Terrorism – Studies, Analyses, Prevention, 2025, special edition: 13–34

https://doi.org/10.4467/27204383TER.25.013.21516

Article

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

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

Faculty of Management, Warsaw University of Technology
Government Centre for Security

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

Permanent Representation of the Republic of Poland to the European Union in Brussels
Government Centre for Security

Abstract

The article presents an analysis of critical infrastructure (CI) as a target for attack in hybrid operations, which combine various forms of action – from conventional to terrorist. The authors identify the reasons for attacking CI. The considerations are based on Warden's 5 rings theory. The article discusses Operation Allied Force, disinformation campaigns prior to the synchronisation of the Baltic states' energy networks, and the attack on the Colonial Pipeline. The authors conduct a comparative analysis of solutions for building CI resilience derived from the CER and NIS 2 Directives of the European Parliament and the Council of the European Union.

Keywords

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

Introduction

The current level of civilisation development is characterised by a profound dependence of societies on systems and services related to broadly understood critical infrastructure (CI). The legislation of European Union Member States may differ in details regarding the number of systems classified as CI, the criteria for recognising an entity or service as essential, or the threshold for service disruption, the importance of CI in the functioning of the state and society is unquestionable. This article discusses how CI has been and continues to be a target of hybrid attacks. Moreover, the authors present the extent to which the provisions of *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC* (hereinafter: CER Directive) and *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148* (hereinafter: NIS2 Directive), contribute to strengthening the resilience of CI against these threats. The analysis is based on Warden's 5 rings theory[1] and the concept of hybrid warfare understood as a conflict in which the adversary employs a combination of conventional, irregular, terrorist, and criminal means to achieve its political objectives. However, the most important element of hybrid warfare, according to Frank Hoffman, is to influence the adversary's society in such a way that it puts pressure on the government and forces certain actions or concessions[2].

Critical infrastructure as a target of hybrid attack

Critical infrastructure underpins the functioning of any state, and its importance makes it particularly vulnerable to destabilisation efforts. There are several reasons why CI is a priority target for hybrid attacks.

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

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

Attacks on CI can paralyse an entire state. Unlike traditional military operations, which focus on military forces and infrastructure, hybrid attacks on CI hit systems (e.g. electricity grid) on which citizens' daily lives and the functioning of the economy depend. In the case of a coordinated attack on several sectors, such as energy, transport and telecommunications, without the use of conventional military force, the effects can be comparable to warfare.

This is best illustrated by the blackout that occurred in New York on 13 July 1977. The city was plunged into darkness, causing chaos and a crime wave the likes of which had not been seen there for years. Lightning strikes on transmission lines led to the gradual overloading of the power system. At around 9.27 p.m., the first lightning strikes damaged a transmission line in Westchester County, causing an automatic load transfer to other parts of the grid. Another strike at 9.29 p.m. led to further disruption, and a third strike at 9.34 p.m. immobilised major transmission stations and had a domino effect.

Unlike the earlier 1965 blackout, which went relatively peacefully, this incident became the catalyst for mass riots, looting and violence. Overnight, 1809 acts of robbery and arson were reported, 1037 fires broke out and 2931[3] people were arrested. The Blackout exacerbated the social tensions and economic crisis that the then 12-million-strong New York City was facing. This American metropolis in the 1970s was experiencing a recession linked to deindustrialisation, rising unemployment and high crime rates. The city's budget deficit, which ran into billions of dollars, led to cuts in public administration, including a reduction in the number of police and firefighters. The police were unable to contain the riots. In many places, officers avoided confrontation and allowed to loot freely. Thieves carried away everything from department stores and electronics shops, and even took out cars. Public transport was paralysed. Residents who were away from home had to walk back through the chaos-ridden streets. Electricity began to be restored gradually on the morning of 14 July, and full power was restored throughout the city at around 10.39 a.m. The effects of the event were felt for months afterwards. Many small businesses failed to recover from the looting, further exacerbating

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

the economic crisis. There was a growing sense of insecurity and distrust of the authorities, who failed to prevent the violence from escalating. Material losses were estimated at more than USD 300 million[4], which in today's money terms, is the equivalent of approx. USD 1.5 billion.

The infrastructure required to sustain the functioning of a modern state and society is made up of interconnected components or stand-alone systems. This presents an additional difficulty in securing them, as both the components and the connections between them can range from digital technologies to physical interactions and flows to process automation. Many sectors, such as electricity grids or transport systems, rely on complex interdependencies. The failure of one component can have a knock-on effect, e.g. an attack on a rail or air traffic control system can paralyse a national transport system. In addition, the basis of many systems is technology designed before the era of the ubiquitous internet, making them vulnerable to hacking attacks.

The scale and nature of the attack do not allow the incident to be considered an armed conflict, i.e. it is below the threshold of war. Such attacks, especially those conducted in the digital sphere, are difficult to attribute. Perpetrators often use intermediary networks, botnets or false traces, making it almost impossible to pinpoint the attacker. In the case of acts of physical sabotage, such as damage to undersea cables or pipelines, perpetrators may pose as unexplained failures or the actions of terrorist groups. This leaves the attacked state with limited options to respond. The persecutor carries out destabilising actions and avoids official armed confrontation.

Hybrid operations (e.g. ransomware attack or industrial sabotage) are characterised by a relatively low cost of attack with a high cost of recovery for the attacked entity. Conducting a successful cyber attack on an electricity grid, banking or transport system requires much less money than classic military operations. An example is the attack on the Colonial Pipeline in 2021, which is discussed in more detail later in this article.

One reason for the high effectiveness of hybrid attacks is their multi-vector nature, i.e. the ability to combine different forms of attack. An example scenario for an attack on CI could include simultaneously:

[4] Ibid., p. 11.

- cyber attack on transmission networks that triggers power outages;
- sabotage, such as planting an explosive charge on an important infrastructure node;
- disinformation campaign suggesting that the failure is the result of corruption or government incompetence;
- financial speculation that hits the value of the national currency and destabilises the economy.

Such activities, if well coordinated, can cause chaos on a scale comparable to an armed conflict. Attacks on CI often aim not only to physically damage infrastructure, but also to have a psychological effect. In societies that lose access to basic services, discontent grows, conspiracy theories emerge and trust in government and public institutions declines. In a crisis situation, riots, mass protests and consequent political destabilisation can occur.

Regardless of this destabilisation, an attack on CI can be an element of economic warfare and a tool of political blackmail. Modern rivalry between states is increasingly shifting to the infrastructural level. Blocking major transport routes, destroying pipelines or disrupting banking systems are all actions that can force political concessions. An example is the sabotage of the Nord Stream pipelines in 2022, which had both an economic and political dimension, while affecting Europe's energy security.

An additional problem with CI protection is that it often involves both public and private elements. In many countries, power grids are managed by private companies with primarily business objectives, and providing public access to the service is not a priority for them.

Cyber attacks are one of the main vectors of hybrid attacks on CI. Tools such as ransomware, malware or DDoS attacks can be used to destabilise electricity grids, financial systems or logistics chains. Cyberspace makes it possible to launch an attack from anywhere in the world, making it difficult to identify the perpetrators. This was the case with the cyber attack on the Ukrainian electricity grid in 2015. At the time, hackers used Black Energy malware to take control of control systems and shut down power substations, resulting in massive power outages. The attack was suspected to have been carried out by Russian hacking groups, but no evidence of this was found[5].

[5] K. Gapiński, *Blackout w zachodniej Ukrainie – cyberatak o wymiarze międzynarodowym* (Eng. Blackout in western Ukraine – cyberattack with an international dimension), Fundacja im. Kazimierza Pułaskiego, 20.01.2016, https://pulaski.pl/komentarz-blackout-w-zachodniej-ukrainie-cyber-atak-o-wymiarze-miedzynarodowym/ [accessed: 23.03.2025].

Attacks such as sabotage of gas pipelines, undersea telecommunications cables or vital transport infrastructure nodes can be presented as an accident or technical failure. This was the case with the mentioned damage to the Nord Stream pipelines. Many countries considered the incident to be deliberate sabotage, but there was a lack of clear evidence to identify the principal[6]. The same was true in 2019 in Saudi Arabia, where drone attack on Aramco's oil installations was carried out. This led to a temporary halt in oil production, which affected global crude prices[7]. Although the attack was claimed by the Yemeni Houthi rebel group, many studies have suggested that the operation may have been supported by Iran[8].

Attacks on CI are often combined with disinformation activities. After a cyber-attack on banking systems or energy infrastructure, manipulated information may appear online that the authorities are not handling the situation or that the failure was the result of internal problems, such as corruption or government weakness. Such campaigns aim to undermine public confidence in state institutions and create panic.

A cyber attack on CI is difficult to classify unequivocally as an act of war, which, from the perpetrator's perspective, is the biggest advantage. While a direct military attack on CI could meet with a military response, an attack carried out over the internet or sabotage could be considered as an action of an unclear nature. If the perpetrator cannot be clearly identified, it is difficult to retaliate or involve allies. Even if there are

---

[6] See i.e. S. Kardaś, A. Łoskot-Strachota, *Sabotage of the Nord Stream 1 and Nord Stream 2 pipelines*, Ośrodek Studiów Wschodnich, 29.09.2022, https://www.osw.waw.pl/en/publikacje/analyses/2022-09-29/sabotage-nord-stream-1-and-nord-stream-2-pipelines [accessed: 23.03.2025].

[7] A. Polus, *Atak na rafinerię w Arabii Saudyjskiej i jego konsekwencje dla Afryki* (Eng. Attack on a refinery in Saudi Arabia and its consequences for Africa), Polskie Centrum Studiów Afrykanistycznych, 18.09.2019, https://pcsa.org.pl/atak-na-rafinerie-w-arabii-saudyjskiej-i-konsekwencje-dla-afryki/ [accessed: 23.03.2025].

[8] See i.e. G. Psujek, *Tajemnica ataku na saudyjską rafinerię* (Eng. The mystery of the attack on the Saudi refinery), Rzeczpospolita, 22.09.2019, https://radar.rp.pl/przemysl-obronny/art17499861-tajemnica-ataku-na-saudyjska-rafinerie [accessed: 23.03.2025]; R. Muczyński, *Atak na saudyjskie rafinerie* (Eng. Attack on Saudi refineries), Milmag, 16.09.2019, https://milmag.pl/atak-na-saudyjskie-rafinerie/ [accessed: 23.03.2025]; *CNN: Według ekspertów atak na Aramco nastąpił z Iranu* (Eng. CNN: According to experts, the attack on Aramco originated from Iran), Interia Wydarzenia, 18.09.2019, https://wydarzenia.interia.pl/zagranica/news-cnn-wedlug-ekspertow-atak-na-aramco-nastapil-z-iranu,nId,3209902 [accessed: 23.03.2025].

suspicions about the responsibility of a particular country, doubts about the evidence may make the options for a diplomatic or military response limited. Attacks on CI are effective not only because they cause massive damage, but also because perpetrators can act anonymously and with impunity.

Theoretical frame of reference

The basis of Warden's 5 rings theory can be traced back to Carl von Clausewitz's work *On War*[9]. Clausewitz notes that in order to successfully defeat an enemy, a state should direct all its efforts against so-called centres of gravity on which the enemy's existence depends. John Ashley Warden III[10] developed this principle into a concept focused on target selection in war. Warden's 5 ring theory is used to identify and prioritise war aims. It assumes that a state can be depicted as a system consisting of 5 concentric rings (circles), each representing a different level of strategic importance. These are shown in Figure 1:

1) leadership (state and military authorities),
2) essential system resources necessary for the functioning of the state and the conduct of war,
3) infrastructure that connects all elements of the system,
4) population (civilians),
5) field forces (troops and military equipment).

[9] C. von Clausewitz, *O wojnie* (Eng. On war), Warszawa 2022.

[10] John Ashley Warden III – born in America in 1943, the United States Air Force military strategist. During the Gulf War (1990-1991), he developed the 5 rings theory, in which he identified the centres of gravity (the most vulnerable elements of a state's structure) and at the same time identified aviation as the only formation that could attack the interior of each ring without penetrating the others.

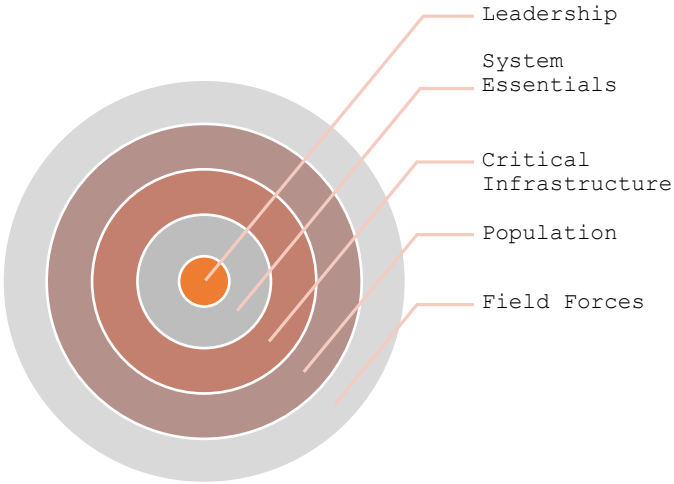

Figure 1. Warden's 5 Ring System Theory.

Source: own elaboration based on: G.M. Jackson, *Warden's five-ring system theory: legitimate wartime military targeting or an increased potential to violate the law and norms of expected behavior?*, Alabama 2000, https://apps.dtic.mil/sti/pdfs/ADA425331.pdf, p. 4 [accessed: 20.02.2025].

Attacking the inner circles (leadership, essential system resources) induces rapid paralysis and an end to the conflict. Attacking the outer circles (population, armed forces) is less effective and may prolong the war.

If the leadership cannot be successfully attacked, Warden identifies the next target, which is the system resources (functions, services) needed by the adversary, including: electricity supply, oil, food and finance. Their destruction can deprive a state of its ability to conduct warfare, but at the same time can threaten the survival of the civilian population. According to Warden, CI are elements such as roads, airports, factories and others that enable the state to function as a whole.

Warden's theory was used to prioritise the aviation used in modern warfare. However, its conclusions have a wider significance. Successive levels (rings) indicate the importance of a particular element to the functioning of a state. It is noteworthy that, according to this theory, 21st century warfare is about military forces being attacked last or not at all. Political objectives are to be achieved by the elimination of the leadership, the blockade of the most important functions of the state and the destruction of the infrastructure that serves these functions. This corresponds remarkably well with considerations of hybrid warfare.

Use of critical infrastructure in hybrid conflicts

Achievement of political objectives without military force

A particular case of achieving political objectives by affecting CI was Operation Allied Force, the bombing campaign conducted by North Atlantic Alliance troops against Yugoslavia (Serbia and Montenegro) during the Kosovo war in 1999. In this way, the intention was to force the regime of Slobodan Milošević to end the ethnic cleansing in Kosovo.

The bombing initially focused on military facilities, but later extended to important infrastructure for the functioning of the state, such as bridges (e.g. on the Danube at Novi Sad, the destruction of which was expected to paralyse transport), roads and railways (including an attack on a passenger train on the Grdelica bridge), aviation infrastructure (Podgorica airport), television and radio stations (e.g. attack on the headquarters of Serbian TV station RTS in Belgrade, which killed 16 civilians), industrial facilities (refineries, factories) and energy facilities (e.g. power plants, the bombing of which led to massive power cuts). Serbia suffered huge economic losses, the cost of reconstruction after the air raids was estimated to be approx. USD 30–100 billion[11]. The deconstruction of civilian facilities was met with international criticism as it caused great hardship to the population. The Allied Force Operation also caused legal controversy, as under international law (including Protocol I to the Geneva Conventions of 12 August 1949 concerning the protection of victims of international armed conflicts[12]) attacking facilities essential for the survival of the civilian population is prohibited. However, the NATO command argued that this infrastructure was also of military importance, e.g. the bridges were used for military transport. Allied Force was NATO's first ever intervention without a United Nations mandate, a fact that remains the subject of legal

[11] N. Stawarz, *„Nielegalne, ale moralne"? Operacja „Allied Force": przyczyny i konsekwencje* (Eng. "Illegal but moral?" Operation "Allied Force": causes and consequences), Histmag.org, 24.03.2019, https://histmag.org/Nielegalne-ale-moralne-Operacja-Allied-Force-przyczyny-i-konsekwencje-18428? [accessed: 23.03.2025]; R. Górski, *Specjalna operacja wojskowa NATO: bombardowanie Jugosławii* (Eng. NATO special military operation: bombing of Yugoslavia), Instytut Spraw Obywatelskich, 24.03.2023, https://instytutsprawobywatelskich.pl/specjalna-operacja-wojskowa-nato-bombardowanie-jugoslawii/ [accessed: 23.03.2025].

[12] *Protocols additional to the Geneva Conventions of 12 August 1949, relating to the protection of victims of international armed conflicts (Protocol I) and relating to the protection of victims of non-international armed conflicts (Protocol II), drawn up in Geneva on 8 June 1977*.

and political debates to this day. Notwithstanding these controversies, the political objectives were achieved without the introduction of troops into the territory of an enemy state.

Impact on society

Hoffman's definition of hybrid war, quoted at the beginning of this article, emphasises the impact on society as the most important element of an adversary's strategy. A similar approach can be found in Valery Gerasimov's concept of non-linear warfare[13], where the main tools are information manipulation, disinformation and psychological action to bring about social destabilisation and change government political decisions under pressure from its own citizens.

Spread of disinformation, propaganda and mmanipulating the information lead to the erosion of public trust, undermining the authority of state as well as international institutions and, consequently, the foundations of democracy, and weakening the state's position in the international arena. To provoke social unrest, protests and internal divisions, attackers use a variety of means, such as social media, fake news or cyber attacks. High electricity prices, fear of 5G technology or nuclear power plant are the examples of issues around which a disinformation narrative is being built. CI plays a special role in these activities.

Prior to the synchronisation of the Baltic States' power grids with the European electricity system, which took place in February 2025, there was an increase in disinformation campaigns in Lithuania, Latvia and Estonia. These activities were particularly intense in the run-up to the disconnection from the Russian BRELL system and connection to the European grid. The main disinformation plots focused on several issues. Firstly, the threats of power cuts. Information was circulated suggesting that synchronisation with the European system would lead to long-term blackouts. In Estonia, such reports led to an increase in the sale of power generators, as residents feared up to three days of blackouts[14].

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

[14] *Rosyjski atak dezinformacją ws. energetyki. Estończycy wykupują generatory, służby w stanie gotowości* (Eng. Russian disinformation attack on the energy sector. Estonians buy up generators, authorities on high alert), Polskie Radio 24, 6.02.2025, https://polskieradio24.

Secondly, an increase in energy prices. There were rumours that connection to the European grid would result in a significant increase in electricity prices for consumers, thus increasing the price of basic products and ultimately making society poorer. Lithuanian Energy Minister Žygimantas Vaičiūnas warned against such misinformation and assured of the stability of the system and the absence of grounds for concern about price increases[15]. Thirdly, the inefficiency of the new system. Theories were promoted about the alleged unreliability of the European electricity system and it was suggested that the Baltic States might experience technical problems after being disconnected from the Russian grid[16]. This disinformation campaign, especially from the Russian media, intensified after the synchronisation of the grid. Research carried out by the Lithuanian company Mediaskopas showed that after the Baltic States disconnected from the post-Soviet system and joined the European CESA transmission system, the number of articles on the subject in the Russian media increased from 3065 to more than 8000. They presented apocalyptic scenarios, suggesting that the Baltic States were facing an energy crisis because of their abandonment of cooperation with Russia[17]. The authorities and energy experts in these countries regularly deny this information. They assure the stability and security of the new system. To undermine these assurances, one of the undersea electricity cables was cut. The cable in question is the EstLink 2 cable connecting Finland and Estonia, with a capacity of 650 MW and a length of 170 km, including 145 km under the bed of the Gulf of Finland.

pl/artykul/3480519,rosyjski-atak-dezinformacja-ws-energetyki-estonczycy-wykupuja-generatory-sluzby-w-stanie-gotowosci [accessed: 20.02.2025].

[15] *Minister ostrzega mieszkańców przed możliwą dezinformacją* (Eng. Minister warns residents about possible disinformation), Made in Vilnius, 04.02.2025, https://madeinvilnius.lt/pl/Aktualno%C5%9Bci/Lietuvos-naujienos/Minister-ostrzega-mieszka%C5%84c%C3%B3w-przed-mo%C5%BCliw%C4%85-dezinformacj%C4%85/ [accessed: 20.02.2025].

[16] *Przed synchronizacją z Europą służby ostrzegają przed dezinformacją* (Eng. Before the synchronisation with Europe, authorities warn of disinformation), TVP Wilno, 3.02.2025, https://wilno.tvp.pl/84820950/przed-synchronizacja-z-europa-sluzby-ostrzegaja-przed-dezinformacja [accessed: 20.02.2025].

[17] *Po synchronizacji sieci energetycznych krajów bałtyckich z Europą zaktywizowała się propaganda Kremla* (Eng. After the synchronisation of the Baltic states' power grids with Europe, Kremlin propaganda became more active), Polska Agencja Prasowa, 20.02.2025, https://www.pap.pl/aktualnosci/po-synchronizacji-sieci-energetycznych-krajow-baltyckich-z-europa-zaktywizowala-sie [accessed: 20.02.2025].

On 25 December 2024, this link, which is an important part of the energy infrastructure between the Baltic countries, was disrupted around midday. The grid operator, Fingrid, reported the disruption to power transmission and launched an investigation to determine the cause of the outage. Finnish authorities have detained the suspected tanker Eagle S. The vessel, flying the flag of the Cook Islands, was carrying unleaded petrol from Russian ports. It was alleged to have belonged to Russia's so-called shadow fleet. Initial findings suggested that the cable cut may have been caused by the ship's anchor[18]. The complicated and costly repair of EstLink 2 is likely to take until 1 August 2025 and cost tens of millions of euros. Despite the outage, electricity supply to Finnish consumers remained uninterrupted. However, the absence of this connection limited Finland's energy exports and, as a result, the average energy price in Estonia almost doubled from January to February 2025 to 184 EUR/MWh. By comparison, in February of the previous year this price was 75.5 EUR[19]. After the cable damage, the average wholesale electricity price in Lithuania increased by 41% during the week from 56 EUR/MWh to 79 EUR /MWh[20]. The EstLink 2 damage incident caused concern among Baltic residents about the stability of energy supply and potential further price increases. The attacker's objectives were achieved.

It is worth noting that similar disinformation campaigns were observed in other EU countries. They attempted to hold the EU responsible for energy price increases.

[18] *Awaria kabla EstLink 2. Rosyjski tankowiec podejrzany o akt sabotażu* (Eng. EstLink 2 cable failure. Russian tanker suspected of sabotage act), PolskieRadio.pl, 26.12.2024, https://www.polskieradio.pl/399/7977/artykul/3463666%2Cawaria-ka%20bla-estlink-2-rosyjski-tankowiec-podejrzany-o-akt-sabotazu? [accessed: 20.02.2025].

[19] *Jak uszkodzenie Estlink 2 wpływa na ceny energii w Estonii* (Eng. How the damage to Estlink 2 affects energy prices in Estonia), Czas Wschodni, 14.02.2025, https://czaswschodni.pl/art/wiadomosci/jak-uszkodzenie-estlink-2-wplywa-na-ceny-energii-w-estonii_116f1090-c456-4bb7-abc1-c340f6da6cf5 [accessed: 20.02.2025].

[20] *Uszkodzenie kabla EstLink 2 podniosło ceny energii w krajach bałtyckich* (Eng. Damage to the EstLink 2 cable raised energy prices in the Baltic states), BalticWind.EU, 3.01.2025, https://balticwind.eu/pl/uszkodzenie-kabla-estlink-2-podnioslo-ceny-energii-w-krajach-baltyckich/ [accessed: 20.02.2025].

Influencing the government

On 7 May 2021, one of the most serious cyber attacks on CI in the United States occurred. The target was Colonial Pipeline[21], the largest pipeline system on the US East Coast, which transports approx. 45% of the region's fuel supply. The hackers used ransomware, encrypted company data and demanded a ransom. As a result of the attack, the pipeline stopped operations, leading to a major disruption in fuel supply. The authorities responded immediately. The administration of US President Joe Biden declared a state of emergency to allow fuel to be transported by alternative means. The owner of Colonial Pipeline, who wanted to get the system functioning again as soon as possible, paid a ransom of USD 4.4 million in bitcoins to the hackers[22]. However, it took several days to restore full operation of the pipeline. During this time, the US East Coast began to run out of fuel. This caused panic among consumers, who bought up gasoline en masse and thus the crisis worsened. In some states, such as North Carolina, more than 70% of gas stations reported supply problems. The hacking group DarkSide, operating from Russia, was responsible for the attack. The attack on the Colonial Pipeline revealed the vulnerability of US CI to cyber attacks, prompting the Biden administration to tighten cyber security regulations for the energy sector[23]. New requirements have been introduced for CI operators, requiring them to take additional measures to protect themselves from ransomware attacks. The incident exacerbated tensions between Washington and Moscow. President Biden pointed out that the Kremlin bears responsibility for enforcing control over cybercrime groups operating within Russia's borders, and DarkSide operated from Russian territory. It is worth noting that in spring 2021 the US and Germany were in intensive talks to complete the Nord Stream 2 pipeline,

[21] M. Perzyński, *Raport: O Colonial Pipline i zimnej wojnie w energetyce* (Eng. Report: On Colonial Pipeline and the Cold War in energy), Biznesalert, 15.05.2021, https://biznesalert.pl/raport-colonial-pipeline-cyberatak-usa-rosja-energetyka/ [accessed: 23.03.2025].

[22] *Prezes Colonial Pipeline potwierdza: zapłaciliśmy okup hakerom* (Eng. Colonial Pipeline CEO confirms: we paid the ransom to hackers), Cyberdefence24, 20.05.2021, https://cyberdefence24.pl/biznes-i-finanse/prezes-colonial-pipeline-potwierdza-zaplacilismy-okup-hakerom [accessed: 23.03.2025]; W. Urbanek, *Colonial Pipeline: niepożądana sława* (Eng. Colonial Pipeline: unwanted fame), CRN, 24.06.2021, https://crn.pl/artykuly/colonial-pipeline-niepozadana-slawa/ [accessed: 23.03.2025].

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

which would deliver Russian gas directly to Germany, bypassing Ukraine and Poland. The Biden administration expressed concerns that the project would increase Europe's dependence on Russian gas and undermine the region's energy security. Despite its opposition to Nord Stream 2, the US government did not impose direct sanctions on Nord Stream 2 AG, i.e. the main company responsible for the construction of the gas pipeline and its CEO Matthias Warnig[24]. Instead, the US has focused on working out an agreement with Germany that addresses the energy security concerns of Central and Eastern Europe. In July 2021 the US and Germany concluded negotiations. Berlin pledged to take action if Russia tried to use energy as a weapon against Ukraine or other countries in the region, and to use all available leverage to extend the Russia-Ukraine transit agreement, which expired in 2024, by 10 years. In addition, Germany has agreed to set up a fund of at least USD 175 million to support the energy transition and improve Ukraine's energy security[25]. No direct links between the hacking group and Russian services have been found. However, one can venture the thesis that the cyber attack on an important link in the US energy system was intended to make the Joe Biden administration realise that actions to the detriment of the Russian Federation could meet with a strong, though not direct, response.

Perceptions of hybrid action over a time horizon

The time horizon is an important issue to take into account when considering the use of CI in hybrid warfare. Its first dimension is the surprise effect, i.e. finding such a vulnerability or coming up with an attack scenario that has not been considered before. This is an attack that will not result in an immediate response, because there is no adequate legal framework, both in terms of the response procedure, the designated

[24] W. Jakóbik, *USA mogą na dniach zadać nowy cios Nord Stream 2, ale unikają deklaracji* (Eng. The US may strike Nord Stream 2 in the coming days but avoids making declarations), Biznes Alert, 14.05.2021, https://biznesalert.pl/nord-stream-2-sankcje-usa-poszerzone-energetyka-gaz/ [accessed: 20.02.2025].

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

authority responsible for CI security and the criminal sanction. The second dimension relates to the fact that the limited ability to carry out risk analysis for hybrid attack vulnerabilities makes it much more difficult to ensure CI protection. It is difficult to predict whether a site will be a potential target of a hybrid attack. Its typical parameters (type of production, interdependencies, potential losses, population affected, etc.) and scenarios may have different meanings for the user and for the adversary. For example, local water and sewage facilities, which are of little importance from the point of view of the state, are of great interest to hacking groups[26]. An attack on this type of site, even if it is severe for the local community, will not cause a national crisis unless the aggressor decides to attack more poorly secured installations simultaneously. Economies of scale can then result in a media response similar to that following an attack on one large installation. The third dimension of the time horizon is the acquisition of information that may have military or disinformation significance in the long term. Hybrid operations are often planned for years. An object that is not strategically important today may have an important function, e.g. as part of some system in the future.

Building the resilience of critical infrastructure using the example of the CER and NIS 2 Directives

The CER Directive aims to achieve a level of resilience of CI to prevent the effects of disruption to the essential services it provides. The Directive requires Member States to establish a list of these services and to identify the critical entities responsible for providing them. Each of these entities must meet resilience requirements in order to counter the effects of disruption (Article 6(1) and (2) of the CER Directive). National resilience strategies for critical entities must include the identification of threats, the assessment of risks and the development of countermeasures, including protection against hybrid threats (Article 5(1)). Furthermore,

[26] See i.e.: *Doniesienia o rosyjskim cyberataku. Pojawił się polski wątek* (Eng. Reports of a Russian cyberattack. A Polish connection emerges), Wirtualna Polska, 17.04.2024, https://wiadomosci.wp.pl/rosyjski-cyberatak-na-polska-infrastrukture-ofiara-oczyszczalnia-sciekow-7017937180834752a [accessed: 20.02.2025]; *Atak hakerski na oczyszczalnię ścieków* (Eng. Cyberattack on a wastewater treatment plant), iSokolka.eu, 8.10.2024, https://isokolka.eu/kuznica/59444-atak-hakerski-na-oczyszczalnie-sciekow [accessed: 20.02.2025].

the CER Directive identifies the challenges that arise from increasingly complex supply chains between entities. They therefore need to assess the risks associated with supply chain dependencies and apply appropriate measures to ensure business continuity. Therefore, the CER Directive identifies the need to determine alternative suppliers and contingency plans (Article 12(2)). Actors are required to maintain operational capacity in crisis situations, taking into account the interdependencies between different actors and the critical sector (Article 11(2)). The Directive requires risk analysis and contingency plans (Article 12(1)), but lacks guidance for anticipating adversarial actions and effective risk management in complex organisational structures. The Directive mandates continuous monitoring and threat assessment, but does not provide for specific mechanisms that can take into account non-obvious targets of hybrid attacks. It is impossible, as has been proven, to predict what will be important to an adversary. Thus, entities that have not been identified as critical may, for some currently unknown reason, be attacked, which will be easier due to their lower level of protection than those providing critical services. It should be recalled that operators and institutions managing a key service are not self-sufficient, i.e. they use subcontractors (often less secure), implement common processes, use common infrastructure (e.g. server rooms), depend on a global supply chain, etc. Attempting to manage risk in such a complex organisational structure results in an exponential increase in costs.

Another approach was applied in the NIS 2 Directive, under which all entities within its scope are required to implement appropriate cybersecurity risk management measures. The application of these measures is not conditioned by whether a potential failure could result in consequences that are unacceptable from the perspective of public safety, nor by whether such consequences are beyond our ability to predict or prove in administrative proceedings. This approach is driven by the pervasiveness of the threat and the fact that cyber links are not traceable, as well as the need to maintain equality of actors in the common market. Such regulation makes the cost of protection comparable for each organisation and none is particularly burdened or favoured. The introduction of a unified approach to the cyber-security of critical entities is intended to address protection gaps resulting from the complexity of the links between entities (Article 20(1)).

Based on the analysis of hybrid attack cases, it is questionable whether the methodology adopted in the CER Directive is complete, i.e. whether it covers all elements of the system, including those that may become (non-obvious) targets of hybrid attacks. The NIS 2 Directive provides a more comprehensive approach to risk management that covers all actors and guarantees greater resilience of the entire digital system. The different strategies used in both directives for identifying entities of significant importance to national security and the safety of its citizens could lead to a number of inconsistencies in the imposition of obligations on these entities. It is already possible to predict that in a few years, there will be calls to harmonise these two directives.

Bibliography

Clausewitz C. von, *O wojnie* (Eng. On war), Warszawa 2022.

Internet sources

Atak hakerski na oczyszczalnię ścieków (Eng. Cyberattack on a wastewater treatment plant), iSokolka.eu, 8.10.2024, https://isokolka.eu/kuznica/59444-atak-hakerski-na--oczyszczalnie-sciekow [accessed: 20.02.2025].

Awaria kabla EstLink 2. Rosyjski tankowiec podejrzany o akt sabotażu (Eng. East--Link 2 cable failure. Russian tanker suspected of sabotage act), PolskieRadio.pl, 26.12.2024, https://www.polskieradio.pl/399/7977/artykul/3463666%2Cawaria--ka%20bla-estlink-2-rosyjski-tankowiec-podejrzany-o-akt-sabotazu? [accessed: 20.02.2025].

CNN: Według ekspertów atak na Aramco nastąpił z Iranu (Eng. CNN: According to experts, the attack on Aramco originated from Iran), Interia Wydarzenia, 18.09.2019, https://wydarzenia.interia.pl/zagranica/news-cnn-wedlug-ekspertow--atak-na-aramco-nastapil-z-iranu,nId,3209902 [accessed: 23.03.2025].

Doniesienia o rosyjskim cyberataku. Pojawił się polski wątek (Eng. Reports of a Russian cyberattack. A Polish connection emerges), Wirtualna Polska, 17.04.2024, https:// wiadomosci.wp.pl/rosyjski-cyberatak-na-polska-infrastrukture-ofiara-oczyszczal-nia-sciekow-7017937180834752a [accessed: 20.02.2025].

Gapiński K., *Blackout w zachodniej Ukrainie – cyberatak o wymiarze międzynarodowym* (Eng. Blackout in western Ukraine – cyberattack with an international dimension), Fundacja im. Kazimierza Pułaskiego, 20.01.2016, https://pulaski.pl/komentarz-blackout-w-zachodniej-ukrainie-cyber-atak-o-wymiarze-miedzynarodowym/ [accessed: 23.03.2025].

Górski R., *Specjalna operacja wojskowa NATO: bombardowanie Jugosławii* (Eng. NATO special military operation: bombing of Yugoslavia), Instytut Spraw Obywatelskich, 24.03.2023,https://instytutsprawobywatelskich.pl/specjalna-operacja-wojskowa-nato-bombardowanie-jugoslawii/ [accessed: 23.03.2025].

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

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

Jackson G.M., *Warden's five-ring system theory: legitimate wartime military targeting or an increased potential to violate the law and norms of expected behavior?*, Alabama 2000, https://www.ferc.gov/sites/default/files/2020-05/impact-77.pdf [accessed: 20.02.2025].

Jak uszkodzenie Estlink 2 wpływa na ceny energii w Estonii (Eng. How the damage to Estlink 2 affects energy prices in Estonia), Czas Wschodni, 14.02.2025, https://czaswschodni.pl/art/wiadomosci/jak-uszkodzenie-estlink-2-wplywa-na-ceny-energii-w-estonii_116f1090-c456-4bb7-abc1-c340f6da6cf5 [accessed: 20.02.2025].

Jakóbik W., *USA mogą na dniach zadać nowy cios Nord Stream 2, ale unikają deklaracji* (Eng. The US may strike Nord Stream 2 in the coming days but avoids making declarations), Biznes Alert, 14.05.2021, https://biznesalert.pl/nord-stream-2-sankcje-usa-poszerzone-energetyka-gaz/ [accessed: 20.02.2025].

Kardaś S., Łoskot-Strachota A., *Sabotage of the Nord Stream 1 and Nord Stream 2 pipelines*, Ośrodek Studiów Wschodnich, 29.09.2022, https://www.osw.waw.pl/en/publikacje/analyses/2022-09-29/sabotage-nord-stream-1-and-nord-stream-2-pipelines [accessed: 23.03.2025].

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

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

Minister ostrzega mieszkańców przed możliwą dezinformacją (Eng. Minister warns residents about possible disinformation), Made in Vilnius, 4.02.2025, https://made-invilnius.lt/pl/Aktualno%C5%9Bci/Lietuvos-naujienos/Minister-ostrzega-mieszka%C5%84c%C3%B3w-przed-mo%C5%BCliw%C4%85-dezinformacj%C4%85/ [accessed: 20.02.2025].

Muczyński R., *Atak na saudyjskie rafinerie* (Eng. Attack on Saudi refineries), Milmag, 16.09.2019, https://milmag.pl/atak-na-saudyjskie-rafinerie/ [accessed: 23.03.2025].

Perzyński M., *Raport: O Colonial Pipline i zimnej wojnie w energetyce* (Eng. Report: On Colonial Pipeline and the Cold War in energy), Biznesalert, 15.05.2021, https://biznesalert.pl/raport-colonial-pipeline-cyberatak-usa-rosja-energetyka/ [accessed: 23.03.2025].

Polus A., *Atak na rafinerię w Arabii Saudyjskiej i jego konsekwencje dla Afryki* (Eng. Attack on a refinery in Saudi Arabia and its consequences for Africa), Polskie Centrum Studiów Afrykanistycznych, 18.09.2019, https://pcsa.org.pl/atak-na-rafinerie-w-arabii-saudyjskiej-i-konsekwencje-dla-afryki/ [accessed: 23.03.2025].

Po synchronizacji sieci energetycznych krajów bałtyckich z Europą zaktywizowała się propaganda Kremla (Eng. After the synchronisation of the Baltic states' power grids with Europe, Kremlin propaganda became more active), Polska Agencja Prasowa, 20.02.2025, https://www.pap.pl/aktualnosci/po-synchronizacji-sieci-energetycznych-krajow-baltyckich-z-europa-zaktywizowala-sie [accessed: 20.02.2025].

Prezes Colonial Pipeline potwierdza: zapłaciliśmy okup hakerom (Eng. Colonial Pipeline CEO confirms: we paid the ransom to hackers), Cyberdefence24, 20.05.2021, https://cyberdefence24.pl/biznes-i-finanse/prezes-colonial-pipeline-potwierdza-zaplacilismy-okup-hakerom [accessed: 23.03.2025].

Przed synchronizacją z Europą służby ostrzegają przed dezinformacją (Eng. Before the synchronisation with Europe, authorities warn of disinformation), TVP Wilno, 3.02.2025, https://wilno.tvp.pl/84820950/przed-synchronizacja-z-europa-sluzby-ostrzegaja-przed-dezinformacja [accessed: 20.02.2025].

Psujek G., *Tajemnica ataku na saudyjską rafinerię* (Eng. The mystery of the attack on the Saudi refinery), Rzeczpospolita, 22.09.2019, https://radar.rp.pl/przemysl-obronny/art17499861-tajemnica-ataku-na-saudyjska-rafinerie [accessed: 23.03.2025].

Rosyjski atak dezinformacją ws. energetyki. Estończycy wykupują generatory, służby w stanie gotowości (Eng. Russian disinformation attack on the energy sector. Estonians buy up generators, authorities on high alert), Polskie Radio 24, 6.02.2025, https://polskieradio24.pl/artykul/3480519,rosyjski-atak-dezinformacja-ws-energetyki-estonczycy-wykupuja-generatory-sluzby-w-stanie-gotowosci [accessed: 20.02.2025].

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

Stawarz N., *„Nielegalne, ale moralne"? Operacja „Allied Force": przyczyny i konsekwencje* (Eng. "Illegal but moral?" Operation "Allied Force": causes and consequences), Histmag.org, 24.03.2019, https://histmag.org/Nielegalne-ale-moralne-Operacja-Allied-Force-przyczyny-i-konsekwencje-18428? [accessed: 23.03.2025].

Urbanek W., *Colonial Pipeline: niepożądana sława* (Eng. Colonial Pipeline: unwanted fame), CRN, 24.06.2021, https://crn.pl/artykuly/colonial-pipeline-niepozadana-slawa/ [accessed: 23.03.2025].

Uszkodzenie kabla EstLink 2 podniosło ceny energii w krajach bałtyckich (Eng. Damage to the EstLink 2 cable raised energy prices in the Baltic states), BalticWind.EU, 3.01.2025, https://balticwind.eu/pl/uszkodzenie-kabla-estlink-2-podnioslo-ceny-energii-w-krajach-baltyckich/ [accessed: 20.02.2025].

Legal acts

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Official Journal of the EU L 333/164 of 27.12.2022).

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) – (Official Journal of the EU L 333/80 of 27.12.2022).

Protocols additional to the Geneva Conventions of 12 August 1949, relating to the protection of victims of international armed conflicts (Protocol I) and relating to the protection of victims of non-international armed conflicts (Protocol II), drawn up in Geneva on 8 June 1977 (Journal of Laws of 1992 no. 41, item 175).

Witold Skomra, PhD

The Head of the Critical Infrastructure Protection Department in the Government Centre for Security. Expert in civil planning, crisis management and critical infrastructure protection. National delegate to the group preparing the CER Directive and to the Organisation for Economic Co-operation and Development (OECD High Level Risk Forum). Lecturer at the Faculty of Management, Warsaw University of Technology. He teaches courses in business continuity, risk management, public safety management and critical infrastructure protection. He is a former Commander-in-Chief of the State Fire Service, graduate of the Main School of Fire Service and the National Defence University in Warsaw.

Contact: witold.skomra@rcb.gov.pl

Karolina Wojtasik, PhD, MBA

Security specialist, court expert, academic researcher, vice-president for scientific affairs of the Polish Association for National Security (PTBN), chief expert of the Government Centre for Security (RCB). During Polish presidency of the European Council, she plays the role of the president of PROCIV–CER working party. She deals with the broadly understood security of critical infrastructure, especially in the context of threats to physical and personal security. In addition, she analyses the activities of Salafi terrorist organisations, the modus operandi of the perpetrators of terrorist attacks in the EU and the USA, as well as instructional publications on methods of carrying out attacks on civilians and facilities. Author of books: *Anatomy of a Terrorist Attack. On the Strategy and Tactics of Terrorists, Paths of Jihadi Radicalisation. A textbook for students of sociology, political science and security.*

Co-author of the book *The Polish anti-terrorist system and the realities of the attacks of the second decade of the 21st century* and many other publications related to terrorism, as well as security and building the resilience of critical infrastructure. Creator of the popular science channel Anatomia zamachu on YouTube.

Contact: karolina.wojtasik@rcb.gov.pl