

POLSKIE
TOWARZYSTWO
BEZPIECZEŃSTWA
NARODOWEGO



Polskie
Towarzystwo
Bezpieczeństwa
Narodowego

ROSYJSKIE ATAKI
MILITARNE NA UKRAINĘ
I DZIAŁANIA WOJENNE
WYMIERZONE
W INFRASTRUKTURĘ
SIECI ENERGETYCZNYCH
(2022–2024)

RAPORT PTBN
TOM V (2025)
WYDANIE SPECJALNE

ISSN 2720-037X | E-ISBN 978-83-962605-7-4



*This project
is supported by:*

The NATO Science for Peace
and Security Programme

ROSYJSKIE ATAKI MILITARNE NA UKRAINĘ I DZIAŁANIA WOJENNE WYMIERZONE W INFRASTRUKTURĘ SIECI ENERGETYCZNYCH (2022–2024)

Raport PTBN

Tom V (2025)

WYDANIE SPECJALNE



Polskie
Towarzystwo
Bezpieczeństwa
Narodowego

Warszawa • 2025

© Copyright by Polskie Towarzystwo Bezpieczeństwa Narodowego

Raport PTBN. Wydanie specjalne, Tom V (2025): „Rosyjskie ataki militarne na Ukrainę i działania wojenne wymierzone w infrastrukturę sieci energetycznych (2022–2024)”

Raport PTBN. Wydanie specjalne, Tom V (2025) został opublikowany w ramach projektu R-GRID: Algorytmy sztucznej inteligencji do przewidywania zagrożeń i ochrony sieci elektroenergetycznych [G6249], sfinansowanego w ramach Programu NATO „Nauka dla Pokoju i Bezpieczeństwa”.

Opracowany przez zespół w składzie:

Dr Marcin Lipka

Dr Michał Piekarski

Treść Raportu PTBN zawiera wyłącznie prywatne poglądy autorów i nie mogą być one utożsamiane z instytucjami, w których autorzy są zatrudnieni.

Raport PTBN. Wydanie specjalne, Tom V (2025): „Rosyjskie ataki militarne na Ukrainę i działania wojenne wymierzone w infrastrukturę sieci energetycznych (2022–2024)” został zamknięty 23 grudnia 2025 r. Wersja online jest jego wersją pierwotną.

Autorem fotografii znajdującej się na okładce jest www.shutterstock.com/anto4ka.

Wersja online czasopisma jest dostępna na stronie www.PTBN.online

ISSN 2720-037X

e-ISBN 978-83-962605-7-4

Polskie Towarzystwo Bezpieczeństwa Narodowego

(KRS 0000583118)

ul. Odkryta 38A/8, 03-140 Warszawa

e-mail: zarzad@ptbn.online

<https://ptbn.online>



9 788396 260574

Spis treści

1.	Wojskowe siły i środki wykorzystane do opanowania infrastruktury krytycznej na Krymie w 2014 r.	7
1.1.	Aneksja Krymu jako paradygmat wojny hybrydowej	7
1.2.	Identyfikacja Sił Zbrojnych	9
1.3.	Analiza klastrów infrastruktury krytycznej i taktyki przejęcia	13
1.4.	Środki niekinetyczne i wojna informacyjna – mnożniki siły	20
1.5.	Środki techniczne i wyposażenie „zielonych ludzików”	23
	Wnioski	26
2.	Wojskowe siły i środki wykorzystywane do atakowania infrastruktury energetycznej Ukrainy	28
2.1.	Ewolucja paradygmatu wojny od starć kinetycznych do hybrydowej wojny systemowej	28
2.2.	Nexus energetyczno-zasobowo-klimatyczny	29
2.3.	Cele operacyjne i strategiczne Federacji Rosyjskiej	30
2.4.	Architektura Sił Zbrojnych Federacji Rosyjskiej w kampanii powietrznej	31
2.5.	Arsenał środków napadu powietrznego	33
2.6.	Taktyka i operacjonalizacja: od „dezorganizacji” do „anihilacji”	35
	Wnioski	37

3.	Metody ochrony infrastruktury energetycznej w Ukrainie w latach 2022–2024	39
3.1.	Paradygmat bezpieczeństwa energetycznego w warunkach wojny totalnej	39
3.2.	Podstawy teoretyczne: analiza ryzyka sabotażu i modelowanie zagrożeń	40
3.3.	Inżynierska ochrona pasywna: system trzystopniowy	41
3.4.	Systemy aktywnej obrony i walka elektroniczna (WRE)	44
3.5.	Decentralizacja i koncepcja „wysp energetycznych”	45
	Wnioski	46
4.	Rosyjska sztuka wojskowa wobec potencjalnych ataków militarnych na infrastrukturę energetyczną państw trzecich – perspektywa 2025–2030	47
4.1.	Ewolucja doktrynalna i ramy strategiczne rosyjskiej sztuki wojennej	47
4.2.	Operacjonalizacja zagrożeń kinetycznych – domena podwodna i morska	50
4.3.	Domeny niekinetyczne	53
4.4.	Walka Elektroniczna (WRE) – zagrożenie dla synchronizacji sieci	55
4.5.	Wojna informacyjna i kognitywna	56
4.6.	„Gig Economy” sabotażu i hybrydowe proxy	56
	Wnioski	58
5.	Scenariusze ataków militarnych na infrastrukturę energetyczną w Ukrainie a bezpieczeństwo krajów NATO	60
5.1.	Redefinicja frontu w wojnie systemowej	60
5.2.	Ewolucja rosyjskiej sztuki operacyjnej wobec infrastruktury energetycznej – lekcje z Ukrainy	61

5.3. Strategia anihilacji (2022–2024) – ewolucja od dezorganizacji do zniszczenia systemowego	61
5.4. Wojskowe i hybrydowe środki rażenia infrastruktury w arsenale rosyjskim	62
5.5. Podatności infrastruktury energetycznej państw NATO	65
5.6. Scenariusze ataków na kraje NATO (Perspektywa 2025–2030)	66
5.7. Odpowiedź NATO i rekomendacje	68
5.8. Rekomendacje dla decydentów	69
Wnioski	70
 Bibliografia	 72
 Autorzy	 87
 O programie NATO Nauka dla Pokoju i Bezpieczeństwa (SPS)	 89
 O projekcie R-GRID	 89
 O Polskim Towarzystwie Bezpieczeństwa Narodowego	 91
 O Ukraińskim Instytucie Przyszłości	 91
 O IDEAS NCBR	 92
 O Laurea University of Applied Sciences	 93

1. Wojskowe siły i środki wykorzystane do opanowania infrastruktury krytycznej na Krymie w 2014 r.

1.1. Aneksja Krymu jako paradygmat wojny hybrydowej

Operacja aneksji Krymu przez Federację Rosyjską w 2014 roku nie była tradycyjną inwazją wojskową. Stanowi ona jeden z najbardziej zaawansowanych i precyzyjnie zaplanowanych przykładów zastosowania strategii współczesnej wojny hybrydowej¹, określanej w rosyjskiej myśli wojskowej również jako „wojna nowej generacji” lub „wojna nieliniowa”². Proces ten, zrealizowany w sposób wieloetapowy i kompleksowy, obejmował skoordynowane działania o charakterze politycznym, militarnym, informacyjnym oraz psychologicznym. Ta synergia działań pozwoliła na de facto przejęcie kontroli nad Półwyspem Krymskim przy minimalnym oporze kinetycznym ze strony państwa ukraińskiego i ograniczonej reakcji społeczności międzynarodowej, tworząc strategiczny fakt dokonany.

Infrastruktura krytyczna (IK) Półwyspu Krymskiego nie była celem pobocznym czy przypadkowym, lecz stanowiła strategiczne centrum ciężkości (ang. *center of gravity*)³ całej rosyjskiej operacji. Zgodnie z doktrynalnym rozumieniem zagrożeń

¹ M. Strzelecki, *Uprzejmi ludzie czy zielone ludziki? Siły Operacji Specjalnych Ministerstwa Obrony Federacji Rosyjskiej*, „Bezpieczeństwo. Teoria i Praktyka” 2017, nr 3, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego w Krakowie, s. 407–413.

² J.R. Haines, *How, Why, and When Russia Will Deploy Little Green Men – and Why the US Cannot*, <https://www.fpri.org/article/2016/03/how-why-and-when-russia-will-deploy-little-green-men-and-why-the-us-cannot>, [dostęp: 10.11.2025].

³ Nawiązanie do klasycznej teorii Carla von Clausewitza, zawartej w jego dziele „O wojnie”, definiuje centrum ciężkości jako punkt, w którym skupia się największa masa sił i stanowi cel o największym znaczeniu strategicznym.

hybrydowych, działania wymierzone w IK mają na celu nie tylko jej fizyczne zniszczenie⁴, ale także „pogorszenie jakości oferowanych towarów i usług”, „zniszczenie kluczowych części infrastruktury” oraz „ograniczenie lub usunięcie możliwości dywersyfikacji dostaw dóbr i usług oraz powodować jednostronną zależność od wrogiego podmiotu”⁵. Operacja krymska była jednak jakościowym rozwinięciem tych koncepcji, przenosząc je ze sfery tajnych działań destabilizacyjnych do poziomu zintegrowanej operacji wojskowej.

Aneksja Krymu nie była improwizowaną reakcją na kryzys polityczny w Kijowie (Euromajdan). Przeciwnie stanowiła pierwszy, dojrzały test doktrynalny nowo zreformowanych rosyjskich sił zbrojnych, a w szczególności nowo utworzonego, strategicznego narzędzia – Sił Operacji Specjalnych (SOS MOFR, ros. CCO MO PΦ). Proces tworzenia tych sił był długi i obciążony problemami, sięgając koncepcyjnie wczesnych lat 90. XX w. Jednak ich formalne ogłoszenie przez Szefa Sztabu Generalnego gen. Walerija Gierasimowa nastąpiło zaledwie rok przed aneksją, 6 marca 2013 roku. Zabezpieczenie Zimowych Igrzysk Olimpijskich w Soczi (luty 2014) było w tym kontekście prawdopodobnie operacyjną „rozgrzewką” i strategicznym pozycjonowaniem sił w regionie⁶. Analizy ekspertów potwierdzają, że operacja krymska była pierwszą dużą operacją, w której nowe Dowództwo Sił Operacji Specjalnych (DSOS, ros. KCCO) „odegrało wiodącą rolę”⁷. W związku z tym kryzys w Ukrainie stał się dogodnym pretekstem do przeprowadzenia zaplanowanej operacji, mającej na celu przetestowanie w warunkach bojowych nowej doktryny i nowego narzędzia do realizacji celów politycznych za pomocą precyzyjnych metod hybrydowych.

⁴ Infrastruktura jako strategiczny cel wynika z modelu zaproponowanego przez pułkownika Johna Wardena. Teoria ta identyfikuje infrastrukturę jako jeden z pięciu kluczowych systemów, które można zaatakować w celu osiągnięcia paraliżu strategicznego. Warden wskazuje, że degradacja infrastruktury zmniejsza zdolność przeciwnika do oporu. J.F. Birchmeier, *The Reliability of Warden's Theory on the Use of Air Power*, School of Advanced Military Studies 2000, s. 6–7.

⁵ M. Piekarski, *Infrastruktura krytyczna jako cel ataków hybrydowych i konwencjonalnych. Wnioski z ukraińskich doświadczeń* „Terroryzm – Studia, Analizy, Prewencja” 2025, s. 117–118.

⁶ M. Strzelecki, dz. cyt., s. 385–408.

⁷ T. Bukkvoll, *Russian Special Operations Forces in Crimea and Donbas*, „Parameters” 2016, Vol. 46, No. 2, The US Army War College Quarterly: Parameters, <https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2917&context=parameters>, [dostęp: 11.11.2025].

1.2. Identyfikacja Sił Zbrojnych

Sukces operacji krymskiej był możliwy dzięki zastosowaniu wielowarstwowej struktury sił, w której każda formacja miała precyzyjnie zdefiniowaną rolę – od tajnej awangardy po konwencjonalne siły blokujące.

Siły Operacji Specjalnych (SOS MOFR) – „uprzejmi ludzie” jako awangarda

Głównym aktorem kinetycznym, odpowiedzialnym za precyzyjne przejęcia kluczowych obiektów IK, były Siły Operacji Specjalnych Ministerstwa Obrony Federacji Rosyjskiej (SOS MOFR).

Identyfikacja

Siły te, działające bez oznaczeń państwowych, zyskały w mediach miano „zielonych ludzików” (ros. *зеленые человечки*) oraz „uprzejmych ludzi” (ros. *вежливые люди*)⁸. Sama Federacja Rosyjska oficjalnie potwierdziła ich rolę, gdy 26 lutego 2015 roku prezydent Władimir Putin podpisał dekret ustanawiający dzień 27 lutego – data zajęcia parlamentu w Symferopolu – „Dniem Sił Operacji Specjalnych”. W skład Sił Operacji Specjalnych wchodził elitarni, zawodowi żołnierze rosyjskich sił zbrojnych⁹.

Struktura Dowodzenia (KSSO)

W przeciwieństwie do tradycyjnych jednostek SpecNazu Głównego Zarządu Wywiadowczego (GRU), które były operacyjnie podporządkowane dowództwom Okręgów Wojskowych, SOS MOFR (KSSO) stanowiły niezależny, samodzielny rodzaj wojsk o statusie operacyjno-strategicznym. Podlegały one bezpośrednio Szefowi Sztabu Generalnego SZ FR (w 2014 roku gen. Walerijowi Gierasimowowi) i Ministrowi Obrony (Siergiejowi Szojgu)¹⁰. Taka struktura dowodzenia zapewniła Kremlowi bezpośrednio, elastyczne i szybko reagujące narzędzie do prowadzenia działań polityczno-wojskowych, przy jednoczesnym zachowaniu wysokiego stopnia maskirowki¹¹ i możliwości politycznego zaprzeczenia („wiarygodnej zaprzeczalności”)¹².

⁸ J.R. Haines, dz. cyt.

⁹ M. Strzelecki, dz. cyt., s. 390.

¹⁰ Tamże, s. 383–413.

¹¹ Maskowanie operacyjne – maskirowka (ros. *маскировка*).

¹² T. Bukkvoll, dz. cyt., s. 13–21.

Kluczowe Jednostki Operacyjne (Filary KSSO)

Dowództwu KSSO podlegały wyspecjalizowane Centra Specjalnego Przeznaczenia (CSP, ros. ЦСН). W operacji krymskiej kluczową rolę odegrały dwa z nich, reprezentujące odmienne filozofie operacyjne:

1. CSP „Sienieź” (JW 92154). Jednostka ta stacjonowała w Sołnechnogorsku, stanowiła historyczny trzon KSSO. Została sformowana w 1999 roku jako Centrum Szkolenia Specjalistów GRU i stała się bazą dla formowania Dowództwa SOS MOFR. Jej operatorzy, znani pod nieoficjalną nazwą „Słoneczniki” (ros. Подсолнухи), wywodzili się z tradycji wojskowego SpecNazu GRU. Wskazuje to na ich specjalizację w klasycznych zadaniach wojskowych operacji specjalnych: rozpoznaniu specjalnym dalekiego zasięgu, dywersji oraz działaniach w terenie górskim i powietrznodesantowym¹³.
2. CSP „Kubinka-2” (JW 01355, „Zapłocie”). Była to nowsza jednostka, utworzona pod koniec pierwszej dekady XXI wieku. Jej formowanie odbywało się przy znaczącym udziale kadry oficerskiej wywodzącej się z Centrum Specjalnego Przeznaczenia Federalnej Służby Bezpieczeństwa (CSP FSB), w tym z elitarnego Zarządu „A” (Alfa). Nadało to „Kubince-2” unikalną specjalizację, zorientowaną przede wszystkim na działania szturmowe w terenie zurbanizowanym i skomplikowane operacje kontrterrorystyczne (CQB/CT)¹⁴. Dowody wizualne (analiza fotografii) silnie sugerują obecność operatorów KSSO, pasujących do profilu „Kubinki-2”, podczas operacji szturmowej na bazę lotniczą Belbek¹⁵.

Ta podwójna kultura organizacyjna KSSO, łącząca tradycje wojskowego GRU („Sienieź”) i policyjno-szturmowe FSB („Kubinka-2”), stanowiła kluczowy mnożnik siły. Pomimo początkowych napięć między jednostkami, wynikających z odmiennych filozofii szkoleniowych¹⁶, Dowództwo KSSO dysponowało elastycznym „menu” zdolności. Mogło elastycznie dobierać siły do charakteru celu: operatorzy „Sienieża” prawdopodobnie odpowiadali za tajne rozpoznanie, ciche przejęcia obiektów i koordynację

¹³ M. Strzelecki, dz. cyt., s. 395–398.

¹⁴ Tamże, s. 398–400.

¹⁵ Presumably SSO Special Purpose Center Kubinka-2 Operators in Belbek during the 2014 Crimea Annexation. Note the Asian Operator in the Middle. If my buddy told it right he is Tuvan and he still serves in thar Unit to this day: r/SpecOpsArchive – Reddit, https://www.reddit.com/r/SpecOpsArchive/comments/1eufpqx/presumably_sso_special_purpose_center_kubinka2, [dostęp: 10.11.2025].

¹⁶ M. Strzelecki, dz. cyt., s. 399.

z lokalnymi aktywami, podczas gdy operatorzy „Kubinki-2” zostali wykorzystani do przeprowadzenia precyzyjnego, siłowego szturmu na ufortyfikowany cel wojskowy (Belbek)¹⁷. Ta wewnętrzna specjalizacja pozwoliła KSSO na efektywne działanie w całym spektrum zadań specjalnych, od głębokiej maskirowki po bezpośrednią akcję.

Siły wsparcia i jednostki konwencjonalne (masa i maskowanie)

Operacja krymska nie była prowadzona wyłącznie przez KSSO. Sukces zapewniła zintegrowana, trójwarstwowa struktura sił, wspierana przez czysto dezinformacyjną „warstwę zero”.

Warstwa 1 (awangarda / przełamanie)

Jak opisano powyżej, były to elitarne jednostki KSSO („Sienież” i „Kubinka-2”), odpowiedzialne za pierwotne, kluczowe i najbardziej wrażliwe politycznie uderzenia na infrastrukturę polityczną (parlament) i transportową (lotniska)¹⁸.

Warstwa 2 (wsparcie specjalne / szybkie wzmocnienie)

KSSO było natychmiast wspierane przez inne jednostki sił specjalnych i elitarnych, które zapewniły masę niezbędną do utrzymania zdobytych obiektów i szybkiego rozszerzenia kontroli.

- SpecNaz GRU: KSSO było wspierane przez jednostki SpecNazu GRU¹⁹. Zidentyfikowane dane wskazują na rozmieszczenie na Krymie elementów z co najmniej czterech brygad SpecNazu oraz 25 Pułku SpecNazu²⁰.
- Wojska Powietrznodesantowe (WDW): kluczową rolę odegrał elitarny 45 Samodzielny Pułk SpecNazu WDW stacjonujący w Kubince²¹. Jako siły szybkiego reagowania, WDW zapewniły natychmiastowe wzmocnienie sił KSSO i zabezpieczenie zdobytych przyczółków, zwłaszcza na lotniskach.

¹⁷ Presumably SSO Special Purpose Center, dz. cyt.

¹⁸ T. Bukkvoll, dz. cyt., s. 13–21.

¹⁹ Tamże.

²⁰ Russian annexation of Crimea – Wikipedia, https://en.wikipedia.org/wiki/Russian_annexation_of_Crimea, [dostęp: 10.11.2025].

²¹ T. Bukkvoll, dz. cyt., s. 13–21.

Warstwa 3 (masa / siły blokujące)

Był to kluczowy element konwencjonalny, który umożliwił neutralizację głównych sił ukraińskich na półwyspie. Na Krymie legalnie stacjonowało ok. 12 000 żołnierzy Floty Czarnomorskiej²². Trzon sił lądowych tej floty stanowiła 810 Samodzielna Brygada Piechoty Morskiej z Sewastopola²³. To właśnie te jednostki, w tym 382 Batalion Piechoty Morskiej²⁴, dysponujące ciężkim sprzętem, takim jak transportery opancerzone BTR, realizowały główne zadanie blokowania (a nie szturmowania) ukraińskich garnizonów²⁵. Ich jawna obecność, choć wciąż bez rosyjskich flag, tworzyła kordon uniemożliwiający jakąkolwiek skoordynowaną reakcję militarną ze strony Ukrainy.

Warstwa Zero (osłona informacyjna / PSYOPS)

Tak zwane „siły samoobrony Krymu”²⁶, rzekomo składające się z lokalnych mieszkańców, nie były niezależnym aktorem ani realną siłą bojową. Analizy operacji opisują je jednoznacznie jako „dekorację” (ang. *décor*)²⁷, „rosyjskich dywersantów” i „współpodróżników”²⁸, mające na celu jedynie „zapewnienie lokalnego wizerunku”. W przedstawionym modelu wielowarstwowym, „samoobrona” stanowiła „Warstwę Zero” – była to czysto informacyjna osłona (maskirowka). Pozwalało to rosyjskiej propagandzie i prominentom (w tym prezydentowi Putinowi) na zaprzeczanie zaangażowaniu militarnemu²⁹, podczas gdy rzeczywiste, profesjonalne warstwy wojskowe (KSSO, WDW/GRU, Piechota Morska) działały bez przeszkód, realizując precyzyjny plan operacyjny.

²² M. Kofman i in., *Lessons from Russia's Operations in Crimea and Eastern Ukraine*, RAND 2017, s. 6, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1498/RAND_RR1498.pdf, [dostęp: 10.11.2025].

²³ Russian annexation of Crimea..., dz. cyt.

²⁴ Russian Naval Infantry – Wikipedia, https://en.wikipedia.org/wiki/Russian_Naval_Infantry, [dostęp: 10.11.2025].

²⁵ A. Wilk, *Russian military intervention in Crimea*, <https://www.osw.waw.pl/en/publikacje/analyses/2014-03-05/russian-military-intervention-crimea>, [dostęp: 10.11.2025].

²⁶ M. Strzelecki, dz. cyt., s. 392, 411.

²⁷ T. Bukkvoll, dz. cyt., s. 16–17.

²⁸ P.A. Kaber, *Russian military buildup in Crimea & destabilization of the Black Sea region*, <https://vm.ee/en/media/283/download>, [dostęp: 10.11.2025].

²⁹ J.R. Haines, dz. cyt.

1.3. Analiza klastrów infrastruktury krytycznej i taktyki przejścia

Operacja rosyjska była precyzyjnie ukierunkowana na kluczowe klastry infrastruktury krytycznej, których przejście gwarantowało całkowitą kontrolę nad półwyspem.

Opanowanie infrastruktury polityczno-administracyjnej (władza)

Studium przypadku: Symferopol (27 lutego 2014). Cel: strategiczna dekapitacja polityczna Autonomicznej Republiki Krymu i natychmiastowa instalacja rządu marionetkowego. Chronologia: operacja rozpoczęła się w godzinach przedświt, około 4:30 czasu lokalnego. Taktyka: grupa operatorów KSSO⁵⁰, działających z chirurgiczną precyzją, jednocześnie zajęła budynki Rady Najwyższej (parlamentu) i Rady Ministrów (rządu) ARK w Symferopolu⁵¹. Był to szybki szturm w stylu kontrterrorystycznym (co może wskazywać na prawdopodobny udział specjalistów z CSP „Kubinka-2”). Wykorzystano granaty hukowo-błyskowe, aby zneutralizować ochronę⁵². Kluczowym czynnikiem sukcesu był fakt, że nieliczni ukraińscy strażnicy nie stawiali oporu lub, jak wskazują źródła, aktywnie współpracowali z napastnikami. Natychmiast po zajęciu budynków, pod lufami operatorów KSSO, prorosyjscy deputowani zostali zmuszeni do przeprowadzenia głosowania, które mianowało Siergieja Aksionowa nowym premierem⁵³. W ten sposób w ciągu kilku godzin „zalegalizowano” przejście władzy.

Neutralizacja infrastruktury transportowej i logistycznej (mobilność)

Cel: całkowita izolacja operacyjna półwyspu, uniemożliwienie przerzutu ukraińskich posiłków z kontynentu oraz zabezpieczenie korytarzy dla przerzutu dodatkowych sił rosyjskich.

⁵⁰ T. Bukkvoll, dz. cyt.

⁵¹ Capture of the Crimean Parliament – Wikipedia, https://en.wikipedia.org/wiki/Capture_of_the_Crimean_Parliament, [dostęp: 15.11.2025].

⁵² *Ukraine: Gunmen seize Crimea government buildings*, <https://www.bbc.co.uk/news/world-europe-26364891>, [dostęp: 15.11.2025].

⁵³ M. Strzelecki, dz. cyt., s. 383–413.

Lotniska (28 lutego 2014)

- Lotnisko cywilne (Symferopol): przejęcie tego obiektu było mistrzowskim przykładem operacji psychologicznej. Terminal został zabezpieczony przez „uprzejmych ludzi” (KSSO), jednak operację przeprowadzono w taki sposób, aby nie zaburzyć codziennego toku pracy portu lotniczego³⁴. Miało to na celu uniknięcie paniki wśród ludności cywilnej i wzmocnienie rosyjskiej narracji o „pokojowej stabilizacji”, a nie wrogiej inwazji.
- Baza Lotnicza Belbek (Sewastopol): był to kluczowy obiekt wojskowy, siedziba ukraińskiej Brygady Lotnictwa Taktycznego³⁵. Początkowo (ok. 28 lutego) baza została zablokowana przez siły KSSO. Ostateczny szturm nastąpił 22 marca 2014 roku. Była to operacja połączona: operatorzy KSSO (prawdopodobnie z „Kubinki-2”) sforsowali bramy i budynki, wspierani przez transportery opancerzone BTR-82A, które przełamały betonowe ogrodzenie³⁶.

Węzły komunikacyjne

Równoległe do działań KSSO, siły Warstwy 3 (głównie Piechota Morska i WDW) przejęły pełną kontrolę nad kluczowymi węzłami drogowymi, przeprawami oraz terminalem promowym w Kerczu. Odcięło to Krym od lądowej Ukrainy i jednocześnie otworzyło główną arterię logistyczną dla masowego przetrzutu rosyjskich wojsk z Terytorium Krasnodarskiego. Rosyjskie statki desantowe dostarczyły około 10 tys. żołnierzy i sprzętu do 7 marca 2014 roku. Transport przez przeprawę Kerczeńską stanowił główną arterię logistyczną dla przetrzutu sił rosyjskich z Terytorium Krasnodaru³⁷.

Przejęcie kontroli nad strefą cyfrową – atak na infrastrukturę telekomunikacyjną

Atak na infrastrukturę telekomunikacyjną był wieloetapowy i obejmował działania kinetyczne, cybernetyczne oraz korporacyjne. Był to priorytetowy cel operacji,

³⁴ Tamże, s. 383–413.

³⁵ M. Kofman i in., *Lessons from Russia's Operations...*, dz. cyt.

³⁶ H. Coynash, *At least 22 Ukrainian websites blocked in Russian-occupied Crimea*, <https://archive.khpg.org/en/1501768045>, [dostęp: 15.11.2025]; *New generation warfare* – Wikipedia, https://en.wikipedia.org/wiki/New_generation_warfare, [dostęp: 15.11.2025].

³⁷ A. Wilk, dz. cyt.

zgodny z doktryną wojny nowej generacji, gdzie dominacja w sferze informacyjnej jest warunkiem zwycięstwa³⁸.

Faza 1: neutralizacja fizyczna i kinetyczna (luty–marzec 2014)

Pierwszym krokiem było fizyczne przejęcie kontroli nad nadajnikami i węzłami sieci. Działania te były prowadzone przez siły KSSO i działające pod ich kontrolą bojówki „samoobrony”.

1. Przejęcie ośrodków RTV: jednym z pierwszych celów były państwowe i prywatne centra radiowo-telewizyjne³⁹. Już na początku marca rosyjskie siły przejęły kontrolę nad państwowym nadajnikiem w Symferopolu⁴⁰ i rozpoczęły proces wyłączenia ukraińskich kanałów. Prywatna stacja Chornomorska TV została zdjeta z anteny, a jej częstotliwość natychmiast przejął rosyjski państwowy kanał propagandowy Rossiya 24. W sierpniu 2014 roku proces ten sfinalizowano, gdy policja i komornicy weszli do siedziby stacji, konfiskując cały sprzęt i pieczętując budynek⁴¹.
2. Przejęcie infrastruktury operatorów: równolegle, już 28 lutego 2014 roku, „nieznani osobnicy” zajęli obiekty kluczowego ukraińskiego operatora telekomunikacyjnego, Ukrtelecom JSC⁴².
3. Chirurgiczne ataki kinetyczne: w tym sektorze, w przeciwieństwie do energetyki, odnotowano celowe ataki kinetyczne. Raport Ukrtelecom z 28 lutego 2014 roku mówił, że „nieznane działania fizycznie uszkodziły kilka kluczowych magistral światłowodowych” łączących półwysep z resztą Ukrainy⁴³. Nie była to przypadkowa awaria, lecz precyzyjne, chirurgiczne cięcia, mające na celu

³⁸ New generation warfare..., dz. cyt.

³⁹ H. Coynash, *Back in the USSR: Russia uses Soviet methods to jam Ukrainian media in occupied Crimea*, <https://khp.org/en/1532985118>, [dostęp: 11.11.2025].

⁴⁰ J. Derleth, *Russian New Generation Warfare Deterring and Winning at the Tactical Level*, <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2020/Derleth-New-Generation-War>, [dostęp: 11.11.2025].

⁴¹ I. Chalupa, *Kremlin Silences Crimea's Last Pro-Ukraine TV Station*, <https://www.atlanticcouncil.org/blogs/ukrainealert/kremlin-silences-crimea-tv>, [dostęp: 11.11.2025].

⁴² J. Rivera, *Has Russia Begun Offensive Cyberspace Operations in Crimea?*, <https://georgetownsecuritystudiesreview.org/2014/03/02/has-russia-begun-offensive-cyberspace-operations-in-crimea>, [dostęp: 11.11.2025].

⁴³ Tamże.

fizyczne odcięcie Krymu od ukraińskiej infosfery i uniemożliwienie Kijowowi technicznego zarządzania siecią.

Faza 2: ataki cybernetyczne i operacje informacyjne

Równolegle do działań fizycznych, Rosja uruchomiła zmasowaną kampanię w cyberprzestrzeni, która miała charakter wspierający i destabilizujący⁴⁴:

1. Ataki DDoS: przeprowadzono ataki typu Distributed Denial of Service (DDoS) na strony internetowe ukraińskiego rządu, mediów oraz organizacji tatarskich, aby zakłócić przepływ informacji.
2. Ataki na telefonię: zastosowano ataki na telefonię IP, polegające na masowym, automatycznym generowaniu tysięcy połączeń i wiadomości tekstowych na telefony komórkowe ukraińskich parlamentarzystów i urzędników. Celem było zapchanie linii i uniemożliwienie im koordynacji działań w krytycznych godzinach przejęcia władzy.
3. Operacje psychologiczne: wykorzystano platformy mediów społecznościowych (Facebook, Vkontakte, Odnoklassniki) do siania paniki, dezinformacji i szerzenia prorosyjskich narracji.

Faza 3: przejście techniczne i korporacyjne (po aneksji)

Po fizycznym i cyfrowym odcięciu Krymu, Rosja przystąpiła do ostatniej fazy: trwałego przejścia technicznego i korporacyjnego:

1. Przekierowanie ruchu (Rerouting): celem było całkowite odłączenie Krymu od ukraińskiego segmentu Internetu i przyłączenie go do „Runetu”⁴⁵.
2. Rola „Miranda-Media”: w tym celu utworzono (w lipcu 2014 r.) operatora „Miranda-Media”, spółkę-córkę rosyjskiego giganta Rostelecom. Pierwszym zadaniem firmy była budowa nowego kabla światłowodowego przez Cieśninę Kerczeńską,

⁴⁴ M. Holloway, *How Russia Weaponized Social Media in Crimea*, <https://thestrategybridge.org/the-bridge/2017/5/10/how-russia-weaponized-social-media-in-crimea>, [dostęp: 11.11.2025].

⁴⁵ *How Occupation regimes Take Over the Information Space*, <https://splintercon.net/wp-content/uploads/2024/01/how-occupation-regimes-take-over-the-information-space.pdf>, [dostęp: 11.11.2025]; M. Holloway, dz. cyt.

aby fizycznie zintegrować Krym z rosyjską siecią⁴⁶. Już w lipcu 2014 roku sieć (ASN) Miranda-Media była widoczna jako dostawca dla sieci krymskich⁴⁷.

3. Wywłaszczenie i konsolidacja: do maja 2014 roku wszyscy ukraińscy operatorzy komórkowi (m.in. Kyivstar, Vodafone/MTS, Lifecell) zostali zmuszeni do opuszczenia półwyspu, obawiając się sankcji lub będąc ofiarą „nacionalizacji”. Ich sprzęt (tysiące stacji bazowych) został przejęty i stał się bazą dla nowych, rosyjskich operatorów wirtualnych⁴⁸.

W ten sposób Rosja, w ciągu kilku miesięcy, zakończyła proces pełnej „rusyfikacji” infosfery Krymu, poddając cały ruch internetowy rosyjskim systemom cenzury i nadzoru (jak DPI, Deep Packet Inspection).

„Atak” na infrastrukturę energetyczną – strategia wywłaszczenia i uzależnienia

Strategia zastosowana wobec sektora energetycznego była diametralnie różna od tej z sektora telekomunikacyjnego. Zamiast szybkiego, „twardego” ataku, Rosja zastosowała „miękki” atak prawno-ekonomiczny. Różnica ta wynikała z fundamentalnej kalkulacji strategicznej.

W 2014 roku Krym był krytycznie uzależniony od dostaw energii elektrycznej z Ukrainy kontynentalnej. Dostawy te, o mocy ok. 900–950 MW, pokrywały 80%⁴⁹ lub więcej⁵⁰ całkowitego zapotrzebowania półwyspu. Rosyjskie dowództwo zdawało sobie sprawę, że jakkolwiek atak na tę infrastrukturę (np. cyberatak na podstacje SCADA lub fizyczne zniszczenie linii) spowodowałby natychmiastowy i katastrofalny blackout.

⁴⁶ *How Occupation regimes...*, dz. cyt.

⁴⁷ R. Fontugne, K. Ermoshina, E. Aben, *The Internet in Crimea: a Case Study on Routing*, https://www.iiijlab.net/en/members/romain/pdf/romain_gi2020.pdf, [dostęp: 11.11.2025]; H. Coynash, *Crimean journalists is prosecuted for calling Crimea Ukrainian*, <https://ccl.org.ua/en/news/crimean-journalists-is-prosecuted-for-calling-crimea-ukrainian>, [dostęp: 15.11.2025]; Warto zauważyć, że Miranda Media zaczęła się pojawiać w lipcu, ale całkowita konwersja wszystkich sieci krymskich na Miranda Media dokonała się w lipcu 2017.

⁴⁸ *How Occupation regimes...*, dz. cyt.

⁴⁹ *DTEK Initiated Investment Dispute against Russia over the Company's Assets in Crimea*, <https://dtek.com/en/media-center/news/dtek-initsiiroval-rassmotrenie-investitsionnogo-spora-s-rossiey-v-otnoshenii-aktivov-gruppy-v-krymu->, [dostęp: 11.11.2025].

⁵⁰ J. Strzelecki, R. Sadowski, *Krym bez prądu*, Ośrodek Studiów Wschodnich, <https://www.osw.waw.pl/pl/publikacje/analizy/2015-11-25/krym-bez-pradu>, [dostęp: 11.11.2025].

Konsekwencje takiego blackoutu byłyby dla Rosji kontrproduktywne:

1. Podważenie propagandy: uniemożliwiłoby to działanie przejętych ośrodków RTV i ograniczyło dostęp do Internetu, odcinając Rosję od kluczowego narzędzia NGW (wojna nowej generacji, ang. *New Generation Warfare*) – kontroli narracji.
2. Chaos społeczny: blackout oznaczałby brak wody (pompy wody zasilane są energią elektryczną) i ogrzewania⁵¹, wywołując panikę i kryzys humanitarny.
3. Załamanie narracji: sytuacja taka podważyłaby rosyjską narrację o „wyzwoleniu” i „powrocie do macierzy”, zastępując ją obrazami chaosu i zapaści.
4. Komplikacje logistyczne: utrudniłoby to logistykę i dowodzenie samym rosyjskim siłom okupacyjnym.

Dlatego, w krótkim terminie, utrzymanie dostaw prądu z Ukrainy było strategicznym priorytetem Rosji, mimo iż tworzyło to oczywistą, długoterminową podatność⁵².

Skoro atak kinetyczny był wykluczony, „atak” Rosji na sektor energetyczny przybrał formę działań prawno-ekonomicznych. Celem nie było zniszczenie sieci, lecz przejęcie kontroli nad aktywami dystrybucyjnymi na półwyspie. Głównym celem stała się firma DTEK Krymenergo PJSC, należąca do ukraińskiej grupy DTEK. Był to główny dostawca energii na półwyspie, obsługujący ponad 80% rynku. Metodą przejęcia była „nacionalizacja” (de facto wywłaszczenie) przeprowadzona przez marionetkowe władze w dwustopniowym procesie realizowanym przez kilka miesięcy – pierwsza „nacionalizacja” miała miejsce 30 kwietnia 2014 roku, czyli bezpośrednio po aneksji, formalnie 21 stycznia 2015 roku Rada Państwowa Republiki Krymu uchwaliła decyzję o nacionalizacji i przeprowadziła nową „nacionalizację”⁵³. W ten sposób Rosja, zamiast sił SOF i hakerów, użyła polityków, prawników i administratorów do przeprowadzenia

⁵¹ Tamże.

⁵² B.E. Humphreys, *Attacks on Ukraine's Electric Grid: Insights for U.S. Infrastructure Security and Resilience*, <https://www.congress.gov/crs-product/R48067>, [dostęp: 11.11.2025].

⁵³ J. Delamer, V. Tsimaylo, *Investment disputes in the crossfire of War*, <https://compass-lexecon.files.svdcn.com/production/editorial/2025/02/The-Analysis-Investment-Disputes-Crossfire-of-War-250225.pdf?dm=1740482534>, [dostęp: 15.11.2025]; *UNCITRAL tribunal finds Russia liable to pay USD 207.8 million for the unlawful expropriation of the assets of a Ukrainian electricity company*, <https://www.iisd.org/itn/2024/01/13/uncitral-tribunal-finds-russia-liable-to-pay-usd-207-8-million-for-the-unlawful-expropriation-of-the-assets-of-a-ukrainian-electricity-company>, [dostęp: 15.11.2025].

„ataku” na sektor energetyczny, przejmując kontrolę nad dystrybucją, jednocześnie cynicznie korzystając z energii produkowanej i przesyłanej przez Ukrainę.

Należy podkreślić, że Rosja równocześnie budowała „most energetyczny” przez Cieśninę Kerczeńską⁵⁴, co wskazuje na równoległy rozwój długoterminowej infrastruktury, a nie czystą zależność od podejścia „prawno-ekonomicznego”.

Izolacja ukraińskich Sił Zbrojnych (obrona)

Cel: neutralizacja znacznego kontyngentu ukraińskich sił zbrojnych stacjonujących na półwyspie, liczącego według różnych szacunków od 15 000 do 18 800 żołnierzy⁵⁵. Taktyka blokowania: podstawową taktyką zastosowaną wobec ukraińskich garnizonów nie był szturm, lecz psychologiczna i fizyczna blokada⁵⁶. 15 Jednostki Warstwy 3 (głównie 810 Brygada Piechoty Morskiej) otaczały ukraińskie bazy wojskowe kordonem żołnierzy i transporterów opancerzonych. Pozbawieni rozkazów (w wyniku paraliżu C2) i możliwości manewru, ukraińscy żołnierze zostali skutecznie sparaliżowani i zdemoralizowani.

Studium przypadku: Teodozja (24 marca 2014). Cel: przejęcie bazy elitarnego 1 Batalionu Piechoty Morskiej Marynarki Wojennej Ukrainy, który jako jeden z nielicznych odmówił poddania się. Taktyka: wobec fiaska negocjacji, Rosjanie przeszli od blokady do bezpośredniego szturmu. Była to operacja połączona: KSSO (jako element szturmowy) wspierane przez transportery BTR (prawdopodobnie BTR-82A) oraz śmigłowce⁵⁷.

Porównanie operacji w Symferopolu, na lotnisku cywilnym i w Teodozji ujawnia kluczowy aspekt taktyczny: „uprzejmość” (ros. вежливость) była świadomą i warunkową taktyką PSYOPS. Gdy cele były „miękkie” – cywile na lotnisku lub współpracujący strażnicy parlamentu – operatorzy KSSO zachowywali się poprawnie, wspierając narrację o „stabilizacji”. Gdy jednak napotkano zdeterminowany opór, jak w przypadku ukraińskich marines w Teodozji, „uprzejmość” została natychmiast zastąpiona brutalną agresją, w tym kopaniem i krępowaniem jeńców⁵⁸.

⁵⁴ *Energy blockade of Crimea reveals shady dealings of the oligarchs*, <https://www.obserwatorfinansowy.pl/in-english/new-trends/energy-blockade-of-crimea-reveals-shady-dealings-of-the-oligarchs>, [dostęp: 15.11.2025].

⁵⁵ M. Kofman i in., *Lessons from Russia's Operations...*, dz. cyt.

⁵⁶ A. Wilk, dz. cyt.

⁵⁷ M. Strzelecki, dz. cyt., s. 383–413.

⁵⁸ Tamże.

Ta elastyczność taktyczna pozwoliła zminimalizować rozlew krwi tam, gdzie było to propagandowo pożądane, ale jednocześnie gwarantowała osiągnięcie celu militarnego, gdy było to konieczne.

1.4. Środki niekinetyczne i wojna informacyjna – mnożniki siły

Fizyczne przejęcie infrastruktury było możliwe tylko dzięki równoległemu, zmasowanemu atakowi na jej komponenty niekinetyczne – systemy dowodzenia, kontroli i komunikacji.

Działania w cyberprzestrzeni – paraliż telekomunikacji i systemów zarządzania

Federacja Rosyjska od początku kryzysu w 2014 roku intensywnie wykorzystywała cyberataki jako narzędzie wojny hybrydowej. Ataki te były skierowane przeciwko infrastrukturze energetycznej, mediom i systemom rządowym⁵⁹.

- Zakłócanie telekomunikacji: kluczowym elementem było przejęcie kontroli nad cyfrową infrastrukturą Ukrainy⁶⁰. Obejmowało to zmasowane ataki DDoS na ukraińskie sieci rządowe i medialne, przeprowadzone m.in. 13 marca 2014 roku, na trzy dni przed nielegalnym referendum⁶¹. Zaatakowano również strony internetowe NATO⁶².
- Spear-phishing i sabotaż: równolegle prowadzone były operacje wywiadowcze. Kampania „Operation Armageddon”, aktywna co najmniej od połowy

⁵⁹ *Russian's war on Ukraine: Timeline of cyber-attacks*, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI\(2022\)733549_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf), [dostęp: 10.11.2025].

⁶⁰ N. Mihaylov, *Cyber Dimensions of a Hybrid Warfare*, CyberPeace Institute, <https://cyberpeaceinstitute.org/news/cyber-dimensions-of-a-hybrid-warfare>, [dostęp: 10.11.2025].

⁶¹ K. Chincharadze, *From Georgia to Ukraine: seventeen years of russian cyber capabilities at war*, Modern War Institute, <https://mwi.westpoint.edu/from-georgia-to-ukraine-seventeen-years-of-russian-cyber-capabilities-at-war>, [dostęp: 10.11.2025].

⁶² *Russia's strategy in cyberspace*, NATO Strategic Communications Centre of Excellence, https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf, [dostęp: 10.11.2025]; B. Price, *'Operation Armageddon' Cyber Espionage Campaign Aimed at Ukraine: Lookingglass*, <https://www.securityweek.com/operation-armageddon-cyber-espionage-campaign-aimed-ukraine-lookingglass>, [dostęp: 15.11.2025].

2013 roku, wykorzystywała ukierunkowany spear-phishing do kradzieży wrażliwych danych od ukraińskich urzędników rządowych, wojskowych i organów ścigania⁶³. W jednym z najbardziej zaawansowanych przykładów taktycznej wojny cybernetycznej, rosyjski wywiad wojskowy „zatrojanizował” aplikację na system Android (Попр-Д30.apk), która została opracowana przez ukraińskiego oficera artylerii (Yaroslav Sherstuk) do obliczeń balistycznych dla haubic D-30. Złośliwy kod wbudowany w aplikację miał potencjał do pobrania danych geolokalizacyjnych ukraińskich baterii, co hipotetycznie mogłoby umożliwić ich precyzyjny ostrzał kontrbaterijny⁶⁴.

Walka Radioelektroniczna (REB) – dezorganizacja dowodzenia

Rosja od lat mocno inwestowała w zdolności walki radioelektronicznej (REB, ros. РЭБ) jako kluczowy, asymetryczny środek odpowiedzi na technologiczną przewagę NATO w zakresie C4ISR⁶⁵.

- Rozmieszczenie systemów: podczas operacji na Krymie i na Donbasie zidentyfikowano rozmieszczenie najbardziej zaawansowanych rosyjskich systemów REB. Należały do nich kompleksy RB-301B „Borisoglebsk-2” (przeznaczone do zaawansowanego monitorowania i zagłuszania komunikacji HF/VHF) oraz RB-341W „Leer-3”⁶⁶.
- Taktyka „Leer-3”: system „Leer-3” jest szczególnie istotny dla operacji hybrydowych. Składa się on ze stacji naziemnej oraz bezzałogowych statków powietrznych (dronów) Orlan-10. Jego podstawową funkcją jest zagłuszanie komunikacji w standardzie GSM⁶⁷. Co ważniejsze, system ten jest zdolny do precyzyjnej

⁶³ K. Chinchardze, dz. cyt.

⁶⁴ P. Meissner, *Assessing Russian Cyber Effects*, <https://www.war.gov/News/Releases/Release/Article/2585399/assessing-russian-cyber-effects>, [dostęp: 10.11.2025]; Ch. Miller, *'Fancy Bear' Tried to Hack E-Mail of Ukrainian Making Artillery-Guidance App*, <https://www.rferl.org/a/ukraine-russia-fancy-bear-hacking-artillery-guidance-app/28831564.html>, [dostęp: 15.11.2025].

⁶⁵ R.N. McDermott, *Russia's Electronic Warfare Capabilities do 2025*, International Centre for Defence and Security, 2017, https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf, [dostęp: 10.11.2025].

⁶⁶ R. Scott, *From the JED Archives: Tuning In, Turning On: Russia Brings Radio-Electronic Combat to the Fore*, „The Jurnal of Electromagnetic Dominance”, <https://www.jedonline.com/2023/02/16/from-the-jed-archives-tuning-in-turning-on-russia-brings-radio-electronic-combat-to-the-fore-2>, [dostęp: 10.11.2025].

⁶⁷ S. Sukhankin, *Blind, Confuse and Demoralize: Russian Electronic Warfare Operations in Donbas*, Jamestown Foundation 2021, <https://jamestown.org/program/blind-confuse-and-demoralize-russian-electronic-warfare-operations-in-donbas>, [dostęp: 10.11.2025].

geolokalizacji telefonów komórkowych, co pozwala na namierzanie całych jednostek wojskowych dla rosyjskiej artylerii⁶⁸.

Operacje psychologiczne (PSYOPS) i informacyjne (maskirowka)

Działania niekinetyczne osiągnęły najwyższy poziom integracji w sferze psychologicznej i informacyjnej.

- Integracja REB-PSYOPS: najbardziej zaawansowaną taktyką hybrydową było wykorzystanie systemów REB, takich jak „Leer-3”, nie tylko do zagłuszania, ale także do przechwytywania i tworzenia fałszywych stacji bazowych sieci GSM. Pozwoliło to siłom rosyjskim na wysyłanie masowych, zindywidualizowanych i silnie demoralizujących wiadomości SMS bezpośrednio do ukraińskich żołnierzy na linii frontu oraz do ich rodzin⁶⁹.
- „Farmy trolli”: równolegle prowadzono zmasowaną kampanię w przestrzeni informacyjnej. Rosyjskie „brygady internetowe” lub „farmy trolli”, takie jak Internet Research Agency, zintensyfikowały swoje działania pod koniec lutego 2014 roku⁷⁰. Ich zadaniem było zalewanie mediów społecznościowych i forów dyskusyjnych treściami wspierającymi rosyjską narrację, promowanie hasztagów takich jak #PolitePeople⁷¹ i #KrymP_t_NaRodinu (Krym Droga do Domu) oraz dyskredytowanie władz w Kijowie (np. po zestrzeleniu MH17)⁷².

Działania te wskazują na istnienie wysoce zintegrowanej, taktycznej pętli „REB-PSY-OPS-Kinetic”. Proces ten przebiegał następująco:

1. Wykrycie (REB): system „Leer-3” identyfikuje skupisko sygnałów GSM, wskazujące na pozycję ukraińskiej jednostki.

⁶⁸ R. Scott, dz. cyt.

⁶⁹ Tamże.

⁷⁰ *Analysis of Russia's Information Campaign against Ukraine*, https://stratcomcoe.org/cuploads/pfiles/russian_information_campaign_public_12012016fin.pdf, [dostęp: 10.11.2025].

⁷¹ Tamże.

⁷² O. Nedelnyuk, *How Russian „Troll factory tried to effect on Ukraine's agenda. Analysis of 755 000 tweets*, <https://voxukraine.org/en/how-russian-troll-factory-tried-to-effect-on-ukraine-s-agenda>, [dostęp: 10.11.2025]; E. Lange-Ionatamišvili, *Analysis of Russia's information campaign against Ukraine*, NATO Strategic Communications Centre of Excellence, 2015, <https://stratcomcoe.org/publications/analysis-of-russias-information-campaign-against-ukraine/151>, [dostęp: 10.11.2025].

2. Demoralizacja (PSYOPS): ten sam system wysyła do żołnierzy w tej lokalizacji wiadomości SMS (np. „Jesteście otoczeni, poddajcie się”)⁷³.
3. Zbieranie danych (Cyber): zatrojanizowana aplikacja artyleryjska na urządzeniu jednego z żołnierzy potwierdza dokładną lokalizację GPS⁷⁴.
4. Zniszczenie (Kinetic): możliwość, że dane geolokalizacyjne (z REB lub Cyber) są przekazywane w czasie rzeczywistym do rosyjskiej jednostki artylerii w celu wykonania precyzyjnego uderzenia⁷⁵.

Taka integracja domen stanowi kwintesencję wojny hybrydowej na poziomie taktycznym.

1.5. Środki techniczne i wyposażenie „zielonych ludzików”

Wyposażenie „uprzejmych ludzi” samo w sobie stanowiło kluczowy element maskirowki i operacji psychologicznej.

Paradoks maskirowki

Celowy brak jakichkolwiek insygniów, oznaczeń przynależności państwowej czy stopni wojskowych był podstawą maskirowki. Pozwalało to rosyjskim prominentom, z prezydentem Putinem na czele, na polityczne zaprzeczanie zaangażowaniu regularnej armii i przedstawianie operatorów KSSO jako „lokalnych sił samoobrony”⁷⁶. Jednakże jakość, nowoczesność i standaryzacja ich wyposażenia były celowym sygnałem skierowanym do ukraińskich żołnierzy i ekspertów wojskowych.

⁷³ R. Scott, dz. cyt.

⁷⁴ P. Meissner, dz. cyt.; *Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units* – CROWDSTRIKE BLOG, 2016, <https://www.crowdstrike.com/en-us/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units>, [dostęp: 10.11.2025]; T. Eshel, *Russians Used Cyber Bots to Target Ukrainian Artillery*, Defence Update, 2016, https://defense-update.com/20161223_trojan-2.html, [dostęp: 10.11.2025].

⁷⁵ R. Scott, dz. cyt.

⁷⁶ J.R. Haines, dz. cyt.

Analiza wyposażenia

Szczegółowa analiza materiałów wizualnych z Krymu⁷⁷ pozwala na precyzyjną identyfikację sprzętu używanego przez „zielonych ludzików”, który był wydawany wyłącznie elitarnym jednostkom Sił Zbrojnych FR:

1. Mundury: nowoczesny kamuflaż cyfrowy EMR („cyfrowa flora”). Zidentyfikowano również specjalistyczne mundury Gorka-3 (używane przez siły specjalne i górskie) oraz kamizelki taktyczne Smersh (używane przez siły specjalne).
2. Hełmy: nowe hełmy kompozytowe 6B27, 6B7-1M oraz 6B26 (te ostatnie używane wyłącznie przez Wojska Powietrznodesantowe – WDW).
3. Kamizelki: nowe modułowe kamizelki taktyczne 6Sh112 lub 6Sh117 oraz 6Sh92-5 (również identyfikowane jako sprzęt WDW).
4. Uzbrojenie: oprócz standardowych karabinków z rodziny Kałasznikowa 30, operatorzy byli wyposażeni w broń specjalistyczną, niedostępną dla „sił samoobrony”: nowoczesne karabiny maszynowe 7,62 mm PKP „Peczeneg” oraz wyciszone karabiny snajperskie VSS Vintorez, będące na wyposażeniu jednostek SpecNazu⁷⁸.

Wyposażenie to miało zatem podwójny cel. Dla publiczności międzynarodowej i mediów, brak naszywek pozwalał Kremlowi na „wiarygodne” zaprzeczenie. Jednak dla ukraińskich żołnierzy zablokowanych w bazach, widok operatorów wyposażonych w najnowszy rosyjski sprzęt (kamizelki 6Sh117, hełmy 6B27, karabiny VSS) – sprzęt, którego ukraińska armia w 2014 roku nie posiadała i który był postrzegany jako znacznie nowocześniejszy od ich własnego – mógł być znaczącym komunikatem psychologicznym. Sygnalizował on jednoznacznie: „Jesteśmy elitarnymi, regularnymi siłami Federacji Rosyjskiej. Wasz sprzęt jest przestarzały, a opór jest daremny”. Ten paradoks „wiarygodnego zaprzeczania” przy jednoczesnej „profesjonalnej identyfikowalności” był kluczem do zdemoralizowania i sparaliżowania ukraińskich sił, co doprowadziło do minimalnego rozlewu krwi.

⁷⁷ S. Sotilas, *Weapons and Equipment Analysis of Little Green Men in Crimea* (March 2014), [za:] *Little Green Men: A Primer on Modern Russian Unconventional Warfare, Ukraine 2013–2014*, USASOC, Fort Bragg, 2014, <https://nsarchive.gwu.edu/media/16170/ocr>, [dostęp: 10.11.2025].

⁷⁸ Little green men (Russo-Ukrainian war) – Wikipedia, [https://en.wikipedia.org/wiki/Little_green_men_\(Russo-Ukrainian_war\)](https://en.wikipedia.org/wiki/Little_green_men_(Russo-Ukrainian_war)), [dostęp: 10.11.2025].

Dyskusja – synteza skuteczności operacji

Operacja aneksji Krymu w lutym–marcu 2014 roku była, z perspektywy rosyjskich celów strategicznych i operacyjnych, zdecydowanym sukcesem. Rosji udało się osiągnąć kluczowe cele polityczne poprzez szybkie i mobilne wykonanie operacji⁷⁹. Cała operacja, od zajęcia parlamentu do podpisania traktatu akcesyjnego, trwała zaledwie 19 dni⁸⁰ w najbardziej widocznej fazie, według rosyjskiego Ministerstwa Obrony trwała od 20 lutego do 18 marca.

Sukces ten nie był wynikiem pojedynczego czynnika, ale synergii wszystkich zaangażowanych sił i środków:

1. Szybkość i zaskoczenie: Rosja w pełni wykorzystwała próżnię polityczną i chaos decyzyjny w Kijowie po rewolucji Euromajdanu⁸¹. Błyskawiczne tempo operacji KSSO uniemożliwiło Ukrainie sformułowanie i wdrożenie zorganizowanej odpowiadzi militarnej⁸².
2. Integracja sił: kluczem była płynna integracja trzech warstw sił zbrojnych. Elitarne KSSO (Warstwa 1) działały jako „skalpel”, dokonując precyzyjnych cięć w infrastrukturze politycznej i transportowej. Były natychmiast wzmacniane przez jednostki specjalne drugiego rzutu (WDW, GRU – Warstwa 2), podczas gdy siły konwencjonalne (Piechota Morska – Warstwa 3) działały jako „młot”, realizując otwartą, konwencjonalną blokadę ukraińskich garnizonów. Całość była osłonięta przez dezinformacyjną Warstwę Zero (tzw. „samoobrona”).
3. Integracja domen: krytycznym czynnikiem sukcesu była bezprecedensowa w tym czasie integracja działań kinetycznych (zajmowanie budynków, blokowanie baz) z działaniami niekinetycznymi. Ataki cybernetyczne, walka radioelektroniczna (REB) oraz operacje psychologiczne (PSYOPS) były ważnymi działaniami wspierającymi i równoległymi znaczącymi liniami operacji. Ich celem i efektem było sparaliżowanie ukraińskich systemów dowodzenia (C2), telekomunikacji oraz woli walki żołnierzy i dowódców.

⁷⁹ M. Kofman i in., *Lessons from Russia's Operations...*, dz. cyt.

⁸⁰ T. Bukkvoll, dz. cyt.

⁸¹ P.A. Kaber, dz. cyt.

⁸² T. Bukkvoll, dz. cyt.

Wnioski

1. Operacja krymska z 2014 roku stanowiła modelowy, niemal podręcznikowy przykład realizacji rosyjskiej doktryny wojny hybrydowej. Wykazała zdolność Rosji do elastycznego i zintegrowanego wykorzystania nowo utworzonych, elitarnych sił KSSO, wsparcia jednostek konwencjonalnych (WDW, Piechota Morska) oraz zaawansowanych, asymetrycznych środków niekinetycznych (REB, Cyber, PSYOPS).
2. Opanowanie infrastruktury krytycznej Krymu osiągnięto nie poprzez jej zniszczenie – jak w późniejszych fazach wojny – ale poprzez paraliż systemowy. Siły rosyjskie fizycznie przejęły kluczowe węzły polityczne i transportowe, jednocześnie częściowo odcinając je od ukraińskiego „układu nerwowego” (sieci dowodzenia i telekomunikacji) za pomocą precyzyjnie wymierzonych środków hybrydowych.
3. Analiza operacji aneksji Krymu w 2014 roku dowodzi, że Rosja z powodzeniem zneutralizowała i przejęła infrastrukturę krytyczną półwyspu, stosując wysoce zróżnicowaną i dostosowaną do sektora strategię hybrydową. Działania te nie były ani czysto militarne, ani czysto polityczne, lecz stanowiły płynną kombinację wielu narzędzi państwowych, działających w pełnej koordynacji:
 - Wobec sektora telekomunikacyjnego (informacji) zastosowano szybki, „twardy” atak, łączący siły specjalne (do zajęcia fizycznego), Wojnę Radioelektroniczną (do paraliżu), ataki kinetyczne (do izolacji) i cybernetyczne (do destabilizacji). Celem była natychmiastowa dominacja w sferze informacyjnej, kluczowa dla sukcesu NGW.
 - Wobec sektora energetycznego (stabilności) zastosowano powolny, „miękki” atak, oparty na działaniach politycznych, prawnych i ekonomicznych. Nie był on jednak wyborem, lecz następstwem ograniczeń technicznych i logistycznych. Celem było przejęcie kontroli nad aktywami przy jednoczesnym unikaniu destabilizacji społecznej, która zniweczyłaby cel polityczny.
4. Analiza modus operandi Rosji wskazuje, że odporność infrastruktury krytycznej państw Sojuszu Północnoatlantyckiego musi być budowana w sposób holistyczny, uwzględniając zagrożenia:
 - Fizyczno-elektromagnetyczne: synergia działań sił specjalnych (SOF) i środków WRE, zdolna do fizycznego zajęcia lub sparaliżowania węzłów infrastruktury (podstacji, central telekomunikacyjnych, centrów danych) bez wypowiedzenia wojny.

- Prawno-ekonomiczne: wykorzystanie instrumentów prawnych i korporacyjnych (wrogie przejęcia, nieprzejrzysta struktura własności, instalowanie operatorów-wydmuszek jak Miranda-Media) do przejęcia kontroli nad infrastrukturą bez jednego wystrzału.
 - W „szarej strefie”: prowadzenie działań w sposób, który utrudnia jednoznaczną atrybucję (np. „nieznani sprawcy” przecinający światłowody) i nie przekracza formalnego progu wojny, może stanowić wyzwanie dla procesów decyzyjnych NATO.
5. Odporność infrastruktury krytycznej nie może być zatem domeną wyłącznie inżynierów i specjalistów od cyberbezpieczeństwa. Wymaga ona zintegrowanego podejścia, łączącego ochronę fizyczną (przed SOF), bezpieczeństwo domeny elektromagnetycznej (przed WRE), higienę cybernetyczną (przed SCADA-malware) oraz przejrzystość prawną i ekonomiczną (przed wrogim przejęciem).

2. Wojskowe siły i środki wykorzystywane do atakowania infrastruktury energetycznej Ukrainy

2.1. Ewolucja paradygmatu wojny od starć kinetycznych do hybrydowej wojny systemowej

Rosyjska operacja przeciwko ukraińskiej energetyce od 2022 roku stanowi unikalny przykład zastosowania w praktyce koncepcji tzw. Strategicznej Operacji Zniszczenia Krytycznie Ważnych Celów (SODCIT). Ataki te polegały na zmasowanym i systematycznym użyciu precyzyjnych środków napadu powietrznego (rakiet, dronów) przeciwko obiektom energetycznym, wodnym i ciepłym z zamiarem paraliżu systemów podtrzymujących życie państwa oraz wywarcia psychologicznej i politycznej presji na społeczeństwo ukraińskie. To nowoczesna realizacja celu strategicznego opisanego przez Clausewitza nie poprzez zajęcie terytorium, lecz obniżenie odporności państwa przez dewastację kluczowej infrastruktury⁸³.

Choć precedensów dla tego rodzaju operacji można doszukiwać się w historii konfliktów XX wieku (np. doktryna Douheta, alianckie naloty strategiczne podczas II wojny światowej, operacja NATO przeciwko Serbii w 1999 r.), to w przypadku Federacji Rosyjskiej do czynienia mamy z pierwszym systematycznym i zintegrowanym wdrożeniem SODCIT w ramach aktualnej rosyjskiej doktryny wojennej, wykorzystującym zarówno środki kinetyczne, jak i cyberataki oraz działania informacyjne na niespotykaną dotąd skalę⁸⁴.

⁸³ S. Matuszak, *Nowe zmasowane ataki Rosji na ukraińską infrastrukturę energetyczną – straty i wyzwania*, <https://www.osw.waw.pl/pl/publikacje/analizy/2024-04-17/nowe-zmasowane-ataki-rosji-na-ukrainska-infrastruktura-energetyczna>, [dostęp: 11.11.2025]; M. Piekarski, dz. cyt., s. 115–135; Carl von Clausewitz, *O wojnie*, Warszawa 2006.

⁸⁴ M. Piekarski, dz. cyt.

Celem tego rodzaju działań jest uzyskanie przewagi strategicznej bez konieczności fizycznej okupacji terenu, co stanowi istotne odejście od klasycznych założeń Clausewitza. Realizowane przez Rosję uderzenia na ukraińską infrastrukturę krytyczną miały doprowadzić do masowych przerw w dostawach energii, ogrzewania i wody, a tym samym wymusić kapitulację lub ustępstwa polityczne Ukrainy przez złamanie woli oporu społeczeństwa. Skuteczność tej strategii okazała się jednak ograniczona, bowiem mimo poważnych strat w systemie energetycznym, państwo ukraińskie wykazało się wysoką odpornością organizacyjną, a społeczeństwo – gotowością do ponoszenia kosztów długotrwałego konfliktu⁸⁵.

2.2. Nexus energetyczno-zasobowo-klimatyczny

Analiza konfliktu wymaga uwzględnienia nowego wymiaru, zdefiniowanego w literaturze jako „nexus bezpieczeństwa energetyczno-zasobowo-klimatycznego”. Rosyjskie ataki nie są wymierzone w próżnię; odbywają się w kontekście globalnej transformacji energetycznej i zmian klimatycznych. Zniszczenie ukraińskich mocy wytwórczych, w tym niskoemisyjnych elektrowni wodnych i infrastruktury gazowej niezbędnej do transformacji energetycznej Europy, jest elementem szerszej strategii hybrydowej⁸⁶.

Ma ona na celu nie tylko osłabienie Ukrainy, ale także destabilizację rynków energetycznych Unii Europejskiej, podważenie celów klimatycznych oraz uzależnienie odbudowy powojennej od technologii i surowców kontrolowanych przez mocarstwa rewizjonistyczne. Zielona transformacja, paradoksalnie, tworzy nowe wektory zagrożeń – systemy oparte na OZE i rozproszonej generacji wymagają specyficznych surowców (metale ziem rzadkich) i technologii, które mogą stać się przedmiotem wojny hybrydowej. W tym ujęciu, atak na ukraińską energetykę jest atakiem na przyszłą architekturę bezpieczeństwa energetycznego całego kontynentu europejskiego⁸⁷.

⁸⁵ Tamże, s. 115–135.

⁸⁶ M. Geri, *Understanding Russian Hybrid Warfare against Europe in the energy sector and in the future ‘energy-resources-climate’ security nexus*, „Journal of Strategic Security” 2024, Vol. 17, No. 3, s. 15–28.

⁸⁷ Tamże, s. 26–28.

2.3. Cele operacyjne i strategiczne Federacji Rosyjskiej

Analizując dyslokację sił, dobór celów oraz zmiany w intensywności ataków od lutego 2022 roku, można wyodrębnić hierarchię celów rosyjskich, która łączy wymiary psychologiczny, gospodarczy i militarno-operacyjny, stanowiąc integralną część strategii *hybrid warfare* zdefiniowanej przez rosyjską doktrynę wojskową:

1. Cel polityczno-psychologiczny: terroryzm energetyczny i presja negocjacyjna. Rosyjskie ataki na infrastrukturę energetyczną służą jako instrument terroryzmu energetycznego – celowego pozbawienia ludności cywilnej dostępu do ciepła, elektryczności i wody w celu osiągnięcia celów politycznych. Strategię tę, znaną jako *weaponizing winter*, uruchomiono masowo po nieudanych atakach frontowych w 2022 roku, kiedy Rosja straciła znaczną część zdolności konwencjonalnych⁸⁸.
2. Cel gospodarczy: „deindustrializacja” Ukrainy poprzez fizyczną likwidację infrastruktury przemysłowej zasilanej energią elektryczną, co prowadzi do załamania PKB i uzależnienie państwa od pomocy zewnętrznej⁸⁹. Ataki na energetykę służą jako instrument długoterminowej deindustrializacji Ukrainy. Rosja celowo zniszczyła lub poważnie uszkodziła większość ukraińskich mocy generacyjnych, zmuszając gospodarkę do operowania z deficytem energetycznym, który nie może być lokalnie pokryty.
3. Cel militarno-operacyjny: zakłócenie logistyki wojskowej (zasilanie kolei elektrycznych) oraz funkcjonowania przemysłu obronnego i systemów dowodzenia.
4. Wymiar hybrydowy: integracja z innymi narzędziami ataku. Ataki energetyczne nie stanowią izolowanego działania, lecz część zintegrowanej strategii *hybrid warfare*, łączącej⁹⁰:
 - komponenty wojskowe: ataki balistyczne i dronami na stacje elektroenergetyczne,
 - komponenty cybernetyczne: ataki na systemy zarządzania siecią energetyczną,

⁸⁸ Ch. Carpenter, *‘Dual Use’ Can’t Justify Russia’s Attacks on Ukraine’s Energy Grid*, [w:] M. Geri, dz. cyt.

⁸⁹ A. Davydiuk, V. Zubok, *Analytical Review of the Resilience of Ukraine’s Critical Energy Infrastructure to Cyber Threats in Times of War*, 15th International Conference on Cyber Conflict: Meeting Reality (CyCon), Tallinn, Estonia 2023, s. 121–139; A.R. Kozłowski, *The war and tourism: security issues and business opportunities in shadow of Russian war against Ukraine*, Qual Quant (2023).

⁹⁰ M. Geri, dz. cyt.; Ch. Carpenter, dz. cyt.

- komponenty informacyjne: propaganda i dezinformacja mające uzasadnić „celowość wojskową” atakowania infrastruktury cywilnej z powołaniem się na koncepcję „dual-use” (podwójnego zastosowania),
- komponenty psychologiczne: stosowanie terroru wobec ludności cywilnej, mające na celu zmianę jej postaw wobec konfliktu.

2.4. Architektura Sił Zbrojnych Federacji Rosyjskiej w kampanii powietrznej

Realizacja tak złożonej operacji wymagała zaangażowania i koordynacji trzech głównych rodzajów sił zbrojnych: Sił Powietrzno-Kosmicznych (WKS), Marynarki Wojennej (WMF) oraz Wojsk Lądowych.

Lotnictwo Dalekiego Zasięgu (LRA)

Lotnictwo Dalekiego Zasięgu stanowi kręgosłup rosyjskich zdolności uderzeniowych, odpowiadając za przenoszenie pocisków manewrujących. Główne operacje prowadzone są z baz lotniczych położonych głęboko w terytorium Rosji, co zapewnia im względne bezpieczeństwo przed ukraińskimi uderzeniami odwetowymi (choć niecałkowitą bezkarność).

22 Gwardyjska Dywizja Ciężkich Bombowców

Dywizja ta z dowództwem w bazie Engels-2 (obwód saratowski) jest kluczową formacją realizującą uderzenia na ukraińską infrastrukturę. W jej skład wchodzi trzy pułki bombowców: dwa w Engels-2 (121 Pułk z Tu-160 i 184 Pułk z Tu-95MS) oraz 52 Gwardyjski Pułk z Tu-22M3 (Backfire) w Szajkowce⁹¹. Samoloty te są nosicielami naddźwiękowych pocisków przeciwookrętowych Ch-22/Ch-32, które w tej wojnie są wykorzystywane do atakowania celów lądowych. Ponadto w bazie Ukrainka na Dalekim Wschodzie stacjonuje 326 Dywizja, wyposażona w bombowce Tu-95MS oraz Tu-22M3.

⁹¹ 22nd Guards Heavy Bomber Aviation Division – Wikipedia, https://en.wikipedia.org/wiki/22nd_Guards_Heavy_Bomber_Aviation_Division, [dostęp: 1.12.2025]; B. Volodymyr, *Spiderweb Operation: How Many Tu-95MSs, Tu-22M3s and A-50s Destroyed at Russian Airbases*, <https://militaryni.com/en/news/spiderweb-operation-how-many-tu-95ms-tu-22m3-and-a-50s-destroyed-at-russian-airbases>, [dostęp: 1.12.2025].

W odpowiedzi na ukraińskie ataki dronowe na bazę Engels, rosyjskie dowództwo przebazowało część bombowców strategicznych (zarówno Tu-95MS, jak i Tu-160) do bazy Olenya na Półwyspie Kolskim (obwód murmański). Baza ta, oddalona o tysiące kilometrów od linii frontu, służyła jako główne miejsce przygotowania maszyn do uderzeń raketowych, co wydłuża czas reakcji ukraińskiej obrony (ze względu na dłuższy czas dolotu pocisków), ale jednocześnie zwiększa zużycie zasobów rosyjskich płatowców⁹².

Flota Czarnomorska (FCS) – transformacja z dominacji morskiej na platformę raketową

Rola Floty Czarnomorskiej uległa drastycznej ewolucji. Po utracie krążownika „Moskwa” i zagrożeniu ze strony ukraińskich dronów morskich (USV), duże okręty nawodne zostały wycofane z bazy w Sewastopolu do Noworosyjska. Mimo to flota pozostaje kluczowym komponentem uderzeniowym dzięki pociskom Kalibr, w tym odpalanych z okrętów podwodnych. W roku 2024 Flota Czarnomorska posiadała 5 okrętów podwodnych, 6 fregat oraz kilkadziesiąt mniejszych jednostek.

Wojska Lądowe i wsparcie sojusznicze (KRLD)

Wsparcie dla kampanii powietrznej zapewniają również jednostki lądowe, w tym brygady raketowe wyposażone w systemy Iskander-M, operujące z obwodów biełgorodzkiego, kurskiego i woroneskiego, a także z okupowanego Krymu. Co istotne od 2024 roku odnotowuje się obecność północnokoreańskich oficerów i techników wspierających obsługę systemów balistycznych KN-23, które zostały zintegrowane z rosyjskimi wyrzutniami, stanowiąc nowy, niebezpieczny element arsenału⁹³.

⁹² B. Volodymyr, dz. cyt., A. Wilk, P. Żochowski, *Ukraine deals blow to Russian strategic aviation. Day 1196 of the war*, <https://www.osw.waw.pl/en/publikacje/analyses/2025-06-03/ukraine-deals-blow-to-russian-strategic-aviation-day-1196-war>, [dostęp: 1.12.2025].

⁹³ O. Goncharova, *North Korean missiles with Western parts fuel Russian attacks on Ukraine, CNN reports*, <https://kyivindependent.com/ukraine-faces-wave-of-attacks-with-north-korean-missiles-with-western-components-cnn-reports>, [dostęp: 1.12.2025]; *Russian Offensive Campaign Assessment*, <https://understandingwar.org/research/russia-ukraine/russian-offensive-campaign-assessment-october-22-2025>, [dostęp: 1.12.2025].

2.5. Arsenał środków napadu powietrznego

Rosja wykorzystuje szerokie spektrum środków rażenia, tworząc tzw. „High-Low Mix” – mieszanekę drogich, zaawansowanych technologicznie pocisków oraz tanich, masowo produkowanych dronów.

Ewolucja Pocisku Ch-101

Pocisk Ch-101 przeszedł znaczącą modernizację w toku konfliktu. W 2024 roku Rosjanie wprowadzili modyfikację polegającą na zmniejszeniu zbiornika paliwa (zasięg spadł do ok. 2000–2500 km w stosunku do pierwotnych ~ 4000 km) na rzecz zainstalowania drugiej głowicy bojowej. Dzięki temu całkowita masa ładunku wzrosła do 800 kg⁹⁴. Druga głowica często zawiera subamunicję kasetową (stalowe sześciangy lub kulki), co drastycznie zwiększa pole rażenia. Taka konfiguracja jest idealna do niszczenia rozległych, nieopancerzonych celów takich jak otwarte rozdzielnie (switchyards) przy elektrowniach, gdzie jeden pocisk może wyeliminować wiele transformatorów jednocześnie⁹⁵.

Ch-69 – pocisk nowej generacji

Zaskoczeniem dla analityków było bojowe użycie pocisku Ch-69, który pierwotnie miał stanowić uzbrojenie myśliwców V generacji Su-57. Posiada on kwadratowy przekrój kadłuba (dla minimalizacji odbicia radarowego) i jest zaprojektowany do lotu na ekstremalnie niskich wysokościach – rzędu 20 metrów nad ziemią⁹⁶. To właśnie ta cecha, w połączeniu z technologią stealth, pozwoliła rosyjskim siłom powietrznym na skuteczne porażenie i całkowite zniszczenie Trypolskiej Elektrowni Ciepłej w kwietniu 2024 roku⁹⁷. Pociski te, odpalane z taktycznych samolotów Su-34, okazały się trudniejsze do wykrycia niż strategiczne Ch-101.

⁹⁴ J. Daly, *The KH-101 Missiles that Russia Uses To Strike Ukraine. What Are They?*, <https://united-24media.com/war-in-ukraine/the-kh-101-missiles-that-russia-uses-to-strike-ukraine-what-are-they-1193>, [dostęp: 1.12.2025].

⁹⁵ M. Geri, dz. cyt.

⁹⁶ *Kh-69 X-69*, <https://www.armyrecognition.com/military-products/army/missiles/cruise-missiles/kh-69-h-69>, [dostęp: 1.12.2025].

⁹⁷ *Russian Kh-69 that destroyed Kyiv region's largest thermal power plant: overview and characteristics of missile*, <https://global.espresso.tv/military-news-kh-69-missile-used-by-russians-to-destroy-trypillia-thermal-power-plant>, [dostęp: 1.12.2025].

Hipersoniczny debiut – Cyrkon i Kindżał

Rosja wykorzystuje Ukrainę jako poligon doświadczalny dla swojej broni hipersonicznej. Pocisk 3M22 Cyrkon, pierwotnie przeciwokrętowy, został zaadaptowany do ataków na cele lądowe. Podczas fazy rozpędu Cyrkon osiąga prędkości Mach 8–9, jednak w fazie terminalnej, gdy przechodzi na niską wysokość, zwalnia do około 4,5 Mach. Pociski te okazały się możliwe do przechwycenia przez zestawy Patriot PAC-3. Użycie Zirconów w atakach na Kijów w 2024 i 2025 roku miało na celu nie tylko zniszczenie celów, ale także przetestowanie możliwości przełamania systemów Patriot⁹⁸. Kindżały są wykorzystywane do ataków na głęboko ukryte obiekty i pozycje dowodzenia. Ich zastosowanie w operacjach przeciwko magazynom energetycznym pozostaje w sferze możliwości, chociaż potwierdzone użycie dotyczy przede wszystkim obiektów wojskowych.

Północnokoreański wkład – KN-23

Istotnym nowym elementem są pociski balistyczne KN-23 (Hwasong-11A) dostarczane przez Koreę Północną. Są one wizualnie podobne do rosyjskich Iskanderów, mają zasięg ok. 690 km i głowicę 500 kg. Choć istnieją podejrzenia dotyczące jakości wykonania i ograniczonej celności w porównaniu z rosyjskimi systemami, dokładne dane dotyczące niezawodności KN-23 nie są publicznie dostępne. Analizy szczątków wykazały, że pociski te zawierają liczne komponenty elektroniczne produkcji zachodniej⁹⁹.

Rewolucja bezzałogowa – Gerbera i Parodiya

W latach 2024–2025 Rosja wprowadziła do użycia nową klasę dronów, które redefiniują ekonomię pola walki:

1. Gerbera i Parodiya: są to tanie drony wykonane z pianki, sklejk i plastiku, często pozbawione głowicy bojowej lub wyposażone w mały ładunek. Ich kluczowym elementem jest soczewka Lüneburga – pasywne urządzenie, które odbija fale

⁹⁸ 3M22 Zircon – Wikipedia, https://en.wikipedia.org/wiki/3M22_Zircon, [dostęp: 1.12.2025]; T. Safranov, *Russia Launches New Zircon Anti-Ship Missile at Sumy Region*, <https://military.com/en/news/russia-launches-new-zircon-anti-ship-missile-at-sumy-region>, [dostęp: 1.12.2025].

⁹⁹ KN-23, <https://missilethreat.csis.org/missile/kn-23>, [dostęp: 1.12.2025]; D. Dmytriieva, *North Korean KN-23 missiles: Russia's new weapon in war against Ukraine*, <https://newsukraine.rbc.ua/news/north-korean-kn-23-missiles-russia-s-new-1723384830.html>, [dostęp: 1.12.2025]; O. Goncharova, dz. cyt.

radarowe w taki sposób, że mały dron na ekranie radaru wygląda jak duży dron szturmowy Shahed lub nawet samolot bojowy¹⁰⁰.

2. Cel taktyczny: wprowadzenie tych dronów do rojów uderzeniowych w proporcji nawet 50% (stosunek fałszywych celów do bojowych) ma na celu drenaż ukraińskich zasobów obrony powietrznej. Zestrzelenie drona-przynęty (koszt 10–20 tysięcy dolarów) przy użyciu rakiety systemu NASAMS (koszt pocisku AMRAAM ~300–400 tysięcy dolarów) czy Patriot (koszt pocisku PAC-3 ~3–7 milionów dolarów) stanowi asymetrię kosztów sięgającą proporcji 1:30 do 1:700 na korzyść strony atakującej. Dodatkowo Rosja rozpoczęła produkcję głowic termobarycznych do dronów Shahed-136, zwiększając ich siłę rażenia przeciwko celom wewnątrz budynków¹⁰¹.

2.6. Taktyka i operacjonalizacja: od „dezorganizacji” do „anihilacji”

Rosyjska strategia ataków na ukraińską energetykę nie była statyczna. Analiza chronologiczna pozwala wyróżnić wyraźne fazy, świadczące o procesie uczenia się (ang. *learning curve*) rosyjskiego dowództwa i adaptacji do zmieniających się warunków.

Faza I: atak na sieć dystrybucyjną (zima 2022/2023)

Pierwsza kampania strategiczna, rozpoczęta w październiku 2022 roku, miała na celu wywołanie ogólnokrajowego blackoutu.

- Taktyka: ataki koncentrowały się na autotransformatorach w stacjach wysokiego napięcia (750 kV i 330 kV). Rosjanie zakładali, że zniszczenie węzłów przesyłowych odetnie elektrownie (zwłaszcza jądrowe) od odbiorców¹⁰².

¹⁰⁰ I. Anokhin, S. Faragasso, *Russian Decoy Drones that Depend on Western Parts Pose a Great Challenge to Ukrainian Defenses*, <https://isis-online.org/isis-reports/russian-decoy-drones-that-depend-on-western-parts-pose-a-great-challenge>, [dostęp: 1.12.2025]; V. Kushnikov, *Western-made components found in Parody decoy drone*, <https://military.com/en/news/western-made-components-found-in-parody-decoy-drone>, [dostęp: 1.12.2025].

¹⁰¹ *Russia massively launching decoy drone with Western components to distract Ukrainian air defenses*, <https://english.nv.ua/nation/parody-russians-use-a-new-type-of-uav-to-imitate-the-shahed-what-is-known-50465488.html>, [dostęp: 1.12.2025]; D. Albright i in., *Alabuga's Shahed 136 (Geran 2) Warheads: A Dangerous Escalation*, <https://isis-online.org/isis-reports/alabugas-shahed-136-geran-2-warheads-a-dangerous-escalation>, [dostęp: 1.12.2025].

¹⁰² M. Geri, dz. cyt.

- Wynik: mimo poważnych uszkodzeń i konieczności wprowadzenia grafików wyłączeń, system przetrwał. Ukraińcy wykazali się niezwykle zdolnością do improwizacji, a zachodnia pomoc pozwoliła na szybkie naprawy. Strategia dezorganizacji okazała się nieskuteczna w długim terminie.

Faza II: Strategia Anihilacji Generacji (Od Wiosny 2024)

Wiosną 2024 roku, po zgromadzeniu zapasów rakiet, Rosja zmieniła cel. Zamiast atakować łatwe do zastąpienia podstacje, uderzyła w serce systemu – wielkoskalową generację.

- Cele: skoncentrowano się na elektrowniach cieplnych (TPP) i wodnych (HPP). Są to obiekty, których naprawa trwa lata¹⁰³.
- Skutki: do jesieni 2025 roku zniszczono lub okupowano około 65% operacyjnych zdolności wytwórczych Ukrainy (łącznie ~24–25 GW z ~37 GW w momencie inwazji). Zniszczono lub poddano zajęciu 90% zdolności wytwórczych DTEK oraz ponad 70% mocy cieplnej całego sektora; ok. 40% elektrowni wodnych zostało poważnie uszkodzonych. Zniszczenie takich gigantów jak Elektrownia Trypolska czy Zmijiwska pozbawiło system ukraiński tzw. mocy manewrowych, niezbędnych do bilansowania szczytów zapotrzebowania¹⁰⁴.
- Adaptacja taktyki „Double Tap”: Rosjanie zaczęli stosować taktykę podwójnego uderzenia w ten sam cel w odstępie czasowym, mającą na celu zabicie ekip ratunkowych i strażaków, co potęguje chaos i straty w ludziach.

Zima 2024/2025: wojna totalna o zasoby

W fazie przygotowań do zimy 2024/2025, Rosja rozszerzyła bank celów o infrastrukturę gazową. Uderzenia w magazyny gazu (w tym największe w Europie magazyny podziemne w zachodniej Ukrainie) oraz stacje kompresorów miały na celu uniemożliwienie Ukrainie wykorzystania gazu jako paliwa zastępczego dla zniszczonych

¹⁰³ Tamże.

¹⁰⁴ B. Murdoch, *Russian strikes on Ukraine's Energy grid follow systematic pattern, analysis shows*, <https://euromaidanpress.com/2025/11/20/russian-strikes-on-ukraines-energy-grid-follow-systematic-pattern>, [dostęp: 1.12.2025]; *The Russia-Ukraine War Report Card, Nov. 19, 2025*, <https://www.russiamatters.org/news/russia-ukraine-war-report-card/russia-ukraine-war-report-card-nov-19-2025>, [dostęp: 1.12.2025].

elektrowni węglowych oraz zablokowanie potencjalnego eksportu/magazynowania gazu dla UE. W listopadzie 2024 roku przeprowadzono masowy atak przy użyciu blisko 200 rakiet i dronów, celując jednocześnie w generację i dystrybucję¹⁰⁵.

Taktyka przełamania OPL: ataki saturacyjne i wielokierunkowe

Ataki charakteryzują się niezwykle złożonością. Typowy zmasowany atak wygląda następująco¹⁰⁶:

1. Nocne uderzenie dronów: setki dronów Shahed i przynęt (Gerbera) nadlatują z różnych kierunków, klucząc i zmieniając wysokość, aby zmusić OPL do zużycia amunicji i ujawnienia radarów.
2. Uderzenie raketowe: w momencie największego obciążenia systemu obrony, nadlatują pociski manewrujące Ch-101 (często programowane na skomplikowane trasy, np. zawracające nad zachodnią Ukrainą).
3. Ataki pociskami balistycznymi: na wybrane, kluczowe cele spadają pociski Iskander-M, KN-23 lub Kindżał, których czas dolotu jest minimalny, a przechwycenie wymaga systemów klasy Patriot/SAMP-T, których Ukraina ma deficyt.

Wnioski

1. Analiza wojskowych sił i środków wykorzystywanych przez Rosję do niszczenia ukraińskiej infrastruktury energetycznej ujawnia obraz nowoczesnego konfliktu totalnego, w którym technologia służy realizacji ludobójczych celów politycznych.
2. Rosja zademonstrowała zdolność do adaptacji taktycznej (przejście na ataki nocne, użycie przynęt), innowacji technicznej (modyfikacje Ch-101, Ch-69) oraz skutecznego wykorzystania sojuszy (drony irańskie, rakiety północnokoreańskie)

¹⁰⁵ V. Rafalovych, *The Fourth Winter: Inside Russia's Evolving War on Ukraine's Energy*, <https://www.cyis.org/post/the-fourth-winter-inside-russia-s-evolving-war-on-ukraine-s-energy>, [dostęp: 1.12.2025]; A. Kryzhnyi, *Russia changes tactics in attacks on Ukraine's energy sector*, <https://www.pravda.com.ua/eng/news/2025/11/09/8006535>, [dostęp: 1.12.2025].

¹⁰⁶ *Russian Offensive Campaign Assessment*, dz. cyt.

do podtrzymania tempa operacji mimo sankcji. Z drugiej strony, kampania ta obnażyła również ograniczenia rosyjskiej broni precyzyjnej (konieczność użycia masowych ilości, niska celność KN-23) i zmusiła Ukrainę do bezprecedensowej innowacyjności w zakresie obrony przeciwlotniczej i naprawy sieci.

3. Wniosek jest jednoznaczny: obrona infrastruktury energetycznej nie jest już tylko kwestią inżynierską, ale stała się główną domeną walki, wymagającą integracji systemów obrony powietrznej (zwłaszcza przeciwbalistycznej), wywiadu oraz strategii decentralizacji zasobów.

3. Metody ochrony infrastruktury energetycznej w Ukrainie w latach 2022–2024

3.1. Paradygmat bezpieczeństwa energetycznego w warunkach wojny totalnej

Współczesna doktryna wojenna, obserwowana w ukraińskim teatrze działań, redefiniuje pojęcie frontu, rozszerzając je na głębokie zaplecze cywilne, ze szczególnym uwzględnieniem infrastruktury krytycznej. Sektor energetyczny, będący fundamentem funkcjonowania państwa, gospodarki i dobrostanu społecznego, stał się głównym celem strategicznym agresora. Celem systematycznych ataków nie jest jedynie degradacja potencjału militarnego, ale wywołanie kaskadowych awarii prowadzących do zapaści humanitarnej i gospodarczej.

W latach 2022–2024 Ukraina stanęła przed wyzwaniem ochrony rozległego, scentralizowanego systemu energetycznego, odziedziczonego w dużej mierze po czasach Związku Radzieckiego. System ten, charakteryzujący się dużymi jednostkami wytwórczymi i węzłami przesyłowymi, okazał się podatny na precyzyjne uderzenia raketowe. W listopadzie 2024 roku przeprowadzono jeden z największych ataków przy użyciu blisko 200 rakiet i dronów, celując jednocześnie w generację i dystrybucję energii, pozostawiając ponad milion gospodarstw domowych bez dostępu do prądu. Odpowiedź strony ukraińskiej ewoluowała od doraźnych napraw do systemowych rozwiązań inżynierskich i strategicznych zmian w architekturze sieci.

W niniejszym rozdziale postawiono tezę, że skuteczna ochrona infrastruktury energetycznej w warunkach asymetrycznego konfliktu wymaga holistycznego podejścia, łączącego „twardą” inżynierię fortyfikacyjną z „miękkimi” rozwiązaniami cyfrowymi oraz strukturalną decentralizacją.

3.2. Podstawy teoretyczne: analiza ryzyka sabotażu i modelowanie zagrożeń

Zanim przejdziemy do omówienia fizycznych metod ochrony, konieczne jest zrozumienie teoretycznych podstaw analizy ryzyka, które determinują priorytetyzację obiektów do ochrony. W inżynierii bezpieczeństwa kluczowym narzędziem wykorzystywanym do modelowania działań dywersyjnych jest metoda drzewa ataku (Attack Tree Analysis – ATA).

Ewolucja metodologii: od teorii domina do drzew ataku

Fundamentem sekwencyjnego modelowania awarii obiektów przemysłowych jest teoria domina H.W. Heinricha z 1941 roku, która zakładała liniową sekwencję czynników prowadzących do katastrofy. W kontekście złożonych systemów energetycznych, ta metoda ewoluowała w stronę analizy drzewa niezdatności (Fault Tree Analysis – FTA), opracowanej pierwotnie w latach 60. XX wieku dla systemów raketowych Minuteman. FTA pozwala na dedukcyjną dekompozycję zdarzeń, mapując kombinacje awarii komponentów prowadzące do zdarzenia szczytowego (awarii systemu)¹⁰⁷.

Jednakże w warunkach wojennych, w których mamy do czynienia z celowym działaniem inteligentnego przeciwnika, klasyczne FTA jest niewystarczające. Zastosowanie znajdują tu drzewa ataku, spopularyzowane m.in. przez Bruce'a Schneiera w roku 1999. Drzewo ataku jest modelem koncepcyjnym odwzorowującym sposób, w jaki zasoby lub cele mogą zostać zaatakowane. W przeciwieństwie do FTA, które skupia się na awariach losowych, drzewa ataku modelują intencjonalne działania sabotażowe, cyberataki czy ataki kinetyczne¹⁰⁸.

Zastosowanie tych modeli teoretycznych w praktyce ukraińskiej mogło pozwolić na identyfikację tzw. „wąskich gardeł”. Rosyjskie ataki w fazie II kampanii (od marca 2024) wykazały, że kluczowymi celami strategicznymi stały się autotransformatory wysokiego napięcia (750 kV i 330 kV), których zniszczenie powoduje największe straty systemowe i które są najtrudniejsze do zastąpienia.

¹⁰⁷ L. Chybowski, D. Chybowska, *Ocena istotności zdarzeń pierwotnych związanych z działaniami dywersyjnymi przeciwko infrastrukturze krytycznej*, Assessment of primary events importance related to subversion against critical infrastructure, [w:] Materiały konferencyjne (Poznań, 2022); por. także: B. Schneier, *Attack Trees*, „Dr. Dobbs Journal”, grudzień 1999; H. Heinrich, *Industrial Accident Prevention* (McGraw Hill, 1941); H.A. Watson, *Launch Control Safety Study* (Murray Hill 1961).

¹⁰⁸ L. Chybowski, D. Chybowska, dz. cyt.

Dane empiryczne potwierdzają katastrofalny wpływ: do września 2024 roku 90 elektrociepowni TPP i 40 elektrowni wodnych HPP zostało unieruchomionych, co oznaczało utratę 80% mocy cieplnej i około 50% całkowitych zdolności wytórczych kraju. To właśnie wokół tych elementów (autotransformatorów i źródeł generacji) skoncentrowano zarówno wysiłki inżynieryjne obrony, jak i strategię rosyjskich ataków.

3.3. Inżynieryjna ochrona pasywna: system trzystopniowy

W odpowiedzi na zidentyfikowane zagrożenia dla autotransformatorów i podstacji, Ukraina opracowała i wdrożyła unikalny trzystopniowy system ochrony pasywnej. Podejście to łączy proste rozwiązania na poziomie taktycznym z zaawansowanymi konstrukcjami inżynieryjnymi. Każdy poziom odpowiada innemu spektrum zagrożeń, od dronów kamikadze do pocisków rakietowych.

Poziom 1: Ochrona przed odłamkami i falą uderzeniową

Pierwszy poziom ochrony został wdrożony najszybciej i obejmuje proste, ale skuteczne rozwiązania inżynieryjne.

- **Technologia:** Podstawą są gabiony (kosze z siatki stalowej wypełnione piaskiem, ziemią lub kamieniami) oraz worki typu Big-Bag wypełnione piaskiem. Konstrukcje te są układane wokół wrażliwych elementów infrastruktury¹⁰⁹.
- **Cel:** Ochrona przed odłamkami z zestrzelonych rakiet i dronów oraz przed falą uderzeniową z bliskich eksplozji. Nie chronią one przed bezpośrednim trafieniem, ale minimalizują skutki wybuchów w sąsiedztwie¹¹⁰.

¹⁰⁹ V. Nazarenko, *Ukraine has prepared three levels of protection against Russia's attacks on energy infrastructure*, <https://war.ukraine.ua/war-news/ukraine-protection-russias-attacks-energy-infrastructure>, [dostęp: 1.12.2025]; A. Sheremet, *Concrete blocks and sandbags*, „The Financial Times” reported how Ukraine is preparing for attacks on the energy sector”, <https://babel.ua/en/news/100170-concrete-blocks-and-sandbags-the-financial-times-reported-how-ukraine-is-preparing-for-attacks-on-the-energy-sector>, [dostęp: 1.12.2025].

¹¹⁰ O. Kosharna, *Energy infrastructure facilities will have three levels of protection*, Ukrenergo CEO Kudrytskyi, <https://censor.net/en/n3449115>, [dostęp: 1.12.2025].

- Skala wdrożenia: Do końca 2023 roku zabezpieczono w ten sposób 103 obiekty w 21 regionach Ukrainy¹¹¹.
- Ocena skuteczności: premier Ukrainy Denys Szmyhal ocenił skuteczność tych środków na 80–90% w przypadku dronów, które zboczyły z kursu lub ich szczątków. Są to rozwiązania relatywnie tanie i szybkie w montażu¹¹².

Poziom 2: Ochrona przed bezpośrednim trafieniem dronów

Drugi poziom to zaawansowane konstrukcje inżynieryjne, mające na celu ochronę przed bezpośrednim uderzeniem dronów kamikadze (np. Shahed), które przenoszą głowice o wadze do 50 kg.

- Technologia: Wokół kluczowych autotransformatorów i podstacji wznoszone są żelbetowe konstrukcje ochronne (często nazywane „sarkofagami”). Wykorzystuje się prefabrykowane elementy betonowe, bloki typu „Lego” oraz specjalnie zaprojektowane panele żelbetowe. Ukraińska firma L7 zaprezentowała modele schronów „Forteca” i „Barbet”. Model „Barbet” to cylindryczna konstrukcja żelbetowa wzmocniona przyporami, przeznaczona m.in. do ochrony zbiorników paliwa, która rozprasza falę uderzeniową¹¹³.
- Specyfikacja: Konstrukcje te nie wymagają głębokich fundamentów (montaż na płytach betonowych), co przyspiesza budowę. Ściany mają grubość np. 300 mm i są dodatkowo wzmocnione¹¹⁴.
- Wsparcie materiałowe: Projekt ten wymaga ogromnych ilości stali i betonu. USAID sfinansowało zakup 20 000 ton metalu (zbrojenia) dla Agencji Odbudowy w celu budowy tych osłon¹¹⁵.

¹¹¹ V. Nazarenko, dz. cyt.

¹¹² A. Sheremet, dz. cyt.

¹¹³ V. Nazarenko, dz. cyt.; V. Khrystoforov, *Ukrainian company unveils reinforced concrete shelters to protect critical infrastructure*, <https://www.pravda.com.ua/eng/news/2025/10/04/8001210>, [dostęp: 1.12.2025].

¹¹⁴ V. Khrystoforov, dz. cyt.

¹¹⁵ *Agency for Restoration and Infrastructure Development and USAID work together on passive protection of energy facilities*, <https://www.kmu.gov.ua/en/news/ahentstvo-vidnovlennia-ta-usaid-spilno-pratsiuiut-nad-pasyvnyim-zakhystom-enerhoobiektiv>, [dostęp: 1.12.2025].

- Skala wdrożenia: Ochroną drugiego poziomu objęto 22 podstacje i 63 autotransformatory w 14 kluczowych regionach. Prace rozpoczęto w marcu 2023 roku¹¹⁶.
- Ocena skuteczności: Według danych z października 2024 roku, z 74 chronionych obiektów, tylko jeden autotransformator został zniszczony w wyniku bezpośredniego trafienia ciężką rakietą (przed czym ten poziom nie chroni). W pozostałych przypadkach ataki dronów i lżejszych pocisków zostały skutecznie zneutralizowane przez betonowe osłony, co potwierdza ich 98% skuteczność w zakładanym zakresie działania¹¹⁷.

Poziom 3: Ochrona przeciwrakietowa

Trzeci poziom to najbardziej skomplikowane i kosztowne przedsięwzięcie, mające na celu ochronę przed precyzyjnymi pociskami raketowymi.

- Technologia: Są to masywne, często podziemne lub częściowo zagłębione bunkry, zdolne wytrzymać bezpośrednie trafienie pociskiem balistycznym lub manewrującym. Projekty te przeszły testy poligonowe, gdzie modele struktur poddano próbom wybuchowym symulującym realne zagrożenia¹¹⁸.
- Wyzwania: Główną barierą są ogromne koszty i czasochłonność. Ukrenergo wskazuje, że ukrycie wielkich transformatorów 750 kV pod ziemią jest niezwykle trudne technologicznie (problemy z chłodzeniem, gabaryty) i wymagałoby miliardowych nakładów, dlatego ten poziom ochrony jest wdrażany selektywnie w najbardziej krytycznych węzłach¹¹⁹.
- Status: Prace nad tym poziomem są w fazie eksperymentalnej i ograniczonej realizacji w 22 podstacjach¹²⁰.

¹¹⁶ V. Nazarenko, dz. cyt.

¹¹⁷ *Second-level power grid protection in Ukraine shows 98% effectiveness*, <https://mediacenter.org.ua/second-level-power-grid-protection-in-ukraine-shows-98-effectiveness>, [dostęp: 1.12.2025].

¹¹⁸ *Restoration Agency implements three-tier energy infrastructure protection system – Nayyem*, <https://en.interfax.com.ua/news/economic/953851.html>, [dostęp: 1.12.2025]; „Agency_for_Restoration”, https://www.jica.go.jp/english/information/seminar/2023/_icsFiles/afieldfile/2024/03/12/0216_1-2_Agency_for_Restoration_02.16.pdf, [dostęp: 1.12.2025].

¹¹⁹ H. Nelson, *Ukraine faces its most perilous winter yet*, <https://www.atlanticcouncil.org/blogs/energy-source/ukraine-faces-its-most-perilous-winter-yet>, [dostęp: 1.12.2025].

¹²⁰ V. Nazarenko, dz. cyt.

3.4. Systemy aktywnej obrony i walka elektroniczna (WRE)

Ochrona pasywna jest jedynie ostatnią linią obrony. Pierwszą stanowią aktywne systemy neutralizacji zagrożeń powietrznych.

Obrona Powietrzna (OP)

Ukraina zintegrowała zróżnicowany arsenał systemów OP, tworząc wielowarstwową tarczę.

- Systemy raketowe: Wykorzystywane są zarówno systemy posowieckie (S-300, Buk), jak i nowoczesne zachodnie (Patriot, NASAMS, IRIS-T). Są one kluczowe do zwalczania pocisków balistycznych i manewrujących. Podczas ataku pod koniec listopada 2024 roku, ukraińska OPL zestrzeliła 76 pocisków manewrujących.
- Mobilne Grupy Ogniowe: Ze względu na wysoki koszt rakiet przechwytyjących, do zwalczania tanich dronów Shahed powszechnie stosuje się mobilne grupy ogniowe. Są to zespoły wyposażone w samochody terenowe, reflektory, broń maszynową (np. karabiny maszynowe DSzK, Browning M2) oraz przenośne zestawy przeciwlotnicze (MANPADS). Jest to ekonomicznie efektywna metoda „koszt-efekt”¹²¹.

Walka radioelektroniczna (WRE)

WRE stała się niewidzialną tarczą chroniącą infrastrukturę. Systemy te pozwalają na neutralizację dronów poprzez zakłócanie ich systemów nawigacji i łączności.

- Mechanizm działania: Stosuje się zakłócanie sygnałów sterujących (*jamming*), co powoduje utratę kontroli nad dronem oraz spoofing GPS, czyli emisję fałszywych sygnałów nawigacyjnych, które „mylą” drona co do jego położenia, kierując go w bezpieczne miejsce lub powodując rozbicie.
- Efektywność: W raportach z ataków często pojawiają się informacje o dronach, które „zaginięły” z radarów (ang. *lost track*). Np. podczas ataku w listopadzie

¹²¹ S. Rimutis, *Lessons of War: Ukraine's Energy Infrastructure Damage, Resilience and Future Opportunities*, https://www.gssc.lt/wp-content/uploads/2024/05/v04_Rimutis_Ukrainos-energetikos-sektoriaus-zala_EN_A4.pdf, [dostęp: 1.12.2025].

2024 roku, ukraińskie siły powietrzne podały, że 62 rosyjskie drony „zagięły”, co z dużym prawdopodobieństwem przypisuje się działaniu systemów WRE.

- Cyberprzejęcie: Rozwijane są również technologie cybernetycznego przejmowania kontroli nad wrogimi dronami.

3.5. Decentralizacja i koncepcja „wysp energetycznych”

Tradycyjny, scentralizowany model energetyki okazał się „kruchy” w obliczu wojny. Zniszczenie jednej dużej elektrowni lub węzłowej podstacji pozbawia prądu setki tysięcy odbiorców. Dlatego kluczową strategią adaptacyjną stała się decentralizacja i tworzenie mikrosieci.

Generacja rozproszona (DG)

Generacja rozproszona (*Decentralised Generation* – DG) polega na produkcji energii blisko miejsca jej zużycia, z wykorzystaniem mniejszych jednostek wytwórczych.

- Technologie: Wykorzystuje się energię słoneczną (PV), wiatrową, biomasę oraz małe turbiny gazowe i silniki gazowe. Te ostatnie, o mocy od 5 do 100 MW, są szczególnie cenne jako źródła elastyczne i trudne do zniszczenia pojedynczym atakiem rakietowym¹²².
- Skala: W 2023 roku w Ukrainie zainstalowano ponad 5000 domowych systemów solarnych. W 2024 roku do sieci podłączono 835 MW nowych mocy rozproszonych¹²³.

Wyspy energetyczne (Microgrids)

Koncepcja „wysp energetycznych” zakłada tworzenie autonomicznych obszarów sieci, które mogą funkcjonować niezależnie od krajowego systemu elektroenergetycznego

¹²² R. Bandura, A. Romanishyn, *Striving for Access, Security, and Sustainability: Ukraine’s Transition to a Modern and Decentralized Energy System*, <https://www.csis.org/analysis/striving-access-security-and-sustainability>, [dostęp: 1.12.2025].

¹²³ H. Zinchenko, *835 MW of distributed generation connected in 2024 – Ministry of Energy*, <https://ua-energy.org/en/posts/31-12-2024-812032b8-5207-4ac4-ba71-8bb818b96e8b>, [dostęp: 1.12.2025].

(tryb wyspowy) w przypadku awarii systemowej (blackoutu)¹²⁴. Strategia rozproszonej generacji energii jest priorytetem dla Ukrainy, która rozwija „Strategię Rozproszonej Generacji do 2035” i promuje mikrogrid jako część odbudowy infrastruktury energetycznej¹²⁵.

Wnioski

Analiza metod ochrony ukraińskiej infrastruktury energetycznej w latach 2022–2024 prowadzi do następujących wniosków:

1. Skuteczność ochrony hybrydowej: Żadna pojedyncza metoda nie jest wystarczająca. Skuteczność zapewnia jedynie synergia ochrony fizycznej (betonowe osłony), aktywnej (OPL, WRE) oraz strukturalnej (decentralizacja). Poziom 2 ochrony pasywnej wykazał niemal 100% skuteczność przeciwko dronom, ale jest bezradny wobec ciężkich rakiet, co podkreśla rolę OPL.
2. Decentralizacja jako strategia przetrwania: Przejście od modelu scentralizowanego do rozproszonego (DG, mikrosieci) jest najskuteczniejszą metodą zwiększenia odporności systemowej. Skraca czas przywracania zasilania i utrudnia przeciwnikowi całkowite paraliżowanie systemu.
3. Innowacyjność w warunkach ekstremalnych: Ukraina stała się inkubatorem innowacji w zakresie bezpieczeństwa energetycznego, wdrażając unikalne rozwiązania inżynierskie (sarkofagi dla transformatorów) w niespotykanym tempie i skali.

¹²⁴ R. McIlmoil, *Microgrids Could Enhance Grid Resilience*, <https://www.nrel.gov/news/detail/program/2025/microgrids-could-enhance-grid-resilience>, [dostęp: 1.12.2025]; *Power Grids Unplugged: How Islanding is Changing Autonomous Energy*, <https://www.smpnet.tech/post/power-grids-unplugged-how-islanding-is-changing-autonomous-energy>, [dostęp: 1.12.2025].

¹²⁵ R.W. Stand, *Decentralizing Ukraine's energy future: microgrids as a path to independence*, <https://energytransition.org/2024/10/decentralizing-ukraines-energy-future-microgrids-as-a-path-to-independence>, [dostęp: 1.12.2025]; *Why Ukraine should develop distributed generation?*, <https://golaw.ua/insights/energy-alert/chomu-ukrayini-varto-rozvivati-rozpodilenu-generacziyu>, [dostęp: 1.12.2025].

4. Rosyjska sztuka wojskowa wobec potencjalnych ataków militarnych na infrastrukturę energetyczną państw trzecich – perspektywa 2025–2030

4.1. Ewolucja doktrynalna i ramy strategiczne rosyjskiej sztuki wojennej

Zrozumienie mechanizmów, jakimi Rosja planuje oddziaływać na infrastrukturę energetyczną, wymaga głębokiej analizy ewolucji jej dokumentów doktrynalnych. W latach 2021–2023 nastąpiło znaczące zaostrzenie retoryki i definicji zagrożeń, co bezpośrednio przekłada się na planowanie operacyjne Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej.

Strategia Bezpieczeństwa Narodowego 2021: manifest oblężonej twierdzy

Strategia Bezpieczeństwa Narodowego Federacji Rosyjskiej, zaktualizowana i podpisana przez Władimira Putina w lipcu 2021 roku, stanowi cezurę w rosyjskim myśleniu o bezpieczeństwie globalnym. W przeciwieństwie do poprzedniej wersji z 2015 roku, która dopuszczała jeszcze elementy współpracy, dokument z 2021 roku definiuje relacje z Zachodem jako stan trwałej, systemowej i egzystencjalnej konfrontacji¹²⁶.

Centralnym elementem nowej strategii jest zwrot do wewnątrz i budowa autarkii, co ma uodpornić Rosję na presję zewnętrzną, jednocześnie dając jej wolną rękę do działań ofensywnych w sferze ekonomicznej i infrastrukturalnej. Dokument

¹²⁶ D. Trenin, *Russia's National Security Strategy: A Manifesto for a New Era*, <https://carnegieendowment.org/posts/2021/07/russias-national-security-strategy-a-manifesto-for-a-new-era?lang=en>, [dostęp: 1.12.2025].

ten legitymizuje działania asymetryczne jako formę „aktywnej obrony”. Rosyjscy stratedzy tacy jak Dmitrij Trenin, określają tę strategię jako „manifest nowej ery”, w której hegemonia Zachodu upada, a Rosja musi być gotowa na brutalną walkę o zasoby i wpływy¹²⁷.

W kontekście infrastruktury energetycznej, strategia ta implikuje dwa kluczowe wnioski dla planistów wojskowych na lata 2025–2030:

1. Infrastruktura jako cel strategiczny: Osłabienie potencjału ekonomicznego przeciwnika (w tym jego bezpieczeństwa energetycznego) jest uznawane za kluczowy element obrony interesów narodowych Rosji. Uderzenia w systemy energetyczne nie są już tylko taktyką pola walki, ale narzędziem geopolitycznej presji¹²⁸.
2. Samowystarczalność jako broń: Budowa własnej odporności (ang. *resilience*) ma umożliwić Rosji przetrwanie kontruderzeń gospodarczych po tym, jak sama dokona ataku na infrastrukturę Zachodu.

Doktryna morska 2022: Militaryzacja „Oceanu Światowego”

Przyjęta 31 lipca 2022 roku podczas parady na Dniu Marynarki Wojennej Rosji w Petersburgu, nowa Doktryna Morska Federacji Rosyjskiej wprowadza radykalną zmianę w postrzeganiu domeny morskiej w stosunku do poprzedniej wersji z 2015 roku. Dokument przyjęty już w trakcie pełnoskalowej wojny w Ukrainie wyraźnie identyfikuje Stany Zjednoczone i NATO jako główne zagrożenia dla interesów morskich Rosji i proklamuje stanowczą obronę rosyjskich pozycji na tzw. „Oceanie Światowym”¹²⁹.

¹²⁷ J. Cooper, *Russia's updated National Security Strategy*, <https://www.ndc.nato.int/fr/russias-updated-national-security-strategy>, [dostęp: 1.12.2025]; D. Trenin, dz. cyt.

¹²⁸ C. Hobhouse, *On a war footing: Securing critical energy infrastructure*, <https://www.iss.europa.eu/publications/briefs/war-footing-securing-critical-energy-infrastructure>, [dostęp: 1.12.2025]; E. Massalin, *Strategic Analysis on the Energy Security Measures of Russia*, <https://www.enseccoe.org/wp-content/uploads/2024/01/2021-08-strategic-analysis-on-the-energy-security-measures-of-russia-enrica-massalin.pdf>, [dostęp: 1.12.2025].

¹²⁹ *Strategy for Development of the Arctic Zone of the Russian Federation and Provision of National Security for the Period up to 2035 (Revised)*, https://usnwc.edu/_images/portals/0/NWCDepartments/Russia-Maritime-Studies-Institute/16MAR23_20201026_ENG_RUS_Arctic-Strategy2035_FINAL_16MAR238f95.pdf, [dostęp: 1.12.2025]; R. Czachor, *Ewolucja doktryny morskiej Federacji Rosyjskiej w latach 2001–2022. Ujęcie politologiczne*, <https://www.studiapolitologiczne.pl/pdf-199427-119697?filename=The%20Evolution%20of%20the.pdf>, [dostęp: 1.12.2025]; Y. Weber, *Russia's New Maritime Doctrine*, Marine Corps University Press – MES Insights, sierpień 2022, <https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/MES-Publications/MES-Insights/Russias-New-Maritime-Doctrine>, [dostęp: 1.12.2025].

W porównaniu z poprzednią doktryną z 2015 roku, dokument z 2022 roku przyjmuje znacznie bardziej konfrontacyjny ton, zamieniając język ograniczający się do współpracy globalnej na język podkreślający potrzebę realizacji „obiektywnie istotnych potrzeb” państwa w działaniach morskich. Tekst doktryny definiuje główny cel Rosji jako osiągnięcie statusu „wielkiej mocy morskiej” i utrzymanie zdolności do działań na całej rozciągłości „Oceanu Światowego”¹³⁰.

Doktryna wspomina o konieczności posiadania zdolności do działań w stosunku do instalacji morskich i podwodnych, w tym rurociągów, kabli telekomunikacyjnych oraz platform wiertniczych w przypadku konfliktu. Koncepcja działań przeciwko infrastrukturze dennej morza (ang. *seabed warfare*) jest obecna w rosyjskim myśleniu strategicznym, a jej infrastruktura realizacyjna jest rozproszona pomiędzy Marynarką Wojenną, Głównym Zarządzeniem Badań Hydrograficznych (GUGI) oraz służbami wywiadu (GRU)¹³¹.

Koncepcja „wojny nowej generacji” i nieliniowość pola walki

Rosyjska myśl wojskowa, często utożsamiana na Zachodzie z tzw. „Doktryną Gierasimowa”, w rzeczywistości jest znacznie bardziej złożona i opiera się na koncepcji wojny nieliniowej oraz refleksyjnej kontroli. Generał Walerij Gierasimow w swoim przełomowym artykule z 2013 roku *Wartość nauki w przewidywaniu* podkreślał, że granice między wojną a pokojem uległy zatarciu, a działania militarne stanowią jedynie część (w proporcji 1:4) szerokiego spektrum środków przymusu¹³².

W kontekście lat 2025–2030, analiza publikacji w periodyku „Wojennaja Mysl” wskazuje na ewolucję tej koncepcji w stronę „strategicznego rażenia infrastruktury krytycznej” (SPO – Strategicheskoye Porazheniye Ob’yektov). Rosyjscy teoretycy tacy jak S.G. Czekinow i S.A. Bogdanow, argumentują, że nowoczesna wojna będzie polegać na precyzyjnych uderzeniach w węzły systemowe przeciwnika, aby wywołać chaos i zmusić go do kapitulacji bez konieczności zajmowania terytorium¹³³.

¹³⁰ *Putin Approves Russia’s First Long-Term Naval Strategy Through 2050*, <https://www.themoscowtimes.com/2025/06/09/putin-approves-russias-first-long-term-naval-strategy-through-2050-a89381>, [dostęp: 1.12.2025]; *Strategy for Development of the Arctic...*, dz. cyt.

¹³¹ *Strategy for Development of the Arctic...*, dz. cyt.

¹³² L. Davydenko, *Russian new generation warfare of controlled chaos*, <https://indsr.org.tw/en/respublicationcon?uid=15&resid=2999&pid=5350&typeid=3>, [dostęp: 1.12.2025].

¹³³ T. Thomas, *Russian nonlethal weapons*, <https://www.mitre.org/sites/default/files/2021-11/pr-20-0145-russia-nonlethal-weapon-concept.pdf>, [dostęp: 1.12.2025]; M. Kofman i in., *Russian Military Strategy: Core Tenets and Operational Concepts*, <https://www.cna.org/reports/2021/08/Russian-Military-Strategy-Core-Tenets-and-Operational-Concepts.pdf>, [dostęp: 1.12.2025].

Kluczowe elementy tej teorii w odniesieniu do energetyki to:

1. Targetowanie systemowe: Celem nie jest zniszczenie pojedynczej elektrowni, ale wywołanie kaskadowej awarii (blackoutu) poprzez uderzenie w węzły synchronizacji i sterowania¹³⁴.
2. Przyjazny uścisk (ang. *Friendly Embrace*): Koncepcja V.L. Makhnina, opisana w czasopiśmie „Wojennaja Mysl”, sugeruje wykorzystanie zależności ekonomicznych i infrastrukturalnych do „uduszenia” przeciwnika w pozornie pokojowych relacjach, co następnie przechodzi w fazę kinetyczną¹³⁵.

4.2. Operacjonalizacja zagrożeń kinetycznych – domena podwodna i morska

Najbardziej krytycznym i najtrudniejszym do obrony obszarem w latach 2025–2030 będzie domena podwodna. Rosja systematycznie rozwija unikalne w skali światowej zdolności do prowadzenia działań na dnie morskim, traktując infrastrukturę przesyłową (kable, rurociągi) jako „miękkie podbrzusze” Sojuszu Północnoatlantyckiego.

Siły i środki działań podwodnych

Centralną rolę w rosyjskich operacjach podwodnych odgrywa Główny Zarząd Badań Głębinowych (GUGI) Ministerstwa Obrony FR. Jest to struktura działająca niezależnie od dowództwa Marynarki Wojennej, podlegająca bezpośrednio Ministrowi Obrony, co świadczy o jej strategicznym znaczeniu. GUGI dysponuje flotą specjalistycznych okrętów podwodnych i nawodnych, zaprojektowanych do działań na dużych głębokościach.

¹³⁴ V. Gerasimov, *The Value of Science Is in the Foresight. New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations*, https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf, [dostęp: 1.12.2025]; M.-A. Russon, *The race to shore up Europe's power grids against cyberattacks and sabotage*, https://www.theregister.com/2025/11/03/europe_power_grid_security, [dostęp: 1.12.2025].

¹³⁵ T.L. Thomas, *Russian Military Thought: Concepts and Elements*, <https://www.armyupress.army.mil/Portals/7/Hot-Spots/docs/Russia/Mitre-Thomas.pdf>, [dostęp: 1.12.2025].

Kluczowe jednostki GUGI, które będą stanowić zagrożenie w latach 2025–2030, to:

1. Okręt-matka K-329 Biełgorod: Przystosowany do przenoszenia miniaturowych okrętów podwodnych (np. typu Łoszarik) oraz autonomicznych torped Posejdon. Jego zdolność do skrytego operowania i wypuszczania jednostek dywersyjnych czyni go idealną platformą do niszczenia infrastruktury transatlantyckiej¹³⁶.
2. Okręty badawcze typu Jantar: Jednostki te, oficjalnie oceanograficzne, są wyposażone w zdalnie sterowane pojazdy podwodne (ROV) i zaawansowane systemy sonarowe. Jantar był wielokrotnie obserwowany w pobliżu kluczowych kabli podmorskich, co sugeruje prowadzenie rozpoznania pod kątem przyszłego sabotażu¹³⁷.

System Posejdon (2M39) i zagrożenie dla infrastruktury przybrzeżnej

W perspektywie 2025–2030 operacyjność osiągnie system Posejdon (wcześniej znany jako Status-6). Jest to autonomiczny, bezzałogowy pojazd podwodny (UUV) o napędzie jądrowym i niemal nieograniczonym zasięgu. Choć w mediach często przedstawiany jest jako broń nuklearna „dnia sądu” mająca wywołać radioaktywne tsunami, jego znaczenie taktyczne i operacyjne jest szersze¹³⁸.

Analitycy wskazują, że Posejdon może być wykorzystany do skrytego niszczenia infrastruktury przybrzeżnej o znaczeniu strategicznym, takiej jak terminale LNG, porty energetyczne czy farmy wiatrowe *offshore*, przy użyciu głowic konwencjonalnych. Jego duża prędkość (do 100 węzłów) i głębokość zanurzenia (do 1000 m) czynią go potencjalnie niezwykle trudnym do przechwycenia przez obecne systemy obrony przeciwtorpedowej NATO¹³⁹. Należy jednak zauważyć, że zastosowanie tego rodzaju

¹³⁶ *Russia launches new nuclear submarine carrier of doomsday drone*, <https://www.thehindu.com/news/international/russia-launches-new-nuclear-submarine-carrier-of-doomsday-drone/article70233316.ece>, [dostęp: 1.12.2025]; N. Polmar, ‘Status-6’ Russian Drone Nearly Operational, <https://www.usni.org/magazines/proceedings/2019/april/status-6-russian-drone-nearly-operational>, [dostęp: 1.12.2025].

¹³⁷ L. Ogryzko, A. Rozzi, *Shallow seas and „shadow fleets: Europe’s undersea infrastructure is dangerously vulnerable*, <https://ecfr.eu/article/shallow-seas-and-shadow-fleets-europes-undersea-infrastructure-is-dangerously-vulnerable>, [dostęp: 1.12.2025]; A. Paik, J. Counter, *International law doesn’t adequately protect undersea cables. That must change*, <https://www.atlanticcouncil.org/content-series/hybrid-warfare-project/international-law-doesnt-adequately-protect-undersea-cables-that-must-change>, [dostęp: 1.12.2025].

¹³⁸ N. Polmar, dz. cyt.; Poseidon (unmanned underwater vehicle) – Wikipedia, [https://en.wikipedia.org/wiki/Poseidon_\(unmanned_underwater_vehicle\)](https://en.wikipedia.org/wiki/Poseidon_(unmanned_underwater_vehicle)), [dostęp: 1.12.2025].

¹³⁹ N. Polmar, dz. cyt.

uzbrojenia jest na razie czysto hipotetyczne, ponadto napęd jądrowy oraz możliwość przenoszenia głowicy jądrowej oznaczają, że atrybucja ataku będzie niezwykle łatwa. Może jednak wciąż być narzędziem oddziaływania propagandowego, podobnie jak jest nim już teraz.

„Flota cieni” jako narzędzie hybrydowe

Rosyjska doktryna wojny morskiej zakłada wykorzystanie statków cywilnych do działań militarnych. W kontekście sankcji i izolacji, Rosja zbudowała ogromną „flotę cieni” (ang. *shadow fleet*) tankowców i statków handlowych, które służą nie tylko do transportu ropy, ale także jako platformy wywiadowcze i dywersyjne¹⁴⁰.

Zjawisko to, w latach 2025–2030, będzie ewoluować w kierunku systematycznego wykorzystania tych jednostek do sabotażu infrastruktury energetycznej na Bałtyku i Morzu Północnym. Statki te, często zarejestrowane w rajach podatkowych, z wyłączonymi transponderami AIS, mogą:

1. Mapować infrastrukturę: Wykorzystując sonary cywilne i echosondy do lokalizacji kabli i rurociągów¹⁴¹.
2. Dokonywać fizycznych uszkodzeń: Poprzez celowe „wleczenie” kotwic po dnie w rejonie krytycznych łączy (taktyka obserwowana przy uszkodzeniu Balticconnector i kabli w Zatoce Fińskiej, gdzie podejrzewano udział statków Newnew Polar Bear i Yi Peng 3)¹⁴².
3. Działać jako bazy logistyczne: Dla sił specjalnych i dronów podwodnych.

¹⁴⁰ A. Rolander, *Irregular Warfare at Sea: How Russia’s Shadow Fleet Undermines Maritime Security*, <https://smallwarsjournal.com/2025/12/11/irregular-warfare-at-sea>, [dostęp: 1.12.2025]; A. Caprile, G. Leclerc, *Russia’s ‘shadow fleet’: Bringing the threat to light*, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766242/EPRS_BRI\(2024\)766242_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766242/EPRS_BRI(2024)766242_EN.pdf), [dostęp: 1.12.2025]; *Baltic Sea: the security risk posed by Russia’s shadow fleet*, <https://www.bundeswehr.de/en/baltic-sea-russia-s-shadow-fleet-5892544>, [dostęp: 1.12.2025].

¹⁴¹ *Baltic Sea: the security risk...*, dz. cyt.

¹⁴² S. Himka, *Baltic Sea Undersea Cable Security*, <https://jsis.washington.edu/news/baltic-sea-undersea-cable-security>, [dostęp: 1.12.2025]; 2024 Baltic Sea submarine cable disruptions – Wikipedia, https://en.wikipedia.org/wiki/2024_Baltic_Sea_submarine_cable_disruptions, [dostęp: 1.12.2025]; N. Khorrami, *Subsea sabotage should spark review of critical infrastructure security*, <https://bindinghook.com/subsea-sabotage-should-spark-review-of-critical-infrastructure-security>, [dostęp: 1.12.2025].

Arktyka jako przyszły teatr wojny o zasoby

Rosyjska militaryzacja Arktyki, w tym rozbudowa baz (np. baza lotnicza Temp na wyspie Kotielnyj) i infrastruktury Północnej Drogi Morskiej, tworzy bezpośrednie zagrożenie dla europejskich dostaw energii. Norwegia, która zastąpiła Rosję w roli głównego dostawcy gazu do UE, posiada rozległą sieć rurociągów na dnie Morza Północnego i Norweskiego¹⁴³.

W scenariuszach na lata 2025–2030, rosyjskie zdolności w Arktyce mogą zostać użyte do przecięcia tych linii dostaw, a także kabli światłowodowych łączących Europę z Ameryką Północną i Azją. Strategia Arktyczna do 2035 r. jasno wskazuje na konieczność „obrony” rosyjskich zasobów, co może być pretekstem do działań ofensywnych w szarej strefie wód międzynarodowych¹⁴⁴.

4.3. Domeny niekinetyczne

Współczesne sieci energetyczne (Smart Grids) są systemami cyberfizycznymi, w których przepływ energii jest nierozzerwalnie związany z przepływem danych. Rosyjska sztuka wojenna perfekcyjnie identyfikuje tę zależność, rozwijając zaawansowane zdolności do paraliżowania systemów sterowania (OT/ICS) oraz zakłócania synchronizacji sieci poprzez domenę elektromagnetyczną.

Cyberataki na systemy SCADA i OT: od NotPetya do AI

Rosyjskie grupy APT (ang. Advanced Persistent Threat), takie jak Sandworm (jednostka 74455 GRU), Gamaredon czy Fancy Bear, posiadają udokumentowane zdolności do przeprowadzania niszczycielskich ataków na infrastrukturę krytyczną.

¹⁴³ M. Humpert, *Russia Upgrades Key Arctic Military Base with Expanded Runway*, <https://www.highnorthnews.com/en/russia-upgrades-key-arctic-military-base-expanded-runway>, [dostęp: 1.12.2025].

¹⁴⁴ *STRATEGY for Development of the Arctic Zone of the Russian Federation and Provision of National Security for the Period up to 2035 (Revised)*, https://usnwc.edu/_images/portals/0/NWCDepartments/Russia-Maritime-Studies-Institute/16MAR23_20201026_ENG_RUS_Arctic-Strategy2035_FINAL_16MAR238f95.pdf, [dostęp: 1.12.2025]; E. Buchanan, *Russia's 2021 National Security Strategy: Cool Change Forecasted for the Polar Regions*, <https://www.rusi.org/explore-our-research/publications/commentary/russias-2021-national-security-strategy-cool-change-forecasted-polar-regions>, [dostęp: 1.12.2025]; E. Buchanan, *The overhaul of Russian strategic planning for the Arctic Zone to 2035*, <https://www.ndc.nato.int/fr/the-overhaul-of-russian-strategic-planning-for-the-arctic-zone-to-2035>, [dostęp: 1.12.2025].

Doświadczenia z ataków na ukraińską sieć energetyczną w 2015 i 2016 roku (z użyciem malware BlackEnergy i Industroyer) ewoluowały. W latach 2025–2030 zagrożenie to wejdzie na nowy poziom zaawansowania¹⁴⁵.

Prognozowane wektory ataku obejmują:

1. Ataki na łańcuch dostaw (ang. *supply chain*): Zamiast bezpośrednio atakować dobrze chronione elektrownie, rosyjscy hakerzy infekują oprogramowanie i sprzęt dostarczany przez podwykonawców. Przejęcie aktualizacji oprogramowania dla sterowników PLC może dać dostęp do tysięcy obiektów jednocześnie¹⁴⁶.
2. Eksploatacja systemów zdalnego dostępu: Wzrost liczby urządzeń IoT i zdalnego zarządzania (HMI, VNC) w energetyce tworzy nowe podatności. Grupy „haktywistyczne” wspierane przez Kreml (np. Cyber Army of Russia Reborn) wykorzystują proste techniki (*brute force*, skanowanie portów), aby przejąć kontrolę nad mniejszymi obiektami, co w skali masowej może prowadzić do destabilizacji systemu¹⁴⁷.
3. Wykorzystanie Sztucznej Inteligencji (AI): AI będzie używana do automatyzacji poszukiwania luk w zabezpieczeniach oraz do tworzenia złośliwego oprogramowania (malware) zdolnego do adaptacji i omijania systemów detekcji. Rosja inwestuje również w systemy AI do obrony własnej cyberprzestrzeni, co tworzy asymetrię w wyścigu zbrojeń cyfrowych¹⁴⁸.

¹⁴⁵ B.E. Humphreys, dz. cyt.; M. Khalil, *Cybersecurity in the Power Sector 2025: How Utilities Defend the Grid from Evolving Cyber Threats*, <https://deepstrike.io/blog/cybersecurity-in-the-power-sector-2025>, [dostęp: 1.12.2025]; K. Poireault, *Russian APT Groups Intensify Attacks in Europe with Zero-Day Exploits and Wipers*, [dostęp: 1.12.2025].

¹⁴⁶ *Cybersecurity in the power sector*, <https://www.eurelectric.org/in-detail/cybersecurity-in-the-power-sector>, [dostęp: 1.12.2025].

¹⁴⁷ *Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure*, <https://www.cisa.gov/sites/default/files/2025-12/aa25-343a-pro-russia-hacktivists-conduct-attacks.pdf>, [dostęp: 1.12.2025]; E. Geller, *Pro-Russia hacktivists launching attacks that could damage OT*, <https://www.cybersecuritydive.com/news/russian-hacktivists-critical-infrastructure-remote-access-advisory/807493>, [dostęp: 1.12.2025].

¹⁴⁸ S. Monaghan i in., *NATO's Role in Protecting Critical Undersea Infrastructure*, <https://www.csis.org/analysis/natos-role-protecting-critical-undersea-infrastructure>, [dostęp: 1.12.2025]; A. De'Ath, *The Risks of AI in the Energy Sector*, <https://www.enseccoe.org/wp-content/uploads/2024/10/Energy-Highlights-No.19.pdf>, [dostęp: 1.12.2025].

4.4. Walka Elektroniczna (WRE) – zagrożenie dla synchronizacji sieci

Nowym, krytycznym i często niedocenianym zagrożeniem jest wpływ rosyjskich systemów Walki Radioelektronicznej (WRE) na stabilność sieci elektroenergetycznych. Nowoczesne sieci wykorzystują urządzenia pomiarowe fazorów (PMU – Phasor Measurement Units), które do poprawnej pracy i synchronizacji fazy prądu w rozległych obszarach wymagają ultraprecyzyjnego sygnału czasu z systemów GPS/GNSS¹⁴⁹.

Rosja dysponuje najbardziej zaawansowanymi na świecie systemami zakłócania sygnałów nawigacyjnych i radiowych:

1. Tobol (14Ts227): Stacjonarny, strategiczny system WRE, którego elementy zlokalizowane są m.in. w Obwodzie Królewieckim. Posiada on zdolność do zakłócania sygnałów GPS na ogromnych obszarach, co obserwowano nad Polską i Bałtykiem (zakłócenia lotnicze i morskie). Jego użycie przeciwko infrastrukturze energetycznej może doprowadzić do desynchronizacji PMU, błędnych odczytów w dyspozytorniach mocy i w konsekwencji do automatycznych wyłączeń linii przesyłowych (efekt kaskadowy)¹⁵⁰.
2. Murmańsk-BN: Strategiczny system zakłócania łączności radiowej na falach krótkich (HF) o zasięgu do 5000 km. Jest zdolny do paraliżowania systemów

¹⁴⁹ *GPS Jamming and Ukraine's Electrical Grid – Cisco Talos*, <https://rntfnd.org/2024/04/21/gps-jamming-and-ukraines-electrical-grid-cisco-talos>, [dostęp: 1.12.2025]; D.P. Shepard, T.E. Humphreys, *Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks*, <https://rnl.ae.utexas.edu/images/stories/files/papers/spoofSMUCIP2012.pdf>, [dostęp: 1.12.2025]; S. Bhamidipati, G. Gao, *GPS Spoofing Mitigation and Timing Risk Analysis in Networked Phasor Measurement Units via Stochastic Reachability*, „Journal of the Institute of Navigation September” 2023, 70 (3) navi.574, <https://navi.ion.org/content/70/3/navi.574/tab-article>, [dostęp: 1.12.2025].

¹⁵⁰ *GPS Jamming and Ukraine's Electrical Grid...*, dz. cyt.; P. Satam, *Russia's TOBOL EW System „Cuts Off” Starlink From It's Ground Terminals; How Did Moscow Delink The Starlink*, <https://space4peace.org/russias-tobol-ew-system-cuts-off-starlink-from-its-ground-terminals-how-did-moscow-delink-the-starlink>, [dostęp: 1.12.2025]; E. Kannike, *Tobol System in russian Kaliningrad Jams GPS Over Europe, and It Does Cause Problems*, https://en.defence-ua.com/weapon_and_tech/tobol_system_in_russian_kaliningrad_jams_gps_over_europe_and_it_does_cause_problems-9283.html, [dostęp: 1.12.2025]; B.J. Weichert, *Vladimir Putin Is Preparing for War Against Starlink*, <https://nationalinterest.org/blog/buzz/vladimir-putin-is-preparing-for-war-against-starlink>, [dostęp: 1.12.2025].

dowodzenia i kontroli (C2) oraz komunikacji zapasowej w całej Europie, co w sytuacji kryzysu energetycznego utrudniłoby koordynację działań naprawczych¹⁵¹.

4.5. Wojna informacyjna i kognitywna

Ataki na infrastrukturę są ściśle skorelowane z operacjami informacyjnymi. Rosyjska doktryna zakłada wywoływanie paniki społecznej poprzez dezinformację dotyczącą dostępności energii, cen i przyczyn awarii. W przypadku udanego ataku na sieć, kampania dezinformacyjna ma na celu podważenie zaufania do rządów państw zachodnich i wywołanie niepokojów społecznych, co potęguje skutki fizycznego braku prądu¹⁵².

4.6. „Gig Economy” sabotażu i hybrydowe proxy

W perspektywie lat 2025–2030, jednym z najbardziej niepokojących trendów w rosyjskiej sztuce operacyjnej jest przejście od operacji wykonywanych wyłącznie przez kadrowych oficerów wywiadu do modelu „zleconego” sabotażu, opartego na zasadach *gig economy* (gospodarki fuch).

Rekrutacja i profil „jednorazowego” sabotażysty

Po masowych wydaleniach rosyjskich dyplomatów-szpiegów z Europy w latach 2022–2023, rosyjskie służby (głównie GRU) straciły znaczną część swoich aktywów operacyjnych. W odpowiedzi, zmodyfikowano modus operandi. Zamiast wysyłać elitarnych oficerów Jednostki 29155, rekrutuje się amatorów, przestępców i osoby

¹⁵¹ *Murmansk-BN Russian Long-Range Communications Jamming System*, <https://odin.tradoc.army.mil/WEG/Asset/b4cd1efd5c57c88bcfe7ca78a2831903>, [dostęp: 1.12.2025]; *Russian Electronic Warfare Targets NATO Assets*, <https://www.afcea.org/signal-media/international/russian-electronic-warfare-targets-nato-assets>, [dostęp: 1.12.2025]; J. Harvey, *The Russo-Ukrainian war's expansion into the High North poses electronic warfare challenges for NATO*, <https://www.arctictoday.com/the-russo-ukrainian-wars-expansion-into-the-high-north-poses-electronic-warfare-challenges-for-nato>, [dostęp: 1.12.2025].

¹⁵² K. Poireault, dz. cyt.; M. Geri, N. Comini, *NATO's preparedness to hybrid threats must overcome strategic limits and coordination hurdles*, <https://natowatch.org/default/2025/natos-preparedness-hybrid-threats-must-overcome-strategic-limits-and-coordination>, [dostęp: 1.12.2025].

zdesperowane finansowo za pośrednictwem mediów społecznościowych, w szczególności komunikatora Telegram¹⁵³.

Model ten charakteryzuje się¹⁵⁴:

1. Decentralizacją i skalą: Ogłoszenia o „szybkiej pracy” pojawiają się na kanałach związanych z grami, krypto-walutami czy grupami emigracyjnymi.
2. Zbywalnością (*Disposability*): Rekrutowani sprawcy są traktowani jako „amunicja krążąca”. Ich aresztowanie nie powoduje strat w kadrach wywiadu, a jedynie konieczność zwerbowania kolejnej osoby.
3. Spektrum celów: Od wandalizmu (malowanie symboli Z), przez podpalenia magazynów i szaf sterowniczych po ataki na obiekty energetyczne o mniejszym znaczeniu, ale dużej widoczności medialnej.

Finansowanie terroru: kryptowaluty i USDT

Kluczowym elementem umożliwiającym funkcjonowanie tego modelu jest system finansowania, który omija tradycyjny system bankowy i sankcje. Rosja intensywnie wykorzystuje kryptowaluty, w szczególności stablecoiny takie jak USDT (Tether) na blockchainie TRON oraz waluty zapewniające anonimowość (Monero)¹⁵⁵.

¹⁵³ Ch. Edwards, N. Seidenstein, *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure*, <https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure>, [dostęp: 1.12.2025]; D. Belovodyev, *Exclusive: The Russian Neo-Nazi Behind A Shadowy GRU Recruitment Campaign*, <https://www.rferl.org/a/russia-gru-nazi-sabotage-recruitment-telegram/33539661.html>, [dostęp: 1.12.2025]; P. Arak, *Russia's shadow war: How the Kremlin uses sabotage to wear down Europe*, <https://www.atlanticcouncil.org/blogs/new-atlanticist/russias-shadow-war-how-the-kremlin-uses-sabotage-to-wear-down-europe>, [dostęp: 1.12.2025].

¹⁵⁴ D. Richterova i in., *Russian Sabotage in the Gig-Economy Era*, „The RUSI Journal” 2024, 169(5), 10–21, <https://doi.org/10.1080/03071847.2024.2401232>, [dostęp: 1.12.2025]; N. Gurcov, *Behind the lines: How Ukraine has outgunned Russia in sabotage*, <https://acleddata.com/report/behind-lines-how-ukraine-has-outgunned-russia-sabotage>, [dostęp: 1.12.2025].

¹⁵⁵ J. Kennedy i in., *Russia's Use of Crypto Schemes*, <https://www.rand.org/pubs/commentary/2025/08/russias-use-of-crypto-schemes.html>, [dostęp: 1.12.2025]; P. Arak, dz. cyt.

Mechanizm płatności obejmuje:

1. Giełdy w szarej strefie: Wykorzystanie giełd kryptowalut w jurysdykcjach o słabym nadzorze (np. giełda Garantex, podmioty w Kirgistanie) do konwersji rubli na krypto¹⁵⁶.
2. Płatności bezpośrednio: Przelewy na portfele cyfrowe wykonawców za wykonane zadania (udokumentowane zdjęciami lub wideo).
3. Mieszanie funduszy: Użycie mikserów kryptowalut i pośredników na czarnym rynku (*crypto-to-fiat mules*) do zatarcia śladów pochodzenia środków¹⁵⁷.

W latach 2025–2030 należy spodziewać się dalszej profesjonalizacji tego systemu, w tym wykorzystania rosyjskich instrumentów cyfrowych (cyfrowy rubel) oraz pogłębienia współpracy między służbami specjalnymi a zorganizowanymi grupami cyberprzestępczymi (ang. *ransomware gangs*), które piorą pieniądze na potrzeby operacji państwowych¹⁵⁸.

Wnioski

Analiza rosyjskiej sztuki wojennej w perspektywie lat 2025–2030 prowadzi do konkluzji, że zagrożenie dla infrastruktury energetycznej państw trzecich ma charakter systemowy, trwałe i narastające. Nie jest to jedynie element pomocniczy operacji lądowych, lecz samodzielna domena walki strategicznej.

¹⁵⁶ *Europe Announces 19th Sanctions Package on Russia – Including First-Ever Crypto Asset Designations Linked to Moscow*, <https://www.trmlabs.com/resources/blog/europe-announces-19th-sanctions-package-on-russia---including-first-ever-crypto-asset-designations-linked-to-moscow>, [dostęp: 1.12.2025]; *Russia Leveraging Kyrgyzstan’s Crypto Ecosystem to Evade Sanctions*, <https://www.trmlabs.com/resources/blog/russia-leveraging-kyrgyzstans-crypto-ecosystem-to-evade-sanctions>, [dostęp: 1.12.2025].

¹⁵⁷ *Anonymity for sale: the thriving black market of crypto-to-fiat mules*, https://ti-russia.org/wp-content/uploads/2023/10/epaycrypto_.pdf, [dostęp: 1.12.2025].

¹⁵⁸ Ch. Raggett, *Rocket from the Crypto: State-backed Criminal Groups and the Fintech Sector*, <https://cetas.turing.ac.uk/publications/rocket-crypto-state-backed-criminal-groups-and-fintech-sector>, [dostęp: 1.12.2025]; J. MacColl, K. Westmore, *Operation Destabilise: Russia, Organised Crime and Illicit Finance*, <https://www.rusi.org/explore-our-research/publications/commentary/operation-destabilise-russia-organised-crime-and-illicit-finance>, [dostęp: 1.12.2025].

1. Infrastruktura jako zakładnik: Rosja będzie dążyć do utrzymywania europejskiej energetyki w stanie ciągłej niepewności, wykorzystując groźbę sabotażu jako lewar polityczny.
2. Synergia metod: Najskuteczniejsze ataki będą łączyć działania kinetyczne (uszkodzenia kabli), cybernetyczne (SCADA) i elektromagnetyczne (zakłócanie GPS), co utrudni obronę i reakcję.
3. Konieczność nowej definicji odstraszania: Zachód musi wypracować mechanizmy odstraszania w szarej strefie, jasno komunikując, że ataki na infrastrukturę krytyczną spotkają się z dotkliwą, niekoniecznie militarną, ale asymetryczną odpowiedzią.

5. Scenariusze ataków militarnych na infrastrukturę energetyczną w Ukrainie a bezpieczeństwo krajów NATO

5.1. Redefinicja frontu w wojnie systemowej

Współczesne środowisko bezpieczeństwa uległo fundamentalnej transformacji. Wojna w Ukrainie dowiodła, że granica między działaniami militarnymi a cywilnymi uległa zatarciu, a infrastruktura krytyczna stała się pierwszoplanowym celem operacyjnym. Rosyjska doktryna wojenna, ewoluująca od koncepcji „wojny nowej generacji” (Gierasimow) do „Strategicznej Operacji Zniszczenia Krytycznie Ważnych Celów” (SODCIT), zakłada, że degradacja systemu energetycznego przeciwnika jest najskuteczniejszą metodą złamania woli oporu społeczeństwa i paraliżu procesów decyzyjnych państwa.

W kontekście bezpieczeństwa krajów NATO, obserwujemy przejście od teoretycznych rozważań o zagrożeniach hybrydowych do realnych aktów sabotażu i dywersji. Zniszczenie gazociągów Nord Stream, uszkodzenie rurociągu Balticconnector oraz liczne incydenty z przecinaniem kabli podmorskich na Bałtyku świadczą o tym, że domena podwodna i energetyczna stała się nową „szarą strefą” konfrontacji. Celem niniejszego rozdziału jest zbadanie mechanizmów tych zagrożeń poprzez pryzmat doświadczeń ukraińskich oraz ocena gotowości Sojuszu do ich odparcia¹⁵⁹.

¹⁵⁹ R.S. Quinville i in., *Risky Game: Hybrid Attack on Baltic Undersea Cables*, <https://www.wilsoncenter.org/article/risky-game-hybrid-attack-baltic-undersea-cables>, [dostęp: 1.12.2025]; C. Schaller, *Russia's Mapping of Critical Infrastructure in the North and Baltic Seas – International Law as an Impediment to Countering the Threat of Strategic Sabotage?*, „Nordic Journal of International Law” 2024, 93(2), s. 202–236, <https://doi.org/10.1163/15718107-bja10083>.

5.2. Ewolucja rosyjskiej sztuki operacyjnej wobec infrastruktury energetycznej – lekcje z Ukrainy

Analiza działań Federacji Rosyjskiej w Ukrainie pozwala wyodrębnić dwa diametralnie różne modele oddziaływania na infrastrukturę energetyczną, które determinują spektrum zagrożeń dla państw trzecich.

Model krymski (2014): hybrydowe przejęcie i friendly embrace

Operacja aneksji Krymu w 2014 roku stanowi paradygmatyczny przykład wczesnej fazy wojny hybrydowej, w której priorytetem było przejęcie kontroli nad infrastrukturą przy minimalnych szkodach fizycznych. Rosja, będąc świadoma 80-procentowego uzależnienia półwyspu od dostaw energii z Ukrainy kontynentalnej, zrezygnowała z ataków kinetycznych na rzecz działań prawno-ekonomicznych i operacji sił specjalnych.

Kluczowym elementem tej strategii było wykorzystanie tzw. „zielonych ludzików” – żołnierzy Sił Operacji Specjalnych (KSSO), którzy precyzyjnie zajmowali węzły sterownicze i budynki administracyjne, nie przerywając dostaw energii. W sektorze telekomunikacyjnym przeprowadzono jednak „twarde” cięcie, fizycznie niszcząc światłowody łączące Krym z Ukrainą, co zapewniło izolację informacyjną. Wobec energetyki zastosowano taktykę „przyjaznego uścisku” (ang. *friendly embrace*), polegającą na przymusowej nacjonalizacji aktywów (np. DTEK Krymenergo) i instalacji lojalnych zarządców.

Wniosek dla NATO: Zagrożenie dla infrastruktury nie musi objawiać się eksplozjami. Może przybrać formę wrogich przejęć, manipulacji w strukturze właścicielskiej operatorów systemów przesyłowych (TSO) lub infiltracji personelu, co w literaturze przedmiotu określa się mianem zagrożeń w domenie korporacyjno-prawnej.

5.3. Strategia anihilacji (2022–2024) – ewolucja od dezorganizacji do zniszczenia systemowego

Pełnoskalowa inwazja w 2022 roku przyniosła zmianę paradygmatu na strategię totalnego zniszczenia, realizowaną w ramach koncepcji SODCIT. Analiza chronologiczna pozwala wyróżnić wyraźne fazy tej kampanii, świadczące o procesie adaptacji rosyjskiego dowództwa¹⁶⁰.

¹⁶⁰ S. Rimutis, dz. cyt.

Taktyka „High-Low Mix” i innowacje techniczne

Rosja wdrożyła taktykę ataków mieszanych, wykorzystując tanie drony (Shahed, Gerbera z soczewkami Lüneburga) do saturacji (przeciążenia) ukraińskiej obrony przeciwlotniczej (OPL). Pozwala to na stworzenie „korytarzy” dla drogich i precyzyjnych pocisków manewrujących. Zidentyfikowano również modernizację pocisków Ch-101, które wyposażono w podwójne głowice (w tym kasetowe), drastycznie zwiększające pole rażenia nieopancerzonych celów, takich jak otwarte rozdzielnie energetyczne. Szczególnym zagrożeniem okazały się pociski Ch-69, odpalane z taktycznych samolotów Su-34, które dzięki technologii stealth i niskiemu profilowi lotu (ok. 20 m nad ziemią) skutecznie omijały systemy radarowe, niszcząc m.in. elektrownię w Trypolu. Należy zauważyć przy tym, że system obrony Ukrainy jest systemem stworzonym doraźnie łączącym szereg systemów poradzieckich oraz zachodnich.

5.4. Wojskowe i hybrydowe środki rażenia infrastruktury w arsenale rosyjskim

Zdolność Rosji do atakowania infrastruktury NATO opiera się na szerokim spektrum narzędzi, wykraczających poza tradycyjne siły powietrzne.

Domena podwodna: GUGI i „inżynieria dywersyjna”

Najbardziej krytycznym zagrożeniem dla infrastruktury morskiej NATO (kable, rurociągi, farmy wiatrowe) jest Główny Zarząd Badań Głębinowych (GUGI). Jest to elitarna formacja podlegająca bezpośrednio Ministerstwu Obrony, dysponująca unikalnymi w skali światowej środkami¹⁶¹.

- Specjalistyczne okręty podwodne: Okręt-matka K-329 Biełgorod jest zdolny do przenoszenia miniaturowych okrętów podwodnych o napędzie jądrowym (projekt 10831 Łoszarik), które mogą operować na dużych głębokościach, dokonując manipulacji przy kablach podmorskich (zakładanie podsłuchów, przecinanie) lub niszczenia rurociągów.

¹⁶¹ F. Bryjka, *NATO and the EU Respond to Russian Maritime Sabotage*, <https://www.pism.pl/publications/nato-and-the-eu-respond-to-russian-maritime-sabotage>, [dostęp: 1.12.2025]; *Exposing Russia's Undersea Shadow War*, <https://techjournalism.medium.com/exposing-the-russias-undersea-shadow-war-467890fac159>, [dostęp: 1.12.2025].

- System Posejdon (2M39): Autonomiczny bezzałogowy pojazd podwodny (UUV) o napędzie jądrowym. Choć jego pierwotnym przeznaczeniem jest przenoszenie głowic nuklearnych w celu wywołania radioaktywnego tsunami, analitycy wskazują na możliwość jego użycia z głowicami konwencjonalnymi do niszczenia infrastruktury portowej (terminale LNG) i przybrzeżnej.
- Statki „badawcze”: Jednostki takie jak Yantar czy Akademik Włodimirski oficjalnie prowadzą badania oceanograficzne, a w rzeczywistości wyposażone są w zdalnie sterowane pojazdy (ROV) i sonary boczne, służące do mapowania krytycznej infrastruktury podwodnej (CUI) państw NATO¹⁶².

„Flota cieni” i hybrydowe proxy na morzu

Rosja rozwinęła koncepcję wykorzystania cywilnych statków handlowych do działań militarnych. Tzw. „flota cieni” (ang. *shadow fleet*), składająca się z setek tankowców i masowców o niejasnej strukturze własności, służy nie tylko do omijania sankcji, ale również jako platforma wywiadowcza (SIGINT/ELINT) i dywersyjna¹⁶³.

Incydenty z udziałem statków takich jak Newnew Polar Bear (uszkodzenie Balticconnector) czy Yi Peng 3 (uszkodzenie kabli C-Lion1 i BCS) ujawniają taktykę „przypadkowych” awarii. Statki te, często z wyłączonymi transponderami AIS lub fałszującymi dane lokalizacyjne, dokonują uszkodzeń infrastruktury przy użyciu kotwic wleczonych po dnie. Taka metoda działania, realizowana w międzynarodowych wodach lub Wyłącznych Strefach Ekonomicznych (WSE), utrudnia interwencję prawną państw nadbrzeżnych i stwarza problem atrybucji (przypisania winy), co paraliżuje proces decyzyjny w NATO¹⁶⁴.

¹⁶² Europe Builds Deterrence as The Kremlin Escalates Hybrid Warfare, https://gemini.google.com/app/9ccd2a318c891c04?utm_source=app_launcher&utm_medium=owned&utm_campaign=base_all, [dostęp: 10.12.2025]; Armed Russian research vessels regularly spying on infrastructure in North Sea: report, <https://nltimes.nl/2024/09/25/armed-russian-research-vessels-regularly-spying-in-infrastructure-north-sea-report>, [dostęp: 1.12.2025].

¹⁶³ N. Childs, *Russia's 'Shadow Fleet' and Sanctions Evasion: What Is To Be Done?*, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/01/russias_shadow-fleet_and-sanctions-evasion/iiss_russias_shadow-fleet_and-sanctions-evasion_31012025.pdf, [dostęp: 1.12.2025]; Policy briefing: tackling the russian 'shadow' fleet, https://energyandcleanair.org/wp/wp-content/uploads/2024/09/State-Capture_CREA_Shadow-fleet-policy-briefing_Final_08.2024.pdf, [dostęp: 1.12.2025].

¹⁶⁴ R.S. Quinville i in., dz. cyt.; S. Besch, E. Brown, *Securing Europe's Subsea Data Cables*, <https://carnegieendowment.org/research/2024/12/securing-europes-subsea-data-cables?lang=en>, [dostęp: 1.12.2025].

Sabotaż lądowy i gig economy terroru

Rosyjski wywiad wojskowy (GRU), a w szczególności jednostka 29155, zintensyfikował działania dywersyjne na terytorium Europy. Po masowych wydaleniach oficerów wywiadu z placówek dyplomatycznych, GRU przeszło na model rekrutacji „jednorażowych agentów” (ang. *disposable agents*) za pośrednictwem platform społecznościowych takich jak Telegram¹⁶⁵.

Oferując wynagrodzenie w kryptowalutach (głównie USDT), rosyjskie służby zlecają amatorom, przestępcom czy zradykalizowanym aktywistom zadania polegające na podpaleniach magazynów, wandalizmie wobec infrastruktury kolejowej czy monitoringu obiektów wojskowych. W Polsce i Niemczech odnotowano aresztowania osób planujących sabotaż linii kolejowych i energetycznych na zlecenie rosyjskich służb. Ten model „zleconego sabotażu” (ang. *outsourced sabotage*) pozwala Rosji na utrzymanie wysokiego tempa operacji przy niskim ryzyku politycznym i kadrowym¹⁶⁶.

Cyberataki na systemy OT/ICS

Wojna w Ukrainie potwierdziła skuteczność rosyjskich grup hakerskich (np. Sandworm, Gamaredon) w atakowaniu systemów sterowania przemysłowego (OT). Użycie złośliwego oprogramowania typu Industroyer2 czy CaddyWiper miało na celu fizyczne uszkodzenie podstacji energetycznych poprzez manipulację przekaznikami zabezpieczeniowymi.

Nowym wektorem zagrożenia dla NATO są ataki na systemy HVDC (High Voltage Direct Current). Nowoczesne stacje przekształtnikowe, kluczowe dla morskich farm wiatrowych i interkonektorów, są w pełni cyfrowe i podatne na ataki zakłócające synchronizację oraz procesy komutacji, co może prowadzić do fizycznego uszkodzenia drogich modułów IGBT i wyłączenia przesyłu mocy na ogromnych dystansach¹⁶⁷.

¹⁶⁵ S.G. Jones, *Russia's Shadow War Against the West*, <https://www.csis.org/analysis/russias-shadow-war-against-west>, [dostęp: 1.12.2025].

¹⁶⁶ B. Schmitt i in., *Subsea Sabotage: Protecting Energy Infrastructure from Hostile Aggression*, <https://kleinmanenergy.upenn.edu/research/publications/subsea-sabotage-protecting-energy-infrastructure-from-hostile-aggression>, [dostęp: 1.12.2025].

¹⁶⁷ R. Guo i in., *Vulnerability Assessment of High-Voltage Direct Current Transmission Systems to Cyberattacks*, <https://sands.edpsciences.org/articles/sands/pdf/forth/sands20250011.pdf>, [dostęp: 1.12.2025].

5.5. Podatności infrastruktury energetycznej państw NATO

Analiza specyfiki systemu energetycznego Europy w kontekście zagrożeń rosyjskich pozwala zidentyfikować kluczowe punkty krytyczne.

Infrastruktura morska (Offshore) i interkonektory

Morze Północne i Bałtyk stają się „wielką elektrownią” Europy, z planami budowy setek gigawatów mocy w farmach wiatrowych. Ta koncentracja infrastruktury tworzy jednak nowe ryzyka. Morskie farmy wiatrowe są połączone z lądem za pomocą kabli, które są trudne do monitorowania na całej długości. Zniszczenie morskich stacji transformatorowych lub kabli eksportowych może odciąć od sieci znaczne moce wytwórcze¹⁶⁸.

Szczególnie krytyczne są interkonektory HVDC (np. NordLink, Viking Link), które umożliwiają wymianę energii między krajami. Ich uszkodzenie (jak w przypadku EstLink 2) nie tylko zaburza bilans mocy, ale może prowadzić do destabilizacji cen i konieczności uruchamiania emisyjnych rezerw węglowych lub gazowych. Projektowane połączenia transatlantyckie, takie jak NATO-L, choć zwiększają dywersyfikację, również staną się celem strategicznym dla rosyjskich okrętów podwodnych¹⁶⁹.

Terminale LNG i FSRU

Wycofanie się z importu rosyjskiego gazu rurociągowego zmusiło Europę do oparcia bezpieczeństwa gazowego na dostawach LNG. Pływające jednostki regazyfikacyjne (FSRU) w Niemczech (Wilhelmshaven, Brunsbüttel), Polsce (planowany w Zatoce Gdańskiej), Finlandii (Inkoo) czy Litwie (Kłajpeda) stały się strategicznymi węzłami.

Jednostki te są statycznymi celami, podatnymi na ataki z powietrza (drony), wody (łódzie bezzałogowe USV) oraz spod wody (płetwonurkowie, miny). Ich lokalizacja

¹⁶⁸ *Offshore wind and risk management: opportunities and uncharted waters*, https://www.controlrisks.com/our-thinking/insights/offshore-wind-and-risk-management-opportunities-and-uncharted-waters?utm_referrer=https://gemini.google.com, [dostęp: 1.12.2025].

¹⁶⁹ J. Majcin, *Battle of the Baltic: Safeguarding critical undersea infrastructure*, <https://www.epc.eu/publication/Battle-of-the-Baltic-Safeguarding-critical-undersea-infrastructure-645780>, [dostęp: 1.12.2025]; B. Marcoux, *From Telegraph to Terawatt-hours: Why NATO-L Could Be the Great Eastern of the Net-Zero Age*, <https://www.energycentral.com/energy-biz/post/from-telegraph-to-terawatt-hours-why-nato-l-could-be-the-great-eastern-el4z4YFaLCFeaZz>, [dostęp: 1.12.2025].

w pobliżu szlaków żeglugowych zwiększa ryzyko kolizji (przypadkowej lub celowej) oraz ataków hybrydowych. Zniszczenie lub blokada terminala FSRU w okresie zimowym mogłoby wywołać natychmiastowy kryzys w dostawach ciepła i energii elektrycznej dla całych regionów¹⁷⁰.

Systemy synchronizacji i cyberbezpieczeństwo

Europejska sieć elektroenergetyczna (ENTSO-E) działa opierając się na precyzyjnej synchronizacji częstotliwości. Rosyjskie systemy walki radioelektronicznej (WRE) takie jak Tobol czy Murmańsk-BN, mają zdolność zakłócania sygnału GPS/GNSS na dużych obszarach. Urządzenia pomiarowe fazorów (PMU), kluczowe dla stabilności nowoczesnych sieci inteligentnych (Smart Grids), polegają na sygnale czasu z GPS. Jego zakłócenie może prowadzić do desynchronizacji, błędnych decyzji automatyki zabezpieczeniowej i w konsekwencji do kaskadowych wyłączeń (blackoutów) na skalę kontynentalną.

5.6. Scenariusze ataków na kraje NATO (Perspektywa 2025–2030)

Bazując na rosyjskich zdolnościach i doktrynie, można sformułować trzy główne scenariusze eskalacji wymierzonej w energetykę NATO.

Scenariusz A: „pełzający sabotaż” w szarej strefie (Grey Zone Attrition)

Kontekst: Napięta sytuacja polityczna, brak otwartego konfliktu zbrojnego.

Przebieg: Seria nieskoordynowanych czasowo awarii infrastruktury podmorskiej na Bałtyku i Morzu Północnym. Statki „floty cieni” (np. chińskie masowce z rosyjską załogą) „przypadkowo” zrzucają kotwice na kable światłowodowe i energetyczne podczas sztormów. Równolegle, „nieznani sprawcy” (zrekrutowani przez Telegram) dokonują podpaleń stacji transformatorowych obsługujących farmy wiatrowe na lądzie.

¹⁷⁰ M. Pressentin i in., *LNG Projects Are a Bad Deal for Germans and Americans*, <https://www.americanprogress.org/article/lng-projects-are-a-bad-deal-for-germans-and-americans>, [dostęp: 1.12.2025].

Cel: Wywołanie niepewności rynkowej, wzrost cen energii, podsycanie nastrojów antyrządowych, testowanie reakcji NATO i spójności politycznej Sojuszu (dylemat art. 5 vs art. 4).

Prawdopodobieństwo: Wysokie. Jest to kontynuacja obecnych działań obserwowanych w 2023 i 2024 roku¹⁷¹.

Scenariusz B: Cyberfizyczny blackout (Synchronized Chaos)

Kontekst: Kryzys dyplomatyczny lub wczesna faza konfliktu hybrydowego.

Przebieg: Skoordynowany atak w cyberprzestrzeni i domenie elektromagnetycznej. Grupy APT przełamują zabezpieczenia systemów SCADA morskich farm wiatrowych (np. poprzez łańcuch dostaw oprogramowania), powodując ich nagłe odłączenie od sieci. Jednocześnie systemy WRE z Obwodu Królewieckiego zakłócają sygnał GPS nad Polską i krajami Bałtyckimi, destabilizując systemy PMU. Na dnie morza dochodzi do eksplozji ładunków wybuchowych umieszczonych wcześniej przez drony podwodne przy kluczowych interkonektorach gazowych (np. Baltic Pipe).

Cel: Wywołanie kaskadowej awarii w systemie ENTSO-E, paraliż logistyki wojskowej (kolej, porty) w momencie przerzutu wojsk sojuszniczych, chaos informacyjny.

Prawdopodobieństwo: Średnie. Wymaga wysokiej koordynacji i zaawansowanych zasobów, ale mieści się w doktrynie SODCIT.

Scenariusz C: Eskalacja kinetyczna (Seabed Warfare)

Kontekst: Otwarty konflikt zbrojny NATO-Rosja.

Przebieg: Użycie okrętów podwodnych GUGI i marynarki wojennej do fizycznego niszczenia terminali LNG i platform wiertniczych na Morzu Północnym przy użyciu torped i rakiet. Ataki raketowe (Kalibr, Kindżał) na kluczowe węzły energetyczne na lądzie w Europie Środkowej. Zaminowanie cieśnin duńskich.

¹⁷¹ S. Ostanina, *Russia-Directed Sabotage in Europe*, <https://www.spglobal.com/market-intelligence/en/news-insights/research/2025/11/russia-directed-sabotage-europe>, [dostęp: 1.12.2025].

Cel: Całkowite odcięcie Europy od dostaw surowców, uniemożliwienie prowadzenia długotrwałej operacji obronnej, wymuszenie kapitulacji poprzez kryzys humanitarny.

Prawdopodobieństwo: Niskie w czasie pokoju, wysokie w przypadku wybuchu wojny konwencjonalnej.

5.7. Odpowiedź NATO i rekomendacje

Sojusz Północnoatlantycki oraz Unia Europejska podjęły już szereg działań adaptacyjnych, jednak dynamika zagrożeń wymaga dalszych kroków.

Działania podjęte:

1. Instytucjonalizacja ochrony CUI: Powołanie Critical Undersea Infrastructure Coordination Cell w Kwaterze Głównej NATO oraz Maritime Centre for Security of Critical Undersea Infrastructure przy dowództwie MARCOM w Northwood. Ma to na celu lepszą wymianę informacji między wojskiem a sektorem prywatnym¹⁷².
2. Operacje morskie: Uruchomienie operacji Baltic Sentry oraz zwiększenie patroli morskich i lotniczych w rejonie infrastruktury krytycznej po incydentach Nord Stream¹⁷³.
3. Współpraca UE-NATO: Powołanie grupy zadaniowej EU-NATO Task Force on Resilience of Critical Infrastructure, która wypracowała rekomendacje dotyczące odporności sektorów energii, transportu i cyfrowego¹⁷⁴.

¹⁷² *NATO steps up to better address maritime threats*, <https://ec.europa.eu/newsroom/cipr/items/806186/en>, [dostęp: 1.12.2025]

¹⁷³ *NATO launches 'Baltic Sentry' to increase critical infrastructure security*, <https://www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-security>, [dostęp: 1.12.2025].

¹⁷⁴ *Eu-Nato task force on the resilience of critical infrastructure*, https://gemini.google.com/app/9c-cd2a318c891c04?utm_source=app_launcher&utm_medium=owned&utm_campaign=base_all, [dostęp: 1.12.2025]; *NATO and European Union release final assessment report on resilience of critical infrastructure*, <https://www.nato.int/en/news-and-events/articles/news/2023/06/29/nato-and-european-union-release-final-assessment-report-on-resilience-of-critical-infrastructure>, [dostęp: 1.12.2025].

4. Ćwiczenia: Regularne ćwiczenia takie jak REPMUS (testowanie dronów morskich do ochrony infrastruktury) oraz Coherent Resilience (ćwiczenia sztabowe table-top dotyczące hybrydowych zagrożeń dla energetyki)¹⁷⁵.

Luki prawne i operacyjne

Największym wyzwaniem pozostaje prawo morza (UNCLOS). Artykuł 110 Konwencji ogranicza prawo wizyty (ang. *boarding*) na wodach międzynarodowych do wąskiego katalogu przestępstw (piractwo, handel niewolnikami), który nie obejmuje podejrzania o sabotaż kabli czy rurociągów. Sprawia to, że państwa NATO są często bezsilne wobec statków „floty cieni” manewrujących w ich WSE, dopóki nie dojdzie do jawnego naruszenia bezpieczeństwa żeglugi¹⁷⁶.

Kolejnym problemem jest atrybucja. W przypadku ataków hybrydowych (sabotaż, cyber) często brakuje „dymiącego pistoletu”, co utrudnia osiągnięcie konsensusu politycznego w Radzie Północnoatlantyckiej niezbędnego do uruchomienia artykułu 5 lub 4¹⁷⁷.

5.8. Rekomendacje dla decydentów

W celu wzmocnienia bezpieczeństwa energetycznego krajów NATO rekomenduje się:

1. Wdrożenie doktryny „Resilience by Design”: Ochrona infrastruktury musi być elementem projektu, a nie nakładką. Należy wymuszać na inwestorach (np. farm wiatrowych) stosowanie redundantnych systemów łączności, fizycznych zabezpieczeń stacji transformatorowych (wzorem ukraińskich sarkofagów) oraz systemów wykrywania anomalii w sieciach OT.

¹⁷⁵ NATO's Digital Ocean Initiative gets a boost in Portugal, <https://www.nato.int/en/news-and-events/articles/news/2024/09/20/natos-digital-ocean-initiative-gets-a-boost-in-portugal>, [dostęp: 1.12.2025]; NATO exercise strengthens energy security, <https://www.energimyndigheten.se/en/news/2025/nato-exercise-strengthens-energy-security>, [dostęp: 3.12.2025]; Coherent Resilience 2024 Moldova Tabletop Exercise (CORE24-M), [dostęp: 1.12.2025].

¹⁷⁶ P. Thévenin, A legislative route to combat sabotage of undersea cables: A Q&A with Pierre Thévenin, <https://www.sipri.org/commentary/topical-background/2025/legislative-route-combat-sabotage-undersea-cables>, [dostęp: 1.12.2025]; K. Patlove, *Depths of Deception: State-Backed Undersea Cable Disruptions and the Role of International Maritime Law*, [dostęp: 1.12.2025].

¹⁷⁷ E. Bajarūnas, *Using NATO's Article 5 Against Hybrid Attacks*, <https://cepa.org/article/using-natos-article-5-against-hybrid-attacks>, [dostęp: 1.12.2025].

2. Modernizacja ram prawnych i procedur: Państwa NATO powinny dążyć do wypracowania nowej interpretacji przepisów prawa międzynarodowego lub zawarcia regionalnych porozumień, które umożliwią inspekcje podejrzanych jednostek „floty cieni” w WSE pod pretekstem ochrony środowiska lub bezpieczeństwa infrastruktury. Należy opracować jasne progi (ang. *thresholds*), po przekroczeniu których atak hybrydowy na energetykę będzie traktowany jako napaść zbrojna w rozumieniu art. 5.
3. Integracja sensorów cywilno-wojskowych („Digital Ocean”): Sektor prywatny (operatorzy kabli, farm wiatrowych) dysponuje ogromną ilością danych z sensorów. Należy stworzyć mechanizmy bezpiecznego i zautomatyzowanego współdzielenia tych danych z centrami dowodzenia NATO (MARCOM) w celu budowania pełnej świadomości sytuacyjnej pod wodą. Inicjatywa Digital Ocean powinna być priorytetem inwestycyjnym.
4. Rozwój zdolności ASW i zwalczania dronów: Konieczne są inwestycje w autonomiczne systemy podwodne (AUV/UUV) zdolne do długotrwałego patrolowania infrastruktury oraz systemy obrony przeciwlotniczej krótkiego zasięgu (VSHORAD) dedykowane do ochrony obiektów energetycznych przed rojami tanich dronów.
5. Wzmocnienie kontrwywiadu i higieny cyfrowej: Należy zintensyfikować działania mające na celu wykrywanie i neutralizację sieci rekrutacyjnych rosyjskiego wywiadu (m.in. na Telegramie) oraz podnosić świadomość personelu infrastruktury krytycznej na temat zagrożeń insider threat.

Wnioski

1. Wojna w Ukrainie bezpowrotnie zmieniła krajobraz bezpieczeństwa energetycznego Europy. Infrastruktura energetyczna przestała być jedynie zasobem gospodarczym, stając się domeną walki, w której Rosja stosuje pełne spektrum środków – od dezinformacji i cyberataków, po fizyczny sabotaż i ataki raketowe. Dla krajów NATO oznacza to konieczność fundamentalnej zmiany podejścia: bezpieczeństwo dostaw energii musi być traktowane na równi z bezpieczeństwem militarnym granic.

2. Ukraińskie doświadczenia pokazują, że kluczem do przetrwania jest decentralizacja, fizyczna ochrona obiektów (ang. *hardening*) oraz szybkość reakcji naprawczych. Jednak w przypadku NATO, główny ciężar spoczywa na odstraszaniu (ang. *deterrence*) i zapobieganiu. Sojusz musi wykazać, że posiada nie tylko zdolności do wykrycia sprawców sabotażu w „szarej strefie”, ale także wolę polityczną do udzielenia zdecydowanej odpowiedzi. Bezpieczeństwo infrastruktury podmorskiej i energetycznej będzie w nadchodzącej dekadzie papierkiem lakmusowym skuteczności kolektywnej obrony Zachodu.

Bibliografia

- 2024 Baltic Sea submarine cable disruptions* – Wikipedia, https://en.wikipedia.org/wiki/2024_Baltic_Sea_submarine_cable_disruptions, [dostęp: 1.12.2025].
- 22nd Guards Heavy Bomber Aviation Division* – Wikipedia, https://en.wikipedia.org/wiki/22nd_Guards_Heavy_Bomber_Aviation_Division, [dostęp: 1.12.2025].
- 3M22 Zircon* – Wikipedia, https://en.wikipedia.org/wiki/3M22_Zircon, [dostęp: 1.12.2025].
- Agency for Restoration and Infrastructure Development and USAID work together on passive protection of energy facilities*, <https://www.kmu.gov.ua/en/news/ahentstvo-vid-novlennia-ta-usaid-spilno-pratsiuiut-nad-pasyvny-m-zakhystom-enerhoobiektiv>, [dostęp: 1.12.2025].
- Albright D., Burkhard S., Faragasso S., *Alabuga's Shahed 136 (Geran 2) Warheads: A Dangerous Escalation*, <https://isis-online.org/isis-reports/alabugas-shahed-136-geran-2-warheads-a-dangerous-escalation>, [dostęp: 1.12.2025].
- Analysis of Russia's Information Campaign against Ukraine*, https://stratcomcoe.org/uploads/pfiles/russian_information_campaign_public_12012016fin.pdf, [dostęp: 10.11.2025].
- Anokhin I., Faragasso S., *Russian Decoy Drones that Depend on Western Parts Pose a Great Challenge to Ukrainian Defenses*, <https://isis-online.org/isis-reports/russian-decoy-drones-that-depend-on-western-parts-pose-a-great-challenge>, [dostęp: 1.12.2025].
- Anonymity for sale: the thriving black market of crypto-to-fiat mules*, https://ti-russia.org/wp-content/uploads/2023/10/epaycrypto_.pdf, [dostęp: 1.12.2025].
- Arak P., *Russia's shadow war: How the Kremlin uses sabotage to wear down Europe*, <https://www.atlanticcouncil.org/blogs/new-atlanticist/russias-shadow-war-how-the-kremlin-uses-sabotage-to-wear-down-europe>, [dostęp: 1.12.2025].

- Armed Russian research vessels regularly spying on infrastructure in North Sea: report*, <https://nltimes.nl/2024/09/25/armed-russian-research-vessels-regularly-spying-infrastructure-north-sea-report>, [dostęp: 1.12.2025].
- Bajarūnas E., *Using NATO's Article 5 Against Hybrid Attacks*, <https://cepa.org/article/using-natos-article-5-against-hybrid-attacks>, [dostęp: 1.12.2025].
- Baltic Sea: the security risk posed by Russia's shadow fleet*, <https://www.bundeswehr.de/en/baltic-sea-russia-s-shadow-fleet-5892544>, [dostęp: 1.12.2025].
- Bandura R., Romanishyn A., *Striving for Access, Security, and Sustainability: Ukraine's Transition to a Modern and Decentralized Energy System*, <https://www.csis.org/analysis/striving-access-security-and-sustainability>, [dostęp: 1.12.2025].
- Belovodyev D., *Exclusive: The Russian Neo-Nazi Behind A Shadowy GRU Recruitment Campaign*, <https://www.rferl.org/a/russia-gru-nazi-sabotage-recruitment-telegram/33539661.html>, [dostęp: 1.12.2025].
- Besch S., Brown E., *Securing Europe's Subsea Data Cables*, <https://carnegieendowment.org/research/2024/12/securing-europes-subsea-data-cables?lang=en>, [dostęp: 1.12.2025].
- Bhamidipati S., Gao G., *GPS Spoofing Mitigation and Timing Risk Analysis in Networked Phasor Measurement Units via Stochastic Reachability*, „Journal of the Institute of Navigation September” 2023, 70 (3), navi.574, <https://navi.ion.org/content/70/3/navi.574/tab-article>, [dostęp: 1.12.2025].
- Birchmeier J.F., *The Reliability of Warden's Theory on the Use of Air Power*, School of Advanced Military Studies 2000.
- Bryjka F., *NATO and the EU Respond to Russian Maritime Sabotage*, <https://www.pism.pl/publications/nato-and-the-eu-respond-to-russian-maritime-sabotage>, [dostęp: 1.12.2025].
- Buchanan E., *Russia's 2021 National Security Strategy: Cool Change Forecasted for the Polar Regions*, <https://www.rusi.org/explore-our-research/publications/commentary/russias-2021-national-security-strategy-cool-change-forecasted-polar-regions>, [dostęp: 1.12.2025].
- Buchanan E., *The overhaul of Russian strategic planning for the Arctic Zone to 2035*, <https://www.ndc.nato.int/fr/the-overhaul-of-russian-strategic-planning-for-the-arctic-zone-to-2035>, [dostęp: 1.12.2025].
- Bukkvoll T., *Russian Special Operations Forces in Crimea and Donbas*, „Parameters” 2016, Vol. 46, No. 2, The US Army War College Quarterly: Parameters, <https://>

- press.armywarcollege.edu/cgi/viewcontent.cgi?article=2917&context=parameters, [dostęp: 11.11.2025].
- Caprile A., Leclerc G. *Russia's 'shadow fleet': Bringing the threat to light*, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766242/EPRS_BRI\(2024\)766242_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766242/EPRS_BRI(2024)766242_EN.pdf), [dostęp: 1.12.2025].
- Capture of the Crimean Parliament* – Wikipedia, https://en.wikipedia.org/wiki/Capture_of_the_Crimean_Parliament, [dostęp: 15.11.2025].
- Chalupa I., *Kremlin Silences Crimea's Last Pro-Ukraine TV Station*, <https://www.atlanticcouncil.org/blogs/ukrainealert/kremlin-silences-crimea-tv>, [dostęp: 11.11.2025].
- Childs N., *Russia's 'Shadow Fleet' and Sanctions Evasion: What Is To Be Done?*, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/01/russias_shadow-fleet_and-sanctions-evasion/iiss_russias_shadow-fleet_and-sanctions-evasion_31012025.pdf, [dostęp: 1.12.2025].
- Chincharadze K., *From Georgia to Ukraine: seventeen years of russian cyber capabilities at war*, Modren War Institute, <https://mwi.westpoint.edu/from-georgia-to-ukraine-seventeen-years-of-russian-cyber-capabilities-at-war>, [dostęp: 10.11.2025].
- Chybowski L., Chybowska D., *Ocena istotności zdarzeń pierwotnych związanych z działaniami dywersyjnymi przeciwko infrastrukturze krytycznej*, Assessment of primary events importance related to subversion against critical infrastructure, [w:] Materiały konferencyjne, Poznań 2022.
- Clausewitz C. von, *O wojnie*, Warszawa 2006.
- Coherent Resilience 2024 Moldova Tabletop Exercise (CORE24-M)*, [dostęp: 1.12.2025].
- Cooper J., *Russia's updated National Security Strategy*, <https://www.ndc.nato.int/fr/russias-updated-national-security-strategy>, [dostęp: 1.12.2025].
- Coynash H., *At least 22 Ukrainian websites blocked in Russian-occupied Crimea*, <https://archive.khpg.org/en/1501768045>, [dostęp: 15.11.2025].
- Coynash H., *Back in the USSR: Russia uses Soviet methods to jam Ukrainian media in occupied Crimea*, <https://khpg.org/en/1532985118>, [dostęp: 11.11.2025].
- Coynash H., *Crimean journalists is prosecuted for calling Crimea Ukrainian*, <https://ccl.org.ua/en/news/crimean-journalists-is-prosecuted-for-calling-crimea-ukrainian>, [dostęp: 15.11.2025].
- Cybersecurity in the power sector*, <https://www.eurelectric.org/in-detail/cybersecurity-in-the-power-sector>, [dostęp: 1.12.2025].

- Czachor R., *Ewolucja doktryny morskiej Federacji Rosyjskiej w latach 2001–2022. Ujęcie polityczne*, <https://www.studiapolitologiczne.pl/pdf=199427-119697-?filename=The%20Evolution%20of%20the.pdf>, [dostęp: 1.12.2025].
- Daly J., *The KH-101 Missiles that Russia Uses To Strike Ukraine. What Are They?*, <https://united24media.com/war-in-ukraine/the-kh-101-missiles-that-russia-uses-to-strike-ukraine-what-are-they-1193>, [dostęp: 1.12.2025].
- Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units* – CROWDSTRIKE BLOG, 2016, <https://www.crowdstrike.com/en-us/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units>, [dostęp: 10.11.2025].
- Davydenko L., *Russian new generation warfare of controlled chaos*, <https://indsr.org.tw/en/respublicationcon?uid=15&resid=2999&pid=5350&typeid=3>, [dostęp: 1.12.2025].
- Davydiuk A., Zubok V., *Analytical Review of the Resilience of Ukraine's Critical Energy Infrastructure to Cyber Threats in Times of War*, 15th International Conference on Cyber Conflict: Meeting Reality (CyCon), Tallinn, Estonia 2023.
- De'Ath A., *The Risks of AI in the Energy Sector*, <https://www.enseccoe.org/wp-content/uploads/2024/10/Energy-Highlights-No.19.pdf>, [dostęp: 1.12.2025].
- Delamer J., Tsimaylo V., *Investment disputes in the crossfire of War*, <https://compass-lexecon.files.svdcdn.com/production/editorial/2025/02/The-Analysis-Investment-Disputes-Crossfire-of-War-250225.pdf?dm=1740482534>, [dostęp: 15.11.2025].
- Derleth J., *Russian New Generation Warfare Deterring and Winning at the Tactical Level*, <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2020/Derleth-New-Generation-War>, [dostęp: 11.11.2025].
- Dmytriieva D., *North Korean KN-23 missiles: Russia's new weapon in war against Ukraine*, <https://newsukraine.rbc.ua/news/north-korean-kn-23-missiles-russia-s-new-1723384830.html>, [dostęp: 1.12.2025].
- DTEK Initiated Investment Dispute against Russia over the Company's Assets in Crimea*, <https://dtek.com/en/media-center/news/dtek-initsiioval-rassmotrenie-investitsionnogo-spora-s-rossiey-v-otnoshenii-aktivov-gruppy-v-krymu->, [dostęp: 11.11.2025].
- Edwards Ch., Seidenstein N., *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure*, <https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure>, [dostęp: 1.12.2025].

- Energy blockade of Crimea reveals shady dealings of the oligarchs*, <https://www.obserwatorfinansowy.pl/in-english/new-trends/energy-blockade-of-crimea-reveals-shady-dealings-of-the-oligarchs>, [dostęp: 15.11.2025].
- Eshel T., *Russians Used Cyber Bots to Target Ukrainian Artillery*, Defence Update, 2016, https://defense-update.com/20161223_trojan-2.html, [dostęp: 10.11.2025].
- Eu-Nato task force on the resilience of critical infrastructure*, https://gemini.google.com/app/9ccd2a318c891c04?utm_source=app_launcher&utm_medium=owned&utm_campaign=base_all, [dostęp: 1.12.2025].
- Europe Announces 19th Sanctions Package on Russia – Including First-Ever Crypto Asset Designations Linked to Moscow*, <https://www.trmlabs.com/resources/blog/europe-announces-19th-sanctions-package-on-russia---including-first-ever-crypto-asset-designations-linked-to-moscow>, [dostęp: 1.12.2025].
- Europe Builds Deterrence as The Kremlin Escalates Hybrid Warfare*, https://gemini.google.com/app/9ccd2a318c891c04?utm_source=app_launcher&utm_medium=owned&utm_campaign=base_all, [dostęp: 10.12.2025].
- Exposing Russia’s Undersea Shadow War*, <https://techjournalism.medium.com/exposing-the-russias-undersea-shadow-war-467890fac159>, [dostęp: 1.12.2025].
- Fontugne R., Ermoshina K., Aben E., *The Internet in Crimea: a Case Study on Routing*, https://www.iijlab.net/en/members/romain/pdf/romain_gi2020.pdf, [dostęp: 11.11.2025].
- Geller E., *Pro-Russia hacktivists launching attacks that could damage OT*, <https://www.cybersecuritydive.com/news/russian-hacktivists-critical-infrastructure-remote-access-advisory/807493>, [dostęp: 1.12.2025].
- Gerasimov V., *The Value of Science Is in the Foresight. New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations*, https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf, [dostęp: 1.12.2025].
- Geri M., Comini N., *NATO’s preparedness to hybrid threats must overcome strategic limits and coordination hurdles*, <https://natowatch.org/default/2025/natos-preparedness-hybrid-threats-must-overcome-strategic-limits-and-coordination>, [dostęp: 1.12.2025].
- Geri M., *Understanding Russian Hybrid Warfare against Europe in the energy sector and in the future ‘energy-resources-climate’ security nexus*, „Journal of Strategic Security” 2024, Vol. 17, No. 3.

- Goncharova O., *North Korean missiles with Western parts fuel Russian attacks on Ukraine, CNN reports*, <https://kyivindependent.com/ukraine-faces-wave-of-attacks-with-north-korean-missiles-with-western-components-cnn-reports>, [dostęp: 1.12.2025].
- GPS Jamming and Ukraine's Electrical Grid – Cisco Talos*, <https://rntfnd.org/2024/04/21/gps-jamming-and-ukraines-electrical-grid-cisco-talos>, [dostęp: 1.12.2025].
- Guo R., Liu M., Deng R., *Vulnerability Assessment of High-Voltage Direct Current Transmission Systems to Cyberattacks*, <https://sands.edpsciences.org/articles/sands/pdf/forth/sands20250011.pdf>, [dostęp: 1.12.2025].
- Gurcov N., *Behind the lines: How Ukraine has outgunned Russia in sabotage*, <https://acleddata.com/report/behind-lines-how-ukraine-has-outgunned-russia-sabotage>, [dostęp: 1.12.2025].
- Haines J.R., *How, Why, and When Russia Will Deploy Little Green Men – and Why the US Cannot*, <https://www.fpri.org/article/2016/03/how-why-and-when-russia-will-deploy-little-green-men-and-why-the-us-cannot>, [dostęp: 10.11.2025].
- Harvey J., *The Russo-Ukrainian war's expansion into the High North poses electronic warfare challenges for NATO*, <https://www.arctictoday.com/the-russo-ukrainian-wars-expansion-into-the-high-north-poses-electronic-warfare-challenges-for-nato>, [dostęp: 1.12.2025].
- Heinrich H., *Industrial Accident Prevention*, McGraw Hill, 1941.
- Himka S., *Baltic Sea Undersea Cable Security*, <https://jsis.washington.edu/news/baltic-sea-undersea-cable-security>, [dostęp: 1.12.2025].
- Hobhouse C., *On a war footing: Securing critical energy infrastructure*, <https://www.iss.europa.eu/publications/briefs/war-footing-securing-critical-energy-infrastructure>, [dostęp: 1.12.2025].
- Holloway M., *How Russia Weaponized Social Media in Crimea*, <https://thestrategy-bridge.org/the-bridge/2017/5/10/how-russia-weaponized-social-media-in-crimea>, [dostęp: 11.11.2025].
- How Occupation regimes Take Over the Information Space*, <https://splintercon.net/wp-content/uploads/2024/01/how-occupation-regimes-take-over-the-information-space.pdf>, [dostęp: 11.11.2025].
- Humpert M., *Russia Upgrades Key Arctic Military Base with Expanded Runway*, <https://www.highnorthnews.com/en/russia-upgrades-key-arctic-military-base-expanded-runway>, [dostęp: 1.12.2025].

- Humphreys B.E., *Attacks on Ukraine's Electric Grid: Insights for U.S. Infrastructure Security and Resilience*, <https://www.congress.gov/crs-product/R48067>, [dostęp: 11.11.2025].
- Jones S.G., *Russia's Shadow War Against the West*, <https://www.csis.org/analysis/russias-shadow-war-against-west>, [dostęp: 1.12.2025].
- Kaber P.A., *Russian military buildup in Crimea & destabilization of the Black Sea region*, <https://vm.ee/en/media/283/download>, [dostęp: 10.11.2025].
- Kannike E., *Tobol System in russian Kaliningrad Jams GPS Over Europe, and It Does Cause Problems*, https://en.defence-ua.com/weapon_and_tech/tobol_system_in_russian_kaliningrad_jams_gps_over_europe_and_it_does_cause_problems-9283.html, [dostęp: 1.12.2025].
- Kennedy J., Bryan E., Ploom I., Veebel V., *Russia's Use of Crypto Schemes*, <https://www.rand.org/pubs/commentary/2025/08/russias-use-of-crypto-schemes.html>, [dostęp: 1.12.2025].
- Kh-69 X-69*, <https://www.armyrecognition.com/military-products/army/missiles/cruise-missiles/kh-69-h-69>, [dostęp: 1.12.2025].
- Khalil M., *Cybersecurity in the Power Sector 2025: How Utilities Defend the Grid from Evolving Cyber Threats*, <https://deepstrike.io/blog/cybersecurity-in-the-power-sector-2025>, [dostęp: 1.12.2025].
- Khorrami N., *Subsea sabotage should spark review of critical infrastructure security*, <https://bindinghook.com/subsea-sabotage-should-spark-review-of-critical-infrastructure-security>, [dostęp: 1.12.2025].
- KN-23*, <https://missilethreat.csis.org/missile/kn-23>, [dostęp: 1.12.2025].
- Kofman M. i in., *Lessons from Russia's Operations in Crimea and Eastern Ukraine*, RAND 2017, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1498/RAND_RR1498.pdf, [dostęp: 10.11.2025].
- Kofman M. i in., *Russian Military Strategy: Core Tenets and Operational Concepts*, <https://www.cna.org/reports/2021/08/Russian-Military-Strategy-Core-Tenets-and-Operational-Concepts.pdf>, [dostęp: 1.12.2025].
- Kosharna O., *Energy infrastructure facilities will have three levels of protection*, Ukrenergo CEO Kudrytskyi, <https://censor.net/en/n3449115>, [dostęp: 1.12.2025].
- Kozłowski A.R., *The war and tourism: security issues and business opportunities in shadow of Russian war against Ukraine*, Qual Quant (2023).

- Kryzhnyi A., *Russia changes tactics in attacks on Ukraine's energy sector*, <https://www.pravda.com.ua/eng/news/2025/11/09/8006535>, [dostęp: 1.12.2025].
- Kushnikov V., *Western-made components found in Parody decoy drone*, <https://militarnyi.com/en/news/western-made-components-found-in-parody-decoy-drone>, [dostęp: 1.12.2025].
- Lange-Ionatamišvili E., *Analysis of Russia's information campaign against Ukraine*, NATO Strategic Communications Centre of Excellence, 2015, <https://stratcomcoe.org/publications/analysis-of-russias-information-campaign-against-ukraine/151>, [dostęp: 10.11.2025].
- Little green men (Russo-Ukrainian war)* – Wikipedia, [https://en.wikipedia.org/wiki/Little_green_men_\(Russo-Ukrainian_war\)](https://en.wikipedia.org/wiki/Little_green_men_(Russo-Ukrainian_war)), [dostęp: 10.11.2025].
- MacColl J., Westmore K., *Operation Destabilise: Russia, Organised Crime and Illicit Finance*, <https://www.rusi.org/explore-our-research/publications/commentary/operation-destabilise-russia-organised-crime-and-illicit-finance>, [dostęp: 1.12.2025].
- Majcin J., *Battle of the Baltic: Safeguarding critical undersea infrastructure*, <https://www.epc.eu/publication/Battle-of-the-Baltic-Safeguarding-critical-undersea-infrastructure-645780>, [dostęp: 1.12.2025].
- Marcoux B., *From Telegraph to Terawatt-hours: Why NATO-L Could Be the Great Eastern of the Net-Zero Age*, <https://www.energycentral.com/energy-biz/post/from-telegraph-to-terawatt-hours-why-nato-l-could-be-the-great-eastern-el4z4YFaL-CFeaZz>, [dostęp: 1.12.2025].
- Massalin E., *Strategic Analysis on the Energy Security Measures of Russia*, <https://www.ensecce.org/wp-content/uploads/2024/01/2021-08-strategic-analysis-on-the-energy-security-measures-of-russia-enrica-massalin.pdf>, [dostęp: 1.12.2025].
- Matuszak S., *Nowe zmasowane ataki Rosji na ukraińską infrastrukturę energetyczną – straty i wyzwania*, <https://www.osw.waw.pl/pl/publikacje/analizy/2024-04-17/nowe-zmasowane-ataki-rosji-na-ukrainska-infrastruktura-energetyczna>, [dostęp: 11.11.2025].
- McDermott R.N., *Russia's Electronic Warfare Capabilities do 2025*, International Centre for Defence and Security, 2017, https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf, [dostęp: 10.11.2025].
- McIlmoil R., *Microgrids Could Enhance Grid Resilience*, <https://www.nrel.gov/news/detail/program/2025/microgrids-could-enhance-grid-resilience>, [dostęp: 1.12.2025].

- Meissner P., *Assessing Russian Cyber Effects*, <https://www.war.gov/News/Releases/Release/Article/2585399/assessing-russian-cyber-effects>, [dostęp: 10.11.2025].
- Mihaylov N., *Cyber Dimensions of a Hybrid Warfare*, CyberPeace Institute, <https://cyberpeaceinstitute.org/news/cyber-dimensions-of-a-hybrid-warfare>, [dostęp: 10.11.2025].
- Miller Ch., *'Fancy Bear' Tried to Hack E-Mail of Ukrainian Making Artillery-Guidance App*, <https://www.rferl.org/a/ukraine-russia-fancy-bear-hacking-artillery-guidance-app/28831564.html>, [dostęp: 15.11.2025].
- Monaghan S., Svendsen O., Darrah M., Arnold E., *NATO's Role in Protecting Critical Undersea Infrastructure*, <https://www.csis.org/analysis/natos-role-protecting-critical-undersea-infrastructure>, [dostęp: 1.12.2025].
- Murdoch B., *Russian strikes on Ukraine's Energy grid follow systematic pattern, analysis shows*, <https://euromaidanpress.com/2025/11/20/russian-strikes-on-ukraines-energy-grid-follow-systematic-pattern>, [dostęp: 1.12.2025].
- Murmansk-BN Russian Long-Range Communications Jamming System*, <https://odin.tradoc.army.mil/WEG/Asset/b4cd1efd5c57c88bcfe7ca78a2831903>, [dostęp: 1.12.2025].
- NATO and European Union release final assessment report on resilience of critical infrastructure*, <https://www.nato.int/en/news-and-events/articles/news/2023/06/29/nato-and-european-union-release-final-assessment-report-on-resilience-of-critical-infrastructure>, [dostęp: 1.12.2025].
- NATO exercise strengthens energy security*, <https://www.energimyndigheten.se/en/news/2025/nato-exercise-strengthens-energy-security>, [dostęp: 3.12.2025].
- NATO launches 'Baltic Sentry' to increase critical infrastructure security*, <https://www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-security>, [dostęp: 1.12.2025].
- NATO steps up to better address maritime threats*, <https://ec.europa.eu/newsroom/cipr/items/806186/en>, [dostęp: 1.12.2025].
- NATO's Digital Ocean Initiative gets a boost in Portugal*, <https://www.nato.int/en/news-and-events/articles/news/2024/09/20/natos-digital-ocean-initiative-gets-a-boost-in-portugal>, [dostęp: 1.12.2025].
- Nazarenko V., *Ukraine has prepared three levels of protection against Russia's attacks on energy infrastructure*, <https://war.ukraine.ua/war-news/ukraine-protection-russias-attacks-energy-infrastructure>, [dostęp: 1.12.2025].
- Nedelnyuk O., *How Russian „Troll factory tried to effect on Ukraine's agenda. Analysis of 755 000 tweets*, <https://voxukraine.org/en/how-russian-troll-factory-tried-to-effect-on-ukraine-s-agenda>, [dostęp: 10.11.2025].

- Nelson H., *Ukraine faces its most perilous winter yet*, <https://www.atlanticcouncil.org/blogs/energysource/ukraine-faces-its-most-perilous-winter-yet>, [dostęp: 1.12.2025].
- New generation warfare* – Wikipedia, https://en.wikipedia.org/wiki/New_generation_warfare, [dostęp: 15.11.2025].
- Offshore wind and risk management: opportunities and unchartered waters*, https://www.controlrisks.com/our-thinking/insights/offshore-wind-and-risk-management-opportunities-and-unchartered-waters?utm_referrer=https://gemini.google.com, [dostęp: 1.12.2025].
- Ogryzko L., Rozzi A., *Shallow seas and „shadow fleets: Europe’s undersea infrastructure is dangerously vulnerable*, <https://ecfr.eu/article/shallow-seas-and-shadow-fleets-europes-undersea-infrastructure-is-dangerously-vulnerable>, [dostęp: 1.12.2025].
- Ostanina S., *Russia-Directed Sabotage in Europe*, <https://www.spglobal.com/market-intelligence/en/news-insights/research/2025/11/russia-directed-sabotage-europe>, [dostęp: 1.12.2025].
- Paik A., Counter J., *International law doesn’t adequately protect undersea cables. That must change*, <https://www.atlanticcouncil.org/content-series/hybrid-warfare-project/international-law-doesnt-adequately-protect-undersea-cables-that-must-change>, [dostęp: 1.12.2025].
- Patlove K., *Depths of Deception: State-Backed Undersea Cable Disruptions and the Role of International Maritime Law*, [dostęp: 1.12.2025].
- Piekarski M., *Infrastruktura krytyczna jako cel ataków hybrydowych i konwencjonalnych. Wnioski z ukraińskich doświadczeń „Terroryzm – Studia, Analizy, Prewencja” 2025*.
- Poireault K., *Russian APT Groups Intensify Attacks in Europe with Zero-Day Exploits and Wipers*, [dostęp: 1.12.2025].
- Policy briefing: tackling the russian ‘shadow’ fleet, https://energyandcleanair.org/wp/wp-content/uploads/2024/09/State-Capture_CREA_Shadow-fleet-policy-briefing_Final_08.2024.pdf, [dostęp: 1.12.2025].
- Polmar N., *‘Status-6’ Russian Drone Nearly Operational*, <https://www.usni.org/magazines/proceedings/2019/april/status-6-russian-drone-nearly-operational>, [dostęp: 1.12.2025].
- Poseidon (unmanned underwater vehicle) – Wikipedia, [https://en.wikipedia.org/wiki/Poseidon_\(unmanned_underwater_vehicle\)](https://en.wikipedia.org/wiki/Poseidon_(unmanned_underwater_vehicle)), [dostęp: 1.12.2025].
- Power Grids Unplugged: How Islanding is Changing Autonomous Energy*, <https://www.smpnet.tech/post/power-grids-unplugged-how-islanding-is-changing-autonomous-energy>, [dostęp: 1.12.2025].

- Pressentin M., Schmidt J., Schwartzkopff J., *LNG Projects Are a Bad Deal for Germans and Americans*, <https://www.americanprogress.org/article/lng-projects-are-a-bad-deal-for-germans-and-americans>, [dostęp: 1.12.2025].
- Presumably SSO Special Purpose Center Kubinka-2 Operators in Belbek during the 2014 Crimea Annexation. Note the Asian Operator in the Middle. If my buddy told it right he is Tuvan and he still serves in thar Unit to this day: r/SpecOpsArchive – Reddit, https://www.reddit.com/r/SpecOpsArchive/comments/1eufpqx/presumably_sso_special_purpose_center_kubinka2, [dostęp: 10.11.2025].
- Price B., *'Operation Armageddon' Cyber Espionage Campaign Aimed at Ukraine: Looking-glass*, <https://www.securityweek.com/operation-armageddon-cyber-espionage-campaign-aimed-ukraine-lookingglass>, [dostęp: 15.11.2025].
- Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure*, <https://www.cisa.gov/sites/default/files/2025-12/aa25-343a-pro-russia-hacktivists-conduct-attacks.pdf>, [dostęp: 1.12.2025].
- Putin Approves Russia's First Long-Term Naval Strategy Through 2050*, <https://www.themoscowtimes.com/2025/06/09/putin-approves-russias-first-long-term-naval-strategy-through-2050-a89381>, [dostęp: 1.12.2025].
- Quinville R.S., Moyer J. C., Lindholm R., *Risky Game: Hybrid Attack on Baltic Undersea Cables*, <https://www.wilsoncenter.org/article/risky-game-hybrid-attack-baltic-undersea-cables>, [dostęp: 1.12.2025].
- Rafalovych V., *The Fourth Winter: Inside Russia's Evolving War on Ukraine's Energy*, <https://www.cyis.org/post/the-fourth-winter-inside-russia-s-evolving-war-on-ukraine-s-energy>, [dostęp: 1.12.2025].
- Raggett Ch., *Rocket from the Crypto: State-backed Criminal Groups and the Fintech Sector*, <https://cetas.turing.ac.uk/publications/rocket-crypto-state-backed-criminal-groups-and-fintech-sector>, [dostęp: 1.12.2025].
- Restoration Agency implements three-tier energy infrastructure protection system – Nayyem*, <https://en.interfax.com.ua/news/economic/953851.html>, [dostęp: 1.12.2025].
- Richterova D., Grossfeld E., Long M., Bury P., *Russian Sabotage in the Gig-Economy Era*, „The RUSI Journal” 2024, 169(5), <https://doi.org/10.1080/03071847.2024.2401232>, [dostęp: 1.12.2025].
- Rimutis S., *Lessons of War: Ukraine's Energy Infrastructure Damage, Resilience and Future Opportunities*, https://www.gssc.lt/wp-content/uploads/2024/05/v04_Rimutis_Ukrainos-energetikos-sektorius-zala_EN_A4.pdf, [dostęp: 1.12.2025].

- Rivera J., *Has Russia Begun Offensive Cyberspace Operations in Crimea?*, <https://georgetownsecuritystudiesreview.org/2014/03/02/has-russia-begun-offensive-cyberspace-operations-in-crimea>, [dostęp: 11.11.2025].
- Rolander A., *Irregular Warfare at Sea: How Russia's Shadow Fleet Undermines Maritime Security*, <https://smallwarsjournal.com/2025/12/11/irregular-warfare-at-sea>, [dostęp: 1.12.2025].
- Russia launches new nuclear submarine carrier of doomsday drone*, <https://www.thehindu.com/news/international/russia-launches-new-nuclear-submarine-carrier-of-doomsday-drone/article70233316.ece>, [dostęp: 1.12.2025].
- Russia Leveraging Kyrgyzstan's Crypto Ecosystem to Evade Sanctions*, <https://www.trmlabs.com/resources/blog/russia-leveraging-kyrgyzstans-crypto-ecosystem-to-evade-sanctions>, [dostęp: 1.12.2025].
- Russia massively launching decoy drone with Western components to distract Ukrainian air defenses*, <https://english.nv.ua/nation/parody-russians-use-a-new-type-of-uav-to-imitate-the-shahed-what-is-known-50465488.html>, [dostęp: 1.12.2025].
- Russia's strategy in cyberspace*, NATO Strategic Communications Centre of Excellence, https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf, [dostęp: 10.11.2025].
- Russian annexation of Crimea* – Wikipedia, https://en.wikipedia.org/wiki/Russian_annexation_of_Crimea, [dostęp: 10.11.2025].
- Russian Electronic Warfare Targets NATO Assets*, <https://www.afcea.org/signal-media/international/russian-electronic-warfare-targets-nato-assets>, [dostęp: 1.12.2025].
- Russian Kh-69 that destroyed Kyiv region's largest thermal power plant: overview and characteristics of missile*, <https://global.espresso.tv/military-news-kh-69-missile-used-by-russians-to-destroy-trypillia-thermal-power-plant>, [dostęp: 1.12.2025].
- Russian Naval Infantry* – Wikipedia, https://en.wikipedia.org/wiki/Russian_Naval_Infantry, [dostęp: 10.11.2025].
- Russian Offensive Campaign Assessment*, <https://understandingwar.org/research/russia-ukraine/russian-offensive-campaign-assessment-october-22-2025>, [dostęp: 1.12.2025].
- Russian's war on Ukraine: Timeline of cyber-attacks*, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI\(2022\)733549_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf), [dostęp: 10.11.2025].

- Russon M.-A., *The race to shore up Europe's power grids against cyberattacks and sabotage*, https://www.theregister.com/2025/11/03/europe_power_grid_security, [dostęp: 1.12.2025].
- Safronov T., *Russia Launches New Zircon Anti-Ship Missile at Sumy Region*, <https://militaryni.com/en/news/russia-launches-new-zircon-anti-ship-missile-at-sumy-region>, [dostęp: 1.12.2025].
- Satam P., *Russia's TOBOL EW System „Cuts Off” Starlink From It's Ground Terminals; How Did Moscow Delink The Starlink*, <https://space4peace.org/russias-tobol-ew-system-cuts-off-starlink-from-its-ground-terminals-how-did-moscow-delink-the-starlink>, [dostęp: 1.12.2025].
- Schaller C., *Russia's Mapping of Critical Infrastructure in the North and Baltic Seas – International Law as an Impediment to Countering the Threat of Strategic Sabotage?*, „Nordic Journal of International Law” 2024, 93(2), <https://doi.org/10.1163/15718107-bja10083>.
- Schmitt B., Riley A., Kurtyka M., *Subsea Sabotage: Protecting Energy Infrastructure from Hostile Aggression*, <https://kleinmanenergy.upenn.edu/research/publications/subsea-sabotage-protecting-energy-infrastructure-from-hostile-aggression>, [dostęp: 1.12.2025].
- Schneier B., *Attack Trees*, „Dr. Dobbs Journal”, grudzień 1999.
- Scott R., *From the JED Archives: Tuning In, Turning On: Russia Brings Radio-Electronic Combat to the Fore*, „The Journal of Electromagnetic Dominance”, <https://www.jedonline.com/2023/02/16/from-the-jed-archives-tuning-in-turning-on-russia-brings-radio-electronic-combat-to-the-fore-2>, [dostęp: 10.11.2025].
- Second-level power grid protection in Ukraine shows 98% effectiveness*, <https://media-center.org.ua/second-level-power-grid-protection-in-ukraine-shows-98-effectiveness>, [dostęp: 1.12.2025].
- Shepard D.P., Humphreys T.E., *Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks*, <https://rnl.ae.utexas.edu/images/stories/files/papers/spoofSMUCIP2012.pdf>, [dostęp: 1.12.2025].
- Sheremet A., *Concrete blocks and sandbags*, „The Financial Times” reported how Ukraine is preparing for attacks on the energy sector”, <https://babel.ua/en/news/100170-concrete-blocks-and-sandbags-the-financial-times-reported-how-ukraine-is-preparing-for-attacks-on-the-energy-sector>, [dostęp: 1.12.2025].
- Sotilas S., *Weapons and Equipment Analysis of Little Green Men in Crimea* (March 2014), [za:] *Little Green Men: A Primer on Modern Russian Unconventional Warfare*,

- Ukraine 2013–2014”, USASOC, Fort Bragg, 2014, <https://nsarchive.gwu.edu/media/16170/ocr>, [dostęp: 10.11.2025].
- Stand R.W., *Decentralizing Ukraine’s energy future: microgrids as a path to independence*, <https://energytransition.org/2024/10/decentralizing-ukraines-energy-future-microgrids-as-a-path-to-independence>, [dostęp: 1.12.2025].
- Strategy for Development of the Arctic Zone of the Russian Federation and Provision of National Security for the Period up to 2035 (Revised)*, https://usnwc.edu/_images/portals/0/NWCDepartments/Russia-Maritime-Studies-Institute/16MAR23_20201026_ENG_RUS_Arctic-Strategy2035_FINAL_16MAR238f95.pdf, [dostęp: 1.12.2025].
- Strategy for Development of the Arctic Zone of the Russian Federation and Provision of National Security for the Period up to 2035 (Revised)*, https://usnwc.edu/_images/portals/0/NWCDepartments/Russia-Maritime-Studies-Institute/16MAR23_20201026_ENG_RUS_Arctic-Strategy2035_FINAL_16MAR238f95.pdf, [dostęp: 1.12.2025].
- Strzelecki J., Sadowski R., *Krym bez prądu*, Ośrodek Studiów Wschodnich, <https://www.osw.waw.pl/pl/publikacje/analizy/2015-11-25/krym-bez-pradu>, [dostęp: 11.11.2025].
- Strzelecki M., *Uprzejmi ludzie czy zielone ludziki? Siły Operacji Specjalnych Ministerstwa Obrony Federacji Rosyjskiej*, „Bezpieczeństwo. Teoria i Praktyka” 2017, nr 3, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego w Krakowie.
- Sukhankin S., *Blind, Confuse and Demoralize: Russian Electronic Warfare Operations in Donbas*, Jamestown Foundation 2021, <https://jamestown.org/program/blind-confuse-and-demoralize-russian-electronic-warfare-operations-in-donbas>, [dostęp: 10.11.2025].
- The Russia-Ukraine War Report Card*, Nov. 19, 2025, <https://www.russiamatters.org/news/russia-ukraine-war-report-card/russia-ukraine-war-report-card-nov-19-2025>, [dostęp: 1.12.2025].
- Thévenin P., *A legislative route to combat sabotage of undersea cables: A Q&A with Pierre Thévenin*, <https://www.sipri.org/commentary/topical-background/2025/legislative-route-combat-sabotage-undersea-cables>, [dostęp: 1.12.2025].
- Thomas T., *Russian nonlethal weapons*, <https://www.mitre.org/sites/default/files/2021-11/pr-20-0145-russia-nonlethal-weapon-concept.pdf>, [dostęp: 1.12.2025].
- Thomas T.L., *Russian Military Thought: Concepts and Elements*, <https://www.armyupress.army.mil/Portals/7/Hot-Spots/docs/Russia/Mitre-Thomas.pdf>, [dostęp: 1.12.2025].

- Trenin D., *Russia's National Security Strategy: A Manifesto for a New Era*, <https://carnegieendowment.org/posts/2021/07/russias-national-security-strategy-a-manifesto-for-a-new-era?lang=en>, [dostęp: 1.12.2025].
- Ukraine: Gunmen seize Crimea government buildings*, <https://www.bbc.co.uk/news/world-europe-26364891>, [dostęp: 15.11.2025].
- UNCITRAL tribunal finds Russia liable to pay USD 207.8 million for the unlawful expropriation of the assets of a Ukrainian electricity company*, <https://www.iisd.org/itn/2024/01/13/uncitral-tribunal-finds-russia-liable-to-pay-usd-207-8-million-for-the-unlawful-expropriation-of-the-assets-of-a-ukrainian-electricity-company>, [dostęp: 15.11.2025].
- Volodymyr B., *Spiderweb Operation: How Many Tu-95MSs, Tu-22M3s and A-50s Destroyed at Russian Airbases*, <https://militaryni.com/en/news/spiderweb-operation-how-many-tu-95ms-tu-22m3-and-a-50s-destroyed-at-russian-airbases>, [dostęp: 1.12.2025].
- Watson H.A., *Launch Control Safety Study*, Murray Hill 1961.
- Weber Y., *Russia's New Maritime Doctrine*, Marine Corps University Press – MES Insights, sierpień 2022, <https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/MES-Publications/MES-Insights/Russias-New-Maritime-Doctrine>, [dostęp: 1.12.2025].
- Weichert B.J., *Vladimir Putin Is Preparing for War Against Starlink*, <https://nationalinterest.org/blog/buzz/vladimir-putin-is-preparing-for-war-against-starlink>, [dostęp: 1.12.2025].
- Why Ukraine should develop distributed generation?*, <https://golaw.ua/insights/energy-alert/chomu-ukrayini-varto-rozvivati-rozpodilenu-generacziyu>, [dostęp: 1.12.2025].
- Wilk A., *Russian military intervention in Crimea*, <https://www.osw.waw.pl/en/publikacje/analyses/2014-03-05/russian-military-intervention-crimea>, [dostęp: 10.11.2025].
- Wilk A., Żochowski P., *Ukraine deals blow to Russian strategic aviation. Day 1196 of the war*, <https://www.osw.waw.pl/en/publikacje/analyses/2025-06-03/ukraine-deals-blow-to-russian-strategic-aviation-day-1196-war>, [dostęp: 1.12.2025].
- Zinchenko H., *835 MW of distributed generation connected in 2024 – Ministry of Energy*, <https://ua-energy.org/en/posts/31-12-2024-812032b8-5207-4ac4-ba71-8bb-818b96e8b>, [dostęp: 1.12.2025].

Autorzy

Pptk rez. dr inż. Marcin Lipka

Doktor nauk społecznych w dyscyplinie nauki o obronności. Ekspert Centrum Badań nad Ryzykami Społecznymi i Gospodarczymi Uniwersytetu Civitas. Były oficer Oddziału Specjalnego Żandarmerii Wojskowej oraz Biura Ochrony Rządu. Menadżer z wieloletnim doświadczeniem zawodowym w strukturach bezpieczeństwa korporacyjnego sektora telekomunikacyjnego oraz energetycznego. Specjalizuje się w zarządzaniu obszarami związanymi z: ciągłością działania, bezpieczeństwem informacji, bezpieczeństwem fizycznym i technicznym, obowiązkami na rzecz obronności i bezpieczeństwa państwa, sytuacjami kryzysowymi. Jego zainteresowania badawcze koncentrują się na zagadnieniach związanych z odpornością struktur państwa i przedsiębiorstw oraz analizie hipotez konkurencyjnych. Jest absolwentem Wojskowej Akademii Technicznej, Akademii Obrony Narodowej i Wyższej Szkoły Policji w Szczytnie.

Dr Michał Piekarski

Adiunkt w Instytucie Studiów Międzynarodowych i Bezpieczeństwa Uniwersytetu Wrocławskiego. Zajmuje się problematyką bezpieczeństwa narodowego, w szczególności zagrożeń hybrydowych, militarnych, bezpieczeństwa morskiego państwa oraz kultury strategicznej Polski. Wybrane publikacje: *Infrastruktura krytyczna jako cel ataków hybrydowych i konwencjonalnych. Wnioski z ukraińskich doświadczeń* („Terrorizm. Studia – Analizy – Prewencja”, nr specjalny 2025); *Hybrid Threats from Russia to NATO’s Littoral States on the Baltic Sea Maritime Critical Infrastructure and Lessons form the Black Sea: Observations from Poland, a Frontline State* (German Institute for Defence and Strategic Studies, 2025); *Ochrona infrastruktury krytycznej na polskich obszarach morskich w kontekście zagrożeń hybrydowych* („Ekspertyza PTBN”, 2023);

Możliwe scenariusze zagrożeń terrorystycznych na terytorium Rzeczypospolitej Polskiej w kontekście zagrożeń hybrydowych („Terroryzm. Studia – Analizy – Prewencja”, 2/2022); *Ewolucja Sił Zbrojnych Rzeczypospolitej Polskiej w latach 1990–2020 w kontekście kultury strategicznej Polski* (2022). Oprócz tego publikował między innymi w czasopismach i portalach „Frag Out”, oko.press, „Polska Zbrojna”. Członek Polskiego Towarzystwa Bezpieczeństwa Narodowego.

O programie NATO Nauka dla Pokoju i Bezpieczeństwa (SPS)



Program NATO SPS promuje dialog i praktyczną współpracę pomiędzy państwami NATO i krajami partnerskimi w oparciu o badania naukowe, innowacje technologiczne i wymianę wiedzy. Program SPS zapewnia finansowanie, doradztwo eksperckie i wsparcie w zakresie dostosowanych do indywidualnych potrzeb działań mających znaczenie dla bezpieczeństwa cywilnego. Działania SPS opierają się na zestawie zatwierdzonych przez Sojusz kluczowych priorytetów, które odpowiadają na pojawiające się wyzwania w zakresie bezpieczeństwa. SPS wspiera cztery rodzaje działań: wieloletnie projekty badawczo-rozwojowe (MYP), zaawansowane warsztaty badawcze (ARW), zaawansowane kursy szkoleniowe (ATC) i zaawansowane instytuty badawcze (ASI). Jej działania skupiają naukowców, ekspertów i urzędników z NATO i krajów partnerskich, którzy wspólnie prowadzą działania badawcze i wymianę wiedzy. Możliwości współpracy ogłaszane są w formie naborów wniosków na stronie internetowej SPS.

O projekcie R-GRID



Projekt R-GRID to dwuletnie, międzynarodowe przedsięwzięcie badawczo-rozwojowe, którego celem jest stworzenie zaawansowanego symulatora zagrożeń dla sieci elektroenergetycznych, opartego na sztucznej inteligencji i metodach optymalizacji, wspierającego decyzje dotyczące ochrony infrastruktury krytycznej przed atakami hybrydowymi i innymi zakłóceniami.

Głównym celem jest opracowanie narzędzia R-GRID – symulatora predykcji zagrożeń, który modeluje skutki ataków hybrydowych (w tym z użyciem środków militarnych) na sieci elektroenergetyczne oraz wskazuje optymalne wykorzystanie dostępnych środków ochrony. R-GRID ma ograniczać ryzyko przerw w dostawach

energii w kluczowych sektorach gospodarki oraz zapobiegać blackoutom, uwzględniając zarówno tradycyjne, jak i odnawialne źródła energii na różnych poziomach dojrzałości technologicznej.

Symulator *explicite* modeluje sieć elektroenergetyczną (linie, stacje, węzły), dostępne zasoby obronne i ich rozmieszczenie, potencjalnych napastników oraz strategie ataku i obrony; wykorzystuje przy tym m.in. model Stackelberga, metody sztucznej inteligencji i optymalizacji. Do kluczowych funkcji należą: analiza znaczenia elementów sieci z punktu widzenia infrastruktury krytycznej i czynników społeczno-ekonomicznych, identyfikacja „wąskich gardeł” i punktów wrażliwych, analiza złożonych scenariuszy awarii i ataków, wskazywanie najlepszych strategii obrony oraz symulacja modyfikacji sieci w celu zwiększenia jej odporności.

Narzędzie ma wspierać decydentów publicznych i operatorów sieci przy: identyfikacji elementów krytycznych, priorytetyzacji inwestycji wzmacniających odporność, planowaniu rozwoju sieci oraz optymalnym rozmieszczeniu ograniczonych zasobów ochronnych i naprawczych (ludzie, centra zarządzania, sprzęt). Symulator umożliwi m.in. analizę skutków ataków hybrydowych, wykorzystanie sieci średniego napięcia do zasilania wybranych obszarów przy degradacji sieci wysokiego napięcia oraz optymalizację działań w sytuacjach kryzysowych, np. ewakuacji czy masowych uszkodzeń infrastruktury.

Impulsem do uruchomienia projektu była agresja Rosji na Ukrainę oraz systematyczne ataki na infrastrukturę elektroenergetyczną tego kraju, które uwidoczniły podatność systemów energetycznych Europy na zagrożenia militarne i hybrydowe oraz konieczność lepszej analityki ryzyka. Projekt jest współfinansowany przez program NATO Science for Peace and Security (SPS) i wpisuje się w priorytety współpracy NATO–Ukraina w zakresie rozwiązań na rzecz bezpieczeństwa energetycznego i odporności infrastruktury krytycznej państw sojusznicznych i partnerskich.

Projekt R-GRID realizuje międzynarodowe konsorcjum obejmujące: Polskie Towarzystwo Bezpieczeństwa Narodowego, Ukrainian Institute for the Future, IDEAS NCBR oraz Laurea University of Applied Sciences z Finlandii.

O Polskim Towarzystwie Bezpieczeństwa Narodowego



Polskie
Towarzystwo
Bezpieczeństwa
Narodowego

Polskie Towarzystwo Bezpieczeństwa Narodowego jest interdyscyplinarną organizacją naukową. Celem jego działalności jest budowanie odporności państwa wobec zagrożeń dla bezpieczeństwa narodowego i międzynarodowej pozycji Rzeczypospolitej Polskiej. Przedstawiciele PTBN biorą udział w zagranicznych projektach badawczych pod egidą NATO i UE (EU-Hybnnet, EU-CIP oraz IMPRESS), inicjatywach i spotkaniach dedykowanych budowaniu odporności na współczesne zagrożenia dla bezpieczeństwa wewnętrznego państwa oraz instytucji międzynarodowych, prowadzonych przez Polską administrację rządową oraz organy Komisji Europejskiej.

Towarzystwo współpracuje m.in. z EU Protective Security Advisors realizując wspólne przedsięwzięcia podnoszące świadomość operatorów infrastruktury krytycznej w zakresie zagrożeń. PTBN jest współzałożycielem Sektorowej Rady ds. Kompetencji – Ochrona i Bezpieczeństwo Mienia i Osób.

Członkowie PTBN opracowują i wydają m.in. serię „Raport PTBN”, w której analizowane są współczesne zagrożenia dla bezpieczeństwa RP i polskiej racji stanu (terrorizm, walka informacyjna w cyberprzestrzeni, nowoczesne technologie a ochrona infrastruktury krytycznej, zagrożenia hybrydowe wobec sektora energetycznego na lądzie i na morzu). W 2024 roku PTBN we współpracy z NASK opublikowało wspólny raport *Potencjał dezinformacyjny wokół tematu budowy elektrowni jądrowej w Polsce*.

O Ukraińskim Instytucie Przyszłości



UKRAINIAN
INSTITUTE
FOR THE FUTURE

Ukraiński Instytut Przyszłości to niezależny think tank, którego działalność koncentruje się na prognozowaniu strategicznym i opracowywaniu modeli rozwoju Ukrainy. Został założony w 2016 roku przez grupę ukraińskich przedstawicieli biznesu, polityki i sektora publicznego.

Głównym celem instytutu jest kształtowanie pomyślnej przyszłości kraju poprzez gruntowne badania i dyskusje eksperckie. UIF pełni rolę platformy, na której czołowi specjaliści opracowują wizję Ukrainy na 5, 10 i 20 lat. Eksperti centrum analizują wyzwania wewnętrzne i zewnętrzne, formułując konkretne rekomendacje dla liderów rządu i biznesu.

Działania instytutu koncentrują się na kluczowych obszarach: gospodarce, energetyce, bezpieczeństwie, polityce międzynarodowej, organach ścigania i systemie wymiaru sprawiedliwości. UIF opracowuje liczne raporty strategiczne, projekty ustaw i analizy, które wpływają na decyzje rządowe. Organizacja działa z pełną niezależnością finansową i nie wspiera żadnej siły politycznej.

Instytut aktywnie uczestniczy w działalności edukacyjnej, organizując fora i panele dyskusyjne poświęcone transformacjom społecznym. UIF działa jak filtr intelektualny, który odróżnia ulotne trendy od procesów o znaczeniu strategicznym. Obecnie jest to wiodący ukraiński „think tank”, który pomaga krajowi odnaleźć się w przyszłej wspólnocie globalnej.

O IDEAS NCBR



IDEAS NCBR sp. z o.o. to ośrodek badawczo-rozwojowy działający w obszarze sztucznej inteligencji, powołany przez Narodowe Centrum Badań i Rozwoju. Naszą misją jest wsparcie rozwoju tej technologii w Polsce poprzez stworzenie platformy łączącej środowisko akademickie z biznesowym. Budujemy największą w Polsce przestrzeń przyjazną prowadzeniu innowacyjnych badań na światowym poziomie. Kształcimy nowe pokolenie naukowców, ukierunkowanych na praktyczne zastosowanie opracowanych algorytmów oraz ich późniejszą komercjalizację w przemyśle, finansach, medycynie i innych gałęziach gospodarki.

O Laurea University of Applied Sciences



Laurea University of Applied Sciences to jedna z największych i najpopularniejszych instytucji szkolnictwa wyższego w Finlandii, w której studiuje 7800 studentów. Laurea ma sześć kampusów, wszystkie zlokalizowane w regionie metropolitalnym Helsinek. W oficjalnych ocenach Laurea została uznana za wysokiej jakości placówkę edukacyjną, która osiąga najlepsze wyniki w fińskiej edukacji. Program Badań nad Bezpieczeństwem Laurei zapewnia badania wysokiego poziomu dotyczące przyszłych potrzeb w kontekście powiązań bezpieczeństwa wewnętrznego i zewnętrznego. Laurea ma duże doświadczenie w projektach dotyczących bezpieczeństwa finansowanych przez UE, a zainteresowania badawcze i wiedza specjalistyczna Laurei obejmują różne dziedziny, takie jak ochrona infrastruktury krytycznej, zagrożenia hybrydowe, bezpieczeństwo morskie i graniczne, zarządzanie kryzysowe, pierwsze reagowanie w sytuacjach kryzysowych i ochrona ludności, bezpieczeństwo cybernetyczne, zapobieganie przestępczości, jak również bezpieczeństwo Arktyki. Laurea aktywnie uczestniczy w kilku międzynarodowych i krajowych sieciach działających w obszarze bezpieczeństwa i ochrony, takich jak FISC, EOS, ECSO, ESDC, PSCEurope i UArcti.

BEZPIECZEŃSTWO PONAD PODZIAŁAMI



www.PTBN.online