Terroryzm – studia, analizy, prewencja, 2025, wydanie specjalne: 115–135

https://doi.org/10.4467/27204383TER.25.004.21507

Artykuł

Infrastruktura krytyczna jako cel ataków hybrydowych i konwencjonalnych. Wnioski z ukraińskich doświadczeń

Critical infrastructure as a target of hybrid and conventional attacks. Lessons from the Ukrainian experience

MICHAŁ PIEKARSKI

https://orcid.org/0000-0003-1514-7657

Wydział Nauk Społecznych,
Uniwersytet Wrocławski

Abstrakt

Autor omawia problematykę ataków na infrastrukturę krytyczną Ukrainy, podejmowanych zarówno podczas działań hybrydowych (od 2014 r.), jak i w czasie pełnoskalowej rosyjskiej inwazji (od 2022 r.). Na podstawie dostępnych informacji analizuje operacje przeciwko infrastrukturze energetycznej Ukrainy. Zwraca uwagę na to, że ataki prowadzone przez rosyjskie siły mogą sięgać również na terytorium Unii Europejskiej. Przedstawia także wstępne wnioski dotyczące zarówno odporności, jak i obrony infrastruktury krytycznej.

Słowa kluczowe

Ukraina, infrastruktura krytyczna, ochrona infrastruktury krytycznej, wojna hybrydowa, strategiczna kampania powietrzna

Abstract

The author discusses the issue of attacks on Ukraine's critical infrastructure, undertaken both during hybrid operations (since 2014) and during a full-scale Russian invasion (since 2022). Based on the available information, he analyses the operations against Ukraine's energy infrastructure. He points out that attacks conducted by Russian forces may also reach the territory of the European Union. He also presents preliminary conclusions on both the resilience and defence of critical infrastructure.

Keywords

Ukraine, critical infrastructure, critical infrastructure protection, hybrid warfare, strategic air campaign

Wprowadzenie

Rosnące napięcia międzynarodowe, rosyjskie działania hybrydowe i zagrożenie możliwym konfliktem konwencjonalnym wpływają na infrastrukturę krytyczną (IK). Aby lepiej przygotować IK w Unii Europejskiej na potencjalny atak, konieczne jest skorzystanie z doświadczeń płynących z konfliktów toczących się w innych regionach.

Ukraina od 2014 r. była celem rosyjskich działań hybrydowych, a od 2022 r. – konwencjonalnych. Ataki prowadzone w ramach tych działań były wymierzone również w IK. Autor artykułu przedstawia wstępne wnioski wyciągnięte z dotychczasowych ukraińskich doświadczeń. Zaznacza, że bieżące wiadomości na temat rosyjskiej agresji na Ukrainę, zwłaszcza w mediach społecznościowych, są często powierzchowne i mogą być niezgodne z faktami lub zawierać treści propagandowe albo dezinformacyjne. Dogłębną analizę tej wojny będzie można przeprowadzić dopiero po jej zakończeniu. Przykładowo w jednym z cytowanych w artykule tomów, opublikowanym w 2025 r., opisano tylko pierwszy rok pełnoskalowej wojny. Dlatego autor zdecydował się korzystać z wielu źródeł, w tym raportów think tanków, książek i innych publikacji, opisujących różne aspekty ataków na ukraińską IK.

Ataki na infrastrukturę krytyczną w kontekście zagrożenia hybrydowego

Zgodnie z publikacją *The Landscape of Hybrid Threats*[1] wszelkie wrogie działania wymierzone w IK (aktywa lub systemy albo części tych systemów) mogą:

(a) pogorszyć jakość oferowanych towarów i usług (np. zmniejszyć dostępność, niezawodność),
(b) zniszczyć kluczowe części infrastruktury,
(c) zwiększyć koszty ich eksploatacji,
(d) wpłynąć na popyt, wywierać presję na infrastrukturę,
(e) ograniczyć lub usunąć możliwość dywersyfikacji dostaw dóbr i usług oraz powodować jednostronną zależność od wrogiego podmiotu,
(f) uzyskać lub ograniczyć dostęp do kluczowych zasobów dla jej funkcjonalności (surowce, technologia, wiedza specjalistyczna itp.) i nie tylko[2].

Ponadto (...) *każde narzędzie, które może stworzyć bądź wykorzystać lukę w infrastrukturze (luki wewnętrzne lub luki iniekcyjne) i osiągnąć jeden z powyższych efektów, może być potencjalnie wykorzystane jako część zestawu narzędzi hybrydowych*[3]. Ponieważ działania te są określane jako hybrydowe, atak na infrastrukturę może być przeprowadzony przy użyciu narzędzi cybernetycznych i wpływać na gospodarkę, społeczeństwo i administrację publiczną.

Ciekawe wydaje się także spojrzenie na wojnę hybrydową jako część szerszej strategii. Raport *Countering Gray-Zone Hybrid Threats*[4] (pol. Przeciwdziałanie zagrożeniom hybrydowym w szarej strefie), opublikowany w 2016 r. przez Akademię Wojskową Stanów Zjednoczonych, opisuje zagrożenia hybrydowe jako spektrum składające się z 2 głównych części: szarej strefy i otwartej wojny.

---

1 G. Giannopoulos, H. Smith, M. Theocharidou, *The Landscape of Hybrid Threats: A Conceptual Model Public Version*, Publications Office of the European Union, Luxembourg 2021, https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf [dostęp: 15.01.2025].

2 Tamże, s. 28. Tłumaczenia w artykule pochodzą od redakcji (dop. red.).

3 Tamże.

4 J. Chambers, *Countering Gray-Zone Hybrid Threats. An Analysis of Russia's 'New Generation Warfare' and Implications for the US Army*, 2016, https://mwi.westpoint.edu/wp-content/uploads/2016/10/Countering-Gray-Zone-Hybrid-Threats.pdf [dostęp: 15.01.2025].

Szara strefa jest opisywana jako znajdująca się poniżej progu konfliktu konwencjonalnego, mająca niejednoznaczny charakter. Zagrożenia hybrydowe w tej strefie mogą obejmować wykorzystywanie cywilów, agentów wywiadu, sił nieregularnych, działanie w różnych domenach (lądowej, powietrznej, morskiej, cybernetycznej, informacyjnej), z zastosowaniem instrumentów władzy, w tym dyplomacji, polityki gospodarczej, polityki informacyjnej i wojska.

Zagrożenia hybrydowe w otwartej wojnie z kolei bardziej przypominają konflikt konwencjonalny. Agresorzy nie ukrywają swojego zaangażowania, używają zarówno konwencjonalnych, jak i niekonwencjonalnych narzędzi (np. działań wojsk specjalnych, działań nieregularnych). Te ramy koncepcyjne mogą być bardzo ciekawe w szczegółowej analizie ataków na ukraińską IK, ponieważ ten kraj najpierw stanął w obliczu ograniczonej (szarej strefy) agresji, która rozpoczęła się w 2014 r., a następnie w 2022 r. – otwartej wojny.

Ukraińska infrastruktura krytyczna jako cel wojny hybrydowej

Ukraina, wraz z jej IK, była celem szerokiego zakresu rosyjskich działań hybrydowych, w tym wojny politycznej, prób zamachów, użycia siły wojskowej, łącznie z tzw. zielonymi ludzikami na Krymie, oraz buntów inspirowanych przez Rosję na wschodzie Ukrainy. Na przykład celem cyberataku na sieć energetyczną z 2015 r. było 3 operatorów systemu dystrybucji energii elektrycznej w Iwano-Frankiwsku, Czerniowcach i Kijowie. Ten zdalny atak spowodował przerwę w dostawie prądu dla 225 000 odbiorców[5]. Rok później kolejne cyberataki były wymierzone w pojedynczy element systemu dystrybucyjnego – podstację w pobliżu Kijowa[6]. Do następnego ataku doszło w 2017 r., był on jednak bardziej rozległy, ponieważ za pomocą ransmowaree'u Petya zaatakowano systemy nie tylko w Ukrainie[7].

[5] *Cyber-Attack Against Ukrainian Critical Infrastructure*, CISA, 20.07.2021, https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 [dostęp: 15.01.2025].

[6] *Ukraine power cut 'was cyber-attack'*, BBC News, 11.01.2017, https://www.bbc.co.uk/news/technology-38573074 [dostęp: 15.01.2025].

[7] N. Perlroth, M. Scott, S. Frenkel, *Cyberattack Hits Ukraine Then Spreads Internationally*, The New York Times, 27.06.2017, https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html [dostęp: 16.01.2025]; A. Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired, 22.08.2018,

W tym samym czasie odnotowano także inne ataki. Na przykład w maju 2015 r. most kolejowy w Odessie został uszkodzony przez eksplozję improwizowanego ładunku wybuchowego (ang. *improvised explosive device*), która nastąpiła na krótko przed tym, jak pociąg miał przejechać przez miejsce ataku. Eksplozja była częścią szerszej serii zamachów bombowych w tym mieście portowym[8].

Celem agresji były również innego rodzaju infrastruktury. W maju 2014 r. eksplozja uszkodziła gazociąg Urengoj-Pomary-Użhorod w pobliżu Połtawy[9]. Kolejne eksplozje odnotowano w magazynach amunicji w Winnicy[10] w 2017 r. i rok później w Iczni[11]. Rosyjskie operacje hybrydowe od 2014 r. do początku 2022 r. były prowadzone, aby osłabić państwo ukraińskie, podważyć zaufanie obywateli do rządu i służb publicznych. Ponieważ celem politycznym Rosji pozostaje przejęcie kontroli nad Ukrainą i zmiana rządu na prorosyjski, operacje hybrydowe mogły stworzyć ku temu sprzyjające warunki.

Wzrost napięcia był widoczny szczególnie w ostatnich miesiącach przed rozpoczęciem pełnoskalowej inwazji Rosji na Ukrainę. Rosja, według raportu Royal United Services Institute (RUSI), przygotowywała się do przeprowadzenia kampanii niekonwencjonalnych działań wspierających jawną, konwencjonalną agresję, a celem miała być również IK: *Oczekuje się również, że krajowa infrastruktura krytyczna, w tym telekomunikacja, usługi rządowe, energia elektryczna i usługi użyteczności publicznej zostaną zaatakowane zarówno poprzez fizyczny sabotaż, jak i cyberatak. Ukraińskie służby bezpieczeństwa spodziewają się, że nie będą w stanie przerwać wszystkich tych ataków*[12].

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [dostęp: 16.01.2025].

[8] *Explosion in Ukraine's Odessa Destroys Railroad Bridge but Misses Train*, The Moscow Times, 13.05.2015, https://www.themoscowtimes.com/2015/05/13/explosion-in-ukraines-odessa-destroys-railroad-bridge-but-misses-train-a46507 [dostęp: 16.01.2025].

[9] *Major Ukraine gas pipeline hit by blast*, 17.06.2014, BBC, https://www.bbc.com/news/world-europe-27891018 [dostęp: 16.01.2025].

[10] J. Mendel, *In Ukraine a Huge Ammunition Depot Catches Fire*, The New York Times, 27.09.2017, https://www.nytimes.com/2017/09/27/world/europe/ukraine-ammunition-depot-explosion.html?mcubz=0 [dostęp: 16.01.2025].

[11] *Ukraine ammo dump blasts blamed on 'possible sabotage'*, BBC, 9.10.2018, https://www.bbc.co.uk/news/world-europe-45794963 [dostęp: 16.01.2025].

[12] J. Watling, N. Reynolds, *The Plot to Destroy Ukraine*, 15.02.2022, https://static.rusi.org/special-report-202202-ukraine-web.pdf [dostęp: 17.01.2025].

Ataki na infrastrukturę, choć zróżnicowane pod względem skali i metod, były wstępem do znacznie szerszej operacji konwencjonalnej. Ataki hybrydowe nie zakończyły się sukcesem. W sektorze IK podjęto działania mające na celu zwiększenie jej odporności. Na przykład w 2015 r. opublikowano tzw. zieloną księgę ochrony infrastruktury krytycznej[13] w Ukrainie, a w 2022 r. przyjęto specjalną ustawę parlamentu o IK[14].

Warto zauważyć, że ataki na Ukrainę, szczególnie cyberataki, zostały opisane także jako poligon doświadczalny do prowadzenia cyberwojny przeciwko innym krajom, w tym państwom członkowskim UE i Stanom Zjednoczonym[15].

Ukraińska infrastruktura krytyczna jako cel wojny konwencjonalnej

Celem pełnoskalowej inwazji Rosji na Ukrainę, rozpoczętej 24 lutego 2022 r., było przejęcie kontroli nad Ukrainą przez zajęcie Kijowa. Kiedy nie został on osiągnięty, operacja wojskowa skupiła się na innych obszarach, w tym na Donbasie[16]. Rosjanie byli w stanie przejąć znaczne tereny Ukrainy, w tym południową część kraju. W ten sposób powstało połączenie lądowe między Krymem a Rosją kontynentalną. Istniało wiele elementów IK, w tym 2 elektrownie jądrowe, linie kolejowe i inne, które znalazły się pod rosyjską kontrolą, jednak zostały one przejęte głównie dlatego, że znajdowały się na ziemiach zajętych przez rosyjskie siły, nie były zaś oddzielnymi celami. Takim przykładem jest Czarnobylska Elektrownia Jądrowa, którą przejęto, ponieważ znajdowała się na trasie rosyjskich wojsk wkraczających na Ukrainę z Białorusi. Następnie została odzyskana przez Ukrainę, gdy rosyjskie wojska wycofały się po nieudanej

[13] D. Biriukov, S. Kondratov, O. Nasvit, O. Sukhodolia, *Green Paper on Critical Infrastructure Protection in Ukraine. Analytical Report*, Kiev 2015.

[14] *Закон України про критичну інфраструктуру* (Відомості Верховної Ради України (ВВР), 2023, № 5, ст. 13) – [*Zakon Ukrajiny pro krytycznu infrastrukturu* (Widomosti Werchownoji Rady Ukrajiny (WWR), 2023, № 5, st. 13)], https://zakon.rada.gov.ua/laws/show/1882-20#Text [dostęp: 17.01.2025].

[15] A. Greenberg, *How an Entire Nation Became Russia's Test Lab for Cyberwar*, Wired, 20.06.2017, https://www.wired.com/story/russian-hackers-attack-ukraine/ [dostęp: 18.01.2025].

[16] J. Watling, N. Reynolds, *Operation Z. The Death Throes of an Imperial Delusion*, 22.04.2022, https://static.rusi.org/special-report-202204-operation-z-web.pdf [dostęp: 18.01.2025].

bitwie o Kijów. Zniszczenie tamy w Nowej Kachowce także było częścią rosyjskiej operacji wojskowej, przeprowadzonej w celu zakłócenia ukraińskich operacji ofensywnych, ponieważ wyłączyło z użytkowania 1 ważny most i uniemożliwiło dalsze operacje przekraczania rzeki poniżej tamy z powodu katastrofalnej powodzi[17]. Podobny incydent odnotowano w 2023 r.[18] Wiele innych obiektów IK również zostało zaatakowanych lub przejętych podczas walk.

Nowe wyzwania pojawiły się później, gdy stało się jasne, że rosyjskie siły nie są w stanie zająć Kijowa, a ukraińskie siły zbrojne przeprowadzają udane operacje zarówno obronne, jak i ofensywne. Jesienią 2022 r. Rosjanie rozpoczęli pierwszą strategiczną kampanię wymierzoną w ukraiński sektor energetyczny. Ataki nie były tylko kolejnym elementem kampanii na froncie, lecz także – podobnie jak w przypadku innych konfliktów, w tym II wojny światowej – próbą kształtowania sytuacji strategicznej i osłabienia ukraińskiej odporności społecznej. Tego typu ataki mają pogarszać warunki życia ludności cywilnej, zakłócać kluczowe sektory gospodarki. Mogą zmusić rząd do zaakceptowania żądań agresora, w obliczu groźby buntu społeczeństwa wyczerpanego strategiczną kampanią powietrzną. Koncepcja ta nie jest niczym nowym w historii działań wojennych, począwszy od teorii wojny powietrznej Giulio Douheta[19], przez strategiczne ataki w czasie II wojny światowej, aż po teorię 5 pierścieni Johna Ashleya Wardena III. Teoria Wardena, jako najnowocześniejsza, jest szczególnie pomocna w wyjaśnianiu rosyjskich ataków na ukraińską IK, ponieważ umieszcza je w 2 pierścieniach: infrastrukturze (opisywanej głównie jako transportowa) i tzw. krytycznych podstawach (z ang. *critical essentials*) – obejmujących zasilanie[20]. Ponadto w rosyjskiej strategii wojskowej istnieje koncepcja Strategicznej Operacji Zniszczenia Krytycznie Ważnych Celów (ang. Strategic Operation

[17] H. Altman, *Dam Destroyed, Accusations Fly, Waters Rise, War Plans Could Change*, The War Zone, 6.06.2023, https://www.twz.com/dam-destroyed-accusations-fly-waters-rise-war-plans-could-change [dostęp: 18.01.2025].

[18] T. Newdick, *Ukraine Accuses Russia Of Blowing Up Another Dam*, The War Zone, 12.06.2023, https://www.twz.com/ukraine-accuses-russia-of-blowing-up-another-dam [dostęp: 18.01.2025].

[19] G. Douhet, *Panowanie w powietrzu. Przypuszczalne formy przyszłej wojny oraz ostatnie artykuły*, Warszawa 2013.

[20] J.A. Warden III, *The Enemy as System*, „Airpower Journal" 1995, t. 9, nr 1, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-09_Issue-1-Se/1995_Vol9_No1.pdf, s. 44–50 [dostęp: 1.02.2025].

for the Destruction of Critically Important Targets, SODCIT)[21]. Ten rodzaj operacji ma na celu zniszczenie obiektów (systemów), które mogą mieć charakter wojskowy lub niewojskowy, aby zmusić wroga do zaprzestania działań na warunkach korzystnych dla Rosji[22]. Według Michaela Kofmana operacja ta nie została przeprowadzona na początku otwartej inwazji, ale uderzenia na ukraińską sieć energetyczną były w rzeczywistości SODCIT[23]. Zostaną one opisane szczegółowo w dalszej części tekstu.

Rosyjskie ataki powietrzne i rakietowe na ukraińską sieć energetyczną

Pierwsze uderzenia wymierzone w ukraińską infrastrukturę energetyczną, które można interpretować jako część SODCIT, zostały przeprowadzone 10 października 2022 r. Wystrzelono wówczas 84 pociski rakietowe i 24 drony. Celem były elektrownie i podstacje w Kijowie i 11 regionach, co spowodowało przerwy w dostawie prądu[24]. Dodatkowe, ale ograniczone uderzenie (28 pocisków wspieranych przez drony) nastąpiło dzień później. Zmasowane ataki odnotowano 31 października[25] i 15 listopada[26], a także w grudniu. Pod koniec 2022 r. przeprowadzono dziesiąty atak na dużą skalę[27]. Do następnych uderzeń doszło w pierwszych miesiącach 2023 r.,

[21] M. Kofman i in., *Russian Military Strategy: Core Tenets and Operational Concepts*, sierpień 2021, https://www.cna.org/archive/CNA_Files/pdf/russian-military-strategy-core-tenets-and-operational-concepts.pdf [dostęp: 3.02.2025].

[22] M. Depczyński, L. Elak, *Rosyjska sztuka operacyjna w zarysie*, Warszawa 2020, s. 369–376.

[23] M. Kofman, *Russian airpower in context: The first year of war*, w: *The Air War in Ukraine – The First Year of Conflict*, D. Henriksen, J. Bronk (red.), New York 2025.

[24] S. Matuszak, *Rosja destabilizuje system energetyczny Ukrainy*, Ośrodek Studiów Wschodnich, 11.10.2022, https://www.osw.waw.pl/pl/publikacje/analizy/2022-10-11/rosja-destabilizuje-system-energetyczny-ukrainy [dostęp: 5.02.2025].

[25] L. Harding, D. Sabbagh, I. Koshiw, *Russia targets Ukraine energy and water infrastructure in missile attacks*, The Guardian, 31.10.2022, https://www.theguardian.com/world/2022/oct/31/russian-missiles-kyiv-ukraine-cities [dostęp: 5.02.2025].

[26] A. Wilk, P. Żochowski, *Ukraina bez prądu. 265. dzień wojny*, Ośrodek Studiów Wschodnich, 16.11.2022, https://www.osw.waw.pl/pl/publikacje/analizy/2022-11-16/ukraina-bez-pradu-265-dzien-wojny [dostęp: 5.02.2025].

[27] A. Wilk, P. Żochowski, *Dziesiąty zmasowany ostrzał Ukrainy. 309. dzień wojny*, Ośrodek Studiów Wschodnich, 30.12.2022, https://www.osw.waw.pl/pl/publikacje/analizy/2022-12-30/dziesiaty-zmasowany-ostrzal-ukrainy-309-dzien-wojny [dostęp: 5.02.2025].

a w maju odnotowano kolejną falę ataków. Większość z nich koncentrowała się na systemie przesyłowym (podstacjach).

Pod koniec 2023 r. odnotowano wiele mniejszych ataków przy użyciu dronów (z niewielką liczbą różnego rodzaju pocisków) i tylko jeden duży atak (29 grudnia). Zmienił się przebieg kampanii powietrznej, ponieważ celowała ona nie tylko w sieć energetyczną, lecz także w przemysł zbrojeniowy[28]. Do kolejnych ataków doszło w 2024 r. – w styczniu do 5 dużych[29], w lutym nie odnotowano żadnego[30], co może świadczyć o wyczerpaniu zapasu środków rażenia, pod koniec marca przeprowadzono duży atak (łącznie 151 pocisków rakietowych i dronów), w następnych dniach były realizowane dalsze ataki[31].

W maju odnotowano 3 ataki na dużą skalę[32], a w czerwcu – 4, w tym największy z użyciem łącznie 100 rakiet i dronów[33]. Dnia 26 sierpnia 2024 r. siły rosyjskie rozpoczęły atak, określany jako najpotężniejszy od początku otwartej inwazji. Wykryto 236 dronów i pocisków rakietowych, w tym 109 dronów, 77 pocisków manewrujących Ch-101 oraz łącznie 50 pocisków Ch-59, Ch-22 i pocisków balistycznych. Celem były elementy sieci energetycznej w 15 regionach Ukrainy[34]. Jedną z zauważalnych zmian w porównaniu z poprzednimi atakami było skupienie się na elektrowniach, zwłaszcza wodnych i węglowych, w celu destabilizacji sieci elektrycznej[35].

Częstotliwość ataków i zastosowana w nich broń różniły się w późniejszym okresie. Na przykład każdego dnia od maja do września 2024 r.

---

[28] M. Strembski, *Wojna powietrzna nad Ukrainą – grudzień 2023 r.*, „Lotnictwo" 2024, nr 1, s. 38.

[29] M. Strembski, *Wojna powietrzna nad Ukrainą – styczeń 2024 r.*, „Lotnictwo" 2024, nr 2, s. 14, 16, 18–19.

[30] Według publikacji Ośrodka Studiów Wschodnich.

[31] S. Matuszak, *Ukraina: poważny cios w energetykę*, Ośrodek Studiów Wschodnich, 28.03.2024, https://www.osw.waw.pl/pl/publikacje/analizy/2024-03-28/ukraina-powazny-cios-w-energetyke [dostęp: 5.02.2025].

[32] M. Strembski, *Wojna powietrzna nad Ukrainą. Maj 2024 r.*, „Lotnictwo" 2024, nr 6, s. 43, 48–49.

[33] M. Strembski, *Wojna powietrzna nad Ukrainą. Czerwiec 2024 r.*, „Lotnictwo" 2024, nr 7–8, s. 30, 32, 34, 36.

[34] M. Strembski, *Wojna powietrzna nad Ukrainą. Sierpień 2024 r.*, „Lotnictwo" 2024, nr 10, s. 46.

[35] M. Zaniewicz, *Ukraine in Darkness: Preventing the Worst-Case Scenario for Its Energy System*, Forum Energii, 1.07.2024, https://www.forum-energii.eu/en/ukraine-destroyed-system [dostęp: 7.02.2025].

przeprowadzano mniejsze uderzenia z wykorzystaniem dronów, ale 30 września użyto łącznie 76 pocisków i dronów[36].

W listopadzie 2024 r. doszło do poważnego natarcia, np. 17 listopada ok. 210 pocisków i dronów zostało użytych do ataku na sieć energetyczną, w tym elektrownie i podstacje, co spowodowało przerwy w dostawie prądu w całym regionie. Zostały również uszkodzone systemy ciepłownicze i sieci wodociągowe. W dniu 21 listopada celem kolejnego ataku na dużą skalę był obszar Dniepru. Z kolei 28 listopada co najmniej 188 rakiet i dronów użyto do ataku na infrastrukturę energetyczną i cele przemysłowe[37].

Były to przemyślane, nieprzypadkowe uderzenia na sieć energetyczną powodujące wieloaspektowe konsekwencje. Naprawienie lub wymiana uszkodzonych elementów wymaga czasu, dostępu do części lub nowych komponentów, np. transformatorów, dostępności wykwalifikowanej siły roboczej. W przypadku braku części zamiennych możliwości generowania i przesyłania energii są ograniczone[38]. Ponadto system energetyczny wymaga zarówno podsystemów wytwarzania (elektrowni), jak i podsystemów przesyłowych, a wczesne rosyjskie ataki (w latach 2022–2023) były ukierunkowane na część przesyłową – podstacje, co blokowało możliwości dostarczania wytworzonej energii[39].

W wyniku ukraińskich prób złagodzenia skutków ataków i poprawienia odporności, późniejsze rosyjskie ataki były skoncentrowane na systemie wytwarzania energii. Według Macieja Zaniewicza miały one na celu destabilizację systemu przez uniemożliwienie jego zbilansowania i dostarczania energii w godzinach szczytowego zapotrzebowania. Rosja była w stanie zmniejszyć ukraińskie moce wytwórcze o 3/4 – z 40 GW przed wojną do 10 GW w maju 2024 r.[40] Według Międzynarodowej Agencji Energetycznej ok. 70% ukraińskich mocy wytwórczych energii cieplnej, a także połowa podstacji wysokiego

[36] M. Strembski, *Wojna powietrzna nad Ukrainą. Wrzesień 2024 r.*, „Lotnictwo" 2024, nr 11, s. 34.

[37] M. Strembski, *Wojna powietrzna nad Ukrainą – listopad 2024 r.*, „Lotnictwo" 2025, nr 1, s. 33, 36, 38.

[38] B.E. Humpreys, *Attacks on Ukraine's Electric Grid: Insights for U.S. Infrastructure Security and Resilience*, Congressional Research Service, 17.05.2024, https://crsreports.congress.gov/product/pdf/R/R48067 [dostęp: 8.02.2025].

[39] Tamże.

[40] M. Zaniewicz, *Ukraine in Darkness*...

napięcia zostało zajętych lub uszkodzonych. Uszkodzenia zmusiły operatora systemu energetycznego do ograniczenia dostaw energii[41].

Terminy i częstotliwość działań, zwłaszcza w latach 2022–2023, zostały dostosowane do warunków środowiskowych i społecznych. Ataki na sieć energetyczną, w tym elektrownie i elektrociepłownie, mogłyby mieć katastrofalny wpływ na społeczeństwo, gdyby nie było ogrzewania, nawet uzupełniającego z urządzeń zasilanych energią elektryczną. Również inne systemy potrzebujące energii elektrycznej, w tym system wodny, zostałyby zakłócone. Brak elektryczności oznacza także ograniczony dostęp do informacji i zakupów (płatności można dokonywać tylko gotówką).

Taktyka i broń zastosowane podczas ataku rosyjskich sił na ukraińską sieć energetyczną

Zastosowaną broń można podzielić na kilka kategorii, od konwencjonalnych samolotów, przez pociski kierowane różnych typów, do rakiet balistycznych i jednokierunkowych dronów atakujących. Samoloty pilotowane, zwłaszcza wielozadaniowe samoloty bojowe Su-30, Su-34 i bombowce, takie jak Tu-22M, Tu-95 i Tu-160[42], są wykorzystywane wyłącznie jako nośniki pocisków manewrujących, w atakach typu *stand-off* z dala od ukraińskich systemów obrony powietrznej. Nie odnotowano bezpośrednich bombardowań przy użyciu bomb niekierowanych lub kierowanych, ponieważ ten tryb ataku zwiększyłby ryzyko strat.

Większość pocisków manewrujących wystrzeliwanych z powietrza to pociski Ch-59, Ch-69, Ch-22, Ch-32, Ch-101 i Ch-555, uzupełnione przez pociski balistyczne Ch-47. Poddźwiękowe pociski Ch-59 (i ich zmodernizowany wariant Ch-69) mają zasięg do 258 km. Zostały zaprojektowane do atakowania małych celów stacjonarnych lub okrętów wojennych i – w zależności od wariantu[43] – przenoszą głowice o masie 140–258 kg.

Pociski Ch-22 i Ch-32, przenoszone przez bombowce Tu-22M, pełnią podwójną funkcję. Choć zostały zaprojektowane jako broń przeciw okrętom, to są zdolne do rażenia również stacjonarnych celów lądowych.

[41] *Ukraine's Energy Security and the Coming Winter*, IEA, wrzesień 2024, https://iea.blob.core.windows.net/assets/cec49dc2-7d04-442f-92aa-54c18e6f51d6/UkrainesEnergySecurityandtheComing-Winter.pdf, s. 12 [dostęp: 9.02.2025].

[42] P. Butowski, *Russian Air Power*, 2023, s. 7–30, 70–87.

[43] T. Kwasek, *Lotnicze pociski skrzydlate rodziny Ch-59*, „Lotnictwo" 2024, nr 3, s. 42.

Maksymalny zasięg tych pocisków wynosi 500 km (Ch-22) lub 1000 km (Ch-32), a waga ich głowic bojowych to 600 kg. Pociski te po wystrzeleniu osiągają wysokość do 44 km i prędkość naddźwiękową do 3200 km/h. Zarówno Ch-101, jak i Ch-555 to nisko latające pociski manewrujące, wystrzeliwane przez samoloty bombowe. Mają duży zasięg: Ch-555 do 3500 km[44], Ch-101 do 2800 km[45]. Dodatkowo czasami są używane pociski Ch-47. Są one wystrzeliwane z powietrza wariantem pocisku Iskander o zasięgu do 2000 km[46].

Lądowe pociski rakietowe używane przeciwko ukraińskiej sieci energetycznej należą głównie do systemu Iskander, zaprojektowanego do atakowania celów lądowych. Ten zestaw uderzeniowy wykorzystuje pociski balistyczne 9M723, a także 2 warianty pocisków manewrujących: 9M728 i 9M729, które mają maksymalny zasięg 480 km[47]. W przypadku pocisków lądowych czasami zgłaszano użycie zestawów przeciwokrętowych Bastion i Bał lub pocisków ziemia-powietrze S-300, ponieważ wszystkie te pociski są zdolne do uderzania w stacjonarne cele lądowe. Innym rodzajem pocisków, które zostały użyte w atakach, są okrętowe pociski manewrujące 3M14 Kalibr. Mają one zasięg do 2000 km i mogą być wystrzeliwane przez okręty nawodne i podwodne[48].

Oprócz tej rosyjskiej broni konwencjonalnej powszechnie są stosowane irańskie samoloty bezzałogowe Szahed-136 i Szahed-131 (znane również jako Geran-2 i Geran-1). Drony te przenoszą małe głowice bojowe (od 15 do 50 kg), są napędzane silnikami tłokowymi i mają zasięg do 2500 km[49].

To połączenie różnych typów rakiet i dronów pozwala rosyjskim siłom na atakowanie z wielu kierunków, z różną prędkością i wysokością. Z tego powodu nie ma jednego środka obronnego, np. systemu obrony powietrznej umieszczonego tylko na jednym, najbardziej prawdopodobnym

[44] *Kh-55 (AS-15)*, Missile Threat, 23.04.2024, https://missilethreat.csis.org/missile/kh-55/ [dostęp: 12.02.2025].

[45] *Kh-101 / Kh-102*, Missile Threat, 23.04.2024, https://missilethreat.csis.org/missile/kh-101-kh-102/ [dostęp: 12.02.2025].

[46] *Kh-47M2 Kinzhal*, Missile Threat, 23.04.2024, https://missilethreat.csis.org/missile/kinzhal/ [dostęp: 12.02.2025].

[47] T. Kwasek, *Rakiety Putina. Rosyjskie lądowe, lotnicze i morskie systemy rakietowe oraz pociski manewrujące*, „Nowa Technika Wojskowa" 2023, numer specjalny: *Wojna rosyjsko-ukraińska*, s. 44.

[48] *3M-14 Kalibr (SS-N-30A)*, Missile Threat, 23.04.2024, https://missilethreat.csis.org/missile/ss-n-30a/ [dostęp: 12.02.2025].

[49] M. Glajzer, *Irański oręż w rosyjskiej służbie*, „Nowa Technika Wojskowa" 2022, nr 11, s. 13–14.

kierunku. Wystrzelenie wielu rodzajów broni – nazywane atakiem nasycającym – utrudnia ich przechwytywanie, ponieważ liczba systemów obrony powietrznej i ich możliwości są ograniczone. Ponadto użycie różnych rodzajów broni zwiększa szanse powodzenia ataku – nawet jeśli jedna grupa lub typ pocisków zostaną zestrzelone, inne mogą dotrzeć do celów. Użycie różnych rodzajów broni pozwala także odwrócić uwagę obrońców przez skierowanie ognia w stronę ataku dywersyjnego, co również zwiększa szansę na sukces. Zastosowanie zaawansowanej broni, takiej jak nowoczesne pociski kierowane do obrony przed atakiem z użyciem taniej broni, zwłaszcza dronów, wywiera presję na żołnierzy, a ponadto może prowadzić do wyczerpania zapasów wysokiej klasy uzbrojenia. Uzupełnienie tych strat może być trudne i kosztowne.

Problemem dla Rosji są kwestie ekonomiczne. Ataki wymagające użycia dużej liczby broni mogą być przeprowadzone po zgromadzeniu niezbędnych zapasów, a dostępność środków transportu, zwłaszcza samolotów, prawdopodobnie ogranicza rosyjskie możliwości. Z tego powodu ataków nie przeprowadza się w sposób ciągły, lecz raczej falami, co zmusza Rosję do uderzenia tylko wtedy, gdy atak może przynieść największe zniszczenia.

Jeśli chodzi o środki obrony i ochrony, Ukrainie udało się jak dotąd zapobiec najgorszemu. Pomimo uszkodzeń infrastruktury i spowodowanych nimi przerw w dostawie prądu nie ma bezpośredniego, strategicznego wpływu kampanii na ukraińską sieć energetyczną. Ataki z przełomu 2022 i 2023 r. nie zmusiły Ukrainy do zaakceptowania rosyjskich żądań, wręcz przeciwnie, była ona w stanie prowadzić operacje ofensywne. Możliwe, że długoterminowe skutki, zwłaszcza rosnące zmęczenie Ukraińców wojną, mogą stać się ważnym czynnikiem demobilizacji społecznej i spadku poparcia dla kontynuowania wojny, szczególnie jeśli potrwa ona przez następny rok lub dłużej, a dalsze ataki spowodują kolejne uszkodzenia ukraińskiej sieci energetycznej. Inną kwestią jest jednak wytrwałość społeczeństwa, wytrzymałość sieci energetycznej i zdolność do obrony infrastruktury.

Jednym z czynników wzmacniających odporność jest to, że ukraińska sieć energetyczna, produkcji radzieckiej, zaprojektowana do zasilania przemysłu ciężkiego, była w stanie zapewnić dodatkową moc, której zwykle nie wykorzystywano. Ponadto istotna jest również zdolność do naprawy uszkodzeń, zwłaszcza linii przesyłowych i podstacji (może to być jedna ze zmian w wybieraniu celów: od podstacji do elektrowni, które są trudniejsze do naprawy).

Podjęto także inne środki w celu zapewnienia energii elektrycznej, w tym import z europejskiej sieci energetycznej. Tymczasowym rozwiązaniem dla ludności mieszkającej na obszarach dotkniętych awarią było rozmieszczenie generatorów zasilanych olejem napędowym w wyznaczonych punktach pomocy, tzw. punktach niezwyciężoności (ang. *points of invincibility*), które zapewniają dostęp do energii elektrycznej, ciepła i wody. Według doniesień medialnych utworzono ok. 13 000 takich punktów[50].

Obronę zapewniały różnego rodzaju systemy przeciwlotnicze i samoloty. Rozwój ukraińskiej obrony przeciwlotniczej był pozornie szybki i często wymagał improwizacji ze względu na skalę ataków i malejące zasoby systemów obrony przeciwlotniczej. Ukraina w 2022 r. dysponowała systemami produkcji radzieckiej, takimi jak S-300, Buk, Osa, uzupełnionymi przez artylerię i systemy przenośne (np. Strieła)[51]. W późniejszych latach dostarczono więcej systemów z krajów NATO, w tym polskie przenośne przeciwlotnicze zestawy rakietowe Grom i Piorun, systemy krótkiego i średniego zasięgu, takie jak IRIS-T, Hawk, NASAMS, Aspide oraz dalekiego zasięgu Patriot i SAMP/T[52]. Aby zwalczać zagrożenie ze strony nisko latających dronów, dodatkowe tanie systemy – wykorzystujące karabiny maszynowe montowane na ciężarówkach – zostały opracowane na wczesnym etapie rosyjskich ataków w 2022 r.[53] Ponadto przekształcono starsze systemy, co umożliwiło korzystanie z zachodnich pocisków rakietowych lub pozwoliło na użycie dostępnych pocisków powietrze-powietrze w wyrzutniach lądowych. Znane rodzaje tych systemów – tzw. FrankenSAM – to pociski Buk wystrzeliwujące pociski RIM-7[54], wyrzutnie OSA wykorzystujące

[50] *There are almost 13 thousand Invincibility Points in Ukraine*, UNN, 3.04.2024, https://unn.ua/en/news/there-are-almost-13-thousand-invincibility-points-in-ukraine [dostęp: 13.02.2025].

[51] *Russia and Eurasia*, „The Military Balance" 2022, t. 122, nr 1, s. 164–217. https://doi.org/10.1080/04597222.2022.2022930.

[52] Tamże.

[53] M.E. Miller, A. Galouchka, *Ukraine's drone hunters scramble to destroy Russia's Iranian–built fleet*, The Washington Post, 28.11.2022, https://www.washingtonpost.com/world/2022/11/28/ukraine-drone-hunters-mykolaiv-russia/ [dostęp: 13.02.2025].

[54] J. Trevithick, *'FrankenSAM' Systems Are Now Shooting Down Drones In Ukraine*, The War Zone, 17.01.2024, https://www.twz.com/frankensam-systems-are-now-shooting-down-drones-in-ukraine [dostęp: 14.02.2025].

pociski R-73[55] i inne, w tym kontenerowe wyrzutnie R-73[56]. Istnieją również samoloty służące do zestrzeliwania pocisków rakietowych i dronów. Oprócz konwencjonalnych myśliwców (MiG-29, Su-27, F-16) są dostępne także niedrogie rozwiązania. Podano, że śmigłowce były wykorzystywane do zwalczania dronów[57]. Ten szeroki zestaw broni obronnej zmniejszył liczbę pocisków i dronów docierających do celów.

Wnioski

Ukraińska IK od 2014 r. była celem rosyjskich ataków, zarówno w formie hybrydowej, jak i konwencjonalnej. Wojna hybrydowa musi być traktowana jako wstęp do możliwej konwencjonalnej agresji i rozumiana również w kontekście ochrony IK – zagrożenia hybrydowe i konwencjonalne są częścią tego samego kontinuum. Oznacza to również, że nie ma możliwości zastąpienia jednego rodzaju działań wojennych innym lub jednego rodzaju ataków innym. Fakt, że ukraińska sieć energetyczna była celem cyberataków, nie wykluczył ataków konwencjonalnych.

Państwa członkowskie UE mierzą się z podobnym zagrożeniem. Agresywna postawa Rosji oznacza ciągłe, wyraźne i obecne zagrożenie zarówno atakami hybrydowymi, jak i konwencjonalnymi. Należą do nich ataki rakietowe i dronowe, które mogą sięgać głęboko na terytorium UE, zwłaszcza jeśli weźmie się pod uwagę platformy morskie (okręty nawodne i podwodne). Wynik ataku na IK może być druzgocący w wymiarze fizycznym, społecznym i politycznym. Zagrożenie zwiększa się w związku z tym, że rosyjskie siły morskie – z wyjątkiem tych na Morzu Czarnym – nie są dotknięte wojną, a we Flocie Północnej (ros. Северный флот) i Flocie Bałtyckiej Marynarki Wojennej Federacji Rosyjskiej (ros. Балтийский флот

[55] T. Newdick, *Ukraine's SA-8 Gecko 'FrankenSAM' Adapted To Fire Air-To-Air Missiles Seen In New Detail*, The War Zone, 12.12.2024, https://www.twz.com/land/ukraines-sa-8-gecko-frankensam-adapted-to-fire-air-to-air-missiles-seen-in-new-detail [dostęp: 14.02.2025].

[56] J. Trevithick, *Containerized SAM System That Fires Soviet Air-To-Air Missiles For Ukraine Breaks Cover*, The War Zone, 12.02.2025, https://www.twz.com/land/containerized-sam-system-that-fires-soviet-air-to-air-missiles-for-ukraine-breaks-cover [dostęp: 14.02.2025].

[57] D. Axe, *Ukrainian Helicopter Crews Are Shooting Down Russian Drones – Like World War II Turret Gunners*, Forbes, 22.08.2024, https://www.forbes.com/sites/davidaxe/2024/08/22/ukrainian-helicopter-crews-are-shooting-down-russian-drones-like-world-war-ii-turret-gunners/ [dostęp: 14.02.2025].

ВМФ Российской Федерации) znajduje się wiele okrętów zdolnych do wystrzelenia pocisków manewrujących przeciwko celom lądowym.

Kolejne wnioski dotyczą odporności i obrony. Odporność infrastruktury ma kluczowe znaczenie, ponieważ obejmuje ona zdolność do zapewnienia zapasowych źródeł zasilania – w przypadku sieci energetycznej dotyczy to wytwarzania i przesyłu energii. Im więcej źródeł zasilania i dróg przesyłu energii jest dostępnych, tym lepiej, ponieważ nawet jeśli niektóre z nich zostaną uszkodzone, pozostałe mogą przejąć ich rolę. Można to zastosować również do innych rodzajów infrastruktury, takich jak koleje. Podobną formą rezerw jest zapewnienie nadwyżki mocy do wykorzystania w sytuacji kryzysowej, co mogłoby ograniczyć skutki uszkodzeń. Ponadto wysoce zalecane jest posiadanie odpowiedniej liczby części zamiennych lub urządzeń. Jeśli to możliwe, należałoby wziąć pod uwagę rozproszenie infrastruktury, np. w przypadku elementów sieci energetycznej możliwa jest decentralizacja wytwarzania, a małe instalacje, nawet przydomowe, wykorzystujące energię odnawialną mogą być uzupełnieniem dla istniejących elektrowni konwencjonalnych.

Innym wymiarem odporności jest zdolność do zapewnienia odpowiedniej liczby wykwalifikowanego personelu w celu utrzymania, naprawy bądź odbudowy infrastruktury. Zapotrzebowanie na wykwalifikowanych pracowników będzie wyższe niż na co dzień w przypadku ataków na IK, a zazwyczaj właściciele lub operatorzy IK zatrudniają odpowiednią liczbę osób do pracy w normalnych warunkach. W związku z tym zaleca się uwzględnienie w ochronie IK przygotowań do zwiększenia liczby pracowników w sytuacjach kryzysowych. Można to osiągnąć przez włączenie rezerwy personelu do realizacji planów obrony cywilnej.

Odporność społeczna ma również wymiar osobisty. Jeśli obywatele są w stanie wytrzymać okresy ograniczonej dostępności pewnych towarów lub usług, zarządzanie kryzysowe jest łatwiejsze, nawet jeśli wiąże się z drastycznymi decyzjami, takimi jak tymczasowe zawieszenie dostaw energii elektrycznej na pewnym obszarze w celu zasilania najważniejszych miejsc i stref lub innych form reglamentowania. Rozmieszczenie ponad 13 000 punktów pomocy w Ukrainie jest przykładem wspierania odporności społecznej. Dlatego też zaleca się uwzględnienie jej w ochronie IK.

Z uwagi na liczbę ataków konwencjonalnych na ukraińską sieć energetyczną i zastosowaną broń konieczne jest rozważenie ochrony IK w wymiarze militarnym. Ryzyko rosyjskich ataków konwencjonalnych oznacza, że niektóre środki łagodzące są poza zasięgiem operatorów IK. Należy

opracować zintegrowany, wielowarstwowy system obrony powietrznej, zdolny do zapobiegania atakom rakietowym i dronom. Jest to odpowiedzialność państwa i jego sił zbrojnych. Taki system musi być w stanie wykorzystywać broń niskiej i wysokiej klasy, zdolną do przechwytywania małych dronów, a także pocisków manewrujących i balistycznych. Planowanie wojskowe musi obejmować również kwestie ochrony IK, takie jak liczba i lokalizacja elektrowni oraz innych elementów sieci energetycznej, a także systemów uznanych za krytyczne (np. porty, kluczowe węzły systemu kolejowego lub inne obiekty).

Bibliografia

Biriukov D., Kondratov S., Nasvit O., Sukhodolia O., *Green Paper on Critical Infrastructure Protection in Ukraine. Analytical Report*, Kiev 2015.

Butowski P., *Russian Air Power*, 2023.

Depczyński M., Elak L., *Rosyjska sztuka operacyjna w zarysie*, Warszawa 2020.

Douhet G., *Panowanie w powietrzu. Przypuszczalne formy przyszłej wojny oraz ostatnie artykuły*, Warszawa 2013.

Glajzer M., *Irański oręż w rosyjskiej służbie*, „Nowa Technika Wojskowa" 2022, nr 11, s. 12–15.

Kofman M., *Russian airpower in context: The first year of war*, w: *The Air War in Ukraine – The First Year of Conflict*, D. Henriksen, J. Bronk (red.), New York 2025.

Kwasek T., *Lotnicze pociski skrzydlate rodziny Ch-59*, „Lotnictwo" 2024, nr 3.

Kwasek T., *Rakiety Putina. Rosyjskie lądowe, lotnicze i morskie systemy rakietowe oraz pociski manewrujące*, „Nowa Technika Wojskowa" 2023, numer specjalny: *Wojna rosyjsko-ukraińska*, s. 40–55.

Russia and Eurasia, „The Military Balance" 2022, t. 122, nr 1, s. 164–217. https://doi.org/10.1080/04597222.2022.2022930.

Strembski M., *Wojna powietrzna nad Ukrainą – grudzień 2023 r.*, „Lotnictwo" 2024, nr 1, s. 32–39.

Strembski M., *Wojna powietrzna nad Ukrainą – listopad 2024 r.*, „Lotnictwo" 2025, nr 1, s. 28–40.

Strembski M., *Wojna powietrzna nad Ukrainą – styczeń 2024 r.*, „Lotnictwo" 2024, nr 2, s. 14–20.

Strembski M., *Wojna powietrzna nad Ukrainą. Czerwiec 2024 r.*, „Lotnictwo" 2024, nr 7–8, s. 30–42.

Strembski M., *Wojna powietrzna nad Ukrainą. Maj 2024 r.*, „Lotnictwo" 2024, nr 6, s. 42–51.

Strembski M., *Wojna powietrzna nad Ukrainą. Sierpień 2024 r.*, „Lotnictwo" 2024, nr 10, s. 40–49.

Strembski M., *Wojna powietrzna nad Ukrainą. Wrzesień 2024 r.*, „Lotnictwo" 2024, nr 11, s. 21–35.

Źródła internetowe

Altman H., *Dam Destroyed, Accusations Fly, Waters Rise, War Plans Could Change*, The War Zone, 6.06.2023, https://www.twz.com/dam-destroyed-accusations-fly-waters-rise-war-plans-could-change [dostęp: 18.01.2025].

Axe D., *Ukrainian Helicopter Crews Are Shooting Down Russian Drones – Like World War II Turret Gunners*, Forbes, 22.08.2024, https://www.forbes.com/sites/davidaxe/2024/08/22/ukrainian-helicopter-crews-are-shooting-down-russian-drones-like-world-war-ii-turret-gunners/ [dostęp: 14.02.2025].

Chambers J., *Countering Gray-Zone Hybrid Threats. An Analysis of Russia's 'New Generation Warfare' and Implications for the US Army*, 2016, https://mwi.westpoint.edu/wp-content/uploads/2016/10/Countering-Gray-Zone-Hybrid-Threats.pdf [dostęp: 15.01.2025].

Cyber-Attack Against Ukrainian Critical Infrastructure, CISA, 20.07.2021, https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 [dostęp: 15.01.2025].

Explosion in Ukraine's Odessa Destroys Railroad Bridge but Misses Train, The Moscow Times, 13.05.2015, https://www.themoscowtimes.com/2015/05/13/explosion-in-ukraines-odessa-destroys-railroad-bridge-but-misses-train-a46507 [dostęp: 16.01.2025].

Giannopoulos G., Smith H., Theocharidou M., *The Landscape of Hybrid Threats: A Conceptual Model Public Version*, Publications Office of the European Union, Luxembourg 2021, https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf [dostęp: 15.01.2025].

Greenberg A., *How an Entire Nation Became Russia's Test Lab for Cyberwar*, Wired, 20.06.2017, https://www.wired.com/story/russian-hackers-attack-ukraine/ [dostęp: 18.01.2025].

Greenberg A., *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired, 22.08.2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [dostęp: 16.01.2025].

Harding L., Sabbagh D., Koshiw I., *Russia targets Ukraine energy and water infrastructure in missile attacks*, The Guardian, 31.10.2022, https://www.theguardian.com/world/2022/oct/31/russian-missiles-kyiv-ukraine-cities [dostęp: 5.02.2025].

Humpreys B.E., *Attacks on Ukraine's Electric Grid: Insights for U.S. Infrastructure Security and Resilience*, Congressional Research Service, 17.05.2024, https://crsreports.congress.gov/product/pdf/R/R48067 [dostęp: 8.02.2025].

Kh-55 (AS-15), Missile Threat, 23.04.2024, https://missilethreat.csis.org/missile/kh-55/ [dostęp: 12.02.2025].

Kh-47M2 Kinzhal, Missile Threat, 23.04.2024, https://missilethreat.csis.org/missile/kinzhal/ [dostęp: 12.02.2025].

Kh-101 / Kh-102, Missile Threat, 23.04.2024, https://missilethreat.csis.org/missile/kh-101-kh-102/ [dostęp: 12.02.2025].

Kofman M., Fink A., Gorenburg D., Chesnut M., Edmonds J., Waller J., *Russian Military Strategy: Core Tenets and Operational Concepts*, sierpień 2021, https://www.cna.org/reports/2021/08/Russian-Military-Strategy-Core-Tenets-and-Operational-Concepts.pdf [dostęp: 3.02.2025].

Major Ukraine gas pipeline hit by blast, BBC, 17.06.2014, https://www.bbc.com/news/world-europe-27891018 [dostęp: 16.01.2025].

Matuszak S., *Rosja destabilizuje system energetyczny Ukrainy*, Ośrodek Studiów Wschodnich, 11.10.2022, https://www.osw.waw.pl/pl/publikacje/analizy/2022-10-11/rosja-destabilizuje-system-energetyczny-ukrainy [dostęp: 5.02.2025].

Matuszak S., *Ukraina: poważny cios w energetykę*, Ośrodek Studiów Wschodnich, 28.03.2024, https://www.osw.waw.pl/pl/publikacje/analizy/2024-03-28/ukraina-powazny-cios-w-energetyke [dostęp: 5.02.2025].

Mendel J., *In Ukraine a Huge Ammunition Depot Catches Fire*, The New York Times, 27.09.2017, https://www.nytimes.com/2017/09/27/world/europe/ukraine-ammunition-depot-explosion.html?mcubz=0 [dostęp: 16.01.2025].

Miller M.E., Galouchka A., *Ukraine's drone hunters scramble to destroy Russia's Iranian–built fleet*, The Washington Post, 28.11.2022, https://www.washingtonpost.com/world/2022/11/28/ukraine-drone-hunters-mykolaiv-russia/ [dostęp: 13.02.2025].

Newdick T., *Ukraine Accuses Russia Of Blowing Up Another Dam*, The War Zone, 12.06.2023, https://www.twz.com/ukraine-accuses-russia-of-blowing-up-another-dam [dostęp: 18.01.2025].

Newdick T., *Ukraine's SA-8 Gecko 'FrankenSAM' Adapted To Fire Air-To-Air Missiles Seen In New Detail*, The War Zone, 12.12.2024, https://www.twz.com/land/ukraines-sa-8-gecko-frankensam-adapted-to-fire-air-to-air-missiles-seen-in-new-detail [dostęp: 14.02.2025].

Perlroth N., Scott M., Frenkel S., *Cyberattack Hits Ukraine Then Spreads Internationally*, The New York Times, 27.06.2017, https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html [dostęp: 16.01.2025].

There are almost 13 thousand Invincibility Points in Ukraine, UNN, 3.04.2024, https://unn.ua/en/news/there-are-almost-13-thousand-invincibility-points-in-ukraine [dostęp: 13.02.2025].

3M-14 Kalibr (SS-N-30A), Missile Threat, 23.04.2024, https://missilethreat.csis.org/missile/ss-n-30a/ [dostęp: 12.02.2025].

Trevithick J., *'FrankenSAM' Systems Are Now Shooting Down Drones In Ukraine*, The War Zone, 17.01.2024, https://www.twz.com/frankensam-systems-are-now-shooting-down-drones-in-ukraine [dostęp: 14.02.2025].

Trevithick J., *Containerized SAM System That Fires Soviet Air-To-Air Missiles For Ukraine Breaks Cover*, The War Zone, 12.02.2025, https://www.twz.com/land/containerized-sam-system-that-fires-soviet-air-to-air-missiles-for-ukraine-breaks-cover [dostęp: 14.02.2025].

Ukraine ammo dump blasts blamed on 'possible sabotage', BBC, 9.10.2018, https://www.bbc.co.uk/news/world-europe-45794963 [dostęp: 16.01.2025].

Ukraine power cut 'was cyber-attack', BBC News, 11.01.2017, https://www.bbc.co.uk/news/technology-38573074 [dostęp: 15.01.2025].

Ukraine's Energy Security and the Coming Winter, IEA, wrzesień 2024, https://iea.blob.core.windows.net/assets/cec49dc2-7d04-442f-92aa-54c18e6f51d6/UkrainesEnergySecurityandtheComingWinter.pdf [dostęp: 9.02.2025].

Warden III J.A., *The Enemy as System*, „Airpower Journal" 1995, t. 9, nr 1, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-09_Issue-1-Se/1995_Vol9_No1.pdf, s. 41–55 [dostęp: 1.02.2025].

Watling J., Reynolds N., *Operation Z. The Death Throes of an Imperial Delusion*, 22.04.2022, https://static.rusi.org/special-report-202204-operation-z-web.pdf [dostęp: 18.01.2025].

Watling J., Reynolds N., *The Plot to Destroy Ukraine*, 15.02.2022, https://static.rusi.org/special-report-202202-ukraine-web.pdf [dostęp: 17.01.2025].

Wilk A., Żochowski P., *Dziesiąty zmasowany ostrzał Ukrainy. 309. dzień wojny*, Ośrodek Studiów Wschodnich, 30.12.2022, https://www.osw.waw.pl/pl/publikacje/analizy/2022-12-30/dziesiaty-zmasowany-ostrzal-ukrainy-309-dzien-wojny [dostęp: 5.02.2025].

Wilk A., Żochowski P., *Ukraina bez prądu. 265. dzień wojny*, Ośrodek Studiów Wschodnich, 16.11.2022, https://www.osw.waw.pl/pl/publikacje/analizy/2022-11-16/ukraina-bez-pradu-265-dzien-wojny [dostęp: 5.02.2025].

Zaniewicz M., *Ukraine in Darkness: Preventing the Worst-Case Scenario for Its Energy System*, Forum Energii, 1.07.2024, https://www.forum-energii.eu/en/ukraine-destroyed-system [dostęp: 7.02.2025].

Akty prawne

Закон України про критичну інфраструктуру (Відомості Верховної Ради України (ВВР), 2023, № 5, ст. 13) – [*Zakon Ukrajiny pro krytycznu infrastrukturu* (Widomosti Werchownoji Rady Ukrajiny (WWR), 2023, № 5, st. 13)], https://zakon.rada.gov.ua/laws/show/1882-20#Text [dostęp: 17.01.2025].

Dr Michał Piekarski

Adiunkt w Zakładzie Studiów nad Bezpieczeństwem Instytutu Studiów Międzynarodowych i Bezpieczeństwa Uniwersytetu Wrocławskiego. Zajmuje się analizą zjawiska wojny hybrydowej w Europie, współczesnego terroryzmu, problematyką bezpieczeństwa morskiego państwa oraz zagadnieniami z zakresu kultury strategicznej Polski. Uczestnik prac zespołów międzyresortowych oraz grup roboczych administracji państwowej, których zadaniem było budowanie odporności na zagrożenia terrorystyczne oraz hybrydowe obiektów strategicznych dla bezpieczeństwa państwa oraz infrastruktury krytycznej.

Kontakt: michal.piekarski@uwr.edu.pl