dostaw itp. Próba zarządzania ryzykiem w tak złożonej strukturze organizacyjnej powoduje lawinowy wzrost kosztów.

Inne podejście zastosowano w dyrektywie NIS 2, zgodnie z którą wszystkie podmioty objęte jej zakresem muszą stosować odpowiednie środki zarządzania ryzykiem w zakresie cyberbezpieczeństwa. Stosowanie tych środków nie jest warunkowane tym, czy potencjalna awaria może wywołać skutki nieakceptowalne z punktu widzenia bezpieczeństwa publicznego, czy też takiej skali skutków nie jesteśmy w stanie przewidzieć lub udowodnić w postępowaniu administracyjnym. Takie podejście wynika z powszechności zagrożenia oraz tego, że cyberpowiązania nie są możliwe do prześledzenia, a także z potrzeby zachowania równości podmiotów na wspólnym ryku. Taka regulacja powoduje, że koszty ochrony są porównywalne dla każdej organizacji i żadna nie jest szczególnie obciążana czy preferowana. Wprowadzenie jednolitego podejścia do cyberbezpieczeństwa podmiotów krytycznych ma na celu eliminację luk w ochronie wynikających ze złożoności powiązań między podmiotami (art. 20 ust. 1).

Po przeprowadzeniu analizy przypadków ataków hybrydowych pojawia się wątpliwość, czy metodyka przyjęta w dyrektywie CER jest kompletna, tzn. czy obejmuje wszystkie elementy systemu, także te, które mogą stać się (nieoczywistymi) celami ataków hybrydowych. Dyrektywa NIS 2 zapewnia bardziej wszechstronne podejście do zarządzania ryzykiem, które obejmuje wszystkie podmioty i gwarantuje większą odporność całego systemu cyfrowego. Zastosowanie w obu dyrektywach odmiennych strategii wyłaniania podmiotów o dużym znaczeniu dla bezpieczeństwa państwa i jego obywateli może doprowadzić do wielu niespójności w zakresie nakładania obowiązków na te podmioty. Już dziś można przewidywać, że za kilka lat pojawią się głosy, by obie te dyrektywy ujednolicić.

Bibliografia

Clausewitz C. von, *O wojnie*, Warszawa 2022.

Źródła internetowe

Atak hakerski na oczyszczalnię ścieków, iSokolka.eu, 8.10.2024, https://isokolka.eu/kuznica/59444-atak-hakerski-na-oczyszczalnie-sciekow [dostęp: 20.02.2025].

Awaria kabla EstLink 2. Rosyjski tankowiec podejrzany o akt sabotażu, PolskieRadio.pl, 26.12.2024, https://www.polskieradio.pl/399/7977/artykul/3463666%2Cawaria-ka%20bla-estlink-2-rosyjski-tankowiec-podejrzany-o-akt-sabotazu? [dostęp: 20.02.2025].

CNN: Według ekspertów atak na Aramco nastąpił z Iranu, Interia Wydarzenia, 18.09.2019, https://wydarzenia.interia.pl/zagranica/news-cnn-wedlug-ekspertow--atak-na-aramco-nastapil-z-iranu,nId,3209902 [dostęp: 23.03.2025].

Doniesienia o rosyjskim cyberataku. Pojawił się polski wątek, Wirtualna Polska, 17.04.2024, https://wiadomosci.wp.pl/rosyjski-cyberatak-na-polska-infrastrukture-ofiara-oczyszczalnia-sciekow-7017937180834752a [dostęp: 20.02.2025].

Gapiński K., *Blackout w zachodniej Ukrainie – cyberatak o wymiarze międzynarodowym*, Fundacja im. Kazimierza Pułaskiego, 20.01.2016, https://pulaski.pl/komentarz-blackout-w-zachodniej-ukrainie-cyber-atak-o-wymiarze-miedzynarodowym/ [dostęp: 23.03.2025].

Górski R., *Specjalna operacja wojskowa NATO: bombardowanie Jugosławii*, Instytut Spraw Obywatelskich, 24.03.2023, https://instytutsprawobywatelskich.pl/specjalna--operacja-wojskowa-nato-bombardowanie-jugoslawii/ [dostęp: 23.03.2025].

Hoffman F.G., *Conflict in the 21'st Century: The Rise of Hybrid Wars*, Virginia 2007, https://www.comw.org/qdr/fulltext/0712hoffman.pdf [dostęp: 20.02.2025].

Impact Assessment of the 1977 New York City Blackout, lipiec 1978, https://www.ferc.gov/sites/default/files/2020-05/impact-77.pdf [dostęp: 23.03.2025].

Jackson G.M., *Warden's five-ring system theory: legitimate wartime military targeting or an increased potential to violate the law and norms of expected behavior?*, Alabama 2000, https://apps.dtic.mil/sti/pdfs/ADA425331.pdf [dostęp: 20.02.2025].

Jak uszkodzenie Estlink 2 wpływa na ceny energii w Estonii, Czas Wschodni, 14.02.2025, https://czaswschodni.pl/art/wiadomosci/jak-uszkodzenie-estlink-2-wplywa-na-ceny-energii-w-estonii_116f1090-c456-4bb7-abc1-c340f6da6cf5 [dostęp: 20.02.2025].

Jakóbik W., *USA mogą na dniach zadać nowy cios Nord Stream 2, ale unikają deklaracji*, Biznes Alert, 14.05.2021, https://biznesalert.pl/nord-stream-2-sankcje-usa-poszerzone-energetyka-gaz/ [dostęp: 20.02.2025].

Kardaś S., Łoskot-Strachota A., *Dywersja na gazociągach Nord Stream 1 i Nord Stream 2*, Ośrodek Studiów Wschodnich, 29.09.2022, https://www.osw.waw.pl/pl/publikacje/analizy/2022-09-29/dywersja-na-gazociagach-nord-stream-1-i-nord-stream-2 [dostęp: 23.03.2025].

Lewis S., Shalal A., *U.S., Germany strike Nord Stream 2 pipeline deal to push back on Russian 'aggression'*, Reuters, 22.07.2021, https://www.reuters.com/business/energy/us-germany-deal-nord-stream-2-pipeline-draws-ire-lawmakers-both-countries-2021-07-21/ [dostęp: 20.02.2025].

McKew M.K., *The Gerasimov Doctrine. It's Russia's new chaos theory of political warfare. And it's probably being used on you*, Politico, wrzesień/październik 2017, https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/ [dostęp: 23.03.2025].

Minister ostrzega mieszkańców przed możliwą dezinformacją, Made in Vilnius, 4.02.2025, https://madeinvilnius.lt/pl/Aktualno%C5%9Bci/Lietuvos-naujienos/Minister-ostrzega-mieszka%C5%84c%C3%B3w-przed-mo%C5%BCliw%C4%85-dezinformacj%C4%85/ [dostęp: 20.02.2025].

Muczyński R., *Atak na saudyjskie rafinerie*, Milmag, 16.09.2019, https://milmag.pl/atak-na-saudyjskie-rafinerie/ [dostęp: 23.03.2025].

Perzyński M., *Raport: O Colonial Pipline i zimnej wojnie w energetyce*, Biznesalert, 15.05.2021, https://biznesalert.pl/raport-colonial-pipeline-cyberatak-usa-rosja-energetyka/ [dostęp: 23.03.2025].

Polus A., *Atak na rafinerię w Arabii Saudyjskiej i jego konsekwencje dla Afryki*, Polskie Centrum Studiów Afrykanistycznych, 18.09.2019, https://pcsa.org.pl/atak-na-rafinerie-w-arabii-saudyjskiej-i-konsekwencje-dla-afryki/ [dostęp: 23.03.2025].

Po synchronizacji sieci energetycznych krajów bałtyckich z Europą zaktywizowała się propaganda Kremla, Polska Agencja Prasowa, 20.02.2025, https://www.pap.pl/aktualnosci/po-synchronizacji-sieci-energetycznych-krajow-baltyckich-z-europa-zaktywizowala-sie [dostęp: 20.02.2025].

Prezes Colonial Pipeline potwierdza: zapłaciliśmy okup hakerom, CyberDefence24, 20.05.2021, https://wilno.tvp.pl/84820950/przed-synchronizacja-z-europa-sluzby-ostrzegaja-przed-dezinformacja [dostęp: 23.03.2025].

Przed synchronizacją z Europą służby ostrzegają przed dezinformacją, TVP Wilno, 3.02.2025, https://wilno.tvp.pl/84820950/przed-synchronizacja-z-europa-sluzby-ostrzegaja-przed-dezinformacja [dostęp: 20.02.2025].

Psujek G., *Tajemnica ataku na saudyjską rafinerię*, Rzeczpospolita, 22.09.2019, https://radar.rp.pl/przemysl-obronny/art17499861-tajemnica-ataku-na-saudyjska-rafinerie [dostęp: 23.03.2025].

Rosyjski atak dezinformacją ws. energetyki. Estończycy wykupują generatory, służby w stanie gotowości, Polskie Radio 24, 6.02.2025, https://polskieradio24.pl/artykul/3480519,rosyjski-atak-dezinformacja-ws-energetyki-estonczycy-wykupuja-generatory-sluzby-w-stanie-gotowosci [dostęp: 20.02.2025].

Statement from CISA Acting Director Wales on Executive Order to Improve the Nation's Cybersecurity and Protect Federal Networks, America's Cyber Defense Agency, 13.05.2021, https://www.cisa.gov/news-events/news/statement-cisa-acting-director-wales-executive-order-improve-nations-cybersecurity-and-protect [dostęp: 20.02.2025].

Stawarz N., *„Nielegalne, ale moralne"? Operacja „Allied Force": przyczyny i konsekwencje*, Histmag.org, 24.03.2019, https://histmag.org/Nielegalne-ale-moralne-Operacja-Allied-Force-przyczyny-i-konsekwencje-18428? [dostęp: 23.03.2025].

Urbanek W., *Colonial Pipeline: niepożądana sława*, CRN, 24.06.2021, https://crn.pl/artykuly/colonial-pipeline-niepozadana-slawa/ [dostęp: 23.03.2025].

Uszkodzenie kabla EstLink 2 podniosło ceny energii w krajach bałtyckich, BalticWind.EU, 3.01.2025, https://balticwind.eu/pl/uszkodzenie-kabla-estlink-2-podnioslo-ceny-energii-w-krajach-baltyckich/ [dostęp: 20.02.2025].

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz. Urz. L 333/164 z 27.12.2022).

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 (dyrektywa NIS 2) – (Dz. Urz. L 333/80 z 27.12.2022).

Protokoły dodatkowe do Konwencji genewskich z 12 sierpnia 1949 r., dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych (Protokół I) oraz dotyczący ochrony ofiar niemiędzynarodowych konfliktów zbrojnych (Protokół II), sporządzone w Genewie dnia 8 czerwca 1977 r. (DzU z 1992 nr 41 poz. 175).

Dr Witold Skomra

Kierownik Wydziału Ochrony Infrastruktury Krytycznej w Rządowym Centrum Bezpieczeństwa. Ekspert w zakresie planowania cywilnego zarządzania kryzysowego oraz ochrony infrastruktury krytycznej. Krajowy delegat do grupy przygotowującej dyrektywę CER oraz do Wysokiego Forum ds. Ryzyka Organizacji Współpracy Gospodarczej i Rozwoju (OECD High Level Risk Forum). Wykładowca na Wydziale Zarządzania Politechniki Warszawskiej. Prowadzi zajęcia z zakresu ciągłości działania, zarządzania ryzykiem, zarządzania bezpieczeństwem publicznym oraz ochrony infrastruktury krytycznej. Były Komendant Główny Państwowej Straży Pożarnej, absolwent Szkoły Głównej Służby Pożarniczej oraz Akademii Obrony Narodowej.

Kontakt: witold.skomra@rcb.gov.pl

Dr Karolina Wojtasik

Specjalista ds. bezpieczeństwa, biegły sądowy, pracownik naukowy, wiceprezes ds. naukowych Polskiego Towarzystwa Bezpieczeństwa Narodowego, główny specjalista w Rządowym Centrum Bezpieczeństwa. Podczas polskiej prezydencji w Radzie Unii Europejskiej pełni funkcję przewodniczącej grupy roboczej PROCIV CER. Zajmuje się szeroko pojętym bezpieczeństwem infrastruktury krytycznej, szczególnie w kontekście zagrożeń bezpieczeństwa fizycznego i osobowego. Ponadto analizuje działalność salafickich organizacji terrorystycznych, modus operandi sprawców zamachów terrorystycznych w UE i USA, a także publikacje instruktażowe dotyczące metod przeprowadzania ataków na ludność cywilną i obiekty. Autorka książek: *Anatomia zamachu. O strategii i taktyce terrorystów*; *Ścieżki radykalizacji dżihadystycznej. Podręcznik dla studentów socjologii,*

politologii i bezpieczeństwa. Współautorka publikacji *Polski system antyterrorystyczny a realia zamachów drugiej dekady XXI wieku* oraz wielu innych publikacji związanych z terroryzmem, a także bezpieczeństwem i budowaniem odporności infrastruktury krytycznej. Twórca kanału popularnonaukowego Anatomia zamachu na YouTube.

Kontakt: karolina.wojtasik@rcb.gov.pl