Terrorism – Studies, Analyses, Prevention, 2025, special edition: 113–132

https://doi.org/10.4467/27204383TER.25.016.21519

Article

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

MICHAŁ PIEKARSKI

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

Faculty of Social Sciences,
University of Wrocław

Abstract

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

Keywords

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

Introduction

Rising international tensions, Russian hybrid actions and the threat of possible conventional conflict are affecting critical infrastructure (CI). In order to better prepare CI in the European Union for a potential attack, it is necessary to draw on the lessons learned from conflicts taking place in other regions.

Ukraine has been the target of Russian hybrid operations since 2014 and from 2022 – conventional ones. Attacks carried out as part of these operations have also targeted CI. The author of this article presents preliminary lessons learned from the Ukrainian experience to date. He points out that current news coverage of Russian aggression against Ukraine, especially on social media, are often superficial and may be factually incorrect or contain propaganda or disinformation. An in-depth analysis of this war will only be possible once it is over. For example, one of the volumes cited in the article, published in 2025, covers only the first year of the full-scale war. Therefore, the author decided to use a number of sources, including reports of think tanks, books and other publications, describing various aspects of attacks on Ukrainian CI.

Attacks on critical infrastructure in the context of the hybrid threat

According to the publication *The Landscape of Hybrid Threats*[1], any hostile activities targeting CI (assets or systems or parts of these systems) may:

(a) degrade the quality of the offered goods and services (e.g. reduce availability, reliability),
(b) destroy key parts of an infrastructure,
(c) increase their cost of operation,
(d) affect the demand, putting the infrastructure under pressure,
(e) limit or remove the possibility to diversify the supply of goods and services and cause one-sided dependence on a hostile actor,

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

(f) acquire or reduce access to key resources needed for their functionality (raw materials, technology, expertise, etc.) and more[2].

Moreover (...) *any tool that can create or exploit a vulnerability in an infrastructure (home-grown vs injected vulnerabilities) and achieving one of the above effects could potentially be used as part of the hybrid toolbox*[3]. Since those activities are described as hybrid, an attack on infrastructure may be conducted using cyber tools and affect economy, society and public administration.

It also seems interesting to look at hybrid warfare as part of a broader strategy. The report *Countering Gray-Zone Hybrid Threats*[4], published in 2016 by the United States Military Academy, describes hybrid threats as a spectrum consisting of 2 main parts: grey-zone and open-warfare.

The grey-zone is described as being below the threshold of conventional conflict, ambiguous in nature. Hybrid threats in this zone may include the use of civilians, intelligence agents, irregular forces, operating in various domains (land, air, sea, cyber, information), using instruments of power, including diplomacy, economic policy, information policy and the military.

Hybrid threats in open warfare, on the other hand, more closely resemble a conventional conflict. The aggressors do not hide their involvement, use both conventional and unconventional tools (e.g. special forces operations, irregular actions). This conceptual framework may be particularly interesting for deeper analysis of the attacks on Ukraine's CI, as the country first faced limited (grey-zone) aggression, that started in 2014 and then in 2022 – open war.

Ukrainian critical infrastructure as a target of hybrid warfare

Ukraine, along with its CI, has been the target of a wide range of Russian hybrid actions, including political warfare, assassination attempts, the use of military force, ranging from the so-called "green men" in Crimea, and Russian-inspired rebellions in eastern Ukraine. For example, the aim

[2] Ibid., p. 28.

[3] Ibid.

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

of a cyber attack on the power grid in 2015 targeted 3 electricity distribution system operators in Ivano-Frankivsk, Chernivtsi and Kyiv. This remote attack resulted in power outage affecting 225 000 customers[5]. A year later, another cyber attack targeted a single component of distribution system – a substation near Kyiv[6]. The next attack occurred in 2017, but it was much extensive, as systems not only in Ukraine were struck using the Petya ransomware[7].

Other attacks were also reported at the same time. For example, in May 2015, a railway bridge in Odessa was damaged by an explosion of an improvised explosive device, that occurred shortly before a train was due to pass the place of the attack. The explosion was apparently a part of wider wave of bombings in this port city[8].

Other infrastructure was also the target of aggression. In May 2014, an explosion damaged the Urengoy-Pomary-Uzhgorod gas pipeline near Poltava[9]. Further explosions were reported in ammunition storage sites: Vinnitsya[10] in 2017 and a year later in Ichnya[11]. Russian hybrid operations from 2014 to early 2022 were conducted to weaken the Ukraine state, to undermine citizens' trust in the government and public services. As Russia's political goal remains to take control of Ukraine and change government to a pro-Russian one, hybrid operations may have created favourable conditions for this.

---

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

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

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

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

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

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

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

Increased tensions were particularly visible in last months before the start of Russia's full-scale invasion of Ukraine. Russia, according to the Royal United Services Institute (RUSI) report, was preparing to conduct a campaign of unconventional activities supporting overt, conventional aggression and CI also would be targeted: *There is also an expectation that critical national infrastructure including telecommunications, government services, electricity and utilities will be attacked by both physical sabotage and cyber-attack. The Ukrainian security services do not expect to be able to disrupt all of these attacks*[12].

Attacks on infrastructure, although varied in scale and methods, were prelude to much wider conventional operation. The hybrid attacks were not successful. Several actions were taken in CI sector to increase its resilience. For example, in 2015 so-called Green Book on Critical Infrastructure Protection in Ukraine[13] was published and in 2022 a dedicated act of parliament about CI was adopted[14].

It is worth of noting that attacks on Ukraine, especially cyber attacks, were described also as a testing ground of cyber warfare against other countries, including EU Member States and the United States[15].

Ukrainian critical infrastructure as a target of conventional warfare

The aim of Russia's full-scale invasion of Ukraine, launched on 24 February 2022, was to take control of Ukraine by seizing Kyiv. When this goal was denied, military operation focused on other areas including Donbas[16]. Russians were able to seize significant parts of Ukraine, including southern part of country, creating land connection between Crimea and

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

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

[14] *Закон України про критичну інфраструктуру* (Відомості Верховної Ради України (ВВР), 2023, № 5, ст. 13) – [*Zakon Ukrayiny pro krytychnu infrastrukturu* (Vidomosti Verkhovnoyi Radyukrayiny (VVR), 2023, no. 5, p. 13)], https://zakon.rada.gov.ua/laws/show/1882-20#Text [accessed: 17.01.2025].

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

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

mainland Russia. There were multiple elements of CI, including 2 nuclear power plants, railways, and other that fell under Russian control, however they were seized primarily because they were located on lands that were captured by Russian forces and were not separate targets. For example, the Chernobyl Nuclear Power Plant was seized because it was located on a route of Russian troops entering Ukraine from Belarus. It was later recaptured by Ukraine when Russian forces withdrew after the failed battle for Kyiv. In similar manner destruction of Nova Kakhovka dam was a part of Russian military operation, conducted to disrupt Ukrainian offensive operations, since this destroyed 1 important bridge and made further river crossing operations below the dam impossible due to catastrophic flood[17]. A similar incident was reported in 2023[18]. Many other CI facilities were also attacked or seized during the fighting.

Later, when it was clear that Russian forces were not able to seize Kyiv, and Ukrainian armed forces were able to conduct not only successful defensive operations, but offensive ones as well, new challenge arose. In autumn of 2022 Russians started the first strategic campaign targeting Ukrainian energy sector. The attacks were not just another element of a frontline campaign. In manner like other conflicts, including World War II, they were attempts to shape a strategic situation and weaken Ukrainian social resilience. Such attacks are supposed to worsen living conditions of civil population, disrupt key sectors of economy. These attacks may force government to accept demands of aggressor, facing threat of revolt of its own exhausted society. This concept is nothing new in history of warfare, starting from Gulio Douhet's[19] air war theory through strategic attacks during World War II, to Warden's 5 rings theory. The Warden's theory as the most modern offers particular utility in explaining Russian attacks against Ukrainian CI, since it puts them in 2 of those rings: infrastructure (described mostly as transportation one) and so-called critical essentials –

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

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

[19] G. Douhet, *Panowanie w powietrzu. Przypuszczalne formy przyszłej wojny oraz ostatnie artykuły* (Eng. The command of the air. Probable aspects of the war of the future and recent articles), Warszawa 2013.

that include power supply[20]. Moreover, in the Russian military strategy, there is a concept of "Strategic Operation for the Destruction of Critically Important Targets" (SODCIT)[21]. This type of operation is aimed at destruction of facilities (systems) that may be military or non-military in nature and the goal is forcing the enemy to cease hostiles on conditions beneficial for Russia[22]. According to Michael Kofman, this operation was not conducted at the beginning of the open invasion, but the strikes against Ukrainian power grid were, in fact, SODCIT[23]. They shall be described in more detail in the next chapter of the article.

Russian air and missile strikes against Ukrainian power grid

The first strikes aimed at Ukrainian energy infrastructure, which can be interpreted as a part of SODCIT, were conducted on 10 October 2022. A total of 84 missiles and 24 drones were launched. The targets were power plants and substations in Kyiv and 11 regions, resulting in serious power outages[24]. An additional but limited strike (28 missiles supported by drones) took place the following day. Massive strikes were recorded on 31 October[25] and on 15 November[26], as well as in December. By the end 2022, the tenth

[20] J.A. Warden III, *The Enemy as System*, "Airpower Journal" 1995, vol. 9, no. 1, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-09_Issue-1-Se/1995_Vol9_No1.pdf, pp. 44–50 [accessed: 1.02.2025].

[21] M. Kofman et.al, *Russian Military Strategy: Core tenets and Operational Concepts*, August 2021, https://www.cna.org/archive/CNA_Files/pdf/russian-military-strategy-core-tenets and-operational-concepts.pdf [accessed: 3.02.2025].

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

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

[24] S. Matuszczak, *Russia is destabilising the energy system in Ukraine*, Ośrodek Studiów Wschodnich, 11.10.2022, https://www.osw.waw.pl/en/publikacje/analyses/2022-10-11/russia-destabilising-energy-system-ukraine [accessed: 5.02.2025].

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

[26] A. Wilk, P. Żochowski, *Ukraine without electricity. 256th day of war*, Ośrodek Studiów Wschodnich, 16.11.2022, https://www.osw.waw.pl/en/publikacje/analyses/2022-11-16/ukraine-without-electricity-265th-day-war [accessed: 5.02.2025].

large-scale attack had been conducted[27]. Further attacks occurred and in the early months of 2023 and another wave of strikes was reported in May. Most of them focused on transmission system (substations).

At the end of 2023, a number of smaller attacks had been reported using drones (with a limited number of various types of missiles) and only one major attack (on 29 December) targeting the power grid. The course of the air campaign changed, as it targeted not only the power grid but also the defence industry[28]. Further attacks took place in 2024. In January, 5 large-scale attacks were recorded[29]. In February, no attacks were noted[30], which may indicate a depletion of strike capabilities. At the end of March, a major attack was carried out (involving a total of 151 missiles and drones), followed by additional attacks in the following days[31].

In May, 3 large-scale attacks[32] were recorded, and in June – 4, including the largest involving a total of 100 missiles and drones[33]. On 26 August 2024 Russian forces launched an attack, described as the most powerful since the beginning of the full-scale invasion. A total of 236 drones and missiles were detected, including 109 drones, 77 Kh-101 air-launched cruise missiles and a total of 50 Kh-59, Kh-22 and ballistic missiles. Targets were elements of power grid in 15 regions of Ukraine[34].

---

[27] A. Wilk, P. Żochowski, *Tenth massive shelling of Ukraine. 309th day of the war*, Ośrodek Studiów Wschodnich, 30.12.2022, https://www.osw.waw.pl/en/publikacje/analyses/2022-12-30/tenth-massive-shelling-ukraine-309th-day-war [accessed: 5.02.2025].

[28] M. Strembski, *Wojna powietrzna nad Ukrainą – grudzień 2023 r.* (Eng. Air warfare over Ukraine – December 2023), „Lotnictwo" 2024, no. 1, p. 38.

[29] M. Strembski, *Wojna powietrzna nad Ukrainą – styczeń 2024 r.* (Eng. Air warfare over Ukraine – January 2024), „Lotnictwo" 2024, no. 2, p. 14, 16, 18–19.

[30] According to publication of OSW (Centre for Eastern Studies).

[31] S. Matuszczak, *Ukraine: a major blow to the energy sector*, Ośrodek Studiów Wschodnich, 28.03.2024, https://www.osw.waw.pl/en/publikacje/analyses/2024-03-28/ukraine-a-major-blow-to-energy-sector [accessed: 5.02.2025].

[32] M. Strembski, *Wojna powietrzna nad Ukrainą. Maj 2024 r.* (Eng. Air warfare over Ukraine. May 2024), „Lotnictwo" 2024, no. 6, p. 43, 48–49.

[33] M. Strembski, *Wojna powietrzna nad Ukrainą. Czerwiec 2024 r.* (Eng. Air warfare over Ukraine. June 2024), „Lotnictwo" 2024, no. 7–8, p. 30, 32, 34, 36.

[34] M. Strembski, *Wojna powietrzna nad Ukrainą. Sierpień 2024 r.* (Eng. Air warfare over Ukraine. August 2024), „Lotnictwo" 2024, no. 10, p. 46.

One noticeable change from previous attacks was focus on power plants, especially hydroelectric and coal-fired, to destabilise electric grid[35].

The frequency of attacks and the weapons used varied in the later period. For example, every day from May to September 2024, smaller drone attacks were conducted, but on 30 September, a total of 76 missiles and drones were used in a single attack[36].

In November 2024, significant strikes occurred, for example on 17 November approx. 210 missiles and drones were used to attack power grid, including power stations and substations, resulting in region-wide blackouts. Also, district heating systems and water supply networks were affected. On 21 November, the Dnipro area was the target of another large-scale attack. In turn, on 28 November at least 188 rockets and drones were used to attack energy infrastructure and industrial targets[37].

These were premeditated, non-accidental attacks on power grid with multi-faceted consequences. Repairing or replacing damaged power grid components requires time, access to repair parts (or entire new components like transformers), availability of skilled workforce. If there are no spare parts, the ability to generate and transmit power is limited[38]. Also, the energy system needs both generation (power plants) and transmission subsystems, and early Russian attacks (in 2022-2023) targeted transmission part – substations, denying possibility to deliver generated power[39].

Later Russian attacks were focused on power generation instead, as result of Ukrainian efforts to mitigate consequences of attacks and improve resilience. According to Maciej Zaniewicz, these were aimed at destabilising the system by preventing it from balancing and supplying energy during peak demand hours. Russia has been able to reduce Ukrainian generation capacity by 3/4 – from 40 GW before the war

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

[36] M. Strembski, *Wojna powietrzna nad Ukrainą. Wrzesień 2024 r.* (Eng. Air warfare in Ukraine. September 2024), „Lotnictwo" 2024, no. 11, p. 34.

[37] M. Strembski, *Wojna powietrzna nad Ukrainą – listopad 2024 r.* (Eng. Air warfare in Ukraine – November 2024), „Lotnictwo" 2025, no. 1, p. 33, 36, 38.

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

[39] Ibid.

to 10 GW in May 2024[40]. According to International Energy Agency approx. 70% of Ukraine's thermal generation capacity as well as half of high voltage substations were either occupied or damaged. Damages forced operator of energy system to limit supply of power[41].

The timing and frequency of activities, especially between 2022 and 2023, were adjusted to environmental and social conditions. Attacks on power grid including power plants and thermal power plants could have potentially devastating effect on society, if there would be no heating, even supplementary from electric-powered devices. Also, multiple other services, requiring electricity would be disturbed, including water system. The lack of electricity also means limited access to information and purchases (payments can only be made in cash).

Tactics and weapons employed in attack on Ukrainian power grid by Russian forces

Weapons employed may be divided into several categories, from conventional aircrafts, through guided missiles of various types, ballistic missiles and one way attack drones. Piloted aircrafts, especially Su-30, Su-34 multirole combat aircrafts and bombers like Tu-22M, Tu-95 and Tu-160[42] are employed only as carriers of cruise missiles, in stand-off attacks away from Ukrainian air defence systems. There are no noted other types of attacks, like direct bombing using unguided or guided bombs, since this mode of attack would raise risk of losses.

Most of the air-launched cruise missiles that are known to be used are Kh-59, Kh-69, Kh-22, Kh-32, Kh-101 and Kh-555 missiles supplemented by Kh-47 ballistic missiles. Subsonic Kh-59 missiles (and their upgraded variant, Kh-69) have range up to 258 km. They were designed to strike small stationary targets or naval vessels and carry 140–258 kg warhead, depending on variant[43].

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

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

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

[43] T. Kwasek, *Lotnicze pociski skrzydlate rodziny Ch-59* (Eng. Airborne winged missiles of the Kh-59 family), „Lotnictwo" 2024, no. 3, p. 42.

Kh-22 and Kh-32 missiles, carried by Tu-22M bombers, are dual role weapons. Although designed as anti-ship weapons, they are also capable of striking stationary land targets. Maximum range of these weapons is 500 km (Kh-22) or 1000 km (Kh-32) and weight of their warheads is 600 kg. These missiles after launch reach high altitude – up to 44 km and high supersonic speed, up to 3200 km/h. Both Kh-101 and Kh-555 are low flying cruise missiles, launched by bomber aircrafts. They do have long range: Kh-555 up to 3500 km[44], Kh-101 up to 2800 km[45]. Additionally, Kh-47 missiles are sometimes employed. They are air-launched variant of Iskander missile, with range up to 2000 km[46] .

The land based missiles used against Ukrainian power grid belong mostly to the Iskander system, designed to strike land-based targets. This strike complex uses 9M723 ballistic missiles, as well as 2 variants of 9M728 and 9M729 cruise missiles, which have a maximum range of 480 km[47]. In case of land-based missiles, sometimes employment of anti-ship complexes Bastion and Bal or surface to air S-300 missiles was reported, since all of those missiles are capable of striking stationary land targets. Another type of missiles that were used in attacks are shipborne 3M1 Kalibr missiles. They have a range up to 2000 km and may be launched by surface vessels and submarines[48].

In addition to those Russian produced conventional weapons, Iranian designed one-way attack unmanned aircrafts Shaheed -136 and Shaheed -131 (known also as Geran-2 and Geran-1) are widely used. These drones carry small warheads (from 15 to 50 kg), are propelled by piston engines and have range up to 2500 km[49].

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

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

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

[47] T. Kwasek, *Rakiety Putina. Rosyjskie lądowe, lotnicze i morskie systemy rakietowe oraz pociski Manewrujące* (Eng. Putin's missiles. Russian land, air and sea-based missile systems and cruise missiles), „Nowa Technika Wojskowa" 2023, special edition: *Wojna rosyjsko-ukraińska* (Eng. Russian-Ukrainian war), p. 44.

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

[49] M. Glajzer, *Irański oręż w rosyjskiej służbie* (Eng. Iranian weapon in Russian service), „Nowa Technika Wojskowa" 2022, no. 11, pp. 13–14.

This combination of various types of missiles and drones allows Russian forces to attack from multiple directions, with different speeds and altitudes. Due to this there is no one simple defensive measure, like deployment of air defence systems only on one, most probable direction. Launching multiple weapons – known as saturation attack – also makes interception more difficult. Defence systems may not be able to engage all threats, since number of air defence systems and their capabilities are limited. Moreover, employment of different weapons increases chances of successful attack – even if one group or type of missiles is shot down, others may be able to make way to targets. Using various weapons allows to distract attention of defenders, drawing fires towards diversionary strike, thus also increasing chance of success. The use of advanced weapons such as modern guided missiles to defend against attack from low-cost weapons, especially drones, puts pressure on soldiers and can also lead to the depletion of high-end weapon stocks. Replenishing these losses can be difficult and costly.

Economic issues are also a problem for Russia. Attacks requiring the use of a large number of weapons can be carried out after the necessary stockpiles have been accumulated, and the availability of means of transport, especially aircraft, is likely to be a limiting issue for Russian capabilities, therefore attacks are not conducted on regular ongoing basis, but rather in waves, which also forces Russia to strike only when an attack can do the most damage.

Regarding defence and protection measures, Ukraine has been able to prevent the worst outcome so far. Despite damage to infrastructure and blackouts caused by those damages, there are no direct, strategic impact of campaign against Ukrainian power grid. The 2022/2023 attacks did not force Ukraine to accept Russian demands, on the contrary, it was able to conduct offensive operations. It is possible that the long-term results, especially increasing public fatigue with the war, could become an important factor in public demobilisation and a decline in support for continuing the war, especially if it continuous for another year or more and further attacks cause further damage to the Ukrainian power grid. However, another component of the equation is the resilience of society, the power grid and the ability to defend infrastructure.

One factor strengthening the resilience is that Ukrainian power grid, of Soviet manufacture, designed to power heavy industry, was able to provide additional capacity that was not normally used. In addition, the ability to repair damage, especially to transmission lines and substations

(this may be one of the changes in target selection: from substations to power plants that are more difficult to repair).

There were also other measures to provide electricity, including import from European power grid. Temporary solution for population living in blackout affected areas was deployment of diesel-powered generators to designated aid stations, known as points of invincibility, that provide access to power, heat and water. There were approx. 13 000 such points created, according to media reports[50].

Defence was provided by various types of anti-aircraft systems and aircraft. The development of Ukrainian air defence was apparently rapid and often required improvisation, due to scale of the attacks and the dwindling resources of air defence systems. Ukraine in 2022 had systems inherited from Soviet Union like S-300, Buk, Osa, supplemented by artillery and portable systems (e.g. Striela)[51]. In later years, more systems were delivered from NATO countries, including Polish made portable launchers Grom and Piorun, short and medium range systems such as IRIS-T, Hawk, NASAMS, Aspide and long-range Patrion and SAMP-T[52]. To combat the threat of low flying drones, additional low-cost systems, employing truck-mounted machine guns, were developed for early Russian attacks in 2022[53]. Also, legacy systems were converted, permitting using Western missiles or allowing to use available air-to-air missiles in land launchers. A known cases of these systems – the so-called FrankenSAM – Buk missiles firing RIM-7 missiles[54], OSA launchers employing R-73 missiles[55], and others including container-

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

[51] *Russia and Eurasia*, "The Military Balance" 2022, vol. 122, issue no. 1, pp. 164–217. https://doi.org/10.1080/04597222.2022.2022930.

[52] Ibid.

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

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

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

based R-73 launchers[56]. There are also aircrafts used to shoot down missiles and drones. In addition to conventional fighter aircrafts (MiG-29, Su-27, F-16) low-cost solutions are also available. It was reported that helicopters were used to combat drones[57]. This wide range set of defence weapons resulted in lowering number of missiles and drones reaching targets.

Conclusions

The Ukrainian CI has been the target of Russian attacks since 2014, both in hybrid and conventional forms. Hybrid warfare must be treated as a prequel to possible conventional aggression and needs to be understood also in the context of CI protection – hybrid and conventional threats are part of the same continuum. This also means that it is not possible to substitute one type of warfare for another or one type of attack for another. The fact that Ukrainian power grid was targeted by cyber attacks did not excluded conventional attacks.

EU Member States face similar threat. Russia's aggressive stance means constant, clear and present danger of hybrid attacks and there is a need to include other, conventional threats. These include missile and drone strikes, that may reach deep into EU territory, especially when considering maritime platforms (surface ships and submarines), and the outcome of an attack on CI may be devastating in physical, social and political dimensions. The risk of such attacks is heightened by the fact that Russian naval forces – with the exception of those in the Black Sea area – are not affected by the war, and in the Northern Fleet (Russian: Северный флот) and the Baltic Fleet of the Russian Federation (Russian: Балтийский флот ВМФ России) there are a number of ships capable to launch cruise missiles against land targets.

Further conclusions concern resilience and defence. Infrastructure resilience is crucial, as it includes ability to provide backup sources

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

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

of power – in the case of the power grid, this includes power generation and transmission. The more power sources and transmission routes available, the better, because even if some of them are damaged, the others can take over their role. This can also be applied to other types of infrastructure, such as railways. A similar form of backups is providing excess capacity to be used in crisis situation, limiting results of damage. In addition, having an adequate number of spare parts or equipment is highly recommended. If possible, the dispersion of infrastructure would need to be taken into account, e.g. decentralisation of generation is possible for grid elements, and small installations, even domestic ones, using renewable energy can complement existing conventional power plants.

Another dimension of resilience is the ability to provide an adequate number of skilled employees to maintain, repair or rebuild infrastructure. The demand for qualified personnel will be higher than on a day-to-day basis for CI attacks, and typically CI owners or operators employ an adequate number of workers to operate under normal conditions. Therefore, it is recommended to include emergency workforce surge preparations in protection of CI. That may be achieved by including dedicated reserve of personnel in civil defence plans.

Social resilience also has a personal dimension. If citizens are able to withstand periods of limited availability of certain goods or services, crisis management is easier even if it involves drastic decision, such as temporary suspension of power supply in certain area in order to power most key places and zones or other forms or rationing. The ability to deploy more than 13 000 of aid stations in Ukraine is an example of supporting social resilience. It is therefore recommended that it is taken into account in the protection of CI.

Due to the number of conventional attacks against Ukrainian power grid and weapons employed call for considering a military dimension to CI protection. The risk of Russian conventional attacks means that some mitigation measures are beyond scope of CI operators. An integrated, multi-layered air defence system, able to prevent missile and drone attacks should be developed. This is the responsibility of the state and its armed forces. Such a system must be able to employ low-end and high-end weapons, capable of intercepting small drones, as well as cruise and ballistic missiles. This means that military planning must include issues of CI protection, such as the number and location of power plants and other elements of the power grid, as well as other systems considered critical (e.g. ports, key nodes of the railway system or other facilities).

Bibliography

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

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

Depczyński M., Elak L., *Rosyjska sztuka operacyjna w zarysie* (Eng. Russian operational art in outline), Warszawa 2020.

Douhet G., *Panowanie w powietrzu. Przypuszczalne formy przyszłej wojny oraz ostatnie artykuły* (Eng. The command of the air. Probable aspects of the war of the future and recent articles), Warszawa 2013.

Glajzer M., *Irański oręż w rosyjskiej służbie* (Eng. Iranian weapon in Russian service), „Nowa Technika Wojskowa" 2022, no. 11, pp. 12–15.

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

Kwasek T., *Lotnicze pociski skrzydlate rodziny Ch-59* (Eng. Airborne winged missiles of the Kh-59 family), „Lotnictwo" 2024, no. 3.

Kwasek T., *Rakiety Putina. Rosyjskie lądowe, lotnicze i morskie systemy rakietowe oraz pociski manewrujące* (Eng. Putin's missiles. Russian land, air and sea-based missile systems and cruise missiles), „Nowa Technika Wojskowa" 2023, special edition: *Wojna rosyjsko-ukraińska*, pp. 40–55.

Russia and Eurasia, "The Military Balance" 2022, vol. 122, issue no. 1, pp. 164–217. https://doi.org/10.1080/04597222.2022.2022930.

Strembski M., *Wojna powietrzna nad Ukrainą – grudzień 2023 r.* (Eng. Air warfare over Ukraine – December 2023), „Lotnictwo" 2024, no. 1, pp. 32–39.

Strembski M., *Wojna powietrzna nad Ukrainą – listopad 2024 r.* (Eng. Air warfare over Ukraine – November 2024), „Lotnictwo" 2025, no. 1, pp. 28–40.

Strembski M., *Wojna powietrzna nad Ukrainą – styczeń 2024 r*. (Eng. Air warfare over Ukraine – January 2024), „Lotnictwo" 2024, no. 2, pp. 14–20.

Strembski M., *Wojna powietrzna nad Ukrainą. Czerwiec 2024 r.* (Eng. Air warfare over Ukraine. June 2024), „Lotnictwo" 2024, no. 7–8, pp. 30–42.

Strembski M., *Wojna powietrzna nad Ukrainą. Maj 2024 r.* (Eng. Air warfare over Ukraine. May 2024), „Lotnictwo" 2024, no. 6, pp. 42–51.

Strembski M., *Wojna powietrzna nad Ukrainą. Sierpień 2024 r.* (Eng. Air warfare over Ukraine. August 2024), „Lotnictwo" 2024, no. 10, pp. 40–49.

Strembski M., *Wojna powietrzna nad Ukrainą. Wrzesień 2024 r.* (Eng Air warfare over Ukraine. September 2024), „Lotnictwo" 2024, no. 11, pp. 21–35.

Internet sources

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Matuszak S., *Russia is destabilising the energy system in Ukraine*, Ośrodek Studiów Wschodnich, 11.10.2022, https://www.osw.waw.pl/en/publikacje/analyses/2022-10-11/russia-destabilising-energy-system-ukraine [accessed: 5.02.2025].

Matuszak S., *Ukraine: a major blow to the energy sector,* Ośrodek Studiów Wschodnich, 28.03.2024, https://www.osw.waw.pl/en/publikacje/analyses/2024-03-28/ukraine-a-major-blow-to-energy-sector [accessed: 5.02.2025].

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

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

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

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

Perlroth N., Scott M., Frenkel S., *Cyberattack hits Ukraine then spreads internationally*, The New York Times, 27.06.2017, https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html [accessed: 16.01.2025].

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

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

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

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

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

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

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

Warden III J.A., *The Enemy as System*, "Airpower Journal" 1995, vol. 9, no. 1, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-09_Issue-1-Se/1995_Vol9_No1.pdf, pp. 41–55 [accessed: 1.02.2025].

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

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

Wilk A., Żochowski P., *Tenth massive shelling of Ukraine. 309th day of the war*, Ośrodek Studiów Wschodnich, 30.12.2022, https://www.osw.waw.pl/en/publikacje/analyses/2022-12-30/tenth-massive-shelling-ukraine-309th-day-war [accessed: 5.02.2025].

Wilk A., Żochowski P., *Ukraine without electricity. 256th day of war*, Ośrodek Studiów Wschodnich, 16.11.2022, https://www.osw.waw.pl/en/publikacje/analyses/2022-11-16/ukraine-without-electricity-265th-day-war [accessed: 5.02.2025].

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

Legal acts

Закон України про критичну інфраструктуру (Відомості Верховної Ради України (ВВР), 2023, № 5, ст. 13) – [*Zakon Ukrayiny pro krytychnu infrastrukturu* (Vidomosti Verkhovnoyi Radyukrayiny (VVR), 2023, no. 5, p. 13)], https://zakon.rada.gov.ua/laws/show/1882-20#Text [accessed: 17.01.2025].

Michał Piekarski, PhD

Assistant Professor at the Department of Security Studies of the Institute of International and Security Studies, University of Wrocław. He is involved in the analysis of the phenomenon of hybrid warfare in Europe, contemporary terrorism, issues of maritime security of the state and issues of strategic culture of Poland. Participant in the work of inter-ministerial teams and state administration working groups tasked with building resilience to terrorist and hybrid threats to strategic facilities for state security and critical infrastructure.

Contact: michal.piekarski@uwr.edu.pl