

TERRORIST AND SABOTAGE THREATS

to critical infrastructure



Patronat polski i jarzyczonki w Radzie UE
Patronage of the Polish presidency of the Council of the EU
Patronage de la présidence polonaise du Conseil de l'UE



RCB

Terrorist and sabotage threats to critical infrastructure

Scientific Editing

Karolina Wojtasik, PhD and Damian Szlachter, PhD

Scientific Editors	Karolina Wojtasik, PhD, Damian Szlachter, PhD
Reviewers	Waldemar Zubrzycki, Professor Police Academy in Szczytno Agata Tyburska, PhD with habilitation Police Academy in Szczytno
Editorial team	Damian Szlachter, PhD (editor-in-chief), Agnieszka Dębska (editorial secretary, layout editor), Aleksandra Dąbała, Aneta Olkowska, Izabela Paczesna, Monika Sikora (editing), Sylwia Kłobuszewska (translation, proofreading)
Cover design	Aleksandra Bednarczyk

© Copyright by Agencja Bezpieczeństwa Wewnętrznego 2025

ISSN 2720-4383

e-ISSN 2720-6351

ISBN 978-83-968287-5-0

All texts included in the special issue were peer-reviewed

Texts express the views of the authors and do not represent the position of the Internal Security Agency and the Government Centre for Security

Declaration of the original version:

The printed version of the journal is the original version

The special issue appeared in print only in English

Electronic versions are available in two languages: English and Polish

The online version of the journal is available at: www.abw.gov.pl/wyd/

The journal is available on the Jagiellonian University Scientific Journals Portal at: <https://www.ejournals.eu/Terroryzm/>

Articles for the journal should be submitted through the editorial panel available at: <https://ojs.ejournals.eu/Terroryzm/about/submissions>

Wydawnictwo Agencji Bezpieczeństwa Wewnętrznego
Centralny Ośrodek Szkolenia i Edukacji
im. gen. dyw. Stefana Roweckiego „Grota”
ul. Nadwiślańczyków 2, 05-462 Wiązowna, Poland

Contact

mobile: (+48) 22 58 58 671

e-mail: wydawnictwo@abw.gov.pl

www.abw.gov.pl/wyd/



Printed in May 2025

Print

Mazowieckie Centrum Poligrafii Sp. z o.o.
ul. Ciurlionisa 4, 05-270 Marki
mobile: 505 727 782

TABLE OF CONTENTS

7 Foreword

ARTICLES

- 13** Critical infrastructure as a target for hybrid operations.
Case studies of attacks against the facilities and systems of CI
Witold Skomra, Karolina Wojtasik
- 35** Hybrid threats in the Baltic Sea.
The results of analysis of countermeasure options
Rafał Miętkiewicz
- 71** Terrorist and sabotage attacks on selected
critical infrastructure systems – a historical perspective
Krzysztof Izak
- 113** Critical infrastructure as a target of hybrid and conventional attacks.
Lessons from the Ukrainian experience
Michał Piekarski
- 133** Hybrid threats to critical infrastructure
in the European Union. Selected Hybrid CoE analyses
Aleksander Olech
- 159** Legal and technical methods of protecting critical infrastructure
facilities against threats from unmanned aerial vehicles –
the Polish example
Jędrzej Łukasiewicz, Damian Szlachter

- 185** **Polish individual restrictive measures applied to economic entities in the context of the war in Ukraine and the situation in Russia and Belarus**
Mariusz Cichomski, Konrad Kaczor
- 209** **The hybrid dimension of contemporary terrorism and critical infrastructure. Analysis of Europol's TE-SAT reports from 2021–2024**
Sebastian Wojciechowski
- 225** **Cyber threats as hybrid activity against the European Union in light of the current geopolitical situation**
Monika Stodolnik
- 249** **Results of the survey on the perception of terrorist and sabotage threats among the experts of the EU Protective Security Advisors**
Karolina Wojtasik, Damian Szlachter

EXPERT MATERIALS

- 273** **The role of standardisation and conformity assessment in ensuring security and building resilience of critical infrastructure to hybrid threats**
Adam Tatarowski
- 315** **The value of EU research projects in critical infrastructure protection**
Małgorzata Wolbach, Rashel Talukder

Security, Europe!

Poland first chaired the Council of the European Union in the second half of 2011. Shortly after the beginning of the Presidency, on 22 July, there were terrorist attacks in Oslo and on the Norwegian island of Utoya. They represent one of the most tragic pages in the history of terrorism in Europe. The perpetrator attacked in open public spaces. Since then, protecting such places from the effects of terrorist activity has been a priority, both in the EU Member States and in the EU institutions.

The second Presidency of the Republic of Poland in the Council of the EU began in January 2025. Poland assumed the Presidency at a time of global unrest, when the most important task is to ensure the security of the EU's external borders and the continuity of key services in EU Member States. This is reflected in the slogan of this Presidency: 'Security, Europe!'. For the Internal Security Agency and the Government Centre for Security in Poland, it is a time to undertake initiatives both at home and abroad to support the building of resilience to hybrid threats, with particular emphasis on the protection of critical infrastructure (CI) facilities, national and European (#OchronaIK).

With regard to CI, the leading theme of the Polish Presidency was shaped by:

- the war in Ukraine and the associated increase in the number of hybrid actions, including sabotage by Russian actors against CI facilities in the energy, transport, telecommunications, water supply sectors, as well as under the influence of the support provided to Ukraine by EU and NATO states;

- the implementation of the CER Directive of the European Parliament and the EU Council on the resilience of critical entities, which changes the concept of their protection in Member States and gives their governments a new impetus for action in this strategic area.

The special issue of the scientific journal “Terrorism – Studies, Analyses, Prevention” (T-SAP), prepared under the aegis of the Internal Security Agency and the Government Centre for Security, is a thematic issue. We have collected analyses and case studies on the current challenges of protecting CI on land and sea and in the cyberspace of EU countries. The authors of the articles are civilian and military experts representing academia, think tanks and specialised news portals, as well as government and law enforcement officials. They present CI security issues from different perspectives, taking into account their competences and experiences.

The publication opens with an article discussing the use of CI in hybrid conflicts and providing a comparative analysis of the solutions for building the resilience of this infrastructure arising from the CER and NIS 2 Directives of the European Parliament and the EU Council. The CER Directive is expected to bring about a sea change in building the resilience of CI to terrorist and sabotage activities. In Poland, the basis of the proposed CI protection system will be, inter alia, the idea of standardising the physical security of protected facilities, as discussed in detail in one of the analyses.

An article on past terrorist and sabotage attacks on CI may help to better understand the evolution of threats and how to neutralise them. Instead, data from Europol’s annual TE-SAT (*EU Terrorism Situation & Trend Report*) from 2021–2024 provides a contribution to showing the contemporary landscape of terrorist threats in the EU. The results of the 2025 terrorism and sabotage threat perception survey may also add to this knowledge. Respondents were advisors on building resilience to terrorist threats working within the EU Protective Security Advisors initiative. European experts assessed the current challenges in this area and identified opportunities to enhance prevention and protection efforts. The EU

perspective on hybrid threats, especially in Central and Eastern Europe, is presented in an article devoted to the analysis of reports produced by the European Centre of Excellence for Countering Hybrid Threats in Helsinki.

One of the domains where conflict can take place is the maritime domain. In the special issue, we present the specificity of the hybrid threats in the Baltic Sea, which are intensifying from 2022 onwards, and the possibilities for NATO to counter them. In the article, the author pays particular attention to the threats posed by modern maritime autonomous systems. As the country holding the Presidency of the Council of the EU, we would like to share our experience in building capabilities to protect strategic facilities from unmanned aerial vehicles. We present this issue with legal and technical aspects.

In the special issue, we also address Ukraine's experience in countering and combating Russian hybrid and conventional attacks on CI facilities. Related to the Russian-Ukrainian war is the issue of sanctions. In an article, we discuss the national individual restrictive measures implemented in Poland against economic entities supporting the actions of the Russian Federation and Belarus.

The largest number of hybrid actions against EU countries' CI facilities are undertaken in cyberspace. We present specific cyber security incidents in selected European countries caused by state-sponsored, hacktivist and cybercriminal groups. We also describe the different reporting strategies adopted by the services and teams responsible for the cyber security of EU and NATO countries, giving an overview of the cyber threats currently facing Europe.

An important support in shaping national and EU initiatives to increase CI's resilience to hybrid threats, including terrorism and sabotage, are research projects implemented with EU funds. Therefore, we have decided that it is worth discussing selected topics implemented under Horizon Europe, which is one of the EU's flagship initiatives in this area.

During the Presidency, Poland supports activities strengthening European security in all its dimensions:

external, internal, information, economic, energy, food and health. The special issue of T-SAP fits in with these objectives by showing the multidimensionality of CI protection, which is the common denominator of all these dimensions. We hope that the material presented here will contribute to the knowledge of contemporary threats to CI facilities and effective ways of countering these dangers, and will inspire not only further research and analysis, but also EU initiatives in the area of security under successive presidencies of the Council of the EU.

Karolina Wojtasik, PhD

Government Centre
for Security

Damian Szlachter, PhD

Internal Security
Agency




ARTICLES



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 theory¹ 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 concessions².

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 2931³ 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 million⁴, 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 found⁵.

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 principal⁶. 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 prices⁷. Although the attack was claimed by the Yemeni Houthi rebel group, many studies have suggested that the operation may have been supported by Iran⁸.

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 III¹⁰ 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.

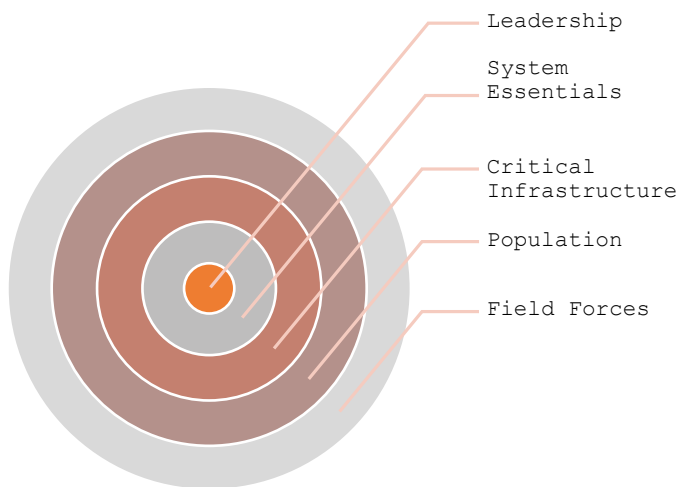


Figure 1. Warden's 5 Ring System Theory.

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 billion¹¹. 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 conflicts¹²) 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 warfare¹³, 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 manipulating 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 blackouts¹⁴.

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 increases¹⁵. 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 grid¹⁶. 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 Russia¹⁷. 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-dezinformacij%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 anchor¹⁸. 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 EUR¹⁹. After the cable damage, the average wholesale electricity price in Lithuania increased by 41% during the week from 56 EUR/MWh to 79 EUR/MWh²⁰. 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/artukul/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 Pipeline²¹, 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 hackers²². 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 sector²³. 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 Pipeline 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 Warnig²⁴. 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 security²⁵. 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. Jakóbiak, *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 groups²⁶. 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-oczyszczalniasciekow-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-oczyszczalnia-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://instytutprawobywatelskich.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].

Jakóbk 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://madeinvilnius.lt/pl/Aktualno%C5%9Bci/Lietuvos-naujienos/Minister-ostreaga-mieszka%C5%84c%C3%B3w-przed-mo%C5%BCliw%C4%85-dezinformacij%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 Pipeline 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-ostreaga-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/arttykul/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-slaw-a/> [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

Hybrid threats in the Baltic Sea. The results of analysis of countermeasure options

RAFAŁ MIĘTKIEWICZ

Polish Naval Academy
of the Heroes of Westerplatte

 <https://orcid.org/0000-0002-3129-7092>

Abstract

The maritime areas of the Baltic region, can be considered a space for the conduct of proxy conflict, i.e. of a substitute nature, between the Russian Federation and Western states. Intensifying since 2022 (the start of Russia's full-scale invasion of Ukraine) hybrid actions on the part of Russia have largely targeted the critical infrastructure facilities of coastal states. The article discusses the various forms of subliminal actions against this infrastructure undertaken by Russia, based on available information on events in the period from 2022 to the end of 2024. It also presents the vulnerabilities to hybrid actions that characterise critical infrastructure in the Baltic (possible ways of affecting port facilities and offshore infrastructure, with a particular focus on undersea transmission lines). The publication also presents the author's views on possible responses from NATO countries, in the form of political, military and technological initiatives, to hybrid threats posed by modern maritime autonomous systems.

Keywords

hybrid threats at sea, hybrid conflict, maritime critical infrastructure

Introduction

The situation in the Baltic Sea is under the influence of dynamic processes shaping the security architecture in the region. It can be concluded that the Baltic Sea basin is a space of substitute rivalry between Russia, which strives to change the current order in Europe, and Western countries (the European Union and NATO), which support Ukraine. At the same time, the Baltic Sea is a corridor enabling the countries of the region (NATO's flank) to become independent of hydrocarbon supplies from Russian sources (which the Kremlin uses as a tool of coercion or reward) and to diversify the supply of energy resources (mainly natural gas and oil). The Baltic Sea is also playing an increasingly important role in the production of electricity using renewable energy sources (offshore wind energy with a potential estimated by the European Commission at 93 GW by 2050¹). In the case of Poland, the energy dependence rate on the Baltic Sea, taking into account the ratio of imports of major energy resources and energy carriers to their total consumption, was 48% in 2024. By 2040, this ratio is expected to reach 60%². At the same time, this basin remains an important area for the implementation of the strategic goals of the Russian Federation (RF). The presence of a heavily militarised exclave of Kaliningrad, the St Petersburg region (anti-access-area denial, A2/AD capabilities) with important ports (oil exports), gas transmission infrastructure (damaged NS1 and NS2 gas pipelines) and the Baltic Fleet of the RF operating in the waters of the Baltic Sea are just the most important elements that make up Russia's Baltic assets. The Russian maritime doctrine introduced in 2022 lowered the rank of the Baltic Sea (the document identifies three levels of importance of the basins, as vital, important and others), indicated the confrontational direction of Russia's policy towards Western countries (total hybrid war) and the desire to remodel the current world order as well as international security architecture³. The challenges that the countries of the Baltic region have been facing for years, and which have been intensifying since the beginning of the war in Ukraine, clearly indicate that the RF has not abandoned its efforts

¹ *Study on Baltic offshore wind energy cooperation under BEMIP. Final report*, ENER/C1/2018-456, Luxembourg 2019, Publications Office of the European Union, p. 10.

² Z. Nowak, M. Maj, *Bałtyk jako przestrzeń strategicznej aktywności energetycznej* (Eng. The Baltic Sea as a space for strategic energy activities), in: *Czy morze pomoże? Bałtyk a bezpieczeństwo energetyczne Polski*, Z. Nowak (ed.), Warszawa 2024, Institute for Foreign Affairs, pp. 33–46.

³ *Maritime Doctrine of the Russian Federation*, A. Davis, R. Vest (trans.), Newport 2022, Russia Maritime Studies Institute, United States Naval War College.

to break the unity of the coastal states using the instruments in its resources. Long before Russia's attack on Ukraine, strategic Polish publications pointed to hybrid activities as an important means of achieving the goals of the RF below the threshold of war⁴ and the main threats of military and non-military origin in the Baltic region⁵.

The reason for increased hybrid threats in the future may be the ineffectiveness of many of the actions taken by Russia against the states on the Baltic Sea⁶. As the situation deteriorates, the anticipated threats of direct nature may include the use of armed forces and threats of their use, as well as indirect forms (in the case of sea basins, we are talking about e.g. maritime blockades, shows of force using fleet, unannounced military exercises, harassment of the enemy, etc.)⁷. A typical state of affairs will be blurring the boundaries between a state of peace and a state of war, asymmetry, the growing importance of non-kinetic activities (especially active operations in cyberspace), or the use of autonomous technologies⁸. The intensification of the conflict and Russia's use of new forms of action is indicated by the events that occurred in the Baltic Sea in 2023–2024. In October 2023, the Balticconnector gas pipeline was damaged by the Hong Kong-flagged vessel Newnew Polar Bear, which was operating a voyage from Kaliningrad to St Petersburg. The Balticconnector was restarted in April 2024⁹. After more than 10 months of investigation into the matter

⁴ *National Security Strategy of the Republic of Poland*, Warszawa 2020.

⁵ *Poland's Strategic Concept for Maritime Security*, Warszawa–Gdynia 2017, Biuro Bezpieczeństwa Narodowego (Eng. National Security Bureau), p. 11.

⁶ P. Mickiewicz, *Bezpieczeństwo energetyczne czy bezpieczeństwo morskie? Dylemat oceny potencjalnych zagrożeń bezpieczeństwa Polski na akwenie Morza Bałtyckiego w trzeciej dekadzie XXI wieku* (Eng. Energy security or maritime security? The dilemma of assessing potential threats to Poland's security in the Baltic Sea area in the third decade of 21st century), „Nautologia” 2024, no. 161, p. 71.

⁷ A. Nowakowska-Krystman, *Potencjał obronny Sił Zbrojnych RP w ujęciu relatywnym* (Eng. Defence potential of the Polish Armed Forces in relative terms), Warszawa 2018, Akademia Sztuki Wojennej, p. 73.

⁸ R. Kasprzyk, *Sztuczna inteligencja i cyberprzestrzeń a proces złośliwego sterowania ludźmi i maszynami* (Eng. Artificial intelligence and cyberspace and the process of malicious control of humans and machines), in: *GlobState*, vol. 2. *Wyzwania dla Polski w kontekście zmian w środowisku bezpieczeństwa*, Ł. Jureńczyk, R. Reczkowski (sci. ed.), Bydgoszcz 2020, Centrum Doktryn i Szkolenia Sił Zbrojnych – Uniwersytet Kazimierza Wielkiego, pp. 277–298.

⁹ J. Hyndle-Hussein, *The Balticconnector gas pipeline damage*, Ośrodek Studiów Wschodnich, 11.10.2023, <https://www.osw.waw.pl/en/publikacje/analyses/2023-10-11/balticconnector-gas-pipeline-damage> [accessed: 2.01.2025].

by the Finnish side, the explanation from the Chinese side that the damage to the facility was accidental has not been confirmed¹⁰. Two fibre-optic telecommunications connections Lithuania – Sweden and Finland – Germany were severed in November 2024, and the EstLink 2 submarine power line connecting Finland and Estonia was damaged in December 2024. One of Russia's activities is the use of the so-called *grey fleet* and the so-called *dark fleet* or *shadow fleet*. The term *grey fleet* refers to a quasi-legal fleet (unclear origin and ownership of the vessel and flag) operating alongside the International Maritime Organization (IMO) positively considered fleet. A *dark fleet* is one that uses illegal practices (tampering with identifiers and location or deliberately disabling automatic identification systems) to circumvent sanctions on Russia's oil trade¹¹.

The research problem boils down to answering the question: how to counteract Russian hybrid activities against critical infrastructure (CI) facilities at sea? The aim of this article is to first present possible forms of hybrid activities in the Baltic Sea as a reference basin (partly based on the analysis of past events) that may occur in the next 2 years in relation to offshore CI facilities. Secondly, the vulnerabilities determining the possibility of creating hybrid threats in relation to CI facilities in the Baltic Sea will be specified. In the next step, proposals for actions will be identified to counter this type of threat and increase the level of protection of CI facilities at sea.

A critical analysis of the following sources was carried out in order to develop this paper¹²:

- documents in the form of: doctrines (*Maritime Doctrine of the Russian Federation*, A. Davis, R. Vest, trans.), strategies (*REPowerEU Plan*, *Communication from the Commission to the European Parliament, the European Council, the Council, The European Economic and Social Committee and the Committee of the Regions*; *Council conclusions on*

¹⁰ *Finlandia: Władze nie potwierdzają informacji o „przypadkowym” uszkodzeniu Balticconnector* (Eng. Finland: Authorities do not confirm information on “accidental” damage to Balticconnector), Portal Morski, 13.08.2024, <https://www.portalmorski.pl/offshore/56252-finlandia-wladze-nie-potwierdzaja-informacji-o-przypadkowym-uszkodzeniu-balticconnector> [accessed: 29.01.2025].

¹¹ *Russia's 'shadow fleet': Bringing the threat to light*, European Parliament, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766242/EPRS_BRI\(2024\)766242_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766242/EPRS_BRI(2024)766242_EN.pdf), p. 3 [accessed: 23.01.2025].

¹² The source materials analysed are only listed here. Their full bibliographic description is given in the appendix bibliography (editor's note).

the Revised EU Maritime Security Strategy (EUMSS) and its Action Plan; National Security Strategy of the Republic of Poland 2020; Poland's Strategic Concept for Maritime Security; Energy Policy of Poland until 2040), official government information (Joint Declaration on cooperation to secure critical subsea infrastructure), report of state institution – Supreme Audit Office (Information on the results of the audit. Preparation of the state for threats related to hybrid actions; Information on the results of the audit. Implementation of measures to improve fuel security in the oil sector) and publications of international organisations: European Parliament (P9_TA(2024)0079 – Russiagate: allegations of Russian interference in the democratic processes of the European Union – European Parliament resolution of 8 February 2024 on Russiagate: allegations of Russian interference in the democratic processes of the European Union (2024/2548(RSP))), European Commission (Joint Statement by the European Commission and the High Representative on the Investigation into Damaged Electricity and Data Cables in the Baltic Sea), Baltic Marine Environment Protection Commission (HELCOM, ensuring safe shipping in the Baltic), NATO (N. Fridbertsson, General Report – Protecting Critical Maritime Infrastructure – The Role of Technology; A. Hagelstam, Cooperating to counter hybrid threats), Atlantic Council (E. Braw, Russia's growing dark fleet: Risks for the global maritime order);

- *available (non-confidential) materials, including press releases (Finland-Estonia power cable hit in latest Baltic Sea incident, “The Guardian”; C. Chiappa, 6 countries move to protect the North Sea from Russians, “Politico”), announcements of the ministries of the Baltic states, post-conference studies by GlobState (K. Kasprzyk, Artificial intelligence and cyberspace and the process of malicious control of humans and machines);*
- *studies of renowned centres dealing with the issue of hybrid threats, such as: Hybrid Centre of Excellence (Handbook on maritime hybrid threats: 15 scenarios and legal scans), Maritime Security Centre of Excellence (D. Doğan, D. Çetikli, Maritime Critical Infrastructure Protection (MCIP) in a Changing Security Environment) and international relations, such as: the International Centre for Defence and Security (N. Aliyev, Does Russia want to revise its water border with the Nordic and Baltic states?), U.S. Helsinki Commission (S. McGrath, Spotlight on the Shadow War: Inside Russia's Attacks*

on NATO Territory), Ośrodek Studiów Wschodnich (J. Hyndle-Hussein, *The Balticconnector gas pipeline damage*), as well as industry portals Baltic Wind EU dealing with international aspects of maritime development wind energy in the Baltic Sea (K. Bulski, *The Role of the New European Commission and Regional Cooperation in Accelerating Offshore Wind in the Baltic Sea*);

- publications of well-established think tanks, such as: The Polish Institute of International Affairs (K. Dudzińska, *Sweden Takes a Nuclear Turn in Energy Policy*), Center for International Maritime Security (O. Chiriac, *The 2022 Maritime Doctrine of the Russian Federation: Mobilization, Maritime Law, and Socio-Economic Warfare*), The Opportunity Institute for Foreign Affairs (R. Miętkiewicz, *The Baltic Sea as a special protection area*), Warsaw Institute (B. Fraszka, *Baltic States and Russian Hybrid Threats*), Polish Society for National Security (K. Wojtasik, *Results of the survey on the perception of terrorist threats among EU PSA participants*), I. Łukasiewicz Institute of Energy Policy (M. Ruszel, P. Ogarek, *Poland's fuel security in the context of ownership changes in the petroleum products logistics market and the European Commission's remedies on the merger between PKN ORLEN and LOTOS Group. Poland at the threshold of the embargo on petroleum products from Russia – opening analysis 2023*);
- cyber threat analyses published by the European Union Agency for Cybersecurity (*ENISA Threat Landscape 2024*), and American Cybersecurity and Infrastructure Security Agency (*Russian Military Cyber Actors Target US and Global Critical Infrastructure*);
- previous research work devoted to the issues of contemporary threats at sea (R. Miętkiewicz, *Dumped conventional warfare (munition) catalog of the Baltic Sea*; R. Miętkiewicz, *High explosive unexploded ordnance neutralization – Tallboy air bomb case study*), including those created in relation to offshore energy infrastructure facilities (R. Miętkiewicz, *Offshore wind farms and national maritime security*; R. Miętkiewicz, *The Baltic Sea as a special protection area*) and works on the use of modern technologies (R. Miętkiewicz, *Autonomous systems in maritime operations*; R. Miętkiewicz, *Offshore energy infrastructure facilities – an attempt to determine vulnerability to attacks by unmanned platforms*). The results of the EU Protective Security Advisors expert survey were also taken into account

(K. Wojtasik, *Results of the survey on the perception of terrorist threats among EU PSA participants*)¹³.

Hybrid threats

Hybrid threats are harmful and intentional activities that are planned and carried out used by authoritarian states and regimes including non-state actors that often act as proxies to undermine a target (state or an institution), through a variety of means, often combined¹⁴. The use of multiple actors and activities promotes synergies that amplify the effectiveness of the attack. Hybrid threats are constantly changing and the tools used cover the full spectrum of activities, including: advanced cyberattacks¹⁵, information manipulation (including by means of fake social media profiles), economic influence as well as behind-the-scenes political maneuvering, coercive diplomacy (influence and interference operations), or threats of military force. The characteristic features of hybrid conflicts are constant change and the problem with defining all its aspects. It combines conventional and unconventional actions, symmetry and asymmetry, state and non-state actors (sometimes difficult to identify operating below the detection and identification threshold). The attacker's objective is to launch coordinated strikes at points of key importance to the opponent (e.g. systemic weaknesses of democratic states)¹⁶.

¹³ A new survey of EU PSA participants was conducted in February 2025, the results of which are presented in the article: K. Wojtasik, D. Szlachter, *Results of the survey on the perception of terrorist and sabotage threats among the experts of the EU Protective Security Advisors*, "Terrorism – Studies, Analyses, Prevention", special issue: *Terrorist and sabotage threats to critical infrastructure*, pp. 249–270. <https://doi.org/10.4467/27204383TER.25.022.21525> (editor's note).

¹⁴ *Hybrid threats as a concept, Frequently asked questions on hybrid threats*, The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/> [accessed: 2.12.2024].

¹⁵ A. Hagelstam, *Cooperating to counter hybrid threats*, NATO Review, 23.11.2018, <https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html> [accessed: 2.12.2024].

¹⁶ B. Fraszka, *Państwa bałtyckie a rosyjskie zagrożenia hybrydowe* (Eng. Baltic States vs. Russian Hybrid Threats), Warsaw Institute, 26.10.2020, <https://warsawinstitute.org/wp-content/uploads/2020/10/Pa%C5%84stwa-ba%C5%82tyckie-a-rosyjskie-zagro%C5%BCenia-hybrydowe-Bartosz-Fraszka.pdf>, p. 4 [accessed: 29.12.2024].

The RF is considered to be the most likely source of hybrid threats, due to the current geopolitical situation. The main purpose of such actions is to discredit the position of attacked state internationally (inter alia, by demonstrating the ineffectiveness of the state's efforts in response to crisis situations), to weaken the cohesion of Western alliances and to force it to meet Russia's politic, economic and military demands. An expert from the Polish Association for National Security points out that due to the shortcomings in the equipment of regular units of the Russian armed forces and the level of losses suffered in Ukraine, the emphasis in terms of impact will shift to hybrid operations. The sea area appears to be particularly advantageous due to the inability to exercise full control over it¹⁷.

The results of the terrorist threat perception survey conducted in early 2023 with EU Protective Security Advisors (EU PSA) experts indicated the highest ranking of CI facilities as primary, secondary and tertiary potential targets for terrorist attacks in the EU (63.63% of all indications). Public transport systems came second (60% of responses). Among the facilities most vulnerable to terrorist attack (the choices were: military bases used within NATO, CI facilities, public transport system, commercial goods transport system, headquarters of constitutional state bodies, tourism infrastructure, sports and entertainment facilities, places of worship, headquarters of EU institutions and agencies), most (40%) respondents indicated energy infrastructure facilities¹⁸. In turn, among many means of carrying out attacks (unmanned aerial vehicles, 3D printing, vehicles used to ram, improvised explosive devices, melee weapons made of composites, CBRN agents, incendiary agents), according to EU PSA experts, it is the autonomous systems that will be most willingly used by terrorists to carry out attacks (49.09%). The vast majority of respondents (81.82%) believed that in the next 3 years, terrorist activity will be used as part of hybrid activities undertaken on the territory of the EU by a foreign country.

¹⁷ M. Piekarski, *Ochrona infrastruktury krytycznej na polskich obszarach morskich w kontekście zagrożeń hybrydowych* (Eng. Protection of critical infrastructure in Polish maritime areas in the context of hybrid threats), Polskie Towarzystwo Bezpieczeństwa Narodowego (Eng. Polish Association for National Security) 2023.

¹⁸ K. Wojtasik, *Analiza wyników badań na temat percepcji zagrożeń o charakterze terrorystycznym wśród uczestników EU PSA* (Eng. Results of the survey on the perception of terrorist threats among EU PSA participants), PTBN Analyses no. 1, Polskie Towarzystwo Bezpieczeństwa Narodowego (Eng. Polish Association for National Security) 2023, p. 5.

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), having conducted research on contemporary hybrid threats occurring in sea basins, indicated that the scope of activities of this type is very wide. Their forms may include: illegal fishing and the use of fishing vessels to conduct aggressive activities, cyberattacks, attacks by fast motorboats, or the use of unfavourable hydro-meteorological conditions as a means of authentication, e.g. dropping anchor in the immediate vicinity of submarine cables. Several scenarios included unlawfully declaring and closing maritime zones under the guise of military exercises, introducing zones of control of passing vessels¹⁹. Between the start of the Russian invasion of Ukraine in February 2022 and September 2024, the U.S. Helsinki Commission Staff identified about 150 hybrid attacks carried out on the territories of NATO countries by Russia or entities associated with it. Among the four separate directions of hybrid operations, attacks on CI facilities were in second place (33%), behind election interference and information campaigns (35%) and ahead of violence campaigns (20%) and the use of migrants as weapons (12%)²⁰.

The importance of the Baltic Sea for the Russian Federation

In 2022, after the full-scale invasion of Ukraine began, the Russian Maritime Doctrine was published, replacing the previous document in force since 2015. Russia's maritime and energy assets are primarily instruments of power, used to achieve strategic goals. Economic and social aspects remain in the background²¹. The most important priorities formulated in relation to the Baltic Sea include the development of port infrastructure and installations responsible for the transit of hydrocarbons (export reorientation), logistics centres, and the system of offshore export pipelines. The aspect of further strengthening the military capabilities

¹⁹ *Hybrid CoE Paper 16: Handbook on maritime hybrid threats: 15 scenarios and legal scans*, The European Centre of Excellence for Countering Hybrid Threats 2023, p. 5.

²⁰ S. McGrath, *Spotlight on the Shadow War: Inside Russia's Attacks on NATO Territory. A Report by the U.S. Helsinki Commission Staff*, 2024, p. 2.

²¹ O. Chiriac, *The 2022 Maritime Doctrine of the Russian Federation: Mobilization, Maritime Law, and Socio-Economic Warfare*, Center for International Maritime Security, 28.11.2022, <https://cimsec.org/the-2022-maritime-doctrine-of-the-russian-federation-mobilization-maritime-law-and-socio-economic-warfare/> [accessed: 7.12.2024].

and base network of the Baltic Fleet (protection of Russian interests in the Baltic Sea) is also important²². The Baltic Sea is important for Russia due to the practice of circumventing Western sanctions (embargo and price caps) imposed on Russian oil exports, in response to the invasion of Ukraine. Russian ports in the Baltic Sea, in September 2023 alone, accounted for 57% of Russia's total oil exports²³. According to data from 2023, the total turnover of the three Russian ports accounted for almost half (46%) of the total volume of transshipments of the ten largest Baltic ports. This value has remained at a similar level since 2021²⁴.

Russian *grey fleet* and *shadow fleet* vessels use disorderly ownership and insurance issues to violate sanctions imposed on Russian oil. This in itself is a source of threat to the countries on the Baltic Sea, due to the age of these ships, their technical condition, their use in reconnaissance operations, crew qualifications, oil transshipments on the high sea²⁵. *Grey fleet* and *shadow fleet*, as the 2024 events mentioned in *the Introduction* show, are also tools for creating hybrid and asymmetric threats.

In the context of security in the Baltic Sea basins, Russia is expected to introduce a whole package of pressure mechanisms calculated to maximise the involvement of NATO forces and resources in monitoring CI facilities. Such activities are to generate costs related to ensuring the security of the Alliance²⁶. Sabotage activities against CI may have consequences for transmission networks, affect the availability of raw materials and energy carriers, and cause perturbations in energy markets. It should be noted that NATO's actions, which will lead to a restriction of Russia's freedom to use *grey fleet* or *shadow fleet* (inspections of Russians ships

²² *Maritime Doctrine of the Russian Federation*, A. Davis, R. Vest (trans.)...

²³ K. Westgaard, *The Baltic Sea Region: A Laboratory for Overcoming European Security Challenges*, Carnegie Endowment FOR International Peace, 21.12.2023, <https://carnegieendowment.org/research/2023/12/the-baltic-sea-region-a-laboratory-for-overcoming-european-security-challenges?lang=en> [accessed: 7.12.2024].

²⁴ P. Frankowski, *Bałtyckie TOP10* (Eng. Baltic TOP10), *Namiary na Morze i Handel*, 9.05.2024, <https://www.namiary.pl/2024/05/09/baltyckie-top10/> [accessed: 3.01.2025].

²⁵ E. Braw, *Russia's growing dark fleet: Risks for the global maritime order*, Atlantic Council, 11.01.2024, <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/russias-growing-dark-fleet-risks-for-the-global-maritime-order/> [accessed: 29.04.2024].

²⁶ Ł. Wyszynski, *Wyszynski: Wejście Szwecji do NATO rodzi korzyści, ale i wyzwania (rozmowa)* (Eng. Wyszynski: Sweden's entry into NATO brings benefits but also challenges (interview)), *Biznes Alert*, 5.03.2024, <https://biznesalert.pl/szwecja-nato-zalety-wady-rosja-morze-baltyckie-bezpieczenstwo/> [accessed: 7.10.2024].

announced in December 2024 by the United Kingdom, Denmark, Sweden, Finland, Poland and Estonia), may be met with reaction from the RF and cause escalation of security threats. Russia may use its available military capabilities (mainly warships) to escort ships suspected of being used to circumvent sanctions²⁷.

Baltic critical infrastructure

Ensuring the energy security of the countries on the Baltic Sea requires the development of CI in the form of seaports, specialised terminals (oil, gas, floating storage regasification units – FSRUs), submarine power lines (connecting the energy systems of individual countries), pipelines (responsible mainly for the transmission of natural gas, and in the future also hydrogen), as well as communication lines (fibre optics), to drilling platforms leading offshore oil and gas production from offshore fields (the only country conducting oil and gas exploration and production in the Baltic Sea is Poland). The Baltic states have a high level of ambition in the development of both offshore wind energy and nuclear energy (as an element stabilising renewable energy sources) and the hydrogen economy. The submarine electricity interconnections linking Lithuania, Latvia and Estonia with the energy systems of Sweden (NordBalt), Finland (EstLink) and Poland (LitPol Link onshore connection) will enable the desynchronisation of these countries with the post-Soviet BRELL electricity system (February 2025). Thanks to the centralised system, Russia has so far had the ability to manage the frequency and stability of the grid, while dependent states have not had the ability to operate in isolated island mode²⁸.

The countries of the Baltic region are undergoing a process of fundamental change in the production of electricity. Sweden's nuclear energy turnaround (10 reactors are to be launched by 2045) has an impact on the energy security situation of countries on the Baltic Sea. For Norway, this means the possibility of temporarily stabilising its own system (based

²⁷ *Russia's Shadow Fleet Tankers Could Get Naval Escorts*, The Maritime Executive, 18.12.2024, <https://maritime-executive.com/article/russia-s-shadow-fleet-tankers-could-get-naval-escorts> [accessed: 9.01.2025].

²⁸ M. Paszkowski, *Litwa, Łotwa oraz Estonia planują stworzenie bałtyckiego hubu energetycznego* (Eng. Lithuania, Latvia and Estonia plan to create a Baltic Energy Hub), „Komentarze IES” 2024, no. 1259, p. 1.

on hydroelectric power plants). Sweden's actions are an incentive for other countries in the region to take similar steps (Estonia and Finland are planning a joint project of Small Modular Reactors – SMRs)²⁹. Sweden also plays a specific role in the process of building the Baltic Energy Ring, for whose members it is the guarantor of access to electricity in the event of a crisis situation. The capacities produced by the Swedish system can be supplied to the HVDC (high-voltage direct current) transmission systems with Lithuania (NordBalt), Finland (Fenno-Skan), Germany (Baltic Cable) and Poland (SwePol Link), if necessary. During the operation of the undersea line with Poland, there have already been at least a dozen incidents, including physical damage (fishing activities and ship anchors)³⁰.

Another country pursuing a nuclear programme is Poland, which intends to obtain a stable source of electricity with a total installed capacity of between 6 GW and 9 GW thanks to the commissioning of 6 units (each with the capacity of between 1 GW and 1.6 GW). The first nuclear power plant will be located on the Baltic coast. Such a location will enable the use of seawater to cool the reactors, as well as ensure the availability of the construction area for the transport of large-size elements, creating the basis for a stable and secure supply chain³¹.

The Scandinavia and Baltic Sea region has a significant potential for hydrogen production from renewable sources (green hydrogen), identified at around 27.1 million tons (including offshore and onshore wind and solar power) by 2040. Also by 2040, the Nordic-Baltic Hydrogen Corridor is expected to enable the cross-border transport of up to 2.7 million tons of renewable hydrogen from Finland through Estonia, Latvia, Lithuania and Poland to Germany to meet the REPowerEU targets. The offshore part of the corridor, with a total length of approx. 2500 km, is to run along the bottom of the Gulf of Finland³², a body of water with a high level of hybrid threats, as evidenced in particular by the events of 2024 previously

²⁹ K. Dudzińska, *Jądrowy zwrot w szwedzkiej polityce energetycznej* (Eng. Sweden Takes a Nuclear Turn in Energy Policy), „Biuletyn PISM” 2024, no. 58.

³⁰ R. Miętkiewicz, *Bałtyk jako obszar szczególnej ochrony* (Eng. The Baltic Sea as a special protection area), in: *Czy morze pomoże? Bałtyk a bezpieczeństwo energetyczne Polski*, Z. Nowak (ed.), Warszawa 2024, pp. 33–46.

³¹ Ibid.

³² *Nordycko-Baltycki Korytarz Wodorowy* (Eng. Nordic-Baltic Hydrogen Corridor), Gaz-System 2024, <https://www.gaz-system.pl/pl/rynek-wodoru/projekty/nordycko-baltycki-korytarz-wodorowy.html> [accessed: 3.01.2025].

mentioned. Taking into account the implementation of European plans for the development of the hydrogen economy, the strategic goals outlined by the Finnish government assume that the country will become the European leader of this technology in the entire value chain. Production in Finland is expected to reach 10% emission-free hydrogen in the EU by 2030³³.

Offshore gas pipelines are of strategic importance for the energy security of the Baltic states. The first of them is the Baltic Pipe, which enables the transit of 10 billion m³ of gas per year from the Norwegian Continental Shelf to Polish (transit through Germany and Denmark). The Balticconnector gas pipeline is responsible for the supply of natural gas to customers on the Finnish-Estonian-Latvian gas market. In the Polish exclusive economic zone, there is also a gas pipeline (2 lines) connecting Polish drilling platforms (gas extraction and discharge of gas associated with oil fields) with the coastal heat and power plant. Finland has the ability to obtain gas through its LNG terminals in the Gulf of Finland – Inkoo and Hamina (the country has 2 more terminals servicing industrial facilities), from where the raw material is further transported via an offshore gas pipeline to customers on the other side of the Gulf of Finland. In 2024, Germany launched the largest FSRU terminal in the Baltic Sea in Mukran (Rügen Island), enabling the receipt of gas from two cryogenic tankers at the same time (annual capacity of 13.5 billion m³ of gas). German plans include the construction of stationary terminals as well as FSRUs with a total regasification capacity of up to 54 billion m³ in 2027³⁴.

The largest LNG terminal in the Baltic Sea (specialist port) remains the terminal in Świnoujście, where work is still underway to increase import (8.3 billion m³ of gas per year) and storage capacity. In the next few years, another terminal (FSRU) is to be launched on the Polish Baltic coast, enabling exports of approx. 6 billion m³ (one vessel), taking into account the possibility of mooring a second regasification vessel³⁵. It should be recalled that as recently as 2018, Poland imported almost 80% of its oil from Russia, and in February 2023 stopped supplying it

³³ *Government adopts resolution on hydrogen – Finland could produce 10% of EU's green hydrogen in 2030*, Ministry of Economic Affairs and Employment, 9.02.2023, <https://valtioneuvosto.fi/en/-/1410877/government-adopts-resolution-on-hydrogen-finland-could-produce-10-of-eu-s-green-hydrogen-in-2030> [accessed: 9.11.2024].

³⁴ M. Kędzierski, *Za wszelką cenę. Niemiecki zwrot ku LNG* (Eng. At all costs. Germany shifts to LNG), „Komentarze OSW” 2023, no. 510.

³⁵ R. Miętiewicz, *Bałtyk jako obszar szczególnej ochrony...*, p. 47.

from that country altogether, due to Russia's attack on Ukraine and the expiry of long-term contracts. This situation was possible thanks to the maximisation of Naftoport's turnover (it supplies 4 refineries), one of the strategic facilities of this type in the Baltic Sea (another 2 are located in Lithuania). In addition, since 2022, none of the directions of oil supplies has exceeded 50% of imports³⁶. Naftoport is part of the logistics chain of oil supplies in Poland and Germany. Given the geopolitical situation, with the limitations of the Rostock terminal, Naftoport plays an important role in meeting the demand for German refineries (Schwedt and Leuna). It is worth mentioning that the Polish oil infrastructure supports the process of fuel supplies to fighting Ukraine. The West remained the only direction of imports of petroleum products (previously estimated at 5–10%). As of 2022, more than 90% of the supply of crude oil and its products comes from this direction, with Poland and Romania being the main suppliers³⁷.

The Baltic Sea, after the North Sea, is the basin with the most favourable conditions (due to wind conditions and sea depths) for the development of offshore wind energy in Europe. However, the reorientation towards renewable energy sources from the Baltic and North Seas will result in a significant dependence on the sea as an energy production area. Forecasts assume the possibility of using the wind potential in the Baltic Sea of up to 45 GW by 2050³⁸. Projects implemented by individual states on the Baltic Sea (Table 1), as is the case with Poland, change the current shape of the power system.

³⁶ Najwyższa Izba Kontroli (Eng. Supreme Audit Office), *Informacja o wynikach kontroli. Realizacja działań w zakresie poprawy bezpieczeństwa paliwowego w sektorze naftowym* (Eng. Information on the results of the audit. Implementation of measures to improve fuel security in the oil sector), KGP.430.7.2023, Warszawa 2023, p. 69.

³⁷ M. Ruszel, P. Ogarek, *Bezpieczeństwo paliwowe Polski w kontekście zmian właścicielskich na rynku logistyki produktów naftowych oraz remedies Komisji Europejskiej w sprawie fuzji PKN ORLEN i Grupy LOTOS. Polska u progu embargo na produkty naftowe z Rosji – analiza otwierająca 2023 rok* (Eng. Poland's fuel security in the context of ownership changes in the petroleum products logistics market and the European Commission's remedies on the merger between PKN ORLEN and LOTOS Group. Poland at the threshold of the embargo on petroleum products from Russia – opening analysis 2023), IPE Analysis no. 1/2023, Instytut Polityki Energetycznej (Eng. Institute for Energy Policy) 2023, p. 14.

³⁸ K. Bulski, *The Role of the New European Commission and Regional Cooperation in Accelerating Offshore Wind in the Baltic Sea*, BalticWind.EU, 11.09.2024, <https://balticwind.eu/the-role-of-the-new-european-commission-and-regional-cooperation-in-accelerating-offshore-wind-in-the-baltic-sea/> [accessed: 7.11.2024].

Table 1. Targets of the Baltic Region countries in the field of electricity production from offshore wind farms (including the North Sea).

A country of the region	Targets declared by countries according to national plans			Area of water bodies under WOFs [km ²]	Potential [GW]
	2030 [GW]	2040 [GW]	2050 [GW]		
Denmark	7.9	7.9	7.9	11 000	42.3
Germany	4.1	4.1	4.1	8400	70
Estonia	1	3.5	7	1850	9
Latvia	0.4	0.4	0.4	300	4
Lithuania	1.4	2.8	4.5	664	2.4 (may be increased to 3.3)
Poland	5.9	10.9	10.9	3600	17.2
Finland	1	5	12	3500	15.7
Sweden	0.7	-	-	1400 (may be increased to 4400)	6–7 (may be increased to 22)
Together for the region	22.5	34.6	46.8	30 714 (may be increased to 33 714) (the entire UE – 52 000)	167.6 (may be increased to 183.5)

Source: own elaboration. The data in the table is taken from the Baltic Energy Market Interconnection Plan (BEMIP) and the *WindEurope Offshore* report entitled *Wind in EU Maritime Spatial Plans* published on 19.10.2022. Quoted after: P. Wróbel, *Analiza: Inicjatywy UE wzmacniające współpracę regionalną na rzecz morskiej energetyki wiatrowej na Bałtyku* (Eng. Analysis: Review of EU initiatives to strengthen regional cooperation for offshore wind in the Baltic Sea), BalticWind.EU, 4.06.2024, <https://balticwind.eu/analysis-review-of-eu-initiatives-to-strengthen-regional-cooperation-for-offshore-wind-in-the-baltic-sea/> [accessed: 9.11.2024].

Projects such as the Balticconnector between Estonia and Finland, the expansion of the interconnection between Latvia and Estonia, the LNG terminal in Klaipėda and the LNG terminal in Świnoujście (long-term contracts for gas supplies from the US and Qatar) have affected market integration and reduced dependence on Russian gas in the region³⁹. What is particularly important, selected Baltic islands (Gotland, Åland

³⁹ REPowerEU Plan. Communication from the Commission to the European Parliament, the European Council, the Council, The European Economic and Social Committee and the Committee of the Regions, COM(2022) 230 final, Brussels 2022.

Islands, Bornholm), in addition to their strategic importance for NATO (the possibility of exercising control over the Baltic Sea waters and airspace), are to play the role of energy islands (places of energy production and distribution). For example, Bornholm Energy Island is expected to significantly contribute to the ecological transformation of both Denmark and the rest of Europe (construction of offshore wind farms with a total capacity of at least 3 GW and an area of about 650 km²). The submarine power lines will connect the offshore wind farms to installations on the island of Bornholm and to the electricity transmission grid in Zealand and Germany⁴⁰. This will require a significant expansion of the transmission infrastructure on the bottom of the Baltic Sea, crossing the most important (the highest traffic volume) sea communication routes leading from the Baltic Straits, to Russian ports among others.

Seaports play an important role in the functioning of the economies of the Baltic Region countries. According to data for 2023, the Russian Ust-Luga (volume of transhipments – 112 million tons) remained the largest port, followed by the Polish Gdańsk (81 million tons), ahead of the Russian ports of Primorsk (63 million tons) and St Petersburg (49.6 million tons). Further down the list are the Swedish Gothenburg (36.3 million tons), the Polish Szczecin-Świnoujście port complex (35.3 million tonnes), the Lithuanian Klaipeda (32.7 million tons)⁴¹. Military equipment is also transhipped in the ports as part of the replacement of military equipment of NATO units (permanent contingents) or exercises and manoeuvres. Seaports also secure the handling of orders for military equipment (in the case of Poland, it is about armament in the form of tanks and artillery systems from the USA and South Korea).

Threats to critical infrastructure facilities in the Baltic Sea

Among the actions taken by the RF in the last 10 years and bearing the hallmarks of hybrid actions in relation to the countries of the Baltic region, the following can be indicated (selected):

⁴⁰ Plan for Program Energy Island Bornholm, Danish Energy Agency 2023, ID: ENØ-FOR-115, p. 9.

⁴¹ P. Frankowski, *Bałtyckie TOP10...*

- attempts to undermine the existing provisions of international law on the delimitation of maritime areas (the course of state borders), as exemplified by the events of 21 May 2024. Russia proposed the establishment of a system of straight baselines in the eastern part of the Gulf of Finland and part of the Kaliningrad Oblast, thus undermining the regulations in force since 1985 (which were revoked by a military-diplomatic source the following day). These activities also included physical attempts to interfere with the course of the border on the Narva River (Estonia) by moving border buoys to the Estonian side⁴². One such activity was also to conduct military exercises in the areas of the exclusive economic zones of Lithuania and Latvia;
- disrupting the operation of satellite navigation systems (especially in the Gulf of Gdańsk, the Gulf of Finland, the Gulf of Riga) and hacking attacks on websites providing information on the current location of maritime facilities⁴³, an activity observed by the intelligence services of Norway, Denmark and the Netherlands since the beginning of 2023;
- increased activity aimed at reconnaissance of seaports, pipelines, fibre optic cables, oil platforms and wind farms⁴⁴;
- low-altitude flights of Russian military aircraft near CI facilities (drilling platforms) or attempts to disrupt military exercises (overflight of USS Donald Cook in 2016);
- the probable violation of the Swedish border by Russian midget submarines⁴⁵.

Actions taken against the infrastructure of ports and specialised terminals may include (generalised):

- the use of the so-called insiders recruited among employees of CI facilities in order to identify protection systems, detect

⁴² N. Aliyev, *Does Russia want to revise its water border with the Nordic and Baltic states?*, International Centre for Defence and Security, 15.08.2024, <https://icds.ee/en/does-russia-want-to-revise-its-water-border-with-the-nordic-and-baltic-states/> [accessed: 16.12.2024].

⁴³ R. Miętkiewicz, *Systemy autonomiczne w działaniach na morzu* (Eng. Autonomous systems in maritime operations), Gdynia 2023, Wydawnictwo AMW, p. 228.

⁴⁴ F. Bryjka, T. Zajac, *Wzmocnienie ochrony infrastruktury krytycznej państw UE i NATO* (Eng. EU and NATO countries strengthen the protection of critical infrastructure), „Biuletyn PISM” 2023, no. 79, p. 2.

⁴⁵ R. Miętkiewicz, *Systemy autonomiczne w działaniach na morzu...*, p. 230.

vulnerabilities or indicate specific objectives of activities (control elements, etc.);

- direct sabotage activities aimed at causing large-scale fires (ports, refineries, specialist terminals) or electrocution of selected infrastructure elements (important from the point of view of maintaining continuity of operation);
- terrorist attacks in various forms and by various means;
- criminal activities against facilities (sensitive elements of the installation) in the form of theft, devastation;
- deliberately causing environmental disasters resulting in large losses in the ecosystem and making it necessary to interrupt or reduce the work of port terminals⁴⁶;
- actions aimed at blocking access to infrastructure from land (carried out against railway lines, traffic control systems, etc.) and from the sea (e.g. by deliberately sinking or grounding a ship with the intention of blocking deep-water fairways, laying sea mines);
- cyber attacks aimed at paralysing systems responsible for the operation of terminals, operation and service centres (offshore wind farms), security systems, etc. This type of activity also includes disrupting the operation of navigation systems and generating avatars of units and aircraft. According to US assessments, cyber actors affiliated with the Russian General Staff Main Intelligence Directorate 161st Specialist Training Center (Unit 29155) and other units (26165 and 74455) have been responsible for operations in cyberspace against global targets (espionage, sabotage, and discrediting activities) since at least 2020⁴⁷. Russian funds are also used to fund hacking groups, such as UNC1151/Ghostwriter or Digital Shadows/Conti, in third countries⁴⁸. The second half of 2023 and the first half of 2024 saw a significant escalation of cyber-attacks. This showed that the scale of the problem has definitely increased,

⁴⁶ D. Doğan, D. Çetikli, *Maritime Critical Infrastructure Protection (MCIP) in a Changing Security Environment*, Istanbul 2023, Maritime Security Centre of Excellence (MARSEC COE), p. 35.

⁴⁷ *Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure*, Cybersecurity and Infrastructure Security Agency 2024, ID: AA24-249A, p. 1.

⁴⁸ A.M. Dyer, *Działania hybrydowe Rosji przeciw państwom NATO i UE* (Eng. Preparing for Russian hybrid activities against NATO and EU countries), „Biuletyn PISM” 2022, no. 183, p. 1.

both in terms of the variety and number of such incidents and their consequences⁴⁹;

- attacks from multiple directions involving the use of autonomous systems (the possibility of occurring in all domains).

Actions taken against offshore infrastructure (offshore wind farms, submarine cables, submarine pipelines) may include (generalised):

- interference with offshore construction work in the form of dangerous manoeuvres carried out in the vicinity of installation fleet vessels (without escort), these risks can be generated by platforms posing as state service vessels;
- violation of protection zones established around the installations, carried out under various pretences (failure of navigation, propulsion equipment, etc.) and the use of legal freedoms and the freedom to conduct scientific activity at sea to penetrate undersea transmission lines and the surroundings of infrastructure facilities⁵⁰;
- attempts to disrupt undersea power connections and gas pipelines by dragging anchors and intentionally manoeuvring ships, sabotage actions carried out by specialised sabotage groups;
- operations with the use of autonomous underwater platforms (autonomous underwater vehicles, AUV), surface platforms (unmanned surface vehicles, USV) and air platforms (autonomous aerial vehicles, AAV) and all derivatives, including those using the latest developments in the field of artificial intelligence, and using swarms (underwater shoals). Threats of this type, as indicated by the naval phase of the war in Ukraine and previous actions by terrorists (e.g. Houthi fighters in the Red Sea), may also be generated by ad hoc improvised measures based on dual-use technologies. A factor that intensifies this type of threat is the progressive process of proliferation of unmanned technologies⁵¹;

⁴⁹ ENISA *Threat Landscape 2024, July 2023 to June 2024*, European Union Agency For Cybersecurity 2024, p. 11. <https://doi.org/10.2824/0710888>.

⁵⁰ P. Mickiewicz, *Bezpieczeństwo energetyczne czy bezpieczeństwo morskie?...*, p. 73.

⁵¹ R. Miętkiewicz, *Systemy autonomiczne (bezzałogowe) jako nowe narzędzie w rękach terrorystów* (Eng. Autonomous (unmanned) systems as a new tool in the hands of terrorists), in: *XX-lecie wojny z terroryzmem: bilans i konsekwencje*. Vol. 2. *Infrastruktura krytyczna – analizy – case study*, B. Wiśniewska-Paź, D. Szlachter (eds.), Toruń 2022, Wydawnictwo Adam Marszałek, pp. 69–98.

- the use of sea mines and water borne improvised explosive devices (WBIED), both in the form of modern, quasi-intelligent sea mines (ensuring selective choice of targets or enabling the delay of action and prolonging the occurrence of threats) and in the form of mines constituting war remains. The fact that there is a huge deposit of chemical and conventional munitions in the Baltic Sea, including between 16 000 and 61 000 sea mines, can be used as an element of camouflage these activities⁵².

Vulnerabilities of critical infrastructure facilities in the Baltic Sea

The analysis of CI facilities, with particular emphasis on those responsible for energy production, storage and transmission, indicates that in relation to many of them (specialised terminals, offshore wind farms) we are dealing with facilities operating at the interface of land, sea and air environments. Another domain that has a very strong impact on the level of security of facilities of this type is cyberspace. Thus, when considering the maintenance of the security of maritime CI, a whole range of factors determining the possibility of intentional threats should be taken into account. In the case of the intended impact using methods typical of hybrid activities, it should be noted that⁵³:

- the threat will be multi-domain, synchronised and combined with a strong disinformation impact in the media;
- subliminal threats will, for political reasons, take the form of sabotage or diversionary actions created against Poland and other countries on the Baltic Sea⁵⁴;
- threats in the maritime domain (underwater and air) may concern both infrastructure facilities and units responsible for the supply of hydrocarbons (cryogenic tankers and tankers for the transport

⁵² R. Miętkiewicz, *Dumped conventional warfare (munition) catalog of the Baltic Sea*, "Marine Environmental Research" 2020, vol. 161, p. 105057. <https://doi.org/10.1016/j.marenvres.2020.105057>.

⁵³ R. Miętkiewicz, *Obiekty morskiej infrastruktury energetycznej – próba określenia podatności na ataki platform bezzałogowych* (Eng. Offshore energy infrastructure facilities – an attempt to determine vulnerability to attacks by unmanned platforms), „Alcumena. Pismo Interdyscyplinarne” 2023, no. 3(15), p. 217. <https://doi.org/10.34813/psc.3.2023.11>.

⁵⁴ P. Mickiewicz, *Bezpieczeństwo energetyczne czy bezpieczeństwo morskie?...*, p. 72.

of crude oil and petroleum products), and in the case of offshore facilities (offshore wind farms and drilling platforms, pipelines and underwater cables for various purposes) – also installation and maintenance fleets;

- location of facilities of strategic importance for the security of the countries of NATO's eastern flank in the immediate vicinity of the borders with Russia (the exclave of Kaliningrad in the case of Poland and Lithuania, the area of St Petersburg in relation to Finland and Estonia) and routes leading from the Gulf of Finland to Kaliningrad. The facilities in the form of the refinery and Naftoport and the planned FSRU terminal in Gdańsk (Poland) or the FSRU terminal in Klaipeda (Lithuania) are located several dozen kilometres from the borders with Russia, which increases vulnerability to hybrid threats;
- the offshore gas and energy infrastructure facilities of the countries on the Baltic Sea are located along the so-called submarine depths and troughs, the depths of which are conducive to sabotage activities. Both submarines and special groups operating from the decks of surface vessels (e.g. research vessels adapted for such activities) can be used to carry out such actions;
- facilities in the form of offshore wind farms, drilling platforms, as well as offshore pipelines and cable connections for various purposes are located outside the territorial sea, in the waters of the exclusive economic zone of the coastal states. The large distance from the shore (the selected investments of the second phase of offshore wind energy development in Poland are adjacent to the outer limits of this zone, with a distance of nearly 80 km from the coastline) and the legal status of international waters (freedom of navigation) increase their vulnerability to hybrid threats⁵⁵;
- many of the infrastructure facilities are cross-border (gas pipelines, power cables, telecommunications connections, etc.) and are exploited by numerous operators from different countries. This aspect requires cooperation and coordination of activities to ensure continuity of operations (in the case of the Baltic Pipe gas pipeline,

⁵⁵ R. Miętiewicz, *Morskie farmy wiatrowe a bezpieczeństwo morskie państwa* (Eng. Offshore wind farms, new elements of maritime security), „Sprawy Międzynarodowe” 2019, vol. 72, no. 1, p. 110. <https://doi.org/10.35757/SM.2019.72.1.06>.

from the place of extraction of raw material on the Norwegian Continental Shelf to the end point of receipt in Poland);

- very intensive shipping traffic (according to HELCOM reports, the Baltic Sea is one of the most crowded waters in the world)⁵⁶, in the vicinity of gas, electricity and telecommunications lines facilitates the generation of dangerous situations (mapping the bottom, dragging anchors, laying sea mines and marine improvised explosive devices - MIED). Such activities can be masked, for example, by switching off AIS (automatic identification system) transponders or manoeuvring suggesting technical problems;
- in the case of specialist terminals (Naftoport in Gdańsk, Gas Terminal in Świnoujście, FSRU terminals), it is necessary to maintain deep-water fairways (artificially deepened) in order to ensure continuity of supply. A potential action enabling a long-term blocking of imports may be the deliberate sinking of the vessel on the axis of the fairway (e.g. under the guise of an accident);
- according to the provisions of strategic documents showing the directions of development of the power system, offshore wind energy is to be one of the pillars (along with nuclear energy and gas as a transitional fuel)⁵⁷. Thus, the disruption of the electricity production chain becomes the main objective of the opponent of Poland and other countries on the Baltic Sea (introducing serious disruptions to the economies and societies of coastal states);
- The RF may attempt to intercept CI-related investments or block them at various stages of project implementation. In resolution P9_TA(2024)0079, the European Parliament pointed to Russian actions and operations aimed at infiltrating European democracies and EU institutions, the presence of a network of agents of influence who affect electoral processes and policies on key strategic issues such as energy infrastructure⁵⁸;

⁵⁶ HELCOM, *ensuring safe shipping in the Baltic*, Helsinki Commission – Baltic Marine Environment Protection Commission 2009, p. 3.

⁵⁷ *Energy Policy of Poland until 2040 (EPP2040)*, Warszawa 2022, Ministerstwo Klimatu i Środowiska (Eng. Ministry of Climate and Environment), p. 7.

⁵⁸ P9_TA(2024)0079 – *Russiagate: allegations of Russian interference in the democratic processes of the European Union – European Parliament resolution of 8 February 2024 on Russiagate: allegations of Russian interference in the democratic processes of the European Union (2024/2548(RSP))*.

- it can be expected that the military potential will be used more and more as a response to the escalation of the situation and the retaliatory nature of the actions of the antagonised parties, reminiscent of “Cold War” scenarios (attempts to physically push ships back in order to enforce their own interpretation of the regulations, helicopters hovering over enemy ships, blocking communication routes under the guise of exercises);
- non-state entities (organisations and movements of activists of various backgrounds), national minorities, criminal groups, used both for direct actions and attempts to test security procedures, cooperation of services, etc., may be involved in the activities;
- the actions taken will be accompanied by massive media attacks and shaping their own version of events (in the case of the RF, aimed at Russian society, in order to maintain the image of a “besieged fortress” and demonise the image of Russia by the West);
- hybrid threats in the Baltic region can be characterised by the use of modern technologies (autonomous platforms) as well as dual-use systems, to completely improvised means⁵⁹;
- with regards to objects of maritime CI, threats can also be created using objects of historical origin. According to the author, data on the location of dangerous chemical and conventional weapons deposits can be used to plan this type of activity. Estimates indicate the presence on the Baltic Sea of between 300 000 and 385 000 tons of conventional and chemical munitions deliberately sunk after World War II. A large number of wrecks with dangerous contents should be added to this ⁶⁰;
- threats may be generated during holiday periods, as was the case with the intersection of the EstLink 2 power line (Christmas 2024), of which the Chinese ship Yi Peng 3 was initially suspected⁶¹.

⁵⁹ R. Miętkiewicz, *Systemy autonomiczne (bezzałogowe) jako nowe narzędzie w rękach terrorystów...*, pp. 69–98.

⁶⁰ R. Miętkiewicz, *High explosive unexploded ordnance neutralization – Tallboy air bomb case study*, “Defence Technology” 2022, vol. 18, no. 3, pp. 524–535. <https://doi.org/10.1016/j.dt.2021.03.011>.

⁶¹ *Finland-Estonia power cable hit in latest Baltic Sea incident*, The Guardian, 25.12.2024, <https://www.theguardian.com/world/2024/dec/25/finland-estonia-power-cable-hit-in-latest-baltic-sea-incident> [accessed: 27.12.2024].

Measures to counter hybrid threats in the Baltic Sea

The nature of hybrid threats occurring and possible to appear in the Baltic Sea requires far-reaching consolidation of activities and cross-border cooperation between institutions (mainly armed forces, coast guards and intelligence) of coastal states. Secondly, it seems necessary to apply the achievements resulting from the development of modern technologies, with particular emphasis on maritime autonomous systems and elements of artificial intelligence. In order to effectively counteract incidents, it is necessary to take actions of a political nature (strategies, doctrines, common road maps of NATO members), legal (tools and legal regulations enabling the creation of solutions and law enforcement), military (presence of forces, exercises, multinational operations and initiatives), technological (directing scientific research, using available solutions to increase the level of protection) and building common data processing and exchange systems (common situational awareness, efficient command). Projects aimed at minimising hybrid threats to CI facilities at sea should include:

- conducting ongoing analyses of the level of security, taking into account identifying risks, estimating probabilities and impacts (risk matrices) and developing methods to mitigate them. This requires close cooperation between sectors (private investors) and state services, as well as the exchange of information between allies;
- conducting monitoring of communication routes in the Baltic Sea, to enable the detection and tracking of ships despite the AIS transponders being switched off, as well as vessels (mainly up to 20 m in length or displacement up to 150 tons) not covered by VTS (vessel traffic service) reporting systems. Due to the large spaces requiring supervision, it is recommended to use the space component (satellite pictures). In order to minimise costs and increase the efficiency of operations, the use of autonomous systems for monitoring (also hidden in the case of submarine infrastructure) should be indicated as expedient. Cooperation in this area is required at the level of the maritime security systems of the countries on the Baltic Sea;
- implementation of EU standards for the protection of CI (even though the management of CI is mainly the responsibility of the EU Member States). The primary documents in this regard include the Revised EU Maritime Security Strategy, whose selected fundamental aims are: improve the resilience of critical entities

and the security of networks and information systems and ensuring the resilience and protection of maritime CI⁶² and The Critical Entities Resilience Directive on reducing the vulnerability of critical entities and strengthening their physical resilience⁶³;

- the use of artificial intelligence methods enabling the selection of units (based on intelligence data, monitoring data on suspicious behaviour in the form of speed reduction, manoeuvring over CI, etc.), which will reduce the freedom of potential perpetrators to use high traffic volume to mask their activities. This type of action was taken by NATO in January 2025, when Joint Expeditionary Force, formed by 10 countries with the United Kingdom in lead, launched a reaction system (codenamed Nordic Warden) to track potential threats to undersea infrastructure and monitor the Russian shadow fleet. The system covers 22 areas of interest, including the Baltic Sea and the Baltic Straits. The warnings generated by the system will be transmitted to NATO members⁶⁴;
- maintaining the capacity of coastal states to respond immediately (within a few hours) to the sabotage and other dangerous events. The above requires the possession of qualified subunits maintained in an appropriate readiness regime, capable of quickly sub-seizing ships and recapturing CI objects at sea and at the interface of environments (seaports);
- support at the international level in the face of emerging events, showing the approval of the EU and uniform line of perception and response to incidents, as was the case with the events of December 2024 and the actions of the Finnish authorities related to the seizure of the vessel Eagle S⁶⁵;

⁶² Council conclusions on the Revised EU Maritime Security Strategy (EUMSS) and its Action Plan, Brussels 2023, Council of the European Union.

⁶³ 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.

⁶⁴ Joint Expeditionary Force activates UK-led reaction system to track threats to undersea infrastructure and monitor Russian shadow fleet, 6.01.2025, <https://www.gov.uk/government/news/joint-expeditionary-force-activates-uk-led-reaction-system-to-track-threats-to-undersea-infrastructure-and-monitor-russian-shadow-fleet> [accessed: 7.01.2025].

⁶⁵ Joint Statement by the European Commission and the High Representative on the Investigation into Damaged Electricity and Data Cables in the Baltic Sea, Brussels 2024, European Commission – Statement.

- strengthening cooperation between the armed forces and other entities responsible for maintaining security in sea basins and stakeholders of the energy industry (especially oil and gas as well as wind offshore) in order to build industry awareness of threats, vulnerabilities and increase resilience, as well as to understand the needs (e.g. expenditure on security systems). Sharing sensitive knowledge can be resented by the private sector;
- the adoption by the NATO countries on the Baltic Sea of an initiative similar to the declaration signed in 2024 by Belgium, the Netherlands, Germany, Norway, the United Kingdom and Denmark on the protection of underwater CI against attacks and acts of sabotage⁶⁶. Such activities are aimed at jointly implementing appropriate solutions, exchanging information and best practices to increase the level of protection and prevention⁶⁷;
- holistic approach to maritime CI risks, including both preventive and protective actions as well as the development of rapid infrastructure recovery (restoration) of infrastructure (cross-border reparability). Such measures should also take into account the mitigation of the effects of attacks on CI through planning alternative supply chains in advance (it took almost half a year to restore the operational efficiency of the Balticconnector). This means that the onus will continue to shift from protection to building resilience. Whereby it is important not only to prevent the occurrence of an adverse event, but also to be prepared to quickly minimise its impact (also by using the potential of foreign partners). International (EU, NATO) unified standards for assessing the resilience of CI should be used to implement such activities;
- development of *the maritime policing* initiative proposed by the Polish Prime Minister, which is to increase the presence of NATO naval forces and groups operating within the framework of bilateral and multinational initiatives of the countries on the Baltic Sea (e.g. on the basis of rotational command and declaration of forces for joint

⁶⁶ C. Chiappa, *6 countries move to protect the North Sea from Russians*, Politico, 9.04.2024, <https://www.politico.eu/article/6-european-countries-sign-pact-protect-critical-energy-infrastructure-north-sea-from-russia/> [accessed: 27.12.2024].

⁶⁷ *Joint Declaration on cooperation to secure critical subsea infrastructure*, Regjeringen, 9.04.2024, <https://www.regjeringen.no/en/aktuelt/joint-declaration-on-cooperation-to-secure-critical-subsea-infrastructure/id3033122/> [accessed: 27.12.2024].

operations). Such a solution will allow to minimise costs and at the same time increase the level of interoperability of forces, as well as build appropriate relationships (trust);

- continuous mapping and analysis of vulnerabilities and shortcomings of CI by its owners (often private entities) and strengthening cooperation between the EU and NATO. Some countries such as Norway or the United Kingdom are members of only one of these organisations;
- taking quick and effective action to minimise the challenges posed by the shadow fleet, which has a great potential to create hybrid threats to maritime CI (destroying undersea lines by dragging anchors, espionage, causing deliberate collisions, the threat of a large-scale environmental disaster and others). To this end, multilateral cooperation between EU countries and the International Maritime Organization, ship owners and insurers is necessary to promote the provisions of international law. These provisions are effective only if the majority of sea users apply to it.

Conclusions

Hybrid threats are a convergence of activities below the threshold of war carried out in many domains, covertly and directly (less frequently), but planned and coordinated using various means (political, military, economic, legal, social and other). Hybrid activities threaten the security of the functioning of the state and its citizens, and a wide range of means is used to create them, including both classic (disinformation) and modern (cyberattacks) tools. A special feature is the creeping, staggered and difficult to immediately diagnose nature of the threats, which additionally take various forms using the synergy effect⁶⁸. Taking into account the considerations contained above, it should be pointed out that the potential package of threats that can be generated by the RF and its related entities in relation to offshore CI facilities in the Baltic Sea is very broad. Taking into account the domain approach and the fact that in the coming

⁶⁸ Najwyższa Izba Kontroli (Eng. Supreme Audit Office), *Informacja o wynikach kontroli. Przygotowanie państwa na zagrożenia związane z działaniami hybrydowymi* (Eng. Information on the results of the audit. Preparing the state for the threats of hybrid activities), KPB.430.002.2023, Warszawa 2023, p. 7.

years numerous offshore facilities will be launched (mainly offshore wind farms, which in the case of the most advanced projects in 2025 will enter the physical construction phases on specific investment locations), cyber threats come to the fore (in addition to cyber-attacks, we are also talking about the generation of avatars of units and aircraft violating zones around CI, as well as disruption of satellite navigation systems) and underwater hazards (resulting in disruption of the functioning of CI on the seabed), and subsequently surface hazards. The purpose of such actions will be to directly disrupt the schedules of construction works, or to interrupt logistics chains by generating incidents involving the use of mine warfare elements (covert laying of sea mines, maritime improvised explosive devices), violation of prohibited zones by autonomous submarine units, submarines and sabotage groups (in order to conduct reconnaissance activities, lay sea mines, map the bottom, identify vulnerabilities weaknesses, etc.). Among the surface threats, the probable forms of action include dangerous manoeuvring in relation to installation vessels and service fleets carrying out complex operations, actions of vessels simulating technical problems (dragging anchors, drifting towards CI objects, intentional collisions, to deliberate sinking of vessels, e.g. shadow fleet). Civilian ships carrying out activities on behalf of Russia may be responsible for transporting sabotage groups, conducting reconnaissance activities, and deliberately causing disruptions to navigation and communication systems in the immediate vicinity of the investment in order to disrupt the work. In the event of further escalation of the situation, it should also be taken into account that threats will be generated by vessels disguised as ships of the state services of the countries on the Baltic Sea. It is also possible to use autonomous aerial platforms (according to the author, also operating from the decks of civilian ships) to create threats in relation to oil platforms and transformer stations (an element of the OWF). It should be assumed that autonomous platforms in the near future will range from hybrid systems (capable of changing the environment of operations) to biomimetic platforms resembling marine organisms. The development of artificial intelligence methods currently makes it possible to create swarms (in the case of underwater vehicles, it seems advisable to use the term: shoals) of unmanned platforms, the joint use of which allows for achieving synergy effect.

The analysis of hybrid threats indicate the growing importance of modern technology in the creation of these threats (increasingly perfect

platforms with constantly growing capabilities), especially in the underwater domain. With regard to the increasing capabilities in this domain, in terms of both attack, protection and defence, there is even talk of seabed warfare⁶⁹.

Bibliography

Bryjka F., Zając T., *Wzmocnienie ochrony infrastruktury krytycznej państw UE i NATO* (Eng. EU and NATO countries strengthen the protection of critical infrastructure), „Biuletyn PISM” 2023, no. 79.

Doğan D., Çetikli D., *Maritime Critical Infrastructure Protection (MCIP) in a Changing Security Environment*, Istanbul 2023, Maritime Security Centre of Excellence (MARSEC COE).

Dudzińska K., *Jądrowy zwrot w szwedzkiej polityce energetycznej* (Eng. Sweden Takes a Nuclear Turn in Energy Policy), „Biuletyn PISM” 2024, no. 58.

Dyner A.M., *Działania hybrydowe Rosji przeciw państwom NATO i UE* (Eng. Preparing for Russian hybrid activities against NATO and EU countries), „Biuletyn PISM” 2022, no. 183.

ENISA Threat Landscape 2024, July 2023 to June 2024, European Union Agency For Cybersecurity 2024. <https://doi.org/10.2824/0710888>.

HELCOM, ensuring safe shipping in the Baltic, Helsinki Commission – Baltic Marine Environment Protection Commission 2009.

Hybrid CoE Paper 16: Handbook on maritime hybrid threats: 15 scenarios and legal scans, The European Centre of Excellence for Countering Hybrid Threats 2023.

Kasprzyk R., *Sztuczna inteligencja i cyberprzestrzeń a proces złośliwego sterowania ludźmi i maszynami* (Eng. Artificial intelligence and cyberspace and the process of malicious control of humans and machines), in: *GlobState*, vol. 2. *Wyzwania dla Polski w kontekście zmian w środowisku bezpieczeństwa*, Ł. Jureńczyk, R. Reczkowski (sci. eds.), Bydgoszcz 2020, Centrum Doktryn i Szkolenia Sił Zbrojnych – Uniwersytet Kazimierza Wielkiego, pp. 277–298.

⁶⁹ N. Fridbertsson, *Protecting Critical Maritime Infrastructure – The Role of Technology. General Report*, NATO Parliamentary Assembly, Science and Technology Committee (STC) 2023, p. 1.

Kędzierski M., *Za wszelką cenę. Niemiecki zwrot ku LNG* (Eng. At all costs. Germany shifts to LNG), „Komentarze OSW” 2023, no. 510.

Mickiewicz P., *Bezpieczeństwo energetyczne czy bezpieczeństwo morskie? Dylemat oceny potencjalnych zagrożeń bezpieczeństwa Polski na akwenie Morza Bałtyckiego w trzeciej dekadzie XXI wieku* (Eng. Energy security or maritime security? The dilemma of assessing potential threats to Poland's security in the Baltic Sea area in the third decade of 21st century), „Nautologia” 2024, no. 161, pp. 71–76.

Miętkiewicz R., *Bałtyk jako obszar szczególnej ochrony* (Eng. The Baltic Sea as a special protection area), in: *Czy morze pomoże? Bałtyk a bezpieczeństwo energetyczne Polski*, Z. Nowak (ed.), Warszawa 2024, pp. 33–46.

Miętkiewicz R., *Dumped conventional warfare (munition) catalog of the Baltic Sea*, “Marine Environmental Research” 2020, vol. 161, p.105057. <https://doi.org/10.1016/j.marenvres.2020.105057>.

Miętkiewicz R., *High explosive unexploded ordnance neutralization – Tallboy air bomb case study*, “Defence Technology” 2022, vol. 18, no. 3, pp. 524–535. <https://doi.org/10.1016/j.dt.2021.03.011>.

Miętkiewicz R., *Morskie farmy wiatrowe a bezpieczeństwo morskie państwa* (Eng. Off-shore wind farms, new elements of maritime security), „Sprawy Międzynarodowe” 2019, vol. 72, no. 1, pp. 97–112. <https://doi.org/10.35757/SM.2019.72.1.06>.

Miętkiewicz R., *Obiekty morskiej infrastruktury energetycznej – próba określenia podatności na ataki platform bezzałogowych* (Eng. Offshore energy infrastructure facilities – an attempt to determine vulnerability to attacks by unmanned platforms), „Alcumena. Pismo Interdyscyplinarne” 2023, no. 3(15), pp. 205–225. <https://doi.org/10.34813/psc.3.2023.11>.

Miętkiewicz R., *Systemy autonomiczne (bezzałogowe) jako nowe narzędzie w rękach terrorystów* (Eng. Autonomous (unmanned) systems as a new tool in the hands of terrorists), in: *XX-lecie wojny z terroryzmem: bilans i konsekwencje*. Vol. 2. *Infrastruktura krytyczna – analizy – case study*, B. Wiśniewska-Paź, D. Szlachter (eds.), Toruń 2022, Wydawnictwo Adam Marszałek, pp. 69–98.

Miętkiewicz R., *Systemy autonomiczne w działaniach na morzu* (Eng. Autonomous systems in maritime operations), Gdynia 2023, Wydawnictwo AMW.

Nowak Z., Maj M., *Bałtyk jako przestrzeń strategicznej aktywności energetycznej* (Eng. The Baltic Sea as a space for strategic energy activities), in: *Czy morze pomoże? Bałtyk a bezpieczeństwo energetyczne Polski*, Z. Nowak (ed.), Warszawa 2024, Institute for Foreign Affairs, pp. 33–46.

Nowakowska-Krystman A., *Potencjał obronny Sił Zbrojnych RP w ujęciu relatywnym* (Eng. Defence potential of the Polish Armed Forces in relative terms), Warszawa 2018, Akademia Sztuki Wojennej.

Paszkowski M., *Litwa, Łotwa oraz Estonia planują stworzenie bałtyckiego hubu energetycznego* (Eng. Lithuania, Latvia and Estonia plan to create a Baltic Energy Hub), „Komentarze IES” 2024, no. 1259.

Piekarski M., *Ochrona infrastruktury krytycznej na polskich obszarach morskich w kontekście zagrożeń hybrydowych* (Eng. Protection of critical infrastructure in Polish maritime areas in the context of hybrid threats), PTBN expert opinions no. 1, Polskie Towarzystwo Bezpieczeństwa Narodowego (Eng. Polish Association for National Security) 2023.

Plan for Program Energy Island Bornholm, Danish Energy Agency, 2023, ID: ENØ-FOR-115.

Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure, Cybersecurity and Infrastructure Security Agency 2024, ID: AA24-249A.

Ruszel M., Ogarek P., *Bezpieczeństwo paliwowe Polski w kontekście zmian właścicielskich na rynku logistyki produktów naftowych oraz remedies Komisji Europejskiej w sprawie fuzji PKN ORLEN i Grupy LOTOS. Polska u progu embargo na produkty naftowe z Rosji - analiza otwierająca 2023 rok* (Eng. Poland's fuel security in the context of ownership changes in the petroleum products logistics market and the European Commission's remedies on the merger between PKN ORLEN and LOTOS Group. Poland at the threshold of the embargo on petroleum products from Russia – opening analysis 2023), IPE analysis no. 1, Instytut Polityki Energetycznej (Eng. Institute for Energy Policy) 2023.

Wojtasik K., *Analiza wyników badań na temat percepcji zagrożeń o charakterze terrorystycznym wśród uczestników EU PSA* (Eng. Results of the survey on the perception of terrorist threats among EU PSA participants), PTBN analyses no. 1, Polskie Towarzystwo Bezpieczeństwa Narodowego (Eng. Polish Association for National Security) 2023.

Internet sources

Aliyev N., *Does Russia want to revise its water border with the Nordic and Baltic states?*, International Centre for Defence and Security, 15.08.2024, <https://icds.ee/en/does-russia-want-to-revise-its-water-border-with-the-nordic-and-baltic-states/> [accessed: 16.12.2024].

Braw E., *Russia's growing dark fleet: Risks for the global maritime order*, Atlantic Council, 11.01.2024, <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/russias-growing-dark-fleet-risks-for-the-global-maritime-order/> [accessed: 29.04.2024].

Bulski K., *The Role of the New European Commission and Regional Cooperation in Accelerating Offshore Wind in the Baltic Sea*, BalticWind.EU, 11.09.2024, <https://balticwind.eu/the-role-of-the-new-european-commission-and-regional-cooperation-in-accelerating-offshore-wind-in-the-baltic-sea/> [accessed: 7.11.2024].

Chiappa C., *6 countries move to protect the North Sea from Russians*, Politico, 9.04.2024, <https://www.politico.eu/article/6-european-countries-sign-pact-protect-critical-energy-infrastructure-north-sea-from-russia/> [accessed: 27.12.2024].

Chiriac O., *The 2022 Maritime Doctrine of the Russian Federation: Mobilization, Maritime Law, and Socio-Economic Warfare*, Center for International Maritime Security, 28.11.2022, <https://cimsec.org/the-2022-maritime-doctrine-of-the-russian-federation-mobilization-maritime-law-and-socio-economic-warfare/> [accessed: 7.12.2024].

Finland-Estonia power cable hit in latest Baltic Sea incident, The Guardian, 25.12.2024, <https://www.theguardian.com/world/2024/dec/25/finland-estonia-power-cable-hit-in-latest-baltic-sea-incident> [accessed: 27.12.2024].

Finlandia: Władze nie potwierdzają informacji o „przypadkowym” uszkodzeniu Balticconnector (Eng. Finland: Authorities do not confirm information on “accidental” damage to Balticconnector), Portal Morski, 13.08.2024, <https://www.portalmorski.pl/offshore/56252-finlandia-wladze-nie-potwierdzaja-informacji-o-przypadkowym-uszkodzeniu-balticconnector> [accessed: 29.01.2025].

Frankowski P., *Bałtyckie TOP10* (Eng. Baltic TOP10), Namiary na Morze i Handel, 9.05.2024, <https://www.namiary.pl/2024/05/09/baltyckie-top10/> [accessed: 3.01.2025].

Fraszka B., *Państwa bałtyckie a rosyjskie zagrożenia hybrydowe* (Eng. Baltic States vs. Russian Hybrid Threats), Warsaw Institute, <https://warsawinstitute.org/wp-content/uploads/2020/10/Pa%C5%84stwa-ba%C5%82tyckie-a-rosyjskie-zagro%C5%B4Cenia-hybrydowe-Bartosz-Fraszka.pdf> [accessed: 29.12.2024].

Government adopts resolution on hydrogen – Finland could produce 10% of EU's green hydrogen in 2030, Ministry of Economic Affairs and Employment, 9.02.2023, <https://valtioneuvosto.fi/en/-/1410877/government-adopts-resolution-on-hydrogen-finland-could-produce-10-of-eu-s-green-hydrogen-in-2030> [accessed: 9.11.2024].

Hagelstam A., *Cooperating to counter hybrid threats*, NATO Review, 23.11.2018, <https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html> [accessed: 2.12.2024].

Hybrid threats as a concept, Frequently asked questions on hybrid threats, The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/> [accessed: 2.12.2024].

Hyndle-Hussein J., *The Balticconnector gas pipeline damage*, Ośrodek Studiów Wschodnich, 11.10.2023, <https://www.osw.waw.pl/en/publikacje/analyses/2023-10-11/balticconnector-gas-pipeline-damage> [accessed: 2.01.2025].

Joint Expeditionary Force activates UK-led reaction system to track threats to under-sea infrastructure and monitor Russian shadow fleet, 6.01.2025, <https://www.gov.uk/government/news/joint-expeditionary-force-activates-uk-led-reaction-system-to-track-threats-to-undersea-infrastructure-and-monitor-russian-shadow-fleet> [accessed: 7.01.2025].

Nordycko-Baltycki Korytarz Wodorowy (Eng. Nordic-Baltic Hydrogen Corridor) (2024), <https://www.gaz-system.pl/pl/rynek-wodoru/projekty/nordycko-baltycki-korytarz-wodorowy.html> [accessed: 3.01.2025].

Russia's 'shadow fleet': Bringing the threat to light, European Parliament, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766242/EPRS_BRI\(2024\)766242_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766242/EPRS_BRI(2024)766242_EN.pdf) [accessed: 23.01.2025].

Russia's Shadow Fleet Tankers Could Get Naval Escorts, The Maritime Executive, 18.12.2024, <https://maritime-executive.com/article/russia-s-shadow-fleet-tankers-could-get-naval-escorts> [accessed: 9.01.2025].

Westgaard W., *The Baltic Sea Region: A Laboratory for Overcoming European Security Challenges*, Carnegie Endowment for International Peace, 21.12.2023, <https://carnegieendowment.org/research/2023/12/the-baltic-sea-region-a-laboratory-for-overcoming-european-security-challenges?lang=en> [accessed: 7.12.2024].

Wróbel P., *Analiza: Inicjatywy UE wzmacniające współpracę regionalną na rzecz morskiej energetyki wiatrowej na Bałtyku* (Eng. Analysis: Review of EU initiatives to strengthen regional cooperation for offshore wind in the Baltic Sea), BalticWind.EU, 4.06.2024, <https://balticwind.eu/pl/analiza-inicjatywy-ue-wzmacniajace-wspolprace-regionalna-na-rzecz-morskiej-energetyki-wiatrowej-na-baltyku/> [accessed: 9.11.2024].

Wyszyński Ł., Wyszyński: *Wejście Szwecji do NATO rodzi korzyści, ale i wyzwania* (rozmowa) (Eng. Wyszyński: Sweden's entry into NATO brings benefits but also challenges (interview)), Biznes Alert, 5.03.2024, <https://biznesalert.pl/szwecja-nato-zalety-wady-rosja-morze-baltyckie-bezpieczenstwo/> [accessed: 7.10.2024].

Legal acts

P9_TA(2024)0079 – *Russiagate: allegations of Russian interference in the democratic processes of the European Union – European Parliament resolution of 8 February 2024 on Russiagate: allegations of Russian interference in the democratic processes of the European Union (2024/2548(RSP))* – (Official Journal of the EU C/2024/6343 of 7.11.2024).

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).

Other documents

Council conclusions on the Revised EU Maritime Security Strategy (EUMSS) and its Action Plan, Brussels 2023, Council of the European Union.

Energy Policy of Poland until 2040 (EPP2040), Warszawa 2022, Ministerstwo Klimatu i Środowiska (Eng. Ministry of Climate and Environment).

Fridbertsson N., *General Report – Protecting Critical Maritime Infrastructure – The Role of Technology*, NATO Parliamentary Assembly 2023, Science and Technology Committee (STC).

Joint Declaration on cooperation to secure critical subsea infrastructure, Regjeringen, 9.04.2024, <https://www.regjeringen.no/en/aktuelt/joint-declaration-on-cooperation-to-secure-critical-subsea-infrastructure/id3033122/> [accessed: 27.12.2024].

Joint Statement by the European Commission and the High Representative on the Investigation into Damaged Electricity and Data Cables in the Baltic Sea, Brussels 2024, European Commission – Statement.

Maritime Doctrine of the Russian Federation, A. Davis, R. Vest (trans.), Newport 2022, Russia Maritime Studies Institute, United States Naval War College.

McGrath S., *Spotlight on the Shadow War: Inside Russia's Attacks on NATO Territory. A Report by the U.S. Helsinki Commission Staff*, 2024.

Najwyższa Izba Kontroli (Eng. Supreme Audit Office), *Informacja o wynikach kontroli. Przygotowanie państwa na zagrożenia związane z działaniami hybrydowymi* (Eng. Information on the results of the audit. Preparing the state for the threats of hybrid activities), KPB.430.002.2023, Warszawa 2023.

Najwyższa Izba Kontroli (Eng. Supreme Audit Office), *Informacja o wynikach kontroli. Realizacja działań w zakresie poprawy bezpieczeństwa paliwowego w sektorze naftowym* (Eng. Information on the results of the audit. Implementation of measures to improve fuel security in the oil sector), KGP.430.7.2023, Warszawa 2023.

National Security Strategy of the Republic of Poland, Warszawa 2020.

REPowerEU Plan. Communication from the Commission to the European Parliament, the European Council, the Council, The European Economic and Social Committee and the Committee of the Regions, COM(2022) 230 final, Brussels 2022.

Poland's Strategic Concept for Maritime Security, Warszawa-Gdynia 2017, Biuro Bezpieczeństwa Narodowego (Eng. National Security Bureau).

Study on Baltic offshore wind energy cooperation under BEMIP. Final report, ENER/C1/2018-456, Luxembourg 2019, Publications Office of the European Union.

Commander Rafał Miętkiewicz, Associate Professor

Professor at the Polish Naval Academy of the Heroes of Westerplatte in Gdynia. Associate professor in social sciences in the field of security sciences. Graduate of the Polish Naval Academy and Gdynia Maritime Academy (postgraduate studies in crisis management). Expert of the Ignacy Łukasiewicz Institute for Energy Policy in Rzeszów, member of the Polish National Security Association and the Polish Nautological Society. Line officer with several years of experience on board naval mine warfare ships, former commander of ORP "Śniardwy"(645). Academic lecturer in military studies, courses and postgraduate studies (Gdańsk University of Technology, University of Gdańsk) and MBA (Collegium Civitas in Warsaw). Author and co-author of several monographs, academic textbooks and dozens of articles, reports and analyses. Commentator publishing on industry portals (Portal Stoczniovy, Biznes Alert, Baltic Wind EU, Polon). Member of Erasmus+ Programme, European and national research programmes (DAIMON, EU Interreg South Baltic, SABUVIS,

SWAT-SHOAL). His research interests include the use of modern autonomous (unmanned) technologies in maritime operations. His research addresses, inter alia, national maritime security, energy security, with particular emphasis on the supply of strategic raw materials, and the security of critical infrastructure in Polish maritime areas.

Contact: r.mietkiewicz@amw.gdynia.pl

Terrorist and sabotage attacks on selected critical infrastructure systems – a historical perspective

KRZYSZTOF IZAK

Independent author

 <https://orcid.org/0000-0001-9815-6035>

Abstract

The article describes terrorist and sabotage attacks carried out worldwide against two major critical infrastructure (CI) systems: energy supply and public transport. The selection of the events described in the article was subjective. In the section on attacks on the energy sector, the author adopted a geographical division – Middle East, Africa and South America. In the section on attacks on public transport, the division includes land transport and air transport. In the case of terrorist attacks on rail infrastructure, the author mainly used Anneli Botha's study covering data from 2000 to 2017 and the work of Brian M. Jenkins and Bruce R. Butterworth, and for air transport, the work of Jacques Duchesneau. Not all data on attacks on CI systems has been updated due to the fact that the information contained in the sources is partial. The author draws the conclusion that with the development of modern technology and the escalation of tensions in international relations, the level of threat to CI will increase.

Keywords

terrorist attacks, energy, critical infrastructure, transport, sabotage

Introduction

Terrorist and sabotage attacks on critical infrastructure (CI) facilities are one of the most serious threats to state security. They often have far-reaching consequences, as the destruction or damage to one CI facility can negatively affect the functioning of others. The development of CI is an essential component of a modern economy. The driving force behind this economy is, among other things, the dynamic development of modern information and communications technology (ICT). The challenge is to ensure the security of systems based on these technologies, including CI systems.

Frequent attacks on oil pipelines, power lines, telecommunications networks and other CI facilities prompted the UN Security Council in 2017 to adopt Resolution 2341 on protecting CI from terrorist attacks¹. The following year, the United Nations Office of Counter-Terrorism (UNOCT) and the United Nations Counter-Terrorism Committee Executive Directorate (UNCTED) produced the first compendium of good practices for protecting CI from terrorist attacks². In 2008, the European Union adopted Directive 2008/114/EC, which established an EU-wide procedure for the identification and designation of European Critical Infrastructures, and identified actions to improve their protection³. This document was repealed by Directive 2022/2557 of the EU Parliament and of the Council, adopted in December 2022, introducing additional measures to protect CI⁴. The directive entered into force on 16 January 2023. On 25 July 2023, the European Commission approved a list of 11 sectors covered by the Critical Entities Resilience (CER) Directive. These are CI sectors that provide essential services in maintaining important elements of the social system, supporting the economy, ensuring public health and safety as well

¹ United Nations, *Security Council resolution 2341 (2017) [on protection of critical infrastructure against terrorist acts]*.

² UNOCT, UNCTED, Interpol, *The protection of critical infrastructure against terrorist attacks. Compendium of good practices*, https://www.un.org/securitycouncil/ctc/sites/www.un.org/securitycouncil.ctc/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf [accessed: 12.12.2024].

³ Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

⁴ 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.

as protecting the environment⁵. Such legislative measures are likely to have real benefits in terms of reducing the level of terrorist and sabotage threats only within a few years after their provisions have been implemented by CI operators.

Currently, few areas of human life and high-tech civilisation remain outside CI systems. These are primarily tourism, culture, spirituality, domestic commerce and related infrastructure (large shopping malls do not count as CI). Bazaars, temples, tourists in hotels, on beaches and in museums continue to be excellent targets for terrorists, mainly in Africa and Asia. The attacks they perpetrate have sometimes caused many deaths, but with few exceptions have not affected the economy of the country. In Egypt, these exceptions were the terrorist campaign by Muslim extremists in the 1990s and the ISIS attacks in the 21st century. As a result of these, the number of tourists visiting the country decreased significantly, which translated into a decrease in national income and the need to increase the number of police officers needed to protect tourists. For these reasons, tourism infrastructure in Egypt is treated as CI.

The purpose of this article was to analyse statistical data on terrorist and sabotage attacks worldwide targeting two CI systems – the energy sector and public transport – together with a brief description of selected incidents. The selection was subjective in nature. The author has refrained from citing definitions of CI due to the limitations of the volume of the text and the analysis of this issue in many other publications. In the case of terrorist attacks on railway infrastructure, the article mainly uses data from the work of Anneli Botha⁶ and the publications of Brian M. Jenkins and Bruce R. Butterworth⁷, and with regard to air transport, from the work of Jacques Duchesneau⁸. As the statistics presented in the first and second

⁵ European Commission, *Enhancing EU resilience: A step forward to identify critical entities for key sectors*, https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_23_3992/IP_23_3992_EN.pdf [accessed: 12.12.2024].

⁶ A. Botha, *Prevention of Terrorist Attacks on Critical Infrastructure*, in: *Handbook of Terrorism Prevention and Preparedness*, A.P. Schmid (ed.), https://icct.nl/sites/default/files/2023-01/Handbook_Schmid_2020.pdf, pp. 841–870 [accessed: 20.11.2024].

⁷ B.M. Jenkins, B.R. Butterworth, *Train Wrecks and Track Attacks: An Analysis of Attempts by Terrorists and Other Extremists to Derail Trains or Disrupt Rail Transportation*, https://transweb.sjsu.edu/sites/default/files/1794_Jenkins_Train-Wrecks-Train-Attacks.pdf [accessed: 3.12.2024].

⁸ J. Duchesneau, *Aviation Terrorism. Thwarting High-Impact Low-Probability Attacks*, Royal Military College of Canada 2015, <https://espace.rmc.ca/jspui/bitstream/11264/741/1/>

publications end with 2017 and in the third with 2011, the author attempted to update them on the basis of other sources. However, the information they contained was partial. In the section on attacks on the energy sector, the author adopted a geographical division – Middle East, Africa and South America – and in the section on public transport, a division between land and air transport. For air transport, incidents were grouped as follows: hijackings, bombings, suicide terrorism, attacks on airports and grounded aircraft, as well as attacks from the ground on aircraft in the air.

Energy sector

In every country, the energy sector is the main link of CI, as without energy the other sectors cannot function efficiently. Between 2000 and 2009, there were 565 terrorist attacks on energy, energy commodity and fuel supply facilities worldwide, and as many as 1745 between 2010 and 2017, a threefold increase in the number of such incidents. Explosives were used in 88% of cases, and arson in 9%. The highest number of attacks was recorded in two years: in 2014 – 347 and in 2015 – 390⁹. In 2003, attacks on power plants, gas and oil network facilities accounted for 25% of all terrorist attacks worldwide. By 2005, this had risen to 35%. In 2016, terrorist attacks targeting the oil and gas industry increased by 14% from the previous year and accounted for almost 42% of the total number of such incidents. These figures also include other criminal activities, including the theft of oil or gas from pipelines, extortion or the sale of raw materials to finance terrorist groups, among others¹⁰.

The energy sector is particularly at risk in areas of insurgency or warfare. An example is Ukraine, whose energy infrastructure is constantly under attack. The war taking place in the country resulted in the sabotage action of blowing up the Nord Stream 1 and Nord Stream 2 gas pipelines

Duchesneau%20PhD%20Thesis%2020150726%20Final%20e-Space%20RMC.pdf [accessed: 6.12.2024].

⁹ A. Botha, *Prevention of Terrorist Attacks...*, pp. 855–856.

¹⁰ A. Olech, *Terrorist Threats to the Energy Sector in Africa and the Middle East*, in: S.J. Lohman et al., *Countering Terrorism on Tomorrow's Battlefield: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 2)*, <https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1953&context=monographs>, p. 166 [accessed: 15.12.2024].

carrying gas from northern Russia to Germany on 26 September 2022¹¹. This event was a symbolic end to Europe's access to cheap energy. The existing strategy of sourcing it from oil, coal and gas deposits in Russia and other countries in the region cannot be continued for political and economic reasons. On the other hand, the continuity of supply from the Gulf countries via the Red Sea and the Suez Canal is threatened by the Shiite rebellion of the Yemeni Houthi movement, also known as the Supporters of Allah (Arabic: Ansar Allah), and earlier by acts of piracy in the Gulf of Aden and the Indian Ocean by Somali bandits supported by the Young Mujahideen Movement (Arabic: Harakat al-Shabab al-Mujahidin).

The energy sector, like other CI systems, is also at risk from cyber attacks. One of the most devastating was carried out in August 2012 using the Shamoon virus. The target was the Saudi oil and chemical company Saudi Aramco. The virus infected 10 000 computers at the company and shut down all important internal networks for almost a month. It was recognised that the attackers were not looking to take over data, but to eliminate as many systems as possible. After the incident, the corporation isolated its electronic systems from the outside world. Five years later, Aramco was attacked again, this time using a new version of malware – Shamoon 2.0 – with the aim of deleting data and causing explosions and fatalities. These cyber attacks, demonstrating how serious the effects of hackers can be, heightened concerns about the security of energy facilities around the world¹². The hacking attack in May 2021 on the computer system controlling the operation of the Colonial Pipeline oil pipeline in the US had severe consequences. There was a six-day disruption in oil supply, which triggered public panic and a massive buyout of propellants¹³. In November 2023, the internal computer network of Canadian company Trans-Northern Pipelines Inc., whose pipeline network connects, among other things, refineries to airports, was attacked. This caused delays in the exchange

¹¹ P. Oltermann, P. Beaumont, D. Sabbagh, *European leaders blame sabotage as gas pours into Baltic from Nord Stream pipelines*, The Guardian, 28.09.2022, <https://www.theguardian.com/business/2022/sep/27/nord-stream-1-2-pipelines-leak-baltic-sabotage-fears> [accessed: 28.12.2024].

¹² A. Olech, *Terrorist Threats...*, p. 168.

¹³ Ł. Kielban, *Zagrożenia Infrastruktury Krytycznej – podstawy dla urzędników i przedsiębiorców* (Eng. Critical Infrastructure Threats – basics for officials and businesses), Polska Platforma Bezpieczeństwa Wewnętrznego, 13.06.2024, <https://ppbw.pl/zagrozenia-infrastruktury-krytycznej-podstawy/> [accessed: 13.12.2024].

of files and the generation of reports on engineering assessments of pipelines and related facilities, but without material damage¹⁴.

Power plants and the lines that feed them are also targets of diversionary-terrorist attacks. In the North Caucasus, this phenomenon has emerged relatively recently. In 2009, one of the jamaats of the Caucasus Emirate took responsibility for a malfunction at the Sayano-Shushenskaya hydroelectric power station in Siberia (an official investigation ruled out a terrorist attack). Earlier, the leader of the Caucasus Emirate, Doku Umarov, had threatened a diversionary war directed against the energy infrastructure deep inside Russia. In the republic of Kabardino-Balkaria, terrorists blew up structures supporting power lines on 22 October 2008. In Ingushetia, high-voltage power lines were attacked three times in September 2009. The first attack, which involved blowing up a high-voltage pole, caused losses of more than 5 million roubles¹⁵. The first successful attack on a strategically important target occurred in the North Caucasus on 21 July 2010. A group of militants sabotaged the Baksan Hydroelectric Power Station in Kabardino-Balkaria. Guards were killed, civilian workers were tortured and explosives were planted. The explosions destroyed 2 of the 3 generators and caused a fire. Losses were estimated at 800 million roubles. On 7 September 2010, a fire broke out at the Irganay Hydroelectric Power Plant in Dagestan. During its extinguishment, explosive charges and a booby-trapped mine were discovered. Dagestan's Jamaat Guraba claimed responsibility for the sabotage and reported that a total of 9 charges had been planted at the power station. Two bombs consisting of TNT cubes, plastic and aluminium dust were found during the refurbishment in February 2011. There is no information on the location of the other charges¹⁶.

There have been a number of airspace violations over nuclear sites in France in the second decade of the 21st century, but the link between these incidents and terrorist activity has not been confirmed. French law prohibits flights within 5 km of a nuclear site and at altitudes below

¹⁴ A. Ribeiro, *Cyber attacks continue to hit critical infrastructure, exposing vulnerabilities in oil, water, healthcare sectors*, Industrial Cyber, 14.02.2024, <https://industrialcyber.co/critical-infrastructure/cyber-attacks-continue-to-hit-critical-infrastructure-exposing-vulnerabilities-in-oil-water-healthcare-sectors/> [accessed: 14.12.2024].

¹⁵ T.W. Grabowski, *Terroryzm północnokaukaski. Źródła, przejawy i przeciwdziałanie zjawisku* (Eng. North Caucasus terrorism. Sources, manifestations and countering the phenomenon), Kraków 2017, p. 272.

¹⁶ Ibid., pp. 272–273.

1000 m. Breach of this ban is punishable by a EUR 75 000 fine and 1 year's imprisonment. In October and November 2014, almost 30 unmanned aerial vehicles (UAVs) were reported flying over 15 nuclear power plants in France. The aim of the provocation was to disrupt the control and security system of these facilities. Initially, it was suspected that the perpetrators were opponents of nuclear power, who were trying to draw attention in this way to the inadequate – in their view – level of security of such plants. Greenpeace denied any connection to the incidents and called them very worrying. In early January 2015, 2 drones appeared over a nuclear power plant in Nogent-sur-Seine in northern France¹⁷. Despite the introduction of systems to detect UAVs, there have been further incidents involving them. In November 2021, Greenpeace members crashed a Superman-shaped drone into the concrete cover of the reactor of the Bugey nuclear power plant in France. The incident did not jeopardise the safety of the reactor, but showed that UAVs can have very unusual shapes, making them difficult to detect¹⁸. In October 2023, drones flew over 7 nuclear power plants in France, and on 1 August 2024, they flew over 6 such facilities¹⁹.

Middle East

Between 1918 and 1939, the first cases of attacks on oil pipelines in the Middle East were recorded. During the anti-Jewish and anti-British uprising in Palestine between 1936 and 1939, the pipeline that carried oil from Iraq to Haifa became the target of sabotage actions²⁰. In 1970, Palestinian organisations with bases in Jordan demanded that King Hussein dismantle

¹⁷ *Au total, 17 sites nucléaires ont été survolés par des drones depuis octobre*, Le Monde, 29.01.2015, https://www.lemonde.fr/planete/article/2015/01/29/dix-sept-sites-nucleaires-ont-ete-survoles-par-des-drones-depuis-octobre_4565967_3244.html [accessed: 29.01.2025]; AFP, *Deux drones ont survolé la centrale nucléaire de Nogent-sur-Seine*, BFMTV, 4.01.2015, https://www.bfmtv.com/police-justice/deux-drones-ont-survole-la-centrale-nucleaire-de-nogent-sur-seine_AN-201501040009.html [accessed: 4.01.2025].

¹⁸ J. Łukasiewicz, *Unmanned aerial vehicles as a source of threats to the states' electricity supply infrastructure and the proposed methods of protecting this infrastructure*, "Terrorism – Studies, Analyses, Prevention" 2022, no. 1. <https://doi.org/10.4467/27204383TER.22.012.15428>.

¹⁹ *De nouvelles centrales nucléaires survolées par de présumés drones*, TF1Info, 2.08.2024, <https://www.tf1info.fr/societe/de-nouvelles-centrales-nucleaires-survoles-par-de-presumes-drones-1562592.html> [accessed: 2.08.2024].

²⁰ K. Gebert, *Pokój z widokiem na wojnę. Historia Izraela* (Eng. Peace with a view to war. Israel's history), Warszawa 2023, p. 122.

the Jordanian part of this pipeline. When he refused, the Palestinians tried to blow up the facility²¹.

After US forces entered Iraq in 2003, the oil pipelines were repeatedly targeted by the rebels and later by ISIS. In 2014 in Syria, ISIS gained control of the pipeline and sold the seized oil to Turkey²². In the same year, ISIS took control of the Iraqi city of Baiji, where the country's largest oil refinery is located. This caused the most powerful crisis in Iraq since the Americans left in December 2011 and local elites took over. The refinery in Baiji, to which pipelines from all Iraqi oil fields lead, supplied 11 of Iraq's 18 provinces with refined products. The jihadists failed to get it up and running. In November 2014, the facility was recaptured by the Iraqi military with US air support. On 13 June 2015, jihadists carried out a suicide bombing at the site. The perpetrators drove a car filled with explosives into the refinery. At the time, 11 people were killed and 27 injured²³.

Gas and oil pipelines are also being targeted by Arab separatists in the south-west of Iran. In February 2024, two gas pipelines were targeted for sabotage. Tehran indirectly accused Israel of this²⁴. A number of terrorist attacks have targeted the gas pipeline that runs through the northern part of the Sinai Peninsula, through which Egypt supplies gas to Israel. In July 2010, Bedouins attempted to blow it up as part of a protest against the government in Cairo. Another attack occurred in February 2011. As a result of the Arab Spring in Egypt, the organisation Supporters of Jerusalem (Arabic: Ansar Bait al-Maqdis) was formed. By the end of 2013, it had attacked this pipeline 13 times²⁵. In November 2014, the Supporters of Jerusalem assumed ISIS authority and continued attacks as the Sinai Province (Wilayat Sinai). It became a target dozens of times

²¹ A. Chiczkina, *Jordania: zamach stanu w odwrotnej kolejności* (Eng. Jordan: coup d'état in reverse), TopWar, 12.04.2021, <https://pl.topwar.ru/181817-iordaniya-perevorot-naoborot.html> [accessed: 12.12.2024].

²² D. Butter, *Does Turkey really get its oil from Islamic State?*, BBC, 1.12.2015, <https://www.bbc.com/news/world-europe-34973181> [accessed: 1.12.2025].

²³ O. Wasiuta, S. Wasiuta, P. Mazur, *Państwo Islamskie ISIS. Nowa twarz ekstremizmu* (Eng. Islamic State ISIS. The new face of extremism), Warszawa 2018, p. 205.

²⁴ *Iran condemns 'terrorist' attack on gas pipelines*, AlJazeera, 14.02.2024, <https://www.aljazeera.com/news/2024/2/14/iranian-gas-pipeline-blasts-due-to-terrorism-and-sabotage-official-says> [accessed: 14.12.2024].

²⁵ D. Barnett, *Ansar Jerusalem claims responsibility for recent Sinai gas pipeline attack*, FDD's Long War Journal, 19.01.2014, https://www.longwarjournal.org/archives/2014/01/ansar-jerusalem-claims_respons.php [accessed: 19.01.2025].

between 2011 and the end of 2015. Terrorists blew up its small sections, resulting in disruptions to Israel's gas supply and significant material damage²⁶.

For the first time, an oil industry hub in Saudi Arabia was attacked on 1 May 2004. The attack on the refinery in Yanbu on the Red Sea was carried out by 4 attackers. At the time, 6 people were killed in the attack – 5 Western employees of the company and a Saudi security officer²⁷. On 29 May 2004, Al-Qaeda attacked oil installations and a settlement for foreigners working on them in Al-Khobar, in eastern Saudi Arabia. As a result, 22 people were killed, including 19 foreigners²⁸.

For several years, petrochemical industry installations in Saudi Arabia have been targeted by the aforementioned Houthi movement. In July 2017, the rebels first attacked oil installations in the port of Yanbu with a missile. The missile did not reach its target²⁹. In the years that followed, the Houthis continued to shell Saudi airports and petrochemical facilities using missiles and drones. A precision attack by more than 20 drones and cruise missiles damaged Aramco's Abqaiq and Khurais oil facilities on 14 September 2019. As a result of the damage, Saudi Arabia's oil production was halved, causing a brief 20% jump in oil prices. The Houthi movement took responsibility for the attack and cited Arab intervention in Yemen as the cause. Saudi Arabia, on the other hand, accused Iran of the attack. Tehran rejected the allegations, supported the Houthi version and threatened US forces in the Gulf. The US was seen as the guarantor of uninterrupted oil exports from the Gulf. The US Navy guarded the shipping lanes not only in this body of water, but also in the rest of the Arabian Sea. However, the share of oil from this region in US imports has declined to 16%. Most of the oil produced (80%) flowed to Asia (as of 2019)³⁰. Between January 2018 and the end of 2021, the Houthis

²⁶ AFP, *Des djihadistes revendiquent l'attaque d'un gazoduc*, 20 Minutes, 8.01.2016, <https://www.20min.ch/fr/story/des-djihadistes-revendiquent-l-attaque-d-un-gazoduc-826827705429> [accessed: 9.01.2025].

²⁷ M. Scheuer, S. Ulph, J.C.K. Daly, *Saudi Arabian Oil Facilities: The Achilles Heel of the Western Economy*, The Jamestown Foundation 2006, <https://jamestown.org/wp-content/uploads/2006/05/Jamestown-SaudiOil.pdf>, p. 43 [accessed: 24.02.2025].

²⁸ K. Izak, *Leksykon organizacji i ruchów islamistycznych* (Eng. Lexicon of Islamist organisations and movements), Warszawa 2014, p. 322.

²⁹ *Atak rakietowy na Rijad* (Eng. Rocket attack on Riyadh), Defence24, 5.11.2017, <https://defence24.pl/atak-rakietowy-na-rijad> [accessed: 5.11.2024].

³⁰ M.A. Piotrowski, *Taktyka oraz konsekwencje strategiczne ataku na instalacje naftowe Arabii Saudyjskiej* (Eng. The tactics and strategic consequences of the attack on oil installations

launched 430 ballistic missiles and 850 drones towards Saudi Arabia. In 2021, they carried out an average of 78 attacks targeting the country per month, compared to an average of 38 in 2020³¹. In 2023, the Houthis began to intensively attack ships passing off the Yemeni coast with rockets and drones. In January 2024, major ship owners stopped shipping through the Red Sea. Oil companies BP and Shell also did so. The situation became so serious that China began to put pressure on Iran to stop Houthi attacks³².

Africa

More than 30 armed terrorists belonging to the organisation Signed-in-Blood Battalion (Arabic: Muwakaum bi ad-Dima), also known as the Masked Men Brigade (Arabic: Katibat al-Mulassamin), attacked an Algerian gas liquefaction base in Tiguentourine, near the Saharan town of In Amenas, on 16 January 2013. The facility belonged to a consortium including the UK's BP, Norway's Statoil and the Algerian state-owned company Sonatrach. There were more than 800 workers at the site, including 137 foreigners. After 4 days of siege and an assault by an Algerian special unit, the hostages were freed. The attack left 38 dead and 29 terrorists were also killed³³.

In the 1990s, in south-eastern Nigeria, armed gangs carried out uncoordinated attacks on oil company workers and property, and on security force officers protecting oil infrastructure. Some of these groups united to form the Movement for the Emancipation of the Niger Delta (MEND). MEND extorted oil companies and carried out oil theft and smuggling. The companies estimated that losses amounted to 9 million

in Saudi Arabia), „Biuletyn PISM” 2019, no. 137, https://www.pism.pl/publications/The_Tactics_and_Strategic_Consequences_of_the_Attack_on_Oil_Installations_in_Saudi_Arabia [accessed: 4.12.2024].

³¹ *Atak rakietowy na Arabię Saudyjską i naloty w Jemenie* (Eng. Missile attack on Saudi Arabia and airstrikes in Yemen), Defence24, 27.12.2024, <https://defence24.pl/geopolityka/arabia-saudyjska-przeprowadza-naloty-huti-w-jemenie-za-atak-na-miasto-jazan> [accessed: 27.12.2024].

³² J. Losik, *Wiadomo, co przewoził zaatakowany statek. Powód do niepokoju dla Moskwy* (Eng. It is known what the attacked ship was carrying. A cause for concern for Moscow), Money.pl, 27.01.2024, <https://www.money.pl/gospodarka/nieoczekiwany-cios-w-handel-rosyjskim-paliwem-zaplona-tankowiec-6989192670440384a.html> [accessed: 27.01.2025].

³³ T. Kijewski, *Atak terrorystyczny na kompleks gazowy Tiguentourine w In Amenas w Algierii w styczniu 2013 r. jako przykład nowych zagrożeń dla energetycznej infrastruktury krytycznej i bezpieczeństwa wewnętrznego państwa* (Eng. Terrorist attack on the gas system in Tiguentourine, Amenas, Algeria, in January 2013, as an example of new threats to critical energy infrastructure and the internal security of the state), „Przegląd Bezpieczeństwa Wewnętrznego” 2013, no. 9, pp. 202–224.

barrels of oil per year. In January 2006, dozens of armed members of the organisation overran one of Shell's facilities and abducted 4 foreign specialists employed by the British-Dutch company. MEND spokesman, Jomo Gbomo, announced at the time that this was only the beginning of his organisation's operations. *Our aim is to totally destroy the capacity of the Nigerian government to export oil*³⁴.

In March 2016, the Niger Delta Avengers (NDA) armed group officially announced its existence. Two months later, it attacked a Chevron oil rig and then oil and gas installations in the Niger Delta. More than 30 attacks were carried out during the three-month operation. They continued to occur in the following months of 2016, but were significantly reduced in intensity. They resulted in a 36 – per cent drop in oil production, which translated into a halving of state revenue. The organisation issued a statement demanding a greater share of oil sales and threatened to disrupt Nigeria's economy if its demands were not met. The NDA are seeking the creation of a sovereign state in the Niger Delta³⁵. The region of the country remains unsettled. Pirates pose a threat in Nigerian waters and Niger Delta residents are stealing oil directly from pipelines³⁶.

In September 2022, the Nigerian authorities announced that the country's oil imports were at their lowest in 25 years and its production had fallen below 1.18 million barrels per day, which, according to OPEC (Organisation of the Petroleum Exporting Countries), ranked the country second only to Angola. According to then President Muhammadu Buhari, this was the fault of massive theft of the commodity in the south-east of the country. The situation strongly affected the state's finances. In August 2022, the scale of oil theft in Nigeria was estimated at 700 000 barrels per day. Some companies claimed that up to more than 80% of the oil that enters the pipelines is stolen as it flows³⁷. In another part

³⁴ D. Howden, *Shell may pull out of Niger Delta after 17 die in boat raid*, The Independent, 17.01.2006, <https://web.archive.org/web/20170527010950/http://www.corpwatch.org/article.php?id=13121> [accessed: 17.01.2025].

³⁵ A. Olech, *Terrorist Threats...*, pp. 173–174.

³⁶ F. Mbah, *In Nigeria's crude capital, a plan to win the war against oil theft*, Al Jazeera, 19.12.2024, <https://www.aljazeera.com/news/2024/12/19/in-nigerias-crude-capital-a-plan-to-win-the-war-against-oil-theft> [accessed: 19.12.2024].

³⁷ *Nigerian oil exports at lowest level in 25 years due to oil theft*, Al Jazeera, 9.09.2022, <https://www.aljazeera.com/news/2022/9/9/nigerian-oil-exports-at-lowest-level-in-25-years-due-to-oil-theft> [accessed: 9.01.2025].

of Africa, in Mozambique, a terrorist attack carried out by the Supporters of the Tradition (Arabic: Ansar al-Sunna) organisation caused huge losses. Its militants seized the port city of Palma in the north-east of the country on 24 March 2021 and occupied it until 8 April. During this time they inflicted severe damage, killed many residents and 12 Western engineers working on a USD 60 billion gas project³⁸.

South America

Colombia is the country with the highest number of terrorist attacks and sabotage operations on pipelines and power lines feeding oil production facilities in the world. Since the mid-1960s, the country's authorities have been fighting groups that are the remnants of Marxist guerrillas. These include the National Liberation Army (Spanish: Ejército de Liberación Nacional, ELN) and the Revolutionary Armed Forces of Colombia (Spanish: Fuerzas Armadas Revolucionarias de Colombia, FARC). Currently, the splinter groups of the FARC are fighting both among themselves (they did not agree to the 2016 peace agreement) and with the ELN and various paramilitary groups for control of lucrative coca crops, illegal gold mining and smuggling routes, and attacking oil pipelines. For Colombia, oil accounts for about 1/3 of export revenues, meaning that even small disruptions in the extraction and transport of this resource have an impact on state revenues³⁹. Attacks on oil infrastructure, owned by national and foreign oil companies, remain one of the primary methods of fighting the government. Between 1987 and 1991, the ELN carried out 141 acts of sabotage on key sections of oil pipelines running through central Colombia. The financial losses incurred during these 4 years were estimated at USD 634 million⁴⁰. From 1986 to 2002, the ELN also carried out 950 bomb attacks (an average of 40 to 50 attacks per year) on an 800-kilometre stretch of pipeline carrying oil from the Caño Limón field in western Colombia. Its shareholder was Occidental Petroleum Corp.

³⁸ T. Mandrup, *The attack on Palma in Mozambique: An insurgency getting out of hand?*, Risk Intelligence, 8.04.2021, <https://www.riskintelligence.eu/analyst-briefings/the-attack-on-palma-in-mozambique-an-insurgency-getting-out-of-hand> [accessed: 8.01.2025].

³⁹ D. Czyżewski, *Ropa pod uprawami koki, czyli problemy Kolumbii* (Eng. Oil under coca crops – Colombia's problems), Energetyka24, 2.10.2021, <https://energetyka24.com/ropa/ropa-pod-uprawami-koki-czyli-problemy-kolumbii-komentarz> [accessed: 2.12.2024].

⁴⁰ *Encyklopedia terroryzmu* (Eng. Encyclopedia of world terrorism), M. Crenshaw, J. Pimlott (eds.) Warszawa 2004, p. 428.

of Los Angeles. Losses were estimated at USD 2.5 billion⁴¹. These activities also resulted in environmental pollution on a massive scale. For example, oil spilled from a pipeline blown up in June 1990 contaminated a large section of the Catatumbo River, along which several thousand people lived. Other attacks have caused, among other things, the destruction of more than 3 000 ha of farmland⁴². Sabotage campaigns forced foreign oil companies to create private armies and fund the training of government forces to protect pipelines. In the 1990s, British Petroleum incurred costs running into tens of millions of dollars for this purpose⁴³. In turn, the US sent a group of military advisers to provide training to Colombian soldiers related to the protection of the pipeline, of which the Los Angeles-based company was a shareholder⁴⁴. Despite this, the sabotage actions continued undeterred and the terrorists made themselves pay to stop them. In 2001, 170 bomb attacks were recorded against the Caño Limón-Coveñas pipeline. An attack carried out in February 2005, in which explosives were used, shut down the pipeline for several weeks as the network supplying the energy needed to exploit the Caño Limón deposit was also destroyed⁴⁵.

The FARC intensified attacks on pipelines following the death of their leader Raul Reyes, who was killed on 1 March 2008 in an operation by government forces. A few days later, a section of an oil pipeline transporting 100 000 barrels of oil per day was blown up. Its repair took several days⁴⁶. In the first half of 2012, FARC armed groups carried out more than 40 attacks on oil pipelines. Kidnappings and murders of engineers working in the oil industry were common. Soldiers protecting the pipelines were also attacked. In July 2013, a squad of soldiers was ambushed by

⁴¹ G. Marx, *Oleoducto en peligro recibe tropas estadounidenses en Colombia*, Amazon Watch, 12.11.2002, <https://amazonwatch.org/es/news/2002/1112-imperiled-pipeline-gets-us-troops-in-colombia> [accessed: 12.11.2024].

⁴² *Encyklopedia terroryzmu...*, p. 428.

⁴³ J. McEvoy, *La Financiación de BP a los militares asesinos de Colombia*, Declassified UK, 18.07.2023, <https://www.declassifieduk.org/es/la-financiacion-de-bp-a-los-militares-asesinos-de-colombia/> [accessed: 18.12.2024].

⁴⁴ K. Wang, D. Kashi, *Major U.S. military operations/actions to protect oil*, <https://nationalsecurityzone.medill.northwestern.edu/archives/oilchangeproject/how-do-we-protect-the-flow-of-oil/index.html> [accessed: 12.12.2024].

⁴⁵ Library of Congress, Federal Research Division, *Country Profile: Colombia*, 2007, <https://maint.loc.gov/rr,/frd/cs/profiles/Colombia.pdf>, p. 19 [accessed: 15.12.2024].

⁴⁶ Reuters, *Terroryści z FARC biorą na cel rurociągi* (Eng. FARC terrorists take aim at pipelines), „Dziennik”, 7.03.2008.

the FARC. Fifteen of them were killed. The incident occurred in sparsely populated areas of Arauca province⁴⁷. In August 2014, near the border with Venezuela, the Bicentenario pipeline was attacked. This caused a massive fire in the region. In May 2019, after another attack, the pipeline was shut down for a while. Attacks with greater or lesser intensity occurred until mid-2023, then ceased for more than a year. On 26 August 2024, the oil company Ecopetrol authorities reported a series of attacks on the country's most important pipelines – Bicentenario was attacked twice, Caño Limón-Coveñas three times. Between 26 August and 9 September 2024, there were 9 attacks on other pipelines. These occurred after the collapse of talks between the guerrilla group ELN and the Colombian government. The ELN believes that foreign oil companies have obtained contracts that are highly beneficial to themselves but detrimental to the country. According to the ELN leadership, Colombia should have full control over its natural resources, like Venezuela. Until this happens, the energy infrastructure is still to be targeted by this group⁴⁸.

Public transport sector – land transport

An analysis of the statistical data shows that public transport is the CI system most vulnerable to terrorism and sabotage⁴⁹. The number of attacks on this sector increased from 1165 between 2000 and 2009 to 1966 between 2010 and 2017. The largest increase was in the number of attacks on trains: from 366 to 647. Between 1970 and 2009, bus transport infrastructure worldwide was the target of 1497 attacks. Most were carried out in Israel and the Occupied Palestinian Territory (142), India (88), the Philippines (72), Pakistan (70), Colombia (38), the Russian Federation (37) and Sri Lanka (36). Almost 60%

⁴⁷ PAP, *Kolumbia: 15 żołnierzy zginęło w zasadzce FARC* (Eng. 15 soldiers killed in FARC ambush), *Wirtualna Polska Wiadomości*, 21.07.2013, <https://wiadomosci.wp.pl/kolumbia-15-zolnierzy-zginelo-w-zasadzce-farc-6079340922217089a> [accessed: 21.12.2024].

⁴⁸ K. Byzdra, *Partyzanci mieli zaatakować rurociągi w Kolumbii. Na miejsce wysłano wojsko* (Eng. Guerrillas were to attack pipelines in Colombia. The military was sent to the site), *Energetyka24*, 27.08.2024, <https://energetyka24.com/ropa/wiadomosci/partyzanci-mieli-zaatakowac-rurociagi-w-kolumbii-na-miejsce-wyslano-wojsko> [accessed: 27.08.2024]; Ch. Kennedy, *Guerrilla Attacks on Pipelines Threaten Colombia's Oil Production*, *Oil Price*, 10.09.2024, <https://oilprice.com/Energy/Crude-Oil/Guerrilla-Attacks-on-Pipelines-Threaten-Colombias-Oil-Production.html> [accessed: 10.12.2024].

⁴⁹ A. Botha, *Prevention of Terrorist Attacks...*, p. 849.

of the targets were attacked using explosives. The perpetrators of attacks in these countries were separatist, far-left and Muslim organisations⁵⁰. Between 2010 and 2017, the number of attacks targeting buses increased from 476 to 740. There was also an increase in the number of attacks and sabotage actions against other facilities, including bus stations and bus stops – from 138 to 179, bridges and tunnels – from 116 to 249 and roads – from 38 to 52⁵¹. They were conducted using mostly firearms (1450 incidents) and arsons (216 incidents)⁵².

The driving force behind the industrial revolution in Europe, European colonial expansion and an effective tool for warfare was the steam railway. It is one of the first CI elements to be targeted by terrorists. In Britain between 1881 and 1885, the Fenians (forerunners of the Irish Republican Army) fought the so-called ‘Dynamite War’. There were 13 attacks in London at the time, including several on railway stations⁵³. The first attack on the London Underground was carried out on 30 October 1883. In the evening, an explosive device exploded in the tunnel between Charing Cross and Westminster stations and another in front of Praed Street station. A total of 72 passengers were injured, many of them seriously. Six carriages were seriously damaged⁵⁴. In January 1885, 2 bombs exploded: one at Gower Street station and the other on a Metropolitan Line train. The depot was damaged and several passengers were injured⁵⁵.

Europe’s dense rail network was crucial to military operations during World War I. The railways enabled the great powers to mobilise armies on a unprecedented scale and keep them in the field, despite growing and

⁵⁰ B.M. Jenkins, B.R. Butterworth, K.S. Shrum, *Terrorist Attacks on Public Bus Transportation: A Preliminary Empirical Analysis*, Mineta Transportation Institute 2010, <https://transweb.sjsu.edu/sites/default/files/2982-Terrorist-Attacks-On-Public-Bus-Transportation.pdf>, pp. 3, 23, 27 [accessed: 3.12.2024].

⁵¹ A. Botha, *Prevention of Terrorist Attacks...*, p. 855.

⁵² Ibid., p. 850.

⁵³ R. Kirkland, ‘A secret, melodramatic sort of conspiracy’: *The disreputable legacies of Fenian violence in nineteenth-century London*, King’s Research Portal, https://kclpure.kcl.ac.uk/ws/portalfiles/portal/114850253/A_secret_melodramatic_sort_KIRKLAND_Accepted25July2017Published12August2019_GREEN_AAM.pdf, pp. 6–7 [accessed: 3.12.2024].

⁵⁴ I. Mansfield, *The first terrorist attack on the London Underground*, IanVisits, 30.10.2013, <https://www.ianvisits.co.uk/articles/130th-anniversary-of-the-first-terrorist-attack-on-the-london-underground-9335/> [accessed: 30.10.2024].

⁵⁵ *List of terrorist incidents in London*, Wikipedia, https://en.wikipedia.org/wiki/List_of_terrorist_incidents_in_London [accessed: 19.12.2024].

increasingly complex logistical needs. Railway infrastructure was therefore the target of attacks and sabotage actions by the opposing side's armies. Attacks organised by the Arabs led by Thomas E. Lawrence on the Hejaz Railway from Damascus to Medina, a line of strategic importance to the Turkish forces. During the Palestinian campaign of 1917–1918, it was one of the main targets of the British offensive and attacks by Arab rebels. Parts of the line were blown up and numerous stations destroyed⁵⁶. The target of German attacks was, in turn, the British Uganda Railway, running from Port Florence (now Kisumu) on Lake Victoria to Mombasa in what was then British East Africa (now Kenya). German diversionary groups set out from Tanganyika (now Tanzania) to blow up the tracks and attack British trains⁵⁷.

In the interwar period, the railway and its infrastructure were used to organise mass murder. On 13 September 1931, Szilveszter Matuska planted a bomb under the railway tracks on the viaduct at Biatorbágy on the outskirts of Budapest. The powerful explosion led to the derailment of the Vienna Express. Twenty-four people were killed and 120 injured, 14 of them seriously. Matuska also made two unsuccessful attempts to derail trains in Austria and detonated a bomb near Berlin. His high-profile trial pointed the way forward for terrorist activity. In the following years, terrorists attacked the entire railway infrastructure, including stations, ticket halls, waiting rooms, station restaurants, bridges, tracks, signals, trains, sidings and steam locomotives. Their aim was to cause as much loss of life and property as possible, thus gaining media publicity⁵⁸.

On 28 August 1939, a German agent, Antoni Guzy, left two suitcases filled with explosives in a luggage room at a railway station in a Polish town. The explosion left 20 people dead and 35 injured. The Tarnów assassination attempt was one of the sabotage actions of the German fifth column, which paralysed the defence activities of the Polish state before the outbreak of World War II⁵⁹. During this conflict, rail sabotage was one of the most

⁵⁶ T.E. Lawrence, *Siedem filarów mądrości* (Eng. Seven pillars of wisdom), Warszawa 1971, pp. 198–203.

⁵⁷ R. Farnworth, *The Uganda Railway during the First World War*, <https://rogerfarnworth.com/2020/12/28/the-uganda-railway-during-the-first-world-war/> [accessed: 28.12.2024].

⁵⁸ *Tragically Explosive – Szilvestre Matuschka: A Fetish For Disaster (Part Three)*, Europe Between East And West, 7.03.2020, <https://europebetweeneastandwest.wordpress.com/tag/hungarian-serial-killers/> [accessed: 7.12.2024].

⁵⁹ M. Biedroń, *Zamach bombowy na tarnowskim dworcu kolejowym* (Eng. Bomb attack at Tarnów railway station), Tarnowskie Centrum Informacji, <https://www.it.tarnow.pl/>

common guerrilla activities in all theatres of the war. Its scale was so large that guerrilla actions in occupied Europe targeting German-controlled railway infrastructure were dubbed the Battle of the Rails or the War of the Rails. The partisans carried out most sabotage actions on the railways in the USSR⁶⁰. Poland was the second country in terms of the number of attacks on railway infrastructure. From 1 January 1941 to 30 June 1944, the Union of Armed Struggle and the Home Army carried out some 29 000 rail sabotage actions. As a result of these actions, 6930 locomotives and 19 058 wagons were damaged, 732 transports were derailed and 443 were set on fire, 1167 tank cars were destroyed and 38 bridges were blown up⁶¹.

On the terrorist attacks carried out worldwide between 1950 and 1970 targeting transport infrastructure, information is contradictory and statistics incomplete. A problem is the assessment of incidents that occurred during decolonisation processes in Asia and Africa. National liberation and nationalist groups called the attacks militant operations against colonialists, while the administration in the colonies, its security forces and the authorities in the metropolises considered them acts of terrorism and the organisations carrying them out as terrorist. Such attacks were organised in Palestine in the 1940s, in French Indochina in the 1940s and 1950s, in Algeria in the 1950s, and in Angola and Mozambique in the 1970s. Incidents that qualified as 'ordinary' train crashes rather than acts of sabotage were questionable. This was the case when the perpetrators remained silent about the incident in question⁶².

Relatively accurate statistics on attacks worldwide targeting public transport infrastructure have been available since the early 1970s thanks to the US-based Mineta Transportation Institute (MTI), established in 1991. It publishes periodic reports on the subject. Public transport facilities are targeted by separatist, far-left, far-right and religious organisations, primarily Muslim extremists (jihadists), and bandit groups. According

atrakcje/tarnow/ciekawostki/taka-jest-historia/zamach-bombowy-na-tarnowskim-dworcu-kolejowym [accessed: 3.12.2024].

⁶⁰ P.W. Blood, *Hitler's Bandit Hunters: The SS and the Nazi Occupation of Europe*, Washington 2006, https://books.google.pl/books?id=jR49G7eyxBUC&pg=PA101&redir_esc=y#v=onepage&q&f=false, p. 101 [accessed: 3.12.2024].

⁶¹ M. Ney-Krwawicz, *Armia Krajowa: siła zbrojna Polskiego Państwa Podziemnego* (Eng. Home Army: the armed forces of the Polish Underground State), Warszawa 1993, p. 214.

⁶² M. Tomczak, *Ewolucja terroryzmu, sprawcy – metody – finanse* (Eng. Evolution of terrorism, perpetrators – methods – finance), Poznań 2010, pp. 40–47.

to MTI data, between 1970 and 2019 there were approx. 5800 attacks on railway infrastructure, with passenger trains being targeted in 346 cases. These resulted in 676 deaths and more than 9720 injuries. The remaining incidents involved goods trains and other railway infrastructure. These figures are from OECD countries, excluding Turkey. In that country, there were 33 attacks on railway infrastructure between 1970 and 2010, resulting in 17 fatalities⁶³.

In developed countries (the MTI report lists 27 countries), terrorist attacks on passenger railways are a statistically rare occurrence. Over the half-century period (1970–2019), there was an average of 7 incidents per year, with attacks carried out in the UK, Spain, France, Germany and Italy accounting for 67% of the total number of attacks. The UK was ranked first because of its long IRA (Irish Republican Army) terrorist campaign. Spain was second because of ETA (Basque: Euskadi Ta Askatasuna) activity. In the United States, the companies that own the passenger railways recorded 27 attacks between 1970 and 2019. In addition, 7 cases of preparations for attacks were detected. In terms of the number of victims, South Korea leads the statistics, where 198 people were killed in a fire started on an underground train in the city of Daegu on 18 February 2003. Spain is in second place. Coordinated attacks on commuter trains carried out in Madrid on 11 March 2004 killed 192 people. Italy comes in third place. The bombing of the Bologna train station on 2 August 1980 killed 85 people⁶⁴.

Analysis of the available data shows that the most common *modus operandi* of the perpetrators was bomb attacks. Of these 346 attacks on passenger trains, as many as 216 (62%) were carried out using explosives placed on trains, railway tracks and cars. In 33 attacks (10%), the perpetrators' actions consisted of mechanically damaging or destroying railway equipment, in 32 (9%) – starting a fire using flammable materials, in 29 (8%) – using a knife, and in 19 (6%) – using firearms. In 17 cases (5%) other methods of attack were used. One attack was carried out using a weapon of mass destruction – chemical weapons. In March 1995, sarin

⁶³ B.M. Jenkins, B.R. Butterworth, *How Sophisticated are Terrorist Attacks on Passenger Rail Transportation*, San José 2020, <https://transweb.sjsu.edu/sites/default/files/SP0520-Jenkins-Terrorist-Attacks-Passenger-Rail-Transportation.pdf>, p. 8 [accessed: 3.12.2024].

⁶⁴ *Ibid.*, p. 11.

was used in the Tokyo underground. It caused the death of 12 people and more than 5000 had symptoms of poisoning⁶⁵.

Another MTI report looked at attacks on passenger railways carried out worldwide between 1970 and 2017, listing train derailments: mechanical (64%) and using explosives (31%). In 39 countries, these methods were used in 282 attacks. The highest number was in: India – 82, Pakistan – 66, Russia – 22, Turkey – 11, Bangladesh – 10, Thailand – 10, Algeria – 7, Italy – 7, UK – 7, Germany – 6 and France – 5. These incidents resulted in 1068 deaths and more than 3040 injuries. The highest number of casualties was in India with 485, Angola, where 278 people were killed in two attacks, followed by Pakistan with 67 and Mozambique, where 58 people were killed in one attack⁶⁶. Most train derailments (37 incidents) were caused by Indian Maoists (Naxalites). These resulted in 199 deaths. However, the highest number of casualties resulted from attacks organised by various jihadist groups. In 10 attacks carried out by them, 208 people were killed⁶⁷.

A separate category of incidents consists of attacks on railway infrastructure, the main purpose of which is to disrupt the functioning of railway communication rather than to kill people. There were 817 such incidents recorded between 1970 and 2017. In 721 incidents (88%), the targets were railway tracks, bridges and tunnels, in 59 (7%) – railway signalling, communications and power systems, in 29 (4%) – personnel and their intended facilities. The means of attack were most often explosive devices, dynamite, mines and grenades – 702 incidents (86%). In other cases it was sabotage involving mechanical damage and arson. The highest number of such incidents was recorded in South Asia – 482 (59%) and Western Europe – 126 (15%), with 48 people killed and 268 injured⁶⁸.

Cyber attacks on the rail network also fall into this category of incidents. The first known case of successful physical sabotage via the internet was recorded in Poland. In January 2008, a 14-year-old boy, a talented electronics engineer, used a self-built transmitter to hack into the city's tram system in Łódź, took control of tram traffic and caused 4 of them to derail. Twelve

⁶⁵ Ibid., pp. 13–14.

⁶⁶ B.M. Jenkins, B.R. Butterworth, *Train Wrecks and Track Attacks...*, pp. 8–9.

⁶⁷ Ibid., p. 26.

⁶⁸ Ibid., pp. 16–17.

people were injured⁶⁹. Between 2014 and 2024, cyber incidents affecting railway systems were reported in countries such as Belgium, Belarus, the Czech Republic, Denmark, France, India, Germany, the United States, Ukraine and Poland. A very large increase in the number of cyber attacks on railways (by 220%) occurred between 2020 and 2024. This has become a global problem⁷⁰. In 2023, unauthorised activation of the 'radio-stop' signal repeatedly immobilised trains in Poland. The repeated incidents had the character of well-organised sabotage actions⁷¹.

Hijackings of trains with passengers in order to force certain actions on the authorities are rare. In 1975 and 1977 in the Netherlands, militants of the Front for the Republic of the South Moluccas (Dutch: Front Republik Maluku Selatan) hijacked a train and demanded that the Netherlands create a state independent of Indonesia, a former Dutch colony. In 2006, 2009, 2012, Naxalites hijacked passenger trains in eastern India⁷². In Nigeria in 2022, bandits detonated an explosive device placed on the tracks just ahead of an oncoming Abuja-Kaduna train, fired machine guns at the depot and abducted more than 150 of the approx. 1000 passengers. Eight people were killed and many others injured. The incident has prompted the Nigerian authorities to treat all bandit groups as terrorist organisations⁷³.

⁶⁹ 14-latek przestawiał zwrotnice (Eng. 14-year-old switched railway crossovers), Policja.pl, 9.01.2008, <https://www.policja.pl/pol/aktualnosci/13278,14-latek-przestawial-zwrotnice.html> [accessed: 9.01.2025].

⁷⁰ C. Sivesind, *Cyber Attacks on Railway Systems Increase by 220%*, SecureWorld, 20.08.2024, <https://www.secureworld.io/industry-news/railway-cyber-attacks> [accessed: 20.08.2024].

⁷¹ M. Olanicki, *Tajemnicze awarie polskich pociągów. O sabotaż podejrzewany producent* (Eng. Mysterious failures of Polish trains. Manufacturer suspected of sabotage), Biznes Info, 6.12.2023, <https://www.biznesinfo.pl/tajemnicze-awarie-polskich-pociagow-o-sabotaz-podejrzewany-producent-mo-wak-061223> [accessed: 6.12.2024].

⁷² N. Shukla, *Maoists briefly hijack Indian train*, Reuters, 22.04.2009, <https://www.reuters.com/article/world/maoists-briefly-hijack-indian-train-idUSTRE53L102/> [accessed: 22.12.2024]; M. Saqib, *Recent Trends of Naxal Violence in India: Need for Comprehensive Approach from the Government*, "International Journal of Research in Social Sciences" 2018, vol. 8, https://www.ijmra.us/project%20doc/2018/IJRSS_NOVEMBER2018/IJMRA-14770.pdf, p. 878 [accessed: 3.12.2024].

⁷³ *Nigeria train resumes operations eight months after major attack*, Al Jazeera, 5.12.2022, <https://www.aljazeera.com/news/2022/12/5/nigeria-train-resumes-eight-months-after-deadly-attack> [accessed: 5.12.2024].

Public transport sector - air transport

For many decades, air transport was a target of choice for various terrorist organisations and individual perpetrators alike. In 1967, there were 15 aircraft hijacked, in 1968 – 30, and in 1969 – 80, and 5 sabotages were carried out on aircraft belonging to 37 countries. These incidents resulted in 6 deaths and 34 injuries. From 1 January to 16 June 1970, 32 aircraft were hijacked and 8 sabotages were carried out on machines belonging to 23 countries. As a result, 90 passengers were killed and 23 injured⁷⁴. The large number of hijackings of civilian aircraft in the late 1960s and early 1970s contributed to attempts to classify them. Terrorist incidents do not include aircraft hijackings carried out for the purpose of escape, media publicity or material gain. They should be considered air banditry, also known as air piracy. These are criminal acts undertaken for the purpose of seizing an aircraft, regardless of the motives, reasons and objectives of the perpetrator(s)⁷⁵. In order to separately collect data on aviation terrorism incidents and those on incidents that cannot be so classified, two databases were created: Aviation Terrorism Sub-Database (ATSD) and Global Aviation Criminal Incidents Database (GACID)⁷⁶.

Hijackings

The first attempted plane hijacking was recorded in 1931. Peruvian revolutionaries captured an American pilot making a flight from Lima to Arequipa. They wanted to use his plane to spread leaflets. The pilot adamantly refused and the hijackers' plan failed. After 10 days, the American was freed and returned safely to Lima. According to the International Civil Aviation Organisation (ICAO), the first aeroplane hijacking after the end of World War II took place in 1948. A Cathay Pacific flight from Macao to Hongkong was hijacked for ransom. The machine plummeted into the Pacific Ocean and 25 people died. In 1958, the first case of hijacking in the US was reported. Four Cubans hijacked a plane flying from Miami

⁷⁴ J. Laskowski, *Terroryzm lotniczy – charakterystyka zjawiska* (Eng. Air terrorism – characteristics of the phenomenon), „Studia Humanistyczno-Społeczne” 2013, vol. 7, p. 146.

⁷⁵ K. Jałoszyński, *Współczesne zagrożenie terroryzmem powietrznym, kierunki przedsięwzięć w zakresie przeciwdziałania mu oraz walka z tym zjawiskiem* (Eng. The contemporary threat of air terrorism, the directions of countermeasures and the fight against this phenomenon), in: „Bezpieczne niebo”. *Materials from the AON (National Defence University in Warsaw) Scientific Conference*, J. Gotowała (ed.), Warszawa 2002, p. 116.

⁷⁶ J. Duchesneau, *Aviation Terrorism...*, p. 5.

to Havana. It crashed while attempting to land in territory controlled by Fidel Castro's rebels. In the early 1960s in Cuba, planes were hijacked by dissidents. They wanted to escape the Castro regime to the USA in this way. Then the situation was reversed. Members of various far-left organisations and criminals fleeing justice were hijacking planes from the United States to reach Cuba. In 1969, aeroplane hijackings between the US and Cuba became so frequent and troublesome that the two governments signed a bilateral agreement to combat it, which essentially solved the problem⁷⁷.

Aircraft terrorism was the *modus operandi* of Palestinian organisations, mostly of a left-wing, Marxist nature, which turned the Palestinian-Israeli conflict into international terrorism. The series of aeroplane hijackings by Palestinians was initiated on 22 July 1968 by three members of the Popular Front for the Liberation of Palestine (PFLP, Arabic: Al-Jabha ash-Shaabiyya li-Tahrir Filastin). They seized an Israeli El Al airline plane flying from Rome to Tel Aviv and forced the crew to land in Algiers. Following negotiations that lasted some 40 days, the terrorists agreed to release the hostages in exchange for the release of a group of Palestinians from Israeli prisons⁷⁸. The incident set a precedent because it showed that hijacking planes are very effective in achieving the terrorists' main objectives, i.e. to put political pressure on the authorities and to focus the attention of world public opinion. George Habash, one of the leaders of the PFLP, pointed out that before the terrorist activities began in 1968, the Palestinian cause was unknown to the world: *Probably less than half of Americans even knew that such a thing existed. We wanted to do something that would make people ask: Why are they doing this? (...) We achieved our goal. The Palestinian cause became instantly known throughout the world. (...) The hijacking of a large plane has a greater propaganda, media effect than killing a hundred Israelis in battle. For decades, world opinion was neither for nor against the Palestinians. Now at least the world is talking about us*⁷⁹.

There were 151 aircraft hijacked between 1968 and 1970⁸⁰. The hijacking on 6 September 1970 of 3 passenger planes taking off from European

⁷⁷ J. Laskowski, *Terroryzm lotniczy...*, pp. 145–146.

⁷⁸ *Encyklopedia terroryzmu...*, p. 295.

⁷⁹ T.R. Aleksandrowicz, K. Liedel, *Zwalczanie terroryzmu lotniczego. Wybrane zagadnienia i źródła prawa międzynarodowego* (Eng. Combating air terrorism. Selected issues and sources of international law), Szczytno 2010, p. 13.

⁸⁰ B.M. Jenkins, *The Terrorist Threat to Commercial Aviation*, Santa Monica 1989, <https://www.rand.org/content/dam/rand/pubs/papers/2008/P7540.pdf>, p. 4 [accessed: 25.02.2025].

airports by members of the PFLP was unprecedented. One of them landed in Cairo and was destroyed after the passengers disembarked. Two were diverted to Dawson's Field airport near Zarqa in Jordan. Three days later, the terrorists hijacked another plane and diverted it to this airport. All 3 planes were blown up on 12 September. Most of the passengers were released, with only American Jews and Israeli citizens remaining in captivity. They were set free in exchange for the release of Palestinians from European prisons⁸¹. In the years that followed, Palestinian militants carried out dozens of terrorist attacks in the Middle East and Europe, including 52 attacks on Israeli airline El Al planes⁸².

Aircraft hijackings often occurred in Eastern Bloc countries, but the propaganda of the time tried to ignore these incidents with silence. The motives of the perpetrators were most often personal. Between 1960 and 1980, around 100 cases of aircraft hijacking were recorded, including for the purpose of escaping from Eastern Bloc countries to West Germany, West Berlin and Denmark⁸³. During the 1970s and 1980s, the number of aircraft hijackings in Poland increased. They were mainly directed to West Berlin. There were more than 20 such incidents. The largest number of planes, as many as 10, were hijacked from Katowice-Pyrzowice airport. Machines performing domestic flights were hijacked on the grounds that it was easier to board them. This was due to the lack of passport control and border checks and the simplified security procedure for such flights⁸⁴. In 1990, the daily *Izvestia* reported that 69 machines were hijacked in the USSR between 1958 and 1990. The perpetrators killed 120 hostages and wounded another 200⁸⁵. A total of 218 incidents of terrorist hijacking (279 victims) and 1067 incidents of criminal hijacking (530 victims) occurred worldwide between 1931 and 2011⁸⁶. According to other data, 553 aircraft hijackings

⁸¹ *Encyklopedia terroryzmu...*, p. 300.

⁸² Ł. Szymankiewicz, *Terroryzm lotniczy wobec Izraela* (Eng. Air terrorism against Israel), Warszawa 2019, p. 7.

⁸³ E. Ciborowska, *Wybrane przypadki piractwa powietrznego w Polsce w latach 80.* (Eng. Selected cases of air piracy in Poland in the 1980s), „Terroryzm” 2008, no. 1, p. 6.

⁸⁴ M. Desler, *Seven five – man with knife, lotnictwo, a terroryzm* (Eng. Seven five – man with knife, aviation, and terrorism), *dlapilota.pl*, 9.04.2014, <https://dlapilota.pl/wiadomosci/monika-desler/seven-five-man-knife-lotnictwo-terroryzm> [accessed: 9.12.2024].

⁸⁵ *Ibid.*

⁸⁶ J. Duchesneau, *Aviation Terrorism...*, p. 139.

were recorded between 1980 and 2022. The fewest (18) were in the decade 2011–2022⁸⁷.

Bombings

According to the ICAO, these involve placing explosives on board aircraft and detonating them while the aircraft is on the ground or in the air. The cargo may be in checked baggage or may be dropped off by a passenger⁸⁸. From 1931 to 2024, 73 terrorist bombings (1644 dead) and 119 criminal attacks (1184 victims) were carried out on aircraft worldwide⁸⁹. There were 48 attacks between 2000 and 2009, 27 of which were hijacking and 14 used explosives. Between 2010 and 2017, there were 26 attacks, of which 5 were hijacking and 10 were attacks using explosives⁹⁰. According to other data, there were 64 aeroplane bombings between 1970 and 2022, killing 2097 people. The fewest (2 bombings) of this kind were in the decade 2011–2022, with 225 deaths⁹¹.

The first aeroplane bombing was carried out on 21 February 1970. PFLP was the perpetrator and the target was a Swissair Convair aircraft flying from Zurich to Tel Aviv. A bomb placed in the baggage hold exploded 9 minutes after take-off. The pilots attempted to return to Zurich airport, but due to loss of controllability the aircraft plummeted to the ground and 47 people were killed⁹². On the same day, an explosive device exploded on an Austrian Airlines Caravelle flight from Frankfurt am Main to Tel Aviv. The bomb had been placed between thick bundles of newspapers, which significantly weakened the force of the explosion. The pilot landed safely. In the early 1970s, bombings by Palestinian terrorist groups mainly targeted El Al airline planes. Due to the US government's support of Israel's anti-Palestinian policy, US carriers' machines also became targets.

⁸⁷ O. Čokorilo, S. Čokorilo, L. Tomic, *A framework for aviation security*, AIIT 4th International Conference on Transport Infrastructure and Systems (TIS ROMA 2024), https://www.researchgate.net/publication/381768379_A_framework_for_aviation_security, p. 5 [accessed: 28.02.2025].

⁸⁸ J. Duchesneau, *Aviation Terrorism...*, p. 118.

⁸⁹ Ibid., p. 139; A. Botha, *Prevention of Terrorist Attacks...*, p. 851; *Timeline of airliner bombing attacks*, Wikipedia, https://en.wikipedia.org/wiki/Timeline_of_airliner_bombing_attacks [accessed: 26.02.2025].

⁹⁰ A. Botha, *Prevention of Terrorist Attacks...*, p. 851.

⁹¹ O. Čokorilo, S. Čokorilo, L. Tomic, *A framework for aviation security...*, p. 3.

⁹² J. Laskowski, *Terroryzm lotniczy...*, p. 149.

In September 1974, a bomb explosion on a TWA Boeing, flying from Tel Aviv via Athens to New York, caused the plane to crash over the Ionian Sea and killed 88 people. The attack was claimed by the PFLP. In the 1970s, a total of 42 bombings were recorded, killing more than 650 people. In the following decade, the number of bombings dropped to 24, but the number of victims increased – to around 1000 people⁹³. The most tragic in terms of casualties were 2 terrorist attacks. Members of the separatist Sikh organisation Babbar Khalsa placed a bomb on board an Air India Boeing 747 flying from Montreal to New Delhi on 22 June 1985. The cargo exploded while the machine was over the Atlantic Ocean off the coast of Ireland. There were 329 casualties, the most in the history of such attacks. The second attack occurred on 21 December 1988 by agents of Libyan intelligence who managed to place an explosive device in the baggage checked in on flight 103 of a Pan Am Boeing 727 flying from London to New York. The plane exploded over Lockerbie. It killed 259 people on board and 11 residents of the Scottish town⁹⁴. One of the most recent attacks, which used the same pattern of operations, occurred on 31 October 2015. Terrorists belonging to the ISIS-linked Sinai Province group planted an explosive device on an Airbus A321 aircraft of Russian airline Metrojet, flying from Sharm el-Sheikh to St Petersburg. The explosion occurred around 23 minutes after take-off. The plane crashed in the Sinai Peninsula and 224 people were killed⁹⁵.

Suicide terrorism

Another method of attacking aircraft is through acts of suicide terrorism, in which the aircraft is used as an instrument of attack. From 1989 to 2011, a total of 17 such attacks and failed and foiled attempts were recorded. A total of 3143 people were killed in these attacks⁹⁶. The first suicide incident was recorded in November 1989. A Saudi attempted to detonate a bomb on board a Saudi Arabian Airlines flight. The explosion did not occur due to a design flaw in the detonator. Little is known about the incident, other

⁹³ Ibid., pp. 149–150.

⁹⁴ *Encyklopedia terroryzmu...*, p. 369.

⁹⁵ PAP, *Egipt: katastrofa samolotu Airbus A321 na Półwyspie Synaj (aktualizacja)* (Eng. Egypt: Airbus A321 plane crashes in the Sinai Peninsula (update)), *dlapilota.pl*, 17.11.2015, <https://dlapilota.pl/wiadomosci/pap/egipt-katastrofa-samolotu-airbus-a321-na-polwyspie-synaj> [accessed: 17.12.2024].

⁹⁶ J. Duchesneau, *Aviation Terrorism...*, p. 139.

than that 10 people were arrested⁹⁷. The 11 September 2001 attacks on the World Trade Center and the Pentagon in the USA fall into this category of terrorist acts. This event is considered the apogee of aviation terrorism and the largest successful terrorist operation in history. It claimed the lives of 2996 people. The number of victims of this attack surpassed those killed by terrorist hijacking (279 people) and terrorist bombings (1418 people)⁹⁸. The 9/11 attacks also caused huge material damage. Very large costs were incurred by insurance and reinsurance companies, airlines and aircraft manufacturers, as well as the travel industry. Swiss reinsurance company Swiss Re estimated that the insurance sector's losses related to the September attack amounted to USD 90 billion, of which 19 billion were direct costs. Total airline losses were estimated at USD 12–13 billion⁹⁹. These events plunged air communications into the deepest crisis since World War II. In the following years, there were several incidents demonstrating the potential for aircraft to be used as a tool of terror. Among them, on 5 January 2002, a flying school student hijacked a small Cessna-type aircraft and crashed it into a high-rise building in Tampa, Florida. The pilot died on the spot and the structure of the building was slightly damaged¹⁰⁰.

Between 1989 and 2011, there were 32 suicide attacks that were classified as criminal. The death toll in these attacks was 691¹⁰¹. Such an event may have been, according to some opinions, the disappearance of a Malaysia Airlines plane in March 2014. A Boeing 777 flying from Kuala Lumpur to Beijing rerouted its flight and disappeared from radar. The plane's captain, Zaharie Ahmad Shah, was killed along with 238 passengers and crew members. There were reports that the captain may have deliberately caused the plane to crash into the waters of the Indian Ocean. His religious radicalism and difficult personal experiences were cited as motives¹⁰². In February

⁹⁷ Ibid., p. 123.

⁹⁸ Ibid., p. 126.

⁹⁹ K. Izak, *Twentieth anniversary of September 11. The plot, the events and the aftermath of the terrorist attack on the USA*, "Internal Security Review" 2021, no. 25. <https://doi.org/10.4467/20801335PBW.21.033.14310>.

¹⁰⁰ M.L. Wald, *Student Pilot, 15, Crashes Plane Into Tower in Florida*, New York Times, 6.01.2002, <https://www.nytimes.com/2002/01/06/us/student-pilot-15-crashes-plane-into-tower-in-florida.html> [accessed: 6.01.2025].

¹⁰¹ J. Duchesneau, *Aviation Terrorism...*, p. 139.

¹⁰² Daily Mail, *New report explores the pilot of MH370 troubled personal life, likely scenario of what happened on flight*, New Zealand Herald, 18.06.2019, <https://www.nzherald.co.nz/world/>

2025, the search for the remains of this aircraft began again¹⁰³. The most recent incident took place on 24 March 2015. A Germanwings Airbus A320 aircraft flying from Barcelona to Düsseldorf crashed in the French Alps. All passengers and crew members were killed – 150 people in total. The crash was deliberately caused by the co-pilot, Andreas Lubitz¹⁰⁴.

In the air transport sector, suicide missions are the least used modus operandi (3% of incidents). However, due to the number of victims of the 11 September 2001 attack, they proved to be the most deadly (51% of victims)¹⁰⁵. Only 8 out of the 17 suicide attacks in preparation were successful and resulted in fatalities. Two of these were attacks by Chechen women, so-called black widows, on Russian aircraft¹⁰⁶. Three attacks were unsuccessful, including that of Briton Richard Reid, known as the shoe bomber. With an explosive charge placed in his shoes, he attempted to board a flight from Paris to Miami¹⁰⁷. Six attacks were foiled, including Operation “Bojinka”, detected in Manila in January 1995, in which terrorists intended to hijack 11 aircraft and use them for suicide attacks on US facilities (along the lines of the 9/11 attack)¹⁰⁸. Another terrorist operation was foiled in London in August 2006. The aim of the suicide terrorists was to cause explosions on planes flying from the UK capital to New York, Washington DC, Chicago, San Francisco, Toronto and Montreal¹⁰⁹. Nigerian Umar Farouk Abdulmutallab intended to blow up a US NorthWest Airlines plane with 289 people on board, flying from Amsterdam to Detroit on

new-report-explores-the-pilot-of-mh370-troubled-personal-life-likely-scenario-of-what-happened-on-flight/TOQ557EGUHWQDXG5DU47E7JOVE/ [accessed: 18.12.2024].

¹⁰³ T. Jones, *MH370: Search resumes to find missing plane 11 years on*, Deutsche Welle, 25.02.2025, <https://www.dw.com/en/mh370-search-resumes-to-find-missing-plane-11-years-on/a-71739469> [accessed: 25.02.2025].

¹⁰⁴ M. Zafimehy, G. Chieze, *Crash de la Germanwings: à quoi ont ressemblé les dernières minutes avant la catastrophe?*, RTL, 26.03.2023, <https://www.rtl.fr/actu/justice-faits-divers/crash-de-la-germanwings-a-quoi-ont-ressemble-les-dernieres-minutes-avant-la-catastrophe-7900246615> [accessed: 26.01.2025].

¹⁰⁵ J. Duchesneau, *Aviation Terrorism...*, p. 123.

¹⁰⁶ *Ibid.*, p. 205.

¹⁰⁷ *Ibid.*

¹⁰⁸ K. Izak, *Leksykon organizacji i ruchów...*, pp. 164–165.

¹⁰⁹ *Ibid.*, p. 411.

25 December 2009. However, he was overpowered by passengers and crew while attempting to detonate a load of pentrite hidden in his underwear¹¹⁰.

Attacks on airports and grounded aircraft and attacks from the ground on airborne aircraft

The final category of incidents consists of attacks at airports and attacks carried out against aircraft on the ground and in the air. This is the most numerous category of incidents. By 2017, a total of 624 such terrorist incidents had been recorded¹¹¹. Between 2010 and 2017, the number of terrorist incidents at airports increased from 83 to 164¹¹². In contrast, 31 terrorist attacks were recorded at ports and aircraft in 2019, 10 more than in the previous year¹¹³. The first recorded terrorist attack at a passenger airport was carried out on 10 February 1970. Three PFLP terrorists at Munich Airport threw grenades at and shot at passengers travelling on an Israeli El Al airline flight. One person was killed and 11 injured¹¹⁴. In the 1970s and 1980s, Palestinian terrorists attacked Italy's Rome-Fiumicino and Leonardo da Vinci airports on several occasions¹¹⁵. In December 1999, an Algerian man, Ahmed Ressay, was arrested at a border crossing between Canada and the US while attempting to enter the US. Explosives and weapons were found in his car. Ressay's aim was to carry out a bomb attack at Los Angeles airport on New Year's Eve 1999¹¹⁶. Civilian airports in Saudi Arabia have also been targeted by the aforementioned Houthi movement in recent years. Militants of this organisation fired a Burkan H-2 missile towards Riyadh's King Khalid International Airport on 4 November 2017. The missile was shot down by a Patriot anti-missile system¹¹⁷. Between 2000 and 2009, there were 83 attacks on airports carried out with firearms,

¹¹⁰ Ibid., p. 478.

¹¹¹ J. Duchesneau, *Aviation Terrorism...*, p. 139.

¹¹² A. Botha, *Prevention of Terrorist Attacks...*, p. 854.

¹¹³ START, *Global Terrorism Overview: Terrorism in 2019*, https://www.start.umd.edu/pubs/START_GTD_GlobalTerrorismOverview2019_July2020.pdf, p. 11 [accessed: 30.07.2024].

¹¹⁴ J. Laskowski, *Terroryzm lotniczy...*, p. 151.

¹¹⁵ M. Zimmerman, „Cud, że tyle osób przeżyło”. Mija 50 lat od zamachu na lotnisku Fiumicino (Eng. 'A miracle that so many people survived'. It's 50 years since the attack at Fiumicino Airport), Onet, 17.12.2023, <https://wiadomosci.onet.pl/swiat/50-lat-od-ataku-na-lotnisku-fiumicino-najbardziej-krwawy-z-tamtych-zamachow/mpd5nm4> [accessed: 17.12.2024].

¹¹⁶ K. Izak, *Leksykon organizacji i ruchów...*, p. 186.

¹¹⁷ *Atak rakietowy na Rijad...*

explosives and incendiary devices. Between 2010 and 2017, there were 169 such attacks¹¹⁸. The last one occurred on 5 August 2024, using a Katyusha missile and targeting the Ain al-Assad airbase in Iraq. Five US soldiers were wounded¹¹⁹.

In recent years, UAVs have become an increasing threat to airports and aircraft taking off and landing. 2013 was the last year in which no such incidents were recorded. In December 2018, traffic was halted at London Gatwick Airport due to numerous drone overflights. In July the previous year, there was a near collision between a UAV and a passenger aircraft there. According to the British Airline Pilots Association, the number of drone incidents has risen sharply. There were 93 in 2017 and 117 between January and November 2018¹²⁰. Similar cases have also been reported in Poland. In March 2014, a drone dropped a small explosive on the runway at the military part of Balice airport. In July 2015, a UAV posed a serious threat to a Lufthansa aircraft approaching from Munich to Warsaw. A similar incident was reported at Balice in June 2022 and at Okęcie and Pyrzowice in May 2023¹²¹. All of these incidents were criminal in nature.

In recent years, there has been a significant increase in the number of cyber attacks on airports and airlines. These are mainly of a criminal nature. There were 178 cyber attacks on airports and 775 cyber attacks on airlines recorded in Europe in 2020. This represents a 530 per cent increase compared to 2019. Cyber attacks on airlines accounted for as much as 61% of all cyber attacks carried out in Europe in 2020. Most of these (735) were financially motivated¹²². It is important to note that in 2023, global CI was the target of more than 420 million cyber attacks, which equates to

¹¹⁸ A. Botha, *Prevention of Terrorist Attacks...*, p. 854.

¹¹⁹ *At least five US personnel injured in rocket attack on Iraq military base*, Al Jazeera, 6.08.2024, <https://www.aljazeera.com/news/2024/8/6/at-least-five-us-personnel-injured-in-attack-on-iraq-military-base> [accessed: 6.08.2024].

¹²⁰ A. Botha, *Prevention of Terrorist Attacks...*, p. 853.

¹²¹ M. Walków, *Coraz więcej incydentów z dronami. Lotnisko Chopina przetestuje rozwiązanie* (Eng. More and more drone incidents. Chopin Airport will test a solution), Money.pl, 30.05.2023, <https://www.money.pl/gospodarka/lotnisko-chopina-sie-zbroi-drony-to-coraz-powazniejsze-zagrozenie-dla-samolotow-6903403450051296a.html> [accessed: 30.12.2024].

¹²² EUROCONTROL, *Aviation under attack from a wave of cybercrime*, <https://www.eurocontrol.int/sites/default/files/2021-07/eurocontrol-think-paper-12-aviation-under-cyber-attack.pdf> [accessed: 5.07.2024].

approx. 13 attacks per second. Most of these were in the US. These attacks are often attributed to hackers linked to China, Russia and Iran¹²³.

The first act of terrorism involving the downing of a passenger plane took place on 21 December 1948. Greek insurgents shot down a Czechoslovak airliner flying from Rome to Athens, killing 24 people. In the 1970s, this type of attack became widespread with the availability of man portable air defence system (MANPADS) missiles. MANPADS were first used by terrorists on 5 September 1973 at Rome-Fiumicino airport. Palestinians attempted to fire an SA-7 missile at a taxiing El Al airline plane, but the attempt failed. The first successful attack of this type was carried out on 12 February 1979 near the town of Kariba in Zimbabwe. Shortly after take-off, an Air Rhodesia airliner was hit by an SA-7 missile, with the loss of 59 lives¹²⁴. MANPADS were widely used by the Afghan Mujahideen against Soviet military aircraft and helicopters, and later by the Taliban. They were also used by insurgent groups in Somalia, Iraq, Syria, Chechen fighters, Tamil fighters from the Liberation Tigers of Tamil Eelam (LTTE) and Colombian fighters from the FARC¹²⁵. The tactic of attacking civilian aircraft with missile systems is regularly used by various terrorist groups, warring armed groups (Sudan) and, in recent years, states. For example, on 17 July 2014 a Malaysia Airlines Boeing 777, flying from Amsterdam to Kuala Lumpur, was shot down in the Donetsk region in eastern Ukraine using a Buk surface-to-air guided missile. The perpetrators were separatists from Russia. Casualties totalled 283 passengers and 15 crew members¹²⁶. On 8 January 2020, Iranian forces shot down a Ukraine International Airlines Boeing 737 flying from Tehran to Kyiv with 176 people on board¹²⁷.

¹²³ B. Candan, *Top 5 critical infrastructure cyberattacks*, Anapaya, 17.10.2024, <https://www.anapaya.net/blog/top-5-critical-infrastructure-cyberattacks> [accessed: 17.10.2024].

¹²⁴ J. Laskowski, *Terroryzm lotniczy...*, pp. 151–152.

¹²⁵ A. Radomyski, D. Michalski, *Managing the Threat of Manpads Use Against Civil Aviation*, „Rocznik Bezpieczeństwa Morskiego” 2023, vol. 17, pp. 569–571. <https://doi.org/10.5604/01.3001.0054.1602>.

¹²⁶ A. Pawluszek, *Malezyjski Boeing 777 zestrzelony przez Rosjan w 2014 r. Sąd w Hadze przedstawił stanowisko* (Eng. Malaysian Boeing 777 shot down by Russians in 2014. The Hague-based court outlined the position), *Gazeta Prawna*, 17.11.2022, <https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8590126,holandia-sad-zestrzelenie-2014-malezyjski-boeing-777-ukraina.html> [accessed: 17.11.2024].

¹²⁷ Reuters, *Teheran proponuje odszkodowania rodzinom ofiar zestrzelonego boeinga. Kijów krytykuje* (Eng. Tehran offers compensation to families of victims of downed boeing. Kyiv criticises), *TVN24*, 30.12.2020, <https://tvn24.pl/swiat/ukrainski-samolot-zestrzelony-nad->

One of the most recent attacks on aircraft occurred on 11 November 2024. Two passenger airbuses, belonging to a US airline, were fired upon by gangs in Port-au-Prince, the capital of Haiti. A flight attendant on one of the planes was slightly injured. Following the incident, US airlines suspended flights to the country. In October 2024, on the other hand, a UN helicopter flying over Port-au-Prince was fired upon and had to turn back to the airport¹²⁸.

Conclusions

Critical infrastructure, due to its multi-sectoral nature, its vastness and the consequent difficulty in providing it with sufficient security, has for many years been a prime target of both terrorist organisations and individual perpetrators. The attacks carried out against it, particularly in the transport sector, cause mass casualties and become fuel for the media. In many cases, thanks to international cooperation, the strengthening of anti-terrorist controls, security measures and intelligence activities, attacks on CI facilities have been successfully prevented. However, this does not ensure a sufficient level of security for CI as a whole. Dynamic scientific and technological advances and civilisational development are accompanied by new outbreaks of tension and armed conflicts around the world, which make use of the latest technological advances. These advances have also been and will continue to be used by terrorists, insurgents and “guerrillas” to carry out attacks and acts of sabotage in hybrid operations. It can therefore be assumed that the threat level to CI worldwide will increase.

Bibliography

Aleksandrowicz T.R., Liedel K., *Zwalczanie terroryzmu lotniczego. Wybrane zagadnienia i źródła prawa międzynarodowego* (Eng. Combating air terrorism. Selected issues and sources of international law), Szczytno 2010.

teheranem-wladze-iranu-oferuja-odszkodowania-dla-rodzin-ofiar-st4851794 [accessed: 30.12.2024].

¹²⁸ *Horror w przestworzach, gangi ostrzelały dwa samoloty. Ranna stewardessa* (Eng. Horror in the skies, gangs fire on two planes. Injured stewardess), Polskie Radio 24, 12.11.2024, <https://polskieradio24.pl/arttykul/3445609,horror-w-przestworzach-gangi-ostrelaly-dwa-samoloty-ranna-stewardessa> [accessed: 21.12.2024].

Ciborowska E., *Wybrane przypadki piractwa powietrznego w Polsce w latach 80.* (Eng. Selected cases of air piracy in Poland in the 1980s), „Terroryzm” 2008, no. 1, pp. 6–9.

Encyklopedia terroryzmu (Eng. Encyclopedia of world terrorism), M. Crenshaw, J. Pimlott (eds.), Warszawa 2004.

Gebert K., *Pokój z widokiem na wojnę. Historia Izraela* (Eng. Peace with a view to war. Israel's history), Warszawa 2023.

Grabowski T.W., *Terroryzm północnokaukaski. Źródła, przejawy i przeciwdziałanie zjawisku* (Eng. North Caucasus terrorism. Sources, manifestations and countering the phenomenon), Kraków 2017.

Izak K., *Twentieth anniversary of September 11. The plot, the events and the aftermath of the terrorist attack on the USA*, „Internal Security Review” 2021, no. 25, pp. 341–369. <https://doi.org/10.4467/20801335PBW.21.033.14310>.

Izak K., *Leksykon organizacji i ruchów islamistycznych* (Eng. Lexicon of Islamist organisations and movements), Warszawa 2014.

Jałoszyński K., *Współczesne zagrożenie terroryzmem powietrznym, kierunki przedsięwzięć w zakresie przeciwdziałania mu oraz walka z tym zjawiskiem* (Eng. The contemporary threat of air terrorism, the directions of counter-terrorism undertakings and the fight against this phenomenon), in: „Bezpieczne niebo”. *Materials from the AON (National Defence University in Warsaw) Scientific Conference*, J. Gotowała (ed.), Warszawa 2002, pp. 114–132.

Kijewski T., *Atak terrorystyczny na kompleks gazowy Tiguentourine w In Amenas w Algierii w styczniu 2013 r. jako przykład nowych zagrożeń dla energetycznej infrastruktury krytycznej i bezpieczeństwa wewnętrznego państwa* (Eng. Terrorist attack on the gas system in Tiguentourine, Amenas, Algeria, in January 2013, as an example of new threats to critical energy infrastructure and the internal security of the state), „Przegląd Bezpieczeństwa Wewnętrznego” 2013, no. 9, pp. 202–224.

Laskowski J., *Terroryzm lotniczy – charakterystyka zjawiska* (Eng. Air terrorism – characteristics of the phenomenon), „Studia Humanistyczno-Społeczne” 2013, vol. 7, pp. 133–163.

Lawrence T.E., *Siedem filarów mądrości* (Eng. Seven pillars of wisdom), Warszawa 1971.

Lukasiewicz J., *Unmanned aerial vehicles as a source of threats to the states' electricity supply infrastructure and the proposed methods of protecting this infrastructure*, "Terrorism – Studies, Analyses, Prevention" 2022, no. 1, pp. 320–349. <https://doi.org/10.4467/27204383TER.22.012.15428>.

Ney-Krwawicz M., *Armia Krajowa: siła zbrojna Polskiego Państwa Podziemnego* (Eng. Home Army: the armed forces of the Polish Underground State), Warszawa 1993.

Radomyski A., Michalski D., *Managing the Threat of Manpads Use Against Civil Aviation*, „Rocznik Bezpieczeństwa Morskiego” 2023, vol. 17, pp. 559–579. <https://doi.org/10.5604/01.3001.0054.1602>.

Reuters, *Terroryści z FARC biorą na cel rurociągi* (Eng. FARC terrorists take aim at pipelines), „Dziennik”, 7.03.2008.

Szymankiewicz Ł., *Terroryzm lotniczy wobec Izraela* (Eng. Air terrorism against Israel), Warszawa 2019.

Tomczak M., *Ewolucja terroryzmu, sprawcy – metody – finanse* (Eng. Evolution of terrorism, perpetrators – methods – finance), Poznań 2010.

Wasiuta O., Wasiuta S., Mazur P., *Państwo Islamskie ISIS. Nowa twarz ekstremizmu* (Eng. Islamic State ISIS. The new face of extremism), Warszawa 2018.

Internet sources

AFP, *Des djihadistes revendiquent l'attaque d'un gazoduc*, 20 Minutes, 8.01.2016, <https://www.20min.ch/fr/story/des-djihadistes-revendiquent-l-attaque-d-un-gazoduc-826827705429> [accessed: 9.01.2025].

AFP, *Deux drones ont survolé la centrale nucléaire de Nogent-sur-Seine*, BFMTV, 4.01.2015, https://www.bfmtv.com/police-justice/deux-drones-ont-survole-la-centrale-nucleaire-de-nogent-sur-seine_AN-201501040009.html [accessed: 4.01.2025].

Atak rakietowy na Arabię Saudyjską i naloty w Jemenie (Eng. Missile attack on Saudi Arabia and air strikes in Yemen), Defence24, 27.12.2024, <https://defence24.pl/geopolityka/arabia-saudyjska-przeprowadza-naloty-huti-w-jemenie-za-atak-na-miasto-jazan> [accessed: 27.12.2024].

Atak rakietowy na Rijad (Eng. Rocket attack on Riyadh), Defence24, 5.11.2017, <https://defence24.pl/atak-rakietowy-na-rijad> [accessed: 5.11.2024].

At least five US personnel injured in rocket attack on Iraq military base, Al Jazeera, 6.08.2024, <https://www.aljazeera.com/news/2024/8/6/at-least-five-us-personnel-injured-in-attack-on-iraq-military-base> [accessed: 6.08.2024].

Au total, 17 sites nucléaires ont été survolés par des drones depuis octobre, Le Monde, 29.01.2015, https://www.lemonde.fr/planete/article/2015/01/29/dix-sept-sites-nucleaires-ont-ete-survoles-par-des-drones-depuis-octobre_4565967_3244.html [accessed: 29.01.2025].

Barnett D., *Ansar Jerusalem claims responsibility for recent Sinai gas pipeline attack*, FDD's Long War Journal, 19.01.2014, <https://www.longwarjournal.org/archives/2014/01/ansar-jerusalem-claims-respons.php> [accessed: 19.01.2025].

Biedroń M., *Zamach bombowy na tarnowskim dworcu kolejowym* (Eng. Bomb attack at Tarnów railway station), Tarnowskie Centrum Informacji, <https://www.it.tarnow.pl/atrakcje/tarnow/ciekawostki/taka-jest-historia/zamach-bombowy-na-tarnowskim-dworcu-kolejowym/> [accessed: 3.12.2024].

Blood P. W., *Hitler's Bandit Hunters: The SS and the Nazi Occupation of Europe*, Washington 2006, https://books.google.pl/books?id=jR49G7eyxBUC&pg=PA101&redir_esc=y#v=onepage&q&f=false [accessed: 3.12.2024].

Botha A., *Prevention of Terrorist Attacks on Critical Infrastructure*, in: *Handbook of Terrorism Prevention and Preparedness*, A.P. Schmid (ed.), https://icct.nl/sites/default/files/2023-01/Handbook_Schmid_2020.pdf, pp. 841–870 [accessed: 20.11.2024].

Butter D., *Does Turkey really get its oil from Islamic State?*, BBC, 1.12.2015, <https://www.bbc.com/news/world-europe-34973181> [accessed: 1.12.2025].

Byzdra K., *Partyzanci mieli zaatakować rurociągi w Kolumbii. Na miejsce wysłano wojsko* (Eng. Guerrillas were to attack pipelines in Colombia. The military was sent to the site), Energetyka24, 27.08.2024, <https://energetyka24.com/ropa/wiadomosci/partyzanci-mieli-zaatakowac-rurociagi-w-kolumbii-na-miejsce-wyslano-wojsko> [accessed: 27.12.2024].

Candan B., *Top 5 critical infrastructure cyberattacks*, Anapaya, 17.10.2024, <https://www.anapaya.net/blog/top-5-critical-infrastructure-cyberattacks> [accessed: 17.10.2024].

Chiczkin A., *Jordania: zamach stanu w odwrotnej kolejności* (Eng. Jordan: coup d'état in reverse), TopWar, 12.04.2021, <https://pl.topwar.ru/181817-iordanija-perevorot-naoborot.html> [accessed: 12.12.2024].

14-latek przestawiał zwrotnice (Eng. 14-year-old switched railway crossovers), Policja.pl, 9.01.2008, <https://www.policja.pl/pol/aktualnosci/13278,14-latek-przestawial-zwrotnice.html> [accessed: 9.01.2025].

Czyżewski D., *Ropa pod uprawami koki, czyli problemy Kolumbii* (Eng. Oil under coca crops – Colombia's problems), Energetyka24, 2.10.2021, <https://energetyka24.com/ropa/ropa-pod-uprawami-koki-czyli-problemy-kolumbii-komentarz> [accessed: 2.12.2024].

Čokorilo O., Čokorilo S., Tomic L., *A framework for aviation security*, AIIT 4th International Conference on Transport Infrastructure and Systems (TIS ROMA 2024), https://www.researchgate.net/publication/381768379_A_framework_for_aviation_security [accessed: 28.02.2025].

Daily Mail, *New report explores the pilot of MH370 troubled personal life, likely scenario of what happened on flight*, New Zealand Herald, 18.06.2019, <https://www.nzherald.co.nz/world/new-report-explores-the-pilot-of-mh370-troubled-personal-life-likely-scenario-of-what-happened-on-flight/TOQ557EGUHWQDXG5DU47E7JOVE/> [accessed: 18.12.2024].

De nouvelles centrales nucléaires survolées par de présumés drones, TF1Info, 2.08.2024, <https://www.tf1info.fr/societe/de-nouvelles-centrales-nucleaires-survolees-par-de-presumes-drones-1562592.html> [accessed: 2.08.2024].

Desler M., *Seven five – man with knife, lotnictwo, a terroryzm* (Eng. Seven five – man with knife, aviation, and terrorism), dlapilota.pl, 9.04.2014, <https://dlapilota.pl/wiadomosci/monika-desler/seven-five-man-knife-lotnictwo-terroryzm> [accessed: 9.12.2024].

Duchesneau J., *Aviation Terrorism. Thwarting High-Impact Low-Probability Attacks*, Royal Military College of Canada, Kingston 2015, <https://espace.rmc.ca/jspui/bitstream/11264/741/1/Duchesneau%20PhD%20Thesis%2020150726%20Final%20e-Space%20RMC.pdf> [accessed: 6.12.2024].

EUROCONTROL, *Aviation under attack from a wave of cybercrime*, <https://www.eurocontrol.int/sites/default/files/2021-07/eurocontrol-think-paper-12-aviation-under-cyber-attack.pdf> [accessed: 5.07.2024].

European Commission, *Enhancing EU resilience: A step forward to identify critical entities for key sectors*, https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_23_3992/IP_23_3992_EN.pdf [accessed: 12.12.2024].

Farnworth R., *The Uganda Railway during the First World War*, <https://rogerfarnworth.com/2020/12/28/the-uganda-railway-during-the-first-world-war/> [accessed: 28.12.2024].

Horror w przestworzach, gangi ostrzelały dwa samoloty. Ranna stewardessa (Eng. Horror in the skies, gangs fire on two planes. Injured stewardess), Polskie Radio 24, 12.11.2024, <https://polskieradio24.pl/arttykul/3445609,horrer-w-przestworzach-gangi-ostrelaly-dwa-samoloty-ranna-stewardessa> [accessed: 21.12.2024].

Howden D., *Shell may pull out of Niger Delta after 17 die in boat raid*, The Independent, 17.01.2006, <https://web.archive.org/web/20170527010950/http://www.corpwatch.org/article.php?id=13121> [accessed: 17.01.2025].

Iran condemns 'terrorist' attack on gas pipelines, Al Jazeera, 14.02.2024, <https://www.aljazeera.com/news/2024/2/14/iranian-gas-pipeline-blasts-due-to-terrorism-and-sabotage-official-says> [accessed: 14.12.2024].

Jenkins B.M., *The Terrorist Threat to Commercial Aviation*, Santa Monica 1989, <https://www.rand.org/content/dam/rand/pubs/papers/2008/P7540.pdf> [accessed: 25.02.2025].

Jenkins B.M., Butterworth B.R., *How Sophisticated are Terrorist Attacks on Passenger Rail Transportation*, San José 2020, <https://transweb.sjsu.edu/sites/default/files/SP0520-Jenkins-Terrorist-Attacks-Passenger-Rail-Transportation.pdf> [accessed: 3.12.2024].

Jenkins B.M., Butterworth B.R., *Train Wrecks and Track Attacks: An Analysis of Attempts by Terrorists and Other Extremists to Derail Trains or Disrupt Rail Transportation*, https://transweb.sjsu.edu/sites/default/files/1794_Jenkins_Train-Wrecks-Train-Attacks.pdf [accessed: 3.12.2024].

Jenkins B.M., Butterworth B.R., Shrum K.S., *Terrorist Attacks on Public Bus Transportation: A Preliminary Empirical Analysis*, Mineta Transportation Institute 2010, <https://transweb.sjsu.edu/sites/default/files/2982-Terrorist-Attacks-On-Public-Bus-Transportation.pdf> [accessed: 3.12.2024].

Jones T., *MH370: Search resumes to find missing plane 11 years on*, Deutsche Welle, 25.02.2025, <https://www.dw.com/en/mh370-search-resumes-to-find-missing-plane-11-years-on/a-71739469> [accessed: 25.02.2025].

Kennedy C., *Guerilla Attacks on Pipelines Threaten Colombia's Oil Production*, Oil Price, 10.09.2024, <https://oilprice.com/Energy/ Crude-Oil/Guerilla-Attacks-on-Pipelines-Threaten-Colombias-Oil-Production.html> [accessed: 10.09.2024].

Kielban Ł., *Zagrożenia dla Infrastruktury Krytycznej – podstawy dla urzędników i przedsiębiorców*, Polska Platforma Bezpieczeństwa Wewnętrznego, 13.06.2024, <https://ppbw.pl/zagrozenia-infrastruktury-krytycznej-podstawy/> [accessed: 13.12.2024].

Kirkland R., “A secret, melodramatic sort of conspiracy”: *The disreputable legacies of Fenian violence in nineteenth-century London*, King’s Research Portal, https://kcl-pure.kcl.ac.uk/ws/portalfiles/portal/114850253/A_secret_melodramatic_sort_KIR-KLAND_Accepted25July2017Published12August2019_GREEN_AAM.pdf [accessed: 3.12.2024].

Library of Congress, Federal Research Division, *Country Profile: Colombia*, 2007, <https://maint.loc.gov/rr/frd/cs/profiles/Colombia.pdf> [accessed: 15.12. 2024].

List of terrorist incidents in London, Wikipedia, https://en.wikipedia.org/wiki/List_of_terrorist_incidents_in_London [accessed: 19.12.2024].

Losik J., *Wiadomo, co przewoził zaatakowany statek. Powód do niepokoju dla Moskwy* (Eng. It is known what the attacked ship was carrying. A cause for concern for Moscow), Money.pl, 27.01.2024, <https://www.money.pl/gospodarka/nieoczekiwany-cios-w-handel-rosyjskim-paliwem-zaplona-tankowiec-6989192670440384a.html> [accessed: 27.01.2025].

Mandrup T., *The attack on Palma in Mozambique: An insurgency getting out of hand?*, Risk Intelligence, 8.04.2021, <https://www.riskintelligence.eu/analyst-briefings/the-attack-on-palma-in-mozambique-an-insurgency-getting-out-of-hand> [accessed: 8.01.2025].

Mansfield I., *The first terrorist attack on the London Underground*, IanVisits, 30.10.2013, <https://www.ianvisits.co.uk/articles/130th-anniversary-of-the-first-terrorist-attack-on-the-london-underground-9335/> [accessed: 30.10.2024].

Marx G., *Oleoducto en peligro recibe tropas estadounidenses en Colombia*, Amazon Watch, 12.11.2002, <https://amazonwatch.org/es/news/2002/1112-imperiled-pipeline-gets-us-troops-in-colombia> [accessed: 12.11.2024].

Mbah F., *In Nigeria’s crude capital, a plan to win the war against oil theft*, Al Jazeera, 19.12.2024, <https://www.aljazeera.com/news/2024/12/19/in-nigerias-crude-capital-a-plan-to-win-the-war-against-oil-theft> [accessed: 19.12.2024].

McEvoy J., *La Financiación de BP a los militares asesinos de Colombia*, Declassified UK, 18.07.2023, <https://www.declassifieduk.org/es/la-financiacion-de-bp-a-los-militares-asesinos-de-colombia/> [accessed: 18.12.2024].

Nigeria train resumes operations eight months after major attack, Al Jazeera, 5.12.2022, <https://www.aljazeera.com/news/2022/12/5/nigeria-train-resumes-eight-months-after-deadly-attack> [accessed: 5.12.2024].

Nigerian oil exports at lowest level in 25 years due to oil theft, Al Jazeera, 9.09.2022, <https://www.aljazeera.com/news/2022/9/9/nigerian-oil-exports-at-lowest-level-in-25-years-due-to-oil-theft> [accessed: 9.01.2025].

Olanicki M., *Tajemnicze awarie polskich pociągów. O sabotaż podejrzewany producent* (Eng. Mysterious failures of Polish trains. Manufacturer suspected of sabotage), Biznes Info, 6.12.2023, <https://www.biznesinfo.pl/tajemnicze-awarie-polskich-pociagow-o-sabotaz-podejrzewany-producent-mo-wak-061223> [accessed: 6.12.2024].

Olech A., *Terrorist Threats to the Energy Sector in Africa and the Middle East*, in: S.J. Lohman et al., *Countering Terrorism on Tomorrow's Battlefield: Critical Infrastructure Security and Resiliency* (NATO COE-DAT Handbook 2), <https://press.armywar-college.edu/cgi/viewcontent.cgi?article=1953&context=monographs> [accessed: 15.12.2024].

Oltermann P., Beaumont P., Sabbagh D., *European leaders blame sabotage as gas pours into Baltic from Nord Stream pipelines*, The Guardian, 28.09.2022, <https://www.theguardian.com/business/2022/sep/27/nord-stream-1-2-pipelines-leak-baltic-sabotage-fears> [accessed: 28.12.2024].

PAP, *Egipt: katastrofa samolotu Airbus A321 na Półwyspie Synaj (aktualizacja)* (Eng. Egypt: Airbus A321 plane crashes in the Sinai Peninsula (update)), [dlapilota.pl](https://dlapilota.pl/wiadomosci/pap/egipt-katastrofa-samolotu-airbus-a321-na-polwyspie-synaj), 17.11.2015, <https://dlapilota.pl/wiadomosci/pap/egipt-katastrofa-samolotu-airbus-a321-na-polwyspie-synaj> [accessed: 17.12.2024].

PAP, *Kolumbia: 15 żołnierzy zginęło w zasadzce FARC* (Eng. Colombia: 15 soldiers killed in FARC ambush), Wirtualna Polska Wiadomości, 21.07.2013, <https://wiadomosci.wp.pl/kolumbia-15-zolnierzy-zginelo-w-zasadzce-farc-6079340922217089a> [accessed: 21.12.2024].

Pawluszek A., *Malezyjski Boeing 777 zestrzelony przez Rosjan w 2014 r. Sąd w Hadze przedstawił stanowisko* (Eng. Malaysian Boeing 777 shot down by Russians in 2014. The Hague-based court outlined the position), Gazeta Prawna, 17.11.2022, <https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8590126,holandia-sad-zestrzelenie-2014-malezyjski-boeing-777-ukraina.html> [accessed: 17.11.2024].

Piotrowski M.A., *Taktyka oraz konsekwencje strategiczne ataku na instalacje naftowe Arabii Saudyjskiej* (Eng. The tactics and strategic consequences of the attack on oil installations in Saudi Arabia), „Biuletyn PISM” 2019, no. 137, https://www.pism.pl/publications/The_Tactics_and_Strategic_Consequences_of_the_Attack_on_Oil_Installations_in_Saudi_Arabia [accessed: 4.12.2024].

Reuters, *One killed, dozens injured in truck ramming at Israeli bus stop*, <https://www.reuters.com/world/middle-east/multiple-injuries-truck-strikes-bus-stop-central-israel-police-say-2024-10-27/> [accessed: 27.02.2024].

Reuters, *Teheran proponuje odszkodowania rodzinom ofiar zestrzelonego boeinga. Kijów krytykuje* (Eng. Tehran offers compensation to families of victims of downed boeing. Kyiv criticises), TVN24, 30.12.2020, <https://tvn24.pl/swiat/ukrainski-samolot-zestrzelony-nad-teheranem-wladze-iranu-oferuja-odszkodowania-dla-rodzin-ofiar-st4851794> [accessed: 30.12.2024].

Ribeiro A., *Cyber attacks continue to hit critical infrastructure, exposing vulnerabilities in oil, water, healthcare sectors*, Industrial Cyber, 14.02.2024, <https://industrialcyber.co/critical-infrastructure/cyber-attacks-continue-to-hit-critical-infrastructure-exposing-vulnerabilities-in-oil-water-healthcare-sectors/> [accessed: 14.12.2024].

Saqib M., *Recent Trends of Naxal Violence in India: Need for Comprehensive Approach from the Government*, “International Journal of Research in Social Sciences” 2018, vol. 8, p. 878, https://www.ijmra.us/project%20doc/2018/IJRSS_NOVEMBER2018/IJMRA-14770.pdf [accessed: 3.12.2024].

Scheuer M., Ulph S., Daly J.C.K., *Saudi Arabian Oil Facilities: The Achilles Heel of the Western Economy*, The Jamestown Foundation 2006, <https://jamestown.org/wp-content/uploads/2006/05/Jamestown-SaudiOil.pdf> [accessed: 24.02.2025].

Shukla N., *Maoists briefly hijack Indian train*, Reuters, 22.04.2009, <https://www.reuters.com/article/world/maoists-briefly-hijack-indian-train-idUSTRE53L102/> [accessed: 22.12.2024].

Sivesind C., *Cyber Attacks on Railway Systems Increase by 220%*, SecureWorld, 20.08.2024, <https://www.secureworld.io/industry-news/railway-cyber-attacks> [accessed: 20.08.2024].

START, *Global Terrorism Overview: Terrorism in 2019*, https://www.start.umd.edu/pubs/START_GTD_GlobalTerrorismOverview2019_July2020.pdf [accessed: 30.07.2024].

Timeline of airliner bombing attacks, Wikipedia, https://en.wikipedia.org/wiki/Timeline_of_airliner_bombing_attacks [accessed: 26.02.2025].

Tragically Explosive – Szilvestre Matuschka: A Fetish For Disaster (Part Three), Europe Between East And West, 7.03.2020, <https://europebetweeneastandwest.wordpress.com/tag/hungarian-serial-killers/> [accessed: 7.12.2024].

UNOCT, CTED, Interpol, *The protection of critical infrastructure against terrorist attacks: Compendium of good practices*, https://www.un.org/securitycouncil/ctc/sites/www.un.org/securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf [accessed: 12.12.2024].

Wald M.L., *Student Pilot, 15, Crashes Plane Into Tower in Florida*, New York Times, 6.01.2002, <https://www.nytimes.com/2002/01/06/us/student-pilot-15-crashes-plane-into-tower-in-florida.html> [accessed: 6.01.2025].

Walków M., *Coraz więcej incydentów z dronami. Lotnisko Chopina przetestuje rozwiązanie* (Eng. More and more drone incidents. Chopin Airport will test a solution), Money.pl, 30.05.2023, <https://www.money.pl/gospodarka/lotnisko-chopina-sie-zbroi-drony-to-coraz-powazniejsze-zagrozenie-dla-samolotow-6903403450051296a.html> [accessed: 30.12.2024].

Wang K., Kashi D., *Major U.S. military operations/actions to protect oil*, <https://nationalsecurityzone.medill.northwestern.edu/archives/oilchangeproject/how-do-we-protect-the-flow-of-oil/index.html> [accessed: 12.12.2024].

Zafimehy M., Chieze G., *Crash de la Germanwings: à quoi ont ressemblé les dernières minutes avant la catastrophe?*, RTL, 26.03.2023, <https://www.rtl.fr/actu/justice-faits-divers/crash-de-la-germanwings-a-quoi-ont-ressemble-les-dernieres-minutes-avant-la-catastrophe-7900246615> [accessed: 26.01.2025].

Zimmerman M., *„Cud, że tyle osób przeżyło”. Mija 50 lat od zamachu na lotnisku Fiumicino* (Eng. ‘It’s a miracle that so many people survived’. It’s 50 years since the attack at Fiumicino Airport), Onet, 17.12.2023, <https://wiadomosci.onet.pl/swiat/50-lat-od-ataku-na-lotnisku-fiumicino-najbardziej-krwawy-z-tamtych-zamachow/mpd5nm4> [accessed: 17.12.2024].

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).

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Official Journal of the EU L 345/75 of 23.12.2008).

Other documents

United Nations, *Security Council resolution 2341 (2017) [on protection of critical infrastructure against terrorist acts]*.

Krzysztof Izak

Retired officer of the Internal Security Agency, who served, inter alia, in divisions carrying out tasks in the field of counteracting terrorist threats. Author of more than 20 articles on terrorism, which were published in many scientific journals. Creator of *Lexicon of Islamist organisations and movements* published by the Internal Security Agency.

Contact: lizior3@wp.pl

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

MICHAŁ PIEKARSKI

Faculty of Social Sciences,
University of Wrocław

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

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 more².

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 customers⁵. A year later, another cyber attack targeted a single component of distribution system – a substation near Kyiv⁶. The next attack occurred in 2017, but it was much extensive, as systems not only in Ukraine were struck using the Petya ransomware⁷.

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 city⁸.

Other infrastructure was also the target of aggression. In May 2014, an explosion damaged the Urengoy-Pomary-Uzhgorod gas pipeline near Poltava⁹. Further explosions were reported in ammunition storage sites: Vinnitsya¹⁰ in 2017 and a year later in Ichnya¹¹. 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 blast*, 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 Ukraine¹³ was published and in 2022 a dedicated act of parliament about CI was adopted¹⁴.

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 States¹⁵.

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 Donbas¹⁶. 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 Ukrainy 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 flood¹⁷. A similar incident was reported in 2023¹⁸. 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 Giulio Douhet's¹⁹ 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 supply²⁰. 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 Russia²². 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, SODCIT²³. 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 outages²⁴. An additional but limited strike (28 missiles supported by drones) took place the following day. Massive strikes were recorded on 31 October²⁵ and on 15 November²⁶, 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 conducted²⁷. 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 industry²⁸. Further attacks took place in 2024. In January, 5 large-scale attacks were recorded²⁹. In February, no attacks were noted³⁰, 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 days³¹.

In May, 3 large-scale attacks³² were recorded, and in June – 4, including the largest involving a total of 100 missiles and drones³³. 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 Ukraine³⁴.

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 grid³⁵.

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 attack³⁶.

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 targets³⁷.

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 limited³⁸. 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 power³⁹.

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. Humphreys, *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 2024⁴⁰. 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 power⁴¹.

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-160⁴² 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 variant⁴³.

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 km⁴⁴, Kh-101 up to 2800 km⁴⁵. Additionally, Kh-47 missiles are sometimes employed. They are air-launched variant of Iskander missile, with range up to 2000 km⁴⁶.

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 km⁴⁷. 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 submarines⁴⁸.

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 km⁴⁹.

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 reports⁵⁰.

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-T⁵². To combat the threat of low flying drones, additional low-cost systems, employing truck-mounted machine guns, were developed for early Russian attacks in 2022⁵³. 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 missiles⁵⁴, OSA launchers employing R-73 missiles⁵⁵, 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 launchers⁵⁶. 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 drones⁵⁷. 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 of 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.

Głajzer 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 (BBP), 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

Hybrid threats to critical infrastructure in the European Union. Selected Hybrid CoE analyses

ALEKSANDER OLECH

Defence24

 <https://orcid.org/0000-0002-3793-5913>

Abstract

The author of the article describes the progression of hybrid threats, particularly in Central and Eastern Europe, with a focus on Russian influence operations. By examining 6 key publications from the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), the author identifies hybrid tactics, from disinformation and cyberattacks to maritime and kinetic threats. The research explores strategic competition, resilience-building, and legal frameworks necessary to counter challenges of these tactics. The findings highlight the need for continuous adaptation to emerging challenges, increased international cooperation, and proactive measures to mitigate the impact of hybrid operations on Western states. Understanding the evolution of these threats is important for strengthening national security, improving resilience, and developing effective counterstrategies.

Keywords

Russia, critical infrastructure, hybrid threats, terrorism, Finland, Baltic Sea

Introduction

Hybrid threats and their evolution are becoming increasingly significant for global security. These are no longer just negative actions that can be easily categorised as competition in Europe between European Union and NATO Member States and the Russian Federation (RF). Today, hybrid threats are evident on a global scale, with the Kremlin's imperial policies amplifying their scope and refining the tools used to exert influence, alongside the malicious activities of other actors, such as North Korea and Iran.

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) defines hybrid threats as actions conducted by state or non-state actors that aim to undermine or harm a target by combining overt and covert military and non-military means. These activities use detection thresholds and attribution, as well as the boundary between war and peace, to influence decision-making processes at different levels – local, regional, state or institutional – in order to achieve the strategic objectives of the attacking entity and simultaneously harm the attacked entity.

The objective of hybrid action is to affect diverse decision-making processes at the regional, national, or institutional levels to promote and/or attain strategic goals while concurrently undermining the target, predominantly Western nations in contemporary contexts.

Apparently benign actions may be a part of a hybrid operation, that according to the perpetrator's plan, should remain hidden or reduce the victim's ability to associate the act to its initiator. This complicates any response, as such operations – evident in the case of countries along NATO's and the EU's eastern border – occur below the threshold of war or involve actors that are challenging to verify. Despite certain attacks being ascribed to Russia, Iran, or China, the reactions from Western states remain constrained.

Some of state and non-state actors are keen to exploit gaps in international law to complicate the collective defence of Western nations against hybrid threats. This constitutes their paramount advantage. A significant obstacle for nations adhering to international law is the protracted process of consultation and decision-making on the appropriate response, which requires the involvement of actors such as the UN, EU, NATO. During this period, the antagonist can carry out hybrid activities. This is also apparent in the creation of tools to minimise threats, as for law-abiding nations, this process is significantly prolonged.

All Central and Eastern European countries are exposed to hybrid threats, which can take any form of attack as long as they remain below the threshold of war. However, the line defining when a conflict actually begins or when an attacked state (or entity) can respond remains blurry.

Since 2014, the frequency of hybrid attacks executed by the RF has been consistently progressing. These assaults are perpetrated by military personnel, intelligence agencies, journalists, and politicians, alongside individuals who are either oblivious to their support of Russian influence or are recruited agents who opt to act in Russia's interest for financial, professional, or political gain, or due to personal convictions. As a result, hybrid threats can be observed not only in the sphere of war, the perspective of compliance with international law, but also in cybersecurity, information (disinformation), politics, economics, culture, religion, and society. Additionally, such threats include kinetic actions, such as maritime and aerial incidents (e.g. airspace violations). Russia seeks every means to negatively impact its chosen adversaries.

This analysis is based on 6 scientific publications from the Hybrid CoE:

1. *The Landscape of Hybrid Threats: A Conceptual Model*¹ – presents the evolution of hybrid threats, the activities of Russia, China, and non-state actors, as well as the areas in which hybrid attacks are carried out.
2. *The concept of hybrid war in Russia: A national security threat and means of strategic coercion*² – primarily focuses on threats to Russia itself, which in turn serves as a justification for developing strategies to protect its own interests and to create strategic competition with Western states in specific areas.

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: 2.01.2025].

² K. Pynnöniemi, *The concept of hybrid war in Russia: A national security threat and means of strategic coercion*, Hybrid CoE Strategic Analysis / 27, May 2021, https://www.hybridcoe.fi/wp-content/uploads/2021/05/20210518_Hybrid_CoE_Strategic_Analysis_27_The_concept_of_hybrid_war_in_Russia_WEB.pdf [accessed: 10.01.2025].

3. *Handbook on maritime hybrid threats: 15 scenarios and legal scans*³ – scrutinises a diverse array of hybrid threats, especially those pertinent to activities in the maritime sphere. This is particularly significant regarding current challenges in the Baltic Sea region.
4. *A comprehensive resilience ecosystem*⁴ – it takes into account increasing complexity of attacks, including hybrid threats, the ability to recover and rebuild infrastructure; it is crucial for understanding resilience – a pillar of national and multinational security.
5. *Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage*⁵ – provides a model example of how the RF instrumentalises hybrid attacks as a tool of destabilisation in its near abroad. This is a particularly valuable publication for countermeasures undertaken by governments and international organisations.
6. *Protecting maritime infrastructure from hybrid threats: legal options*⁶ – examines hybrid threats to maritime infrastructure, highlighting legal gaps and security challenges. It calls for stronger international cooperation and legal reforms to protect critical undersea assets.

The discussed research is important for understanding the concept of hybrid operations carried out against the broadly defined Western states. The analysis demonstrates how the form and scope of hybrid threats have evolved over the years, as well as the main challenges NATO and EU countries face in responding to them. Particular attention has been given to actions conducted by the RF.

³ *Hybrid CoE Paper 16: Handbook on maritime hybrid threats: 15 scenarios and legal scans*, March 2023, https://www.hybridcoe.fi/wp-content/uploads/2023/03/NEW_web_Hybrid_CoE_Paper-16_rgb.pdf [accessed: 17.01.2025].

⁴ R. Jungwirth et al., *Hybrid threats: a comprehensive resilience ecosystem*, Publications Office of the European Union, Luxembourg 2023, https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf [accessed: 22.01.2025].

⁵ H. Praks, *Hybrid CoE Working Paper 32: Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage*, May 2024, <https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240530-Hybrid-CoE-Working-Paper-32-Russias-hybrid-threat-tactics-WEB.pdf> [accessed: 30.01.2025].

⁶ A. Sari, *Hybrid CoE Research Report 14: Protecting maritime infrastructure from hybrid threats: legal options*, March 2025, <https://www.hybridcoe.fi/wp-content/uploads/2025/03/20250306-Hybrid-CoE-Research-Report-14-web.pdf> [accessed: 6.03.2025].

The author has extracted essential components from each reviewed publication to delineate a roadmap of the analysed hybrid threats, emphasising their evolution in recent years. Simultaneously, he indicated that some of them will emerge in various forms and locales in the future, while present actions by adversaries (e.g. damage to critical infrastructure, CI) lay the foundation for subsequent assaults.

An empirical analysis and review of the studies presented are crucial for advancing research on hybrid threats. However, further studies are being carried out analysing emerging security threats from different perspectives. Consequently, it is pertinent to persist in dialogues regarding hybrid threats to elucidate the phenomenon, enhance public awareness, foster resilience, and formulate best practices and responses for both effective reaction and prevention.

Comprehensive resilience ecosystem

Resilience is the capacity of a system – personal, community, or institutional – to withstand, bounce back, and change following disturbances. Academic study has changed over time from seeing resilience as something fixed to seeing it as a dynamic process, where adaptation and transformation are quite important⁷. Resilience is becoming a pillar of national security given the growing complexity of attacks, including hybrid threats, and the need of recovery and repair infrastructure.

Resilience is sometimes defined depending on cultural viewpoints, which influence the development and execution of policies. In Russia, for instance, resilience is usually connected with endurance and stability. While resilience in many Arab countries is shaped by geopolitical events, in China the focus is on adaptation⁸.

The European Union's priorities in the first decade of 21st century were crisis management and safeguarding of CI. The concept of resilience was only formally integrated into the process of EU policy-making in 2017 with the document: *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*. The European Commission first presented the *Joint Communication to the European*

⁷ R. Jungwirth et al., *Hybrid threats: a comprehensive resilience ecosystem...*, p. 17.

⁸ Ibid., p. 19.

Parliament and the Council. Joint Framework on Countering Hybrid Threats a European Union response document in 2016. The paper listed 22 actions meant to counter hybrid threats. Adopted by the European Council on 25 May 2022, the *Strategic Compass for Security and Defence* is currently the guiding concept of the EU's resilience strategy⁹.

The COVID-19 pandemic influenced NATO's strategy. The Allies worked on preparing the healthcare sector. In 2020, NATO undertook a revision of the Seven Baseline Requirements (7BLR) for civil preparedness to take into account the impact of the pandemic. During the Brussels Summit, the Alliance decided to strengthen its resilience through (...) *work across the whole of government, with the private and non-governmental sectors, with programmes and centres of expertise on resilience established by Allies, and with our societies and populations, to strengthen the resilience of our nations and societies*¹⁰.

Democratic systems, in addition to relying on trust in society, government, and state institutions, are built on 7 main pillars:

- 1) feeling of justice and equal treatment, including a belief in a fair and impartial system, protection of property and identity;
- 2) civil rights and liberties such as freedom of speech, the right to vote;
- 3) political responsibility and accountability, expressed through free and fair elections and open public debate;
- 4) rule of law, i.e. equality of all before the law and independence of the judiciary;
- 5) political, social, and economic stability;
- 6) reliability and availability, understood as a guaranteed access to basic goods and services;
- 7) foresight capabilities, i.e. the ability to identify threats and develop intensive public-private cooperation, implementation of innovations).

It is these elements that constitute the foundation of the resilience and durability of modern democracies¹¹.

The foundations of the Comprehensive Resilience Ecosystem (CORE) are 3 main domains: civic (society and culture), governance (administration,

⁹ Ibid., p. 26.

¹⁰ Ibid., p. 29.

¹¹ Ibid., p. 33.

political processes, diplomacy), and services (infrastructure, economy). CORE can promote cross-sectoral efforts involving the entire society by summarising key interconnections. It provides a methodology that enables a better understanding of interactions between systems, institutions, and social factors. It allows for the presentation of incidents and their consequences, as it serves as a mechanism for enhancing resilience against hybrid threats and fortifying democratic societies. CORE concentrates on hybrid threats that aim to exploit systemic vulnerabilities at local, national, or international scales. It can serve as an important signal for the evolution and expansion of resilience capabilities. Support from policymakers is necessary to introduce appropriate legislation and raise public awareness of the potential consequences of hybrid attacks.

In addition, continued development of technologies to detect, warn of, counter and mitigate hybrid threats to enhance resilience is essential¹².

The landscape of hybrid threats

States and regions perceive not only security but also the constantly evolving hybrid threats in different ways¹³. These threats, along with hybrid actions, are understood as a combination of regular and irregular actions (i.e. of varying intensity and frequency), both undertaken by armed forces as well as criminals, terrorists, or even political organisations¹⁴. Such new form of threat, or rather its diverse nature, indicates the need to verify the ability of states to respond to perils of this kind. This is primarily related to actions of governments, efficiency of defence systems, and international security cooperation in terms of security. In this case, it is crucial to view the current situation in Ukraine, the Balkans, Syria, Libya, or Central Africa through the prism of both military and non-military challenges.

Hybrid actions are primarily carried out by actors with authoritarian or totalitarian views on power. Their objective is to direct all possible

¹² Ibid., p. 78.

¹³ G. Giannopoulos, H. Smith, M. Theocharidou, *The Landscape of Hybrid Threats: A Conceptual Model...*, p. 9.

¹⁴ A. Olech, *Cooperation between NATO and the European Union against hybrid threats with a particular emphasis on terrorism*, Institute of New Europe, 17.03.2021, <https://ine.org.pl/en/cooperation-between-nato-and-the-european-union-against-hybrid-threats-with-a-particular-emphasis-on-terrorism/> [accessed: 10.02.2025].

(authoritarian) tools against democratic systems¹⁵. As a result, governments of this nature often last for decades and become more entrenched over time. Importantly, one authoritarian leader is replaced by another.

State actors engaging in hybrid activities are mainly authoritarian or totalitarian states. Their internal strategy for maintaining power is considered identical to the strategy of hybrid warfare, in the context of which democratic states are perceived as an existential threat to these regimes. Therefore, these regimes attempt to undermine and weaken the capabilities of democratic states. Here, information plays a very important role – it is a tool that enables the manipulation of social beliefs and discourages collective action against the regime¹⁶.

The development of media, including social media, has created new opportunities for disinformation and propaganda activities. Now anyone can be a broadcaster and publish from anywhere; new platforms have emerged that are beyond state control; there are new opportunities to distort content; media globalisation has accelerated; new business models have developed, and the economic structure has become data-driven¹⁷. Disinformation from authoritarian countries is far more frequent and powerful in terms of the scope of the information being spread. This is due to the fact that democratic countries have regulatory and verification processes in place¹⁸. It should be noted that debunking fake news is several times more difficult than publishing false information.

In the past, the promotion of democracy was considered a hybrid threat – for example, the activities of NGOs in non-democratic countries and their efforts to promote democracy. These actions are solely intended to push authoritarian states towards democracy. However, as these states become aware of this, they respond by introducing laws on foreign actors or banning the activities of NGOs and think tanks. Currently, a hybrid threat should be defined as a form of covert, coercive, or corrupt use of force (e.g. blackmail). Referring, for instance, to the activities of NGOs aimed

¹⁵ G. Giannopoulos, H. Smith, M. Theocharidou, *The Landscape of Hybrid Threats: A Conceptual Model...*, p. 15.

¹⁶ Ibid., p. 16.

¹⁷ Ibid., p. 17.

¹⁸ Ibid., p. 18.

at promoting democracy¹⁹, it has also been suggested in the past that soft power and public diplomacy could be considered hybrid threats.

It should be noted that the costs of conducting irregular attacks described as hybrid actions are much lower than those of traditional war. Moreover, the attacker is not, at least not entirely, exposed to a strong reaction of international community. The hybrid conflict in Ukraine is part of an evolution that is taking place in post-Soviet countries (as is currently happening in Belarus, for example). It is a multidimensional crisis, comprising the actions of national and supranational entities pursuing their political and economic interests with the available range of methods: from the conventional use of armed forces to fake news distribution. Allowing the development of separatist enclaves, such as those in Moldova, Georgia, and Azerbaijan, is a serious problem and requires these countries to cooperate with NATO and EU Member States and create a common sphere of security.

Russia

In Russia, a strategy of self-regulation is in place. This means that, through ingrained Russian values, citizens – including businesses and other non-state actors – act without prior coordination with the authorities, implementing solutions aligned with the political concepts proposed by Moscow. This approach facilitates the decentralised execution of strategic goals, allowing for flexibility in actions. Russianness serves as a unifying element, binding all Russians together to safeguard Russia's national strategic interests and the objectives set by the highest leadership – critical for mobilising society²⁰.

Reflexive control is a fundamental concept in Russian strategic theory, highlighting the role of psychological manipulation of adversaries. The objective is to establish circumstances in which adversaries make choices that coincide with Russia's strategic aims while perceiving themselves as acting contrary to Moscow's interests²¹.

¹⁹ Ibid.

²⁰ Ibid., p. 19.

²¹ Ibid., pp. 19–20.

China

China bases its attempts to achieve great power status on Halford Mackinder's Heartland theory²². China seeks to achieve this by becoming a maritime power²³. It relies on Sun Tzu and his concept of the art of effectively deceiving the enemy and, ideally, winning a war without the need to resort to weapons²⁴. Three factors determine the strategic behaviour of Chinese military forces: strategic thinking, strategic environment, and military potential. This triad shapes comprehensive planning and strategy execution in response to hybrid threats²⁵.

Traditional Chinese strategy operates within a dialectical framework that recognises dynamic properties such as “weakness” and “strength”. The concepts are fluid and adaptable, functioning both as abstractions and as actions in strategic practice²⁶. The Chinese concept of the 3 wars includes psychological warfare (achieving goals by influencing the psyche, e.g. deterrence, coercion, deception), public opinion warfare (influencing domestic and international support by using selective information provided through various media, shaping a specific system of values in society), and legal warfare (actions taken in order to gain legal advantage by utilising or modifying national and international law to achieve political or military superiority)²⁷.

Non-state actors

A state operating through non-state entity is, for example, Iran, which uses Hezbollah. Another example is Russia and the Wagner Group. One can point to entities such as Islamic militias in Africa and the Middle East, as well as terrorist groups like the IRA (Irish Republican Army), ETA (Basque: Euskadi Ta Askatasuna), or the Tamil Tigers. Another group of non-state actors is beginning to develop, namely private military groups (private military companies, PMC), sometimes referred to as security companies.

²² Heartland (or “pivot area”), according to Mackinder, it is the area of Eurasia – roughly today's Russia and Central Asia – a region less vulnerable to attacks from the sea, difficult to conquer, but crucial for dominance over the continent.

²³ G. Giannopoulos, H. Smith, M. Theodoridou, *The Landscape of Hybrid Threats: A Conceptual Model...*, p. 20.

²⁴ Ibid., p. 21.

²⁵ Ibid.

²⁶ Ibid.

²⁷ Ibid.

The Wagner Group is also among them. The role of PMCs in creating hybrid threats is growing²⁸.

Covert state actions by the aggressor have the advantage that they make it more difficult for target states to not only detect and prevent the possibility of harmful operations, but also to attribute responsibility for these operations to the foreign state, e.g. in the case of the annexation of Crimea, to Russia and the Night Wolves MC (Russian: Ночные Волки). The aggressor states can deny and reject accusations, achieve their goals secretly, e.g. gain access to critical sectors (e.g. Russian interference in the 2016 US presidential election)²⁹.

Criminal organisations operating in target countries are increasingly being used by aggressor countries. For example, they provide these countries with existing smuggling networks, supply forged documents, commit financial crimes, or simply threaten strategic countries, groups, or individuals³⁰.

Understanding hybrid threats as the existence of criminal or terrorist organisations is crucial. However, a small number of these entities have conducted operations against Western states to achieve their goals. So far, they have used violence or threatened to use it, but not on a scale that would clearly classify them as hybrid states³¹.

Hybrid threat domains

There are 13 domains in which hybrid threats may occur: infrastructure, economy, intelligence, information, cyberspace, diplomacy, politics, culture, society, legal, military/defence, outer space and administration³². In the context of hybrid threats the most important are:

1. Cyberspace – as a new field for delivering threats in the form of cybercrime, propaganda, espionage, terrorism, and even war. Smaller actors have greater opportunities to operate in cyberspace than in the real world³³.

²⁸ Ibid., p. 23.

²⁹ Ibid., pp. 23–24.

³⁰ Ibid., p. 24.

³¹ Ibid.

³² Ibid., p. 26.

³³ Ibid., p. 28.

2. Outer space – hybrid actions in this space are increasingly concerning due to the fact that several countries are developing counter-space capabilities. As a result, this may affect other domains, e.g. the military, because the space sphere is its integral part³⁴.
3. Society – the social domain is usually used to generate, deepen, or exploit socio-cultural divisions that will cause social upheavals necessary to continue or succeed in hybrid threat activities³⁵.
4. Legal domain – refers to a set of legal regulations, actions, processes, and institutions. Authoritarian states may use counter-laws, create them to achieve their goal, or exploit gaps in existing law in democratic countries. For example, reliance on the right to freedom of speech creates space for disinformation campaigns³⁶.
5. Intelligence – a state usually uses its intelligence capabilities to support planned or ongoing hybrid threat activities or may attempt to influence the intelligence operations of the target state³⁷.
6. Diplomacy – hybrid actions, especially in this sphere, aim to create divisions at the national or international level, support information campaigns, and interfere in the decision-making process (diplomatic sanctions, using embassies)³⁸. Diplomacy intersects with domestic politics, so state decision-makers must create two-level strategies. Diplomacy is also closely related to the economy, social sphere, and legal sphere. Actions in the sphere of diplomacy may negatively impact the economy of a state³⁹.
7. Information – if it is controlled, falsely disseminated or inspires certain actions, it can become an element of hybrid warfare and influence the adversary.

Since the annexation of the Crimea by Russia in 2014, many initiatives have been undertaken to strengthen the resistance of the EU and NATO to hybrid threats. These efforts must be recognised by the Member States, and the pace of activities and their intensity must be maintained. Due to

³⁴ Ibid.

³⁵ Ibid., p. 30.

³⁶ Ibid.

³⁷ Ibid., p. 31.

³⁸ Ibid.

³⁹ Ibid., p. 32.

the ever-changing nature of hybrid threats, continued vigilance is required. Strategic approach towards combating hybrid threats, which would involve not only international but also national structures, including entire societies, as they are the main victims of terrorism, is essential.

Due to the relatively broad scope of NATO and EU activities, a comprehensive and multi-level structure is currently being created that will enable a multi-phase response to security threats. The improvement of the previously existing response schemes, whether military, political, economic or social, allows for effective intervention and creates a geopolitical apparatus which today is of high necessity. The response is essential to adequately address the emerging challenges posed by hybrid threats.

Russian concept of hybrid war

In the ongoing debate in Russia a hybrid warfare is characterised as a blend of military and non-military actions aimed at achieving political goals⁴⁰. It should be noted that the early implementation of information warfare allows political objectives to be met without the use of armed forces⁴¹. Later, it is only necessary to maintain authoritarian power. This is why, in 2014, military and non-military actions were linked and framed as hybrid warfare with Russia⁴².

Ukraine no longer has any chances of reclaiming the territories taken by Russia in 2014. In other words, hybrid operations, including those conducted as part of the subsequent invasion and the full-scale in 2022, have led to the complete takeover of these territories. Moreover, they have significantly strengthened the RF's capabilities to conduct further hybrid operations in Ukraine and across the EU and NATO eastern flank.

In Russia, hybrid warfare is seen as an endeavour to undermine its sovereignty, civilisational distinctiveness and status of one of the world's major powers. This strategy is described as a combination of destructive and constructive actions, with the ultimate goal of causing the self-disorganization and self-disorientation of the target state. Destructive

⁴⁰ K. Pynnöniemi, *The concept of hybrid war in Russia: A national security...*, p. 3.

⁴¹ Ibid., p. 4.

⁴² Ibid.

actions are those taken by the West to divide Russian society, destroy Russian culture, and erase its traditions. Constructive actions, on the other hand, are simply Russia's defence against these activities. In Russian academic debate, the United States is identified as the main actor behind these efforts. In turn, not only the US but also the EU are mentioned in state documents as those who provoke tensions in Eurasia, especially in Ukraine⁴³.

In 2003, General Makhmut Gareev distinguished 3 categories of threats to Russia:

- 1) threats to Russia's political sovereignty and, as a result, its status as a great power,
- 2) possibility of using nuclear weapons against Russia,
- 3) the third group of threats is multi-dimensional – it includes rapid development of military technology, as well as disruption of the equilibrium of power near Russia's borders⁴⁴.

This division is still relevant. It currently coincides with Russia's persistent antagonism towards NATO and EU nations, especially regarding the situation in Ukraine. In 2013, General Gareev claimed that a significant geopolitical transformation has occurred globally, fundamentally changing the balance of power and the nature of threats, thereby requiring novel strategies and methods of response. The updated threat typology encompasses the creation of controlled chaos to incite diverse forms of unrest in adversarial nations, the subversion of undesirable power structures from within, and the destabilisation of a state's internal cohesion, exemplified by the situations in Libya and Syria⁴⁵.

Following the Crimea attack, Gareev said Russia should be proud of its actions and improve the use of soft power along with political, diplomatic, and informational tools – these components are essential for a strategic deterrent system⁴⁶. Concurrently, hybrid warfare is defined as a strategic coercion tool⁴⁷.

In Russian military terminology, strategic deterrence encompasses a collection of offensive and defensive instruments – nuclear, non-nuclear,

⁴³ Ibid.

⁴⁴ Ibid., p. 5.

⁴⁵ Ibid.

⁴⁶ Ibid.

⁴⁷ Ibid.

and non-military – that collectively constitute a “combined strategy of containment, deterrence, and coercion”⁴⁸. Russia views deterrence as measures intended to avert conflict. Moscow employs intimidation as a deterrent, motivated by the fear of potential repercussions (e.g. threatens nuclear weapon deployment to dissuade others from utilising them against itself). The amalgamation of military and non-military coercive strategies is regarded as a strategic threat to Russia⁴⁹.

Hybrid warfare is defined as a type of non-military strategic coercion that includes economic sanctions, cyberattacks, and information operations. These actions seek to subvert Russia’s political framework, provoke discord in its adjacent territories, and contest its position as a dominant force in a multipolar world⁵⁰. The RF therefore not only identifies hybrid threats for itself, but also makes full use of its capabilities to attack other nations in this way in all domains where it identifies threats. The RF performs these actions before it becomes a target itself.

Russia’s hybrid threat tactics against the Baltic Sea region

A model example of the RF’s actions in the near abroad is the instrumentalisation of hybrid attacks as a tool of destabilisation. The variety of tools at Russia’s disposal – from kinetic threats (such as sabotage) to non-kinetic threats (such as disinformation)⁵¹ – is expanding every year, and Russian intelligence services are consistently intensifying their operations, seemingly without fear of repercussions or countermeasures.

The rise in aggressive activities has been particularly noticeable in the countries of NATO’s eastern flank since February 2022 – namely, Estonia, Latvia, Lithuania, Finland, Poland, and Sweden. The objective is to weaken support for Ukraine, create internal instability in these nations, and destabilise the unity of EU and NATO structures⁵². Given the new

⁴⁸ Ibid., p. 6.

⁴⁹ Ibid.

⁵⁰ Ibid.

⁵¹ H. Praks, *Hybrid CoE Working Paper 32: Russia’s hybrid threat tactics against the Baltic Sea region...*, p. 5.

⁵² Ibid., pp. 6–7.

US administration and the uncertain situation in Ukraine, the eastern flank countries are likely the next targets for destabilisation.

Russia is determined to operate below the threshold of open war, as it understands that a prolonged conflict with NATO could end in Moscow's defeat and the complete restructuring of Russia's political system. The Kremlin's long-term goal is to reorganise Europe's security architecture and expand Russian influence – both by exerting control over Central and Eastern Europe and by securing favourable interlocutors in Western European countries⁵³.

Russian disinformation is built on crafting a false narrative of Ukraine's inevitable defeat, portraying EU and NATO governments as neglecting their own citizens in favour of supporting Ukraine, and exploiting social media to manipulate public opinion and shape societal moods⁵⁴. The volume of fake news aimed at discouraging support for Ukraine and fostering hostility toward its citizens is increasing daily. Some segments of European societies believe these narratives, which in turn fuels reluctance to aid Kyiv. This also serves as a means for the Kremlin to identify which groups are most susceptible to manipulation.

One of Russia's greatest assets is its diaspora in the Baltic states and Central Asia. Moscow actively supports pro-Russian organisations, funds initiatives promoting the Russian language, and strongly opposes the removal of Soviet monuments. It also uses various institutions, including the Orthodox Church, as political tools⁵⁵. On top of that, Russian intelligence agencies work to recruit new operatives.

Russia has established a comprehensive espionage network along NATO's eastern flank, particularly visible during operations in the Baltic states commencing in late 2023. In January 2024, Estonia's Internal Security Service (Estonian: Kaitsepolitseiamet, KAPO) apprehended a Russian political science professor from the University of Tartu, who was purportedly engaged in espionage for over a decade⁵⁶. Around the same time, KAPO uncovered a group suspected of working with Russian intelligence to carry out vandalism and physical attacks in Estonia. By April 2024, authorities had arrested 13 people, some of whom had previous

⁵³ Ibid., pp. 7–8.

⁵⁴ Ibid., pp. 9–10.

⁵⁵ Ibid., pp. 12–13.

⁵⁶ Ibid., p. 14.

criminal records. The group successfully carried out several attacks, including damaging the personal car of Estonia's Minister of Internal Affairs and defacing monuments linked to the country's resistance against the Soviet Union. Estonian officials described these incidents as part of a hybrid warfare strategy⁵⁷.

Russian intelligence also relies heavily on hacker groups to attack CI and government institutions. A December 2023 report from the European Union Agency for Cybersecurity (ENISA) revealed that half of all DDoS attacks that year were connected to Russia's war on Ukraine⁵⁸. This came just as the US announced it was halting its own cyber operations against Russia⁵⁹.

For years, Russia, in cooperation with Belarus, has been using migration as a tool to exert pressure and influence on neighbouring countries. Moscow and Minsk manipulate migration flows through disinformation, using people from the Middle East, Africa, and Central Asia to create controlled migration pressure. This forces NATO countries to strengthen their security infrastructure and intensify discussions on updating legal regulations. Migration pressure was used before the invasion of Ukraine to test NATO's response and stir public opinion, as well as before Finland's accession to the Alliance⁶⁰. Similar tactics are applied against Ukraine and Georgia to prevent their closer integration with NATO or Western structures in general.

Frontline states are the most vulnerable to hybrid threats, such as sabotage of CI. One reason for this is that Europe's underwater network of cables and pipelines was not designed with hybrid warfare threats in mind⁶¹. The same goes for acts of sabotage and efforts to polarise societies, inciting protests and creating tensions. All of this is aimed at destabilising countries that oppose Russia.

⁵⁷ Ibid., p. 15.

⁵⁸ Ibid., p. 18.

⁵⁹ M. Untersinger, *Les Etats-Unis ordonnent une pause des cyberopérations contre la Russie, selon plusieurs médias*, Le Monde, 4.03.2025, https://www.lemonde.fr/pixels/article/2025/03/03/les-etats-unis-ordonnent-une-pause-des-operations-cyber-contre-la-russie_6575971_4408996.html [accessed: 4.03.2025].

⁶⁰ H. Praks, *Hybrid CoE Working Paper 32: Russia's hybrid threat tactics against the Baltic Sea region...*, pp. 19–20.

⁶¹ Ibid., p. 21.

Maritime hybrid threats and legal aspects of maritime infrastructure protection

The definition of hybrid threats by the Hybrid CoE specifies that these are coordinated and synchronised actions deliberately targeting systemic and institutional weaknesses using a wide range of means. This also applies to actions carried out in the maritime domain⁶².

Hybrid actions, such as partial maritime transit blockade or restriction of access to state infrastructure, can pose significant risks for geographically small nations that typically rely on 1 or 2 critical maritime facilities⁶³. This is now more evident in the context of cable disruptions (e.g. fiber optic, energy) in the Baltic Sea, as well as Russia's use of the so-called shadow fleet. Such actions force EU countries to respond and continuously monitor all ship movements in the Baltic Sea.

It should be emphasised that a flagship model of hybrid attack is an attack on underwater CI (e.g. pipelines)⁶⁴. This is an example of an action that will undoubtedly continue to recur in the contemporary competition for resources.

An increasingly common threat, associated with the development of AI and other new technologies, are cyberattacks, categorised as hybrid threats. Such attacks may result in the loss of control over vessels, damage to port infrastructure, and interruptions in supply chains⁶⁵. Cyberspace has similarities to the maritime operating environment, particularly in terms of its dispersion, maneuverability, and difficulty in control.

The maritime domain presents various opportunities for covertly undermining the security of particular CI, with the intent to harm or incapacitate it. An adversarial state may utilise underwater weaponry, deploying it by itself or through someone else and trigger explosions near the CI. A potential scenario entails the establishment of control zones surrounding islands. Although this contradicts the United Nations Convention on the Law of the Sea⁶⁶ (UNCLOS), an adversary may adopt a strategy of *faits accomplis* or assert claims to such regions – typically

⁶² Hybrid CoE Paper 16: *Handbook on maritime hybrid threats...*

⁶³ Ibid., pp. 19–20.

⁶⁴ Ibid., pp. 12–13.

⁶⁵ Ibid., pp. 14–16.

⁶⁶ *United Nations Convention on the Law of the Sea, drawn up at Montego Bay on 10 December 1982.*

to establish a checkpoint, a military installation, or to ensure access to resource deposits, fishing stocks, or a transportation route within an exclusive economic zone⁶⁷.

China has been developing artificial islands and military facilities in regions also claimed by the Philippines, Vietnam, and Malaysia. They implement a policy of faits accomplis, constructing infrastructure and asserting control over navigation in areas where they lack full rights under UNCLOS. Subsequent to the annexation of Crimea, Russia instituted control zones in the Sea of Azov and surrounding the Kerch Strait, thereby impeding Ukraine's access to its ports. Japan and China are embroiled in conflicts regarding the Senkaku Islands, as China consistently dispatches coast guard vessels, establishing a de facto presence that may result in a change of control over the region.

An antagonist is also capable of deliberately carrying out illegal detentions and inspections of maritime vessels, justifying these actions under the pretext of counterterrorism efforts. Boarding a vessel may result in sabotage of its infrastructure or the installation of harmful and espionage software⁶⁸. This is another method of negatively impacting operations in the maritime domain, where vessels remain constant targets of hostile actions.

Hostile states may use fleets of fishing boats (of non-state origin) or instrumentalise non-state groups to exert pressure on CI and maritime units⁶⁹. This tactic involves leveraging ship owners, their fleets, or flags to create the illusion that the perpetrator is from another country and not, for example, Russia.

Unfriendly states may use weather modification technologies, e.g. by spraying chemicals into the atmosphere to induce rain, storms or fog, or even artificially initiate phenomena similar to natural disasters aimed at paralysing the CI of their target. A hostile nation may use these actions as a smokescreen to carry out a hybrid attack, involving for example damaging underwater telecommunications and energy infrastructure⁷⁰.

A hybrid attack may also entail the intentional obstruction of a maritime strait. Firstly, it makes it more difficult for states to guarantee

⁶⁷ *Hybrid CoE Paper 16: Handbook on maritime hybrid threats...*, p. 17, 21.

⁶⁸ *Ibid.*, p. 27.

⁶⁹ *Ibid.*, p. 36.

⁷⁰ *Ibid.*, p. 46.

the unimpeded transit of maritime vessels, and secondly, it can trigger an international political crisis, by paralysing both the domestic and foreign relations of the targeted state⁷¹. Such actions, especially regarding the Suez Canal or the Bab-El-Mandab Strait, should be anticipated in the future due to the establishment of new naval bases in the Horn of Africa. This also illustrates a potential threat that may arise in the Baltic Sea.

Further threats result from violations of international law, mainly violations of the UNCLOS. The recommendations presented in *the Handbook on Maritime Hybrid Threats: 15 Scenarios and Legal Scans* emphasise potential responses that comply with international legal standards. Over-reliance on this legal framework carries significant risks. This is because an asymmetry arises: some entities operate within the limits of the law, while others take advantage of its limitations, which gives them a strategic advantage. In such instances, the benefits gained from a successfully conducted hybrid attack can significantly outweigh the negative consequences resulting from international legal sanctions, which prompts some states to deliberately violate the law. This indicates that in a period of escalating geopolitical competition, addressing the actions of aggressors may prove exceedingly difficult, leaving mitigation and damage repair as the sole alternatives.

A potential protection strategy involves the maximum marginalisation of the hostile state or non-state actor, accompanied by continuous monitoring. This would aid in reducing the implementation of its detrimental actions, particularly in the area of maritime security.

The protection of maritime CI has become a pressing issue in light of recent hybrid threats targeting undersea cables and pipelines. The report highlights the growing vulnerabilities in this domain, particularly as state and non-state actors exploit regulatory gaps and technological weaknesses to conduct disruptive operations⁷². These hazards, which can have significant geopolitical, security, and financial ramifications, include sabotage, cyberattacks, and interference with marine traffic⁷³. Securing maritime assets has become a top concern for EU members and NATO

⁷¹ Ibid., p. 31.

⁷² A. Sari, *Hybrid CoE Research Report 14: Protecting maritime infrastructure from hybrid threats...*, p. 5.

⁷³ Ibid., p. 6.

allies given the vital part marine infrastructure plays in global trade, energy distribution, and communication networks⁷⁴.

Legal systems have great power to solve these problems, but they also impose major constraints. The UNCLOS convention, by establishing jurisdictional zones allowing coastal states different degrees of control over maritime activities, make it difficult for states to act decisively against hybrid threats arising outside their territorial boundaries given the scattered character of legal regulations. Although current legal tools give general authority for preserving situational awareness, they lack clear procedures for reactions, especially in cases of threats developing in international waters⁷⁵.

The vulnerability of submarine communication cables, essential for global internet connectivity and financial transactions, is a significant concern. Hybrid threat actors have exhibited their capacity to target these cables, as evidenced by the recent incidents in the Baltic Sea⁷⁶. The RF, as previously stated, has no qualms about intensifying the nefarious activities it has conducted in Central and Eastern Europe in recent years.

The challenge of assigning accountability for these hybrid attacks complicates adequate response, as offenders may exploit jurisdictional ambiguities to avoid legal liability. The need is for close international collaboration and intelligence-sharing systems to prevent potential threats, considering both the economic and security risks linked to such disruptions⁷⁷.

It is necessary to develop and publish a comprehensive strategy to mitigate these vulnerabilities. Initially, states must guarantee the comprehensive application of their domestic legal frameworks to effectively implement legislative and executive jurisdiction, in accordance with the provisions of UNCLOS. This involves recognising that there are legal deficiencies, which hybrid threat actors can exploit and adapting national legislation to enhance cross-border cooperation in the field of law enforcement. Secondly, legal interpretations must be modified to address emerging threats, including the intentional targeting of undersea infrastructure via cyber and kinetic methods⁷⁸.

⁷⁴ Ibid., p. 8.

⁷⁵ Ibid., pp. 16–17.

⁷⁶ Ibid., p. 27.

⁷⁷ Ibid., pp. 32–36.

⁷⁸ Ibid., p. 32.

Another key recommendation is the reinforcement of diplomatic efforts to establish new international rules for the protection of critical maritime assets. The report suggests that EU and NATO members work collectively to strengthen regulatory measures, including the adoption of binding agreements that enhance the security of submarine cables and pipelines. Additionally, joint exercises and real-time information-sharing initiatives should be expanded to improve threat detection and response capabilities⁷⁹.

The evolving nature of hybrid threats requires a proactive and adaptive legal strategy. States must be prepared to update and expand their policies in response to emerging challenges. Safeguarding maritime infrastructure is not just a national security concern but a global imperative⁸⁰. This issue is particularly relevant in the Baltic Sea region.

Summary

The research analysed, based on Hybrid CoE studies, provides a comprehensive understanding of hybrid threats, particularly their implications for CI in the European Union, with a strong impact on Central-Eastern Europe. The main malicious actor in recent years has been, and still is, the RF. However, more adversaries are using hybrid tools to increase their presence and influence. At the same time, the nature of hybrid threats is rapidly evolving.

The study *The Landscape of Hybrid Threats: A Conceptual Model* provides a broad view of the evolution and mechanisms of hybrid threats posed by both state and non-state actors. In turn, *The Concept of Hybrid War in Russia: A national security threat and means of strategic coercion* provides an understanding of Russia's strategic goals by portraying its hybrid activities in the context of geopolitical competition. *Handbook on maritime hybrid threats: 15 scenarios and legal scans* emphasises the need to focus more on maritime area (mainly in the Baltic Sea), which is vital for the EU and NATO in terms of infrastructure, economic and transport stability, as well as regional security. Equally crucial is *A comprehensive resilience ecosystem*, which underlines the need of resilience against changing hybrid threats and

⁷⁹ Ibid., p. 36.

⁸⁰ Ibid.

supports national and international security structures. This is especially important now since Europe has to concentrate on its own security and cannot rely just on US backing. *Russia's Hybrid Threat Tactics Against the Baltic Sea Region* is an indispensable tool for comprehending attacks and acts of sabotage. It should be taken into account in the development of new policies, as it offers a concrete case study of Russian hybrid tactics together with their impact and required countermeasures. *Protecting maritime infrastructure from hybrid threats: legal options* points up important legal weaknesses in maritime security, supporting global cooperation and legal changes.

Emphasising the need for proactive security policies, resilience-building actions, and legal changes to effectively address emerging challenges, these studies provide essential insights for understanding and minimising hybrid threats to the CI of EU countries. It must also be added that the states on the eastern flank are struggling with the challenge of responding to the RF and non-state actors and have to take care of their own security.

Current research on hybrid threats reveals multiple dysfunctions within the EU's system for countering these threats, which hinder effective action. They must be eliminated immediately by:

- a) developing a transcontinental agreement to counter hybrid threats,
- b) delineation of particular states, organisations, and factions that may be a source of hybrid threats,
- c) revision of existing definitions of hybrid threats, given the phenomenon's continual evolution,
- d) validation of terminology and shared characteristics of hybrid threats, warfare, and terrorism,
- e) standardisation of legal systems of international community in the field of crimes and activities related to hybrid threat, as well as other criminal acts,
- f) preservation of a cohesive counter-hybrid threats policy within international alliances,
- g) reassessment of plans and strategies in state counter-hybrid threats programmes, which would enhance target orientation and funding for pertinent organisations engaged in combating hybrid threats,

- h) implementation of a long-term counter-hybrid threats policy with continuous funding and training for essential counter-hybrid threats units,
- i) thorough education of the public, particularly children and adolescents, regarding the hybrid threats that exist, as well as the perception and comprehension of diverse religions and cultures⁸¹.

Finding an appropriate way to combat hybrid threats is a fundamental objective at both national and international level. An objective assessment of the evolution of this phenomenon is closely linked to the development and coordination of a counter-hybrid threats policy and the raising of public awareness of it. The nature of these threats determines the actions and the emergence of laws that are the government's response to the dangers. Stereotypes should be replaced by in-depth analyses aimed at recognising hybrid threats as an overriding threat to state security, given its diversity depending on the territory in which they occur. Hybrid threats can take different forms in the Baltic States, France, Poland and Ukraine. It is relevant to be aware of its existence, its evolution and its increasing incidence. Counter-hybrid threats activities must be given greater prominence in political debates and scientific research. This is the only way to reach valid conclusions and conceptualise practical actions, also at the international level.

The European Union and NATO have demonstrated that there is a strong mutual will to strengthen security in the Euro-Atlantic area and to combat hybrid threats jointly. Time is needed to develop specific solutions. In a dynamic geopolitical environment, only a multi-level security policy will enable objectives to be achieved. Both the EU and NATO have instruments of military and political cooperation for an effective response. It is crucial not only to eliminate emerging threats, but also undertake global initiatives to prevent them⁸². In this respect, the main focus should be placed on the challenges in Central and Eastern Europe. However, for these to be carried out effectively, the commitment of each Member State is essential. With no permanent and unwavering cooperation, the current efforts of international structures may turn out to be futile.

Hybrid CoE should initiate research on hybrid threats emanating from external actors in Africa and the Middle East, particularly in the context of Europe. It is imperative to provide an annual hybrid threat assessment

⁸¹ A. Olech, *French and Polish fight against terrorism*, Poznań 2022, p. 198.

⁸² A. Olech, *Cooperation between NATO and the European...*

for EU Member States, utilising reports from national security agencies. It would be also beneficial to convene roundtable discussions, both in-person and online, for EU experts specialising in hybrid threats. Their discussion of the most pressing challenges and concepts could result in a report containing multiple perspectives of hybrid threats, taking into account each country's circumstances. From the author's viewpoint, the Hybrid CoE is prepared to establish a transnational strategy for addressing hybrid threats.

In 2025, more than a decade after the Russian assault on Ukraine and 3 years after the full scale invasion and various hybrid attacks on EU Member States, it is imperative to enhance not only policies and resilience but also to respond more effectively. The characteristics of these threats clearly indicate that hybrid warfare is already underway, as confirmed by analyses conducted by the Hybrid CoE. In the current situation, implementing proactive countermeasures and building systemic resilience is just as important as diagnosing and describing the nature of these actions.

Bibliography

Olech A., *French and Polish fight against terrorism*, Poznań 2022.

Internet sources

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: 2.01.2025].

Hybrid CoE Paper 16: Handbook on maritime hybrid threats: 15 scenarios and legal scans, March 2023, https://www.hybridcoe.fi/wp-content/uploads/2023/03/NEW_web_Hybrid_CoE_Paper-16_rgb.pdf [accessed: 17.01.2025].

Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., *Hybrid threats: a comprehensive resilience ecosystem*, Publications Office of the European Union, Luxembourg 2023, https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf [accessed: 22.01.2025].

Olech A., *Cooperation between NATO and the European Union against hybrid threats with a particular emphasis on terrorism*, Institute of New Europe, 17.03.2021, <https://ine.org.pl/en/cooperation-between-nato-and-the-european-union-against-hybrid-threats-with-a-particular-emphasis-on-terrorism/> [accessed: 10.02.2025].

Praks H., *Hybrid CoE Working Paper 32: Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage*, May 2024, <https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240530-Hybrid-CoE-Working-Paper-32-Russias-hybrid-threat-tactics-WEB.pdf> [accessed: 30.01.2025].

Pynnöniemi K., *The concept of hybrid war in Russia: A national security threat and means of strategic coercion*, Hybrid CoE Strategic Analysis / 27, May 2021, https://www.hybridcoe.fi/wp-content/uploads/2021/05/20210518_Hybrid_CoE_Strategic_Analysis_27_The_concept_of_hybrid_war_in_Russia_WEB.pdf [accessed: 10.01.2025].

Sari A., *Hybrid CoE Research Report 14: Protecting maritime infrastructure from hybrid threats: legal options*, March 2025, <https://www.hybridcoe.fi/wp-content/uploads/2025/03/20250306-Hybrid-CoE-Research-Report-14-web.pdf> [accessed: 6.03.2025].

Untersinger M., *Les Etats-Unis ordonnent une pause des cyberopérations contre la Russie, selon plusieurs médias*, Le Monde, 4.03.2025, https://www.lemonde.fr/pixels/article/2025/03/03/les-etats-unis-ordonnent-une-pause-des-operations-cyber-contre-la-russie_6575971_4408996.html [accessed: 4.03.2025].

Legal acts

United Nations Convention on the Law of the Sea drawn up at Montego Bay on 10 December 1982 (Journal of Laws of 2002 item 543).

Aleksander Olech, PhD

Head of International Cooperation at Defence24. Lecturer at both national and international universities, NATO associate, analyst, and publicist. Former Deputy Director of the Department of Africa and the Middle East at the Ministry of Foreign Affairs. Graduate of the European Academy of Diplomacy and War Studies University. Main research interests: French-Russian relations, challenges in Africa and NATO security policy.

Contact: a.olech@defence24.pl

Legal and technical methods of protecting critical infrastructure facilities against threats from unmanned aerial vehicles – the Polish example

JĘDRZEJ ŁUKASIEWICZ

Independent author

 <https://orcid.org/0000-0002-7082-8511>

DAMIAN SZLACHTER

Internal Security Agency

 <https://orcid.org/0000-0003-2763-9325>

Abstract

The aim of this article is to discuss the legal changes introduced in Poland in response to the growing threat to critical infrastructure facilities from unmanned aerial vehicles (UAVs) and to present a recommended method for assessing the effectiveness of UAV detection and neutralisation systems developed by the Government Centre for Security (RCB). The authors discuss the amendment of the *Act of 3 July 2002 – Aviation Law*, which includes provisions relevant to the safety of unmanned platform flights, ensuring that operators of critical infrastructure have the right to defend the protected facility against attacks using unmanned aircraft, and the amendment of the *Act of 24 May 2013 on direct coercive measures and firearms*, which expanded the catalogue of direct coercive measures to include the destruction or immobilisation of UAV or the seizure of control over its flight, and indicated the means of its neutralisation.

Keywords

critical infrastructure, unmanned aerial vehicles, Aviation Law, drone detection and neutralisation systems

Introduction

The miniaturisation of electronics, the construction of efficient energy sources used in UAVs and the relatively simple process of pilot training have all contributed to the development and popularisation of unmanned aviation. The availability of various models of these aircraft, as well as parts and manuals that allow for the independent and anonymous construction of an unmanned platform, as well as access to 3D printing technology, which allows even complex components to be made, have led to the large-scale use of UAVs in, among other things, sabotage operations, including in attacks on critical infrastructure (CI) facilities. Efforts to introduce legal and organisational solutions in Poland to provide CI operators with a chance to build effective anti-drone systems have been underway for several years¹. The finalisation of these activities is the entry into force of the amendment to the Aviation Law (February 2025), which introduces major changes to the use of anti-drone systems by CI operators. The purpose of this article is to discuss these changes and to present the recommendations of Government Centre for Security (RCB) for a method of assessing the effectiveness of detection systems and the neutralisation of unmanned platforms.

Unmanned aerial vehicles as a tool for attacking a critical infrastructure facility

Unmanned aerial vehicles are increasingly being used as a tool for reconnaissance of CI systems or facilities and for attacks on them. In survey

¹ The authors of the article participated in the work of several inter-ministerial working groups (under the aegis of the Polish institutions: the Ministry of the Interior and Administration or the Internal Security Agency) as well as internal teams established by the Government Centre for Security or the European Commission bodies.

studies conducted among representatives of services and institutions within the counter-terrorism system in Poland, as well as government think tank analysts, UAVs were identified as the tool posing the greatest challenge for services, authorities, and institutions responsible for ensuring the security of facilities that could be targeted in a terrorist attack. Along with 3D printing, they accounted for 77.66% of all indications². Until the full-scale Russian invasion of Ukraine, the use of drones in attacks on CI was rare. Warfare has contributed to the rapid development of unmanned technologies as well as to the development of new tactics for attacks using unmanned platforms.

Under current law, CI are systems and their functionally related facilities, including buildings, equipment, installations, services that are key to the security of the state and its citizens and that serve to ensure the efficient functioning of public administration bodies, as well as institutions and entrepreneurs. CI includes the following systems:

- a) energy, energy raw materials and fuels supply,
- b) communications,
- c) ICT networks,
- d) finance,
- e) food supply,
- f) water supply,
- g) health care,
- h) transport,
- i) rescue services,
- j) ensuring continuity of public administration,
- k) production, storage, warehousing and use of chemical and radioactive substances, including pipelines for hazardous substances³.

An unmanned aircraft system is an unmanned aircraft (a platform that floats in the air) together with the equipment for its remote control (a ground station with which the pilot can control the aircraft during flight)⁴. The legislation does not distinguish between aircraft types. The most common types of unmanned platforms include multirotors,

² D. Szlachter, *Terrorism in Poland and trends in its development. Survey results (summary report)*, "Terrorism – Studies, Analyses, Prevention" 2022, no. 2, pp. 335–363. <https://doi.org/10.4467/27204383TER.22.029.16349>.

³ Article 3(2) of the *Act of 26 April 2007 on crisis management*.

⁴ *Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft*.

aircraft, helicopters and hybrids, the design of which combines features of the other types of aircraft. A hybrid can be, for example, an aircraft equipped with additional engines enabling vertical take-off and landing. It will therefore be a hybrid of an aircraft and a multirotor. These vessels may have different masses. Polish law distinguishes between vessel weights of up to 0.25 kg, up to 0.9 kg, up to 4 kg and up to 25 kg. Vessels weighing more than 25 kg require a special permit for the operation issued by the President of the Civil Aviation Authority⁵.

Virtually any air attack scenario can be implemented using UAVs. Their versatility is determined, among other things, by the following features:

1. They can be used in missions with a much higher risk of platform neutralisation than manned vessels. For this reason, drones are used in suicide missions where the price of success is the loss of the platform rather than the pilot.
2. They can perform missions controlled directly by the pilot, in automatic flight or in autonomous flight. Direct pilot control is by radio signal or by optical fibre. Automatic flight is when the route, flight parameters and tasks performed by the craft have been programmed by the pilot before take-off. Such flight takes place using sensors to assist the platform's on-board computer. In this type of flight, the pilot indicates the task, but the way the mission is performed depends on the AI algorithms implemented on the platform's on-board computer. In addition, the on-board computers, based on the sensor data, using AI algorithms, determine the value of the target and the potential losses of the enemy before deciding to attack and make a decision⁶.
3. They have the ability to stay at one point in space for long periods of time, and thus can be used to observe a large area around

⁵ Act of 3 July 2002 – Aviation Law; Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft; Guideline No. 15/2023 of the President of the Civil Aviation Authority of 1 June 2023 on modalities of operations using unmanned aircraft systems in relation to the entry into force of the provisions of Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft.

⁶ J. Łukasiewicz, M. Piekarski, M. Kluczyński, *Bezpieczeństwo infrastruktury krytycznej wobec zagrożeń ze strony platform bezzałogowych* (Eng. Security of critical infrastructure in the face of threats from unmanned platforms), PTBN Report, vol. 2, Polskie Towarzystwo Bezpieczeństwa Narodowego 2021.

the hover point. Aircraft-type drones can carry explosive payloads over long distances and attack targets located far from the take-off point (i.e. where the pilot is). Confirmed distances flown by drones extend to several hundred kilometres⁷.

4. They can be powered by electric motors, reciprocating internal combustion engines, and turbojet engines. Electric motors require a power source, i.e. a battery, fuel cell or generator powered by an internal combustion engine, but are relatively quiet. Internal combustion engines allow for missions over very long distances, while turbojet engines allow the platform to be accelerated to speeds unattainable by other propulsion systems.
5. They can be controlled using different frequencies, where communication is by radio directly between the flying platform and the ground station. Due to the possibility of jamming the radio signal, a mechanism for changing frequencies in flight has been developed. Long-range flights can be carried out using other aircraft carrying a device called a repeater, working as an intermediate station between the ground station and the platform. An unmanned aircraft can also be controlled using GSM communications. The prerequisite for a successful connection is that the flight region is saturated with a sufficient number of base transceiver stations (BTS). An increasingly popular and sometimes the only possible means of communication between the base station and the flying craft is satellite communication. It allows missions whose duration depends only on the energy resources required to power the aircraft's engine⁸. Where one of the methods of defending an attacked facility is to jam the radio frequencies on which the aircraft's connection to the ground station is implemented, a fibre-optic connection can be used. According to reports, the maximum length of fibre-optic

⁷ *Timeline: UAE under drone, missile attacks*, Al Jazeera, 3.02.2022, <https://www.aljazeera.com/news/2022/2/3/timeline-uae-drone-missile-attacks-houthi-yemen> [accessed: 21.02.2025]; G. Faulconbridge, L. Kelly, *Ukrainian drone strikes trigger fires at major oil and gas facilities in Russia*, Reuters, 3.02.2025, <https://www.reuters.com/world/europe/ukraines-drone-attack-sparks-fire-forces-flight-suspensions-several-russian-2025-02-03/> [accessed: 21.02.2025].

⁸ C. Koulouris et al., *A Survey Study and Comparison of Drones Communication Systems*, in: *Flexible Electronics for Electric Vehicles. Proceedings of the 3rd International Conference, FlexEV 2022*, S.K. Goyal et al. (eds.), series: "Lecture Notes in Electrical Engineering", vol. 1065, Springer, Singapore. https://doi.org/10.1007/978-981-99-4795-9_33.

cable wound on a spool is currently 41 km⁹. Obviously, the need to carry a spool of fibre optics results in a reduction in the weight of the explosive charge. The advantage, however, is that the vessel moves in complete radio silence.

6. They can be built using many materials. The most common are injection moulded plastic, glass or carbon laminate moulded or cut with CNC milling machines, aluminium cut with CNC milling machines, 3D printing. Wood, plywood and ebonite are also used in the construction of drones.
7. They can carry any payload. Payloads can include measuring devices, image-recording devices and containers of explosives or chemicals. The use of hand grenades, RPG warheads and other explosives is observed in attacks. The ability to carry a payload has been provided by 3D printing.
8. Simple designs adapted for explosive flight and offering the possibility of observing the target of an attack (so-called FPV drones) can be built for as little as around USD 200¹⁰. More advanced designs and those intended for military use are much more expensive.
9. Acquiring the skills to control a platform is not complicated. Through the use of accelerometers and gyroscopes, as well as barometers and GPS receivers, systems that stabilise the platform, a pilot can acquire such skills in a matter of hours.

In view of the aforementioned characteristics of UAVs, the CI operator should consider the following scenarios and the consequences of an attack carried out with these devices when building their detection and neutralisation system:

1. Disruption of the operation of the facility or installation under attack by unauthorised overflight in the area of the facility. The consequences of an attack can be to cause distress to

⁹ *Jam-Proof Fiber Optics for Drones: Revolutionizing Secure Communications*, Linden Photonics Inc, 22.08.2024, <https://www.lindenphotonics.com/jam-proof-fiber-optics-for-drones-revolutionizing-secure-communications> [accessed: 21.02.2025]; *Ukrainians Made an FPV With Fiber-Optic Cord Stretching For 41 km*, Defence Express, 26.01.2025, https://en.defence-ua.com/industries/ukrainians_made_an_fpv_with_fiber_optic_cord_stretching_for_41_km-13327.html [accessed: 21.02.2025].

¹⁰ B. Wang, *Ukraine's One Million FPV Drones Is Outnumbered by 5 Million Russian Drones*, Next Big Future, 27.01.2024, <https://www.nextbigfuture.com/2024/01/ukraines-one-million-fpv-drones-will-be-outnumbered-by-5-million-russian-drones.html> [accessed: 21.02.2025].

personnel, disrupt their work, take them away from their routine activities, and involve government services in efforts to identify the perpetrator of the attack¹¹.

2. Espionage activities. The consequences of such an attack may include the identification of: the structural features of the facility or the industrial installations used in the facility, the manufacturer of the equipment used in the technological processes, the procedures in place at the facility under attack, the identity of the employees and the methods of communication between the employees working at the facility¹².
3. A kinetic impact, breaking a platform, dropping a load that mechanically damages equipment and installations and then stops their operation, hanging electrically conductive elements such as wires, carbon fibres or carbon dust on electrical equipment. The consequences of an attack can be damage to installations, causing injury to people, causing panic, and short-circuiting the electrical system supplying the facility or installation¹³.
4. Carrying an explosive charge and causing it to explode. The consequences of an attack can be: loss of life or limb to workers, damage to installations causing a long term interruption to the operation of the facility, panic, stress and, in the long term, social unrest¹⁴.
5. Transfer of chemical, biological, radiological or other irritant weapons. The consequences of an attack may be: the long-term contamination of the area of the facility preventing its operation, damage to installations required in the technological process,

¹¹ *It is still unclear whose drone is blocking 6 flights at Sofia Airport*, Fakti.bg, 9.02.2025, <https://fakti.bg/en/bulgaria/948414-it-is-still-unclear-whose-drone-is-blocking-6-flights-at-sofia-airport> [accessed: 21.02.2025].

¹² *Sweden drones: Sightings reported over nuclear plants and palace*, BBC, 18.01.2022, <https://www.bbc.com/news/world-europe-60035446> [accessed: 21.02.2025].

¹³ S. Lyngaas, *Drone at Pennsylvania electric substation was first to 'specifically target energy infrastructure'*, according to federal law enforcement bulletin, CNN, 4.11.2021, <https://edition.cnn.com/2021/11/04/politics/drone-pennsylvania-electric-substation/index.html> [accessed: 21.02.2025]; B. Barrett, *A Drone Tried to Disrupt the Power Grid. It Won't Be the Last*, Wired, 5.11.2021, <https://www.wired.com/story/drone-attack-power-substation-threat/> [accessed: 21.02.2025].

¹⁴ G. Faulconbridge, L. Kelly, *Ukrainian drone strikes trigger fires...*

- causing fires, including in the area surrounding the protected facility¹⁵.
6. Smuggling of unauthorised loads both into and out of the facility outside the fence. The consequence of smuggling may be the appearance of firearms, explosives, electronic warfare agents, drugs etc. on the premises¹⁶. Smuggling out of the facility may result in loss of control over classified information that must not be transferred off-site, loss of protected chemical, biological or nuclear agents, etc.

Legislative changes to the protection of critical infrastructure from unmanned aerial vehicles

The existing legislation in Poland so far has practically failed to take into account the possibility of combating unmanned aircraft, even when they posed a threat to protected facilities, air traffic, health or human life. In the world, the consequence of the lack of proper regulations was the overflight of unmanned aircraft over protected objects and even flights on collision courses with manned aircraft¹⁷. There have also been isolated incidents of unmanned platforms being used in attacks on people¹⁸. Such situations, the war in Ukraine, daily reports of attacks on CI facilities around the world, as well as hybrid actions in the Baltic Sea, have shown that ensuring the security of CI in Poland, for which UAVs are a source of threat, requires serious legal changes.

¹⁵ Drone 'containing radiation' lands on roof of Japanese PM's office, *The Guardian*, 22.04.2015, <https://www.theguardian.com/world/2015/apr/22/drone-with-radiation-sign-lands-on-roof-of-japanese-prime-ministers-office> [accessed: 21.02.2025].

¹⁶ Cheap and They Don't Snitch: Drones Are the New Drug Mules, *RUSI*, 5.01.2024, <https://www.rusi.org/news-and-comment/in-the-news/cheap-and-they-dont-snitch-drones-are-new-drug-mules> [accessed: 21.02.2025].

¹⁷ S. McKenzie, G. Mezzofiore, *Police hunt drone pilots in unprecedented Gatwick Airport disruption*, *CNN*, 20.12.2018, <https://edition.cnn.com/2018/12/20/uk/gatwick-airport-drones-gbr-intl/index.html> [accessed: 21.02.2025]; *Drones paralyzed Stockholm-Arlanda Airport*, *Kronen Zeitung*, 9.09.2024, <https://www.krone.at/3519874> [accessed: 21.02.2025].

¹⁸ Venezuela President Maduro survives 'drone assassination attempt', *BBC*, 5.08.2018, <https://www.bbc.com/news/world-latin-america-45073385> [accessed: 21.02.2025].

The new provisions enshrined in the *Act amending the Aviation Law and certain other acts*¹⁹ are the response to these threats. The draft was received by the Polish Parliament on 24 November 2024²⁰. On 24 January 2025, it was forwarded to the President of Poland, who signed the law on 6 February 2025. It implements those provisions of EU law that relate to UAVs²¹. The Act has put in order the previous legal status on the basis of which unmanned aircraft flights were performed in Poland. A novelty in relation to the current Act – the Aviation Law is the introduction of Part VIa entirely dedicated to unmanned aircraft. It contains, inter alia, Chapter 2, on geographical zones for unmanned aircraft, and Chapter 6, relating to the prevention of unlawful operations using an unmanned aircraft system.

Airspace designated for the operation of aircraft in accordance with the provisions of the Aviation Law is divided into controlled space and uncontrolled space²². The structure of the space is defined, by regulation, by the minister responsible for transport, but in consultation with the minister of national defence and taking into account the rules arising from regulations and international agreements. According to the ordinance of the Minister of Infrastructure of 27 December 2018²³, a controlled space is one in which an air traffic control service is provided to all aircraft, based on the classification of the International Civil Aviation Organization. This service guarantees separation between aircraft, an alerting service and a flight information service. In uncontrolled space, only alerting service and flight information service are provided, and the separation between aircraft and other aircraft flying in the uncontrolled area is ensured by the aircraft pilot himself. In Poland, controlled space extends from FL095 to FL660 (Flight Level 660 – flight level of 66000 feet), while uncontrolled space extends from the ground to FL095 (Flight Level 095 – flight level of 9500 feet). Within controlled and uncontrolled space, fixed and flexible

¹⁹ *Act of 24 January 2025 amending the Aviation Law and certain other acts.*

²⁰ *Government draft Act amending the Aviation Law and certain other acts*, print no. 810, <https://www.sejm.gov.pl/sejm10.nsf/PrzebiegProc.xsp?nr=810> [accessed: 21.02.2025].

²¹ *Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems; Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft.*

²² Article 121(5) of the Act of 3 July 2002 – Aviation Law.

²³ *Regulation of the Minister of Infrastructure of 27 December 2018 on the structure of Polish airspace and the detailed conditions and use of that space.*

airspace elements are further delimited to ensure flight safety, more efficient use of airspace and optimised air traffic management. Fixed elements are those whose horizontal and vertical boundaries are defined and unchangeable. These include, for example: Airways (AWY), Control Zones (CTR), Prohibited Area (P). Flexible elements, separated only for a limited period of time, are e.g. Temporary Selected Areas (TSA) or Aerodrome Traffic Zones (ATZ).

The fixed and flexible elements listed were developed at a time when unmanned aviation was not widespread and the flight rules applicable to these elements were adapted to manned aviation. The rapid development of unmanned aviation made it necessary to structure the airspace for unmanned operations. In view of the lack of appropriate provisions in laws and regulations, under the guidelines of the President of the Civil Aviation Authority, the designation of so-called geographical zones for unmanned aircraft systems began²⁴. The amendment to the Aviation Law allowed the content of these guidelines to be written down in Chapter 2 of the act. Under the new provisions, the Polish Air Navigation Services Agency (hereinafter: the Agency) is responsible for designating the geographical zone, which determines the period of validity of the zone, the area of the geographical zone and the conditions under which flights by UAVs in the zone must be performed²⁵.

According to the new regulations, an application for the designation of a geographical zone may be submitted by an authorised entity, which is:

- 1) public administration body, a body of the Armed Forces of the Republic of Poland, the chairman of the State Commission on Aircraft Accidents Investigation, the chairman of the Commission for Investigation of State Aviation Accidents, the Director General of the State Forests National Forest Holding, an entity authorised to carry out water rescue, an entity authorised to carry out mountain rescue and the director of the Government Centre for Security – in the event of the need to secure airspace in order to carry out statutory tasks;
- 2) manager of a CI, including aviation, maritime, rail or energy infrastructure, or a mining site, where it is necessary to secure airspace in order to discharge the responsibilities of that manager;

²⁴ Guideline No. 17/2023 of the President of the Civil Aviation Authority of 6 June 2023 on the designation of geographical zones for unmanned aircraft systems. These guidelines were updated in a document dated 21 February 2025.

²⁵ Article 156h(13) of the Act of 3 July 2002 – Aviation Law.

- 3) organiser of exercises, training, competitions, air shows or occasional flights, when airspace has to be secured for flights during exercises, training, competitions, air shows or occasional flights;
- 4) operator of an unmanned aircraft system intending to conduct an operation in the 'special' category, where the need for a geographical zone designation results from the authorisation of the operation, the LUC certificate, the standard scenario or the national standard scenario;
- 5) recognised provider of practical training and assessment of the practical skills of an unmanned aircraft pilot for operations in the 'specific' category and a manufacturer of unmanned aircraft systems²⁶.

The above provisions of the amended law allow the CI operator to designate a drone geographical zone over the area where the protected CI facility is located.

The types of geographical zones, detailed conditions and the manner of using them will be specified by the minister responsible for transport by means of a regulation. Currently, the following types of geographical zones are distinguished in Poland:

- 1) DRA-P – a prohibited zone for unmanned aircraft systems, in which operations using unmanned aircraft systems may not be carried out, except under conditions specified by the Agency, the General Commander of the Armed Forces, the Operational Commander of the Armed Forces, the Commander-in-Chief of the Military Police, the Head of the Internal Security Agency, the Head of the Foreign Intelligence Agency, the Head of the Central Anticorruption Bureau, the Head of the Military Counterintelligence Service, the Head of the Military Intelligence Service, the Commander-in-Chief of the Police, the Commander-in-Chief of the Border Guard, the General Director of the Prison Service, the Head of the National Revenue Administration, the Commander-in-Chief of the State Protection Service or the Commander-in-Chief of the State Fire Service – under the conditions specified by the Agency;
- 2) DRA-R – a restricted zone for unmanned aircraft systems, in which operations using unmanned aircraft systems may be carried out with the consent and under conditions specified by the Agency

²⁶ Article 156h(4) of the *Act of 3 July 2002 – Aviation Law*.

or the authorised entity at the request of which the geographical zone has been designated, including:

- a) DRA-RH – a restricted zone for unmanned aircraft systems with a high probability of approval by the geographical zone manager to carry out the operation,
- b) DRA-RM – a restricted zone for unmanned aircraft systems with a medium probability of obtaining approval by the geographical zone manager to carry out the operation,
- c) DRA-RL – a restricted zone for unmanned aircraft systems with a low probability of obtaining approval by the geographical zone manager to carry out the operation;
- 3) DRA-T – a restricted zone for unmanned aircraft systems in which operations with unmanned aircraft systems may only be carried out with unmanned aircraft systems meeting the technical requirements specified by the Agency and under conditions specified by the Agency, for the DRA-T zone, additional conditions for operations are allowed, including the obligation to obtain the approval of the geographical zone manager;
- 4) DRA-I – information zone for unmanned aircraft, containing information necessary to ensure safe operations using unmanned aircraft systems, including navigational warnings²⁷.

The amended Aviation Law also introduces provisions aimed at enabling the destruction, immobilisation or takeover of an unmanned aircraft in cases where the pilot performs a flight operation in such a way that the course of the operation or the operation of the unmanned aircraft:

- 1) threatens or is likely to threaten the life or health of humans or animals,
- 2) poses or is likely to pose a threat to protected objects, equipment or areas,
- 3) disrupts or is likely to disrupt a mass event or endangers the safety of its participants,
- 4) creates or may create a reasonable suspicion that it may be used as a means of a terrorist attack,
- 5) creates or is likely to create a risk to the safety of air traffic, aircraft or the life or health of the crew or passengers on board,

²⁷ Guideline No. 4/2025 of the President of the Civil Aviation Authority of 21 February 2025 on the designation of geographical zones for unmanned aircraft systems.

- 6) obstructs or is likely to obstruct air traffic or causes or is likely to cause its interruption or restriction²⁸.

An unmanned aircraft may also be destroyed, immobilised or its flight may be overtaken if, contrary to the prohibition, it performs an operation in the geographical zone established over: protected facilities of the Polish Armed Forces and organisational units subordinate to the Minister of National Defence or supervised by him or facilities, equipment or areas important for the security or defence of the state, public security or the inviolability of the state border²⁹.

The aforementioned provisions of the amended law are revolutionary with regard to the security of CI facilities. Until the amendment, the law allowed for the detection of UAVs, but did not give the operator the tools to neutralise vessels infringing the geographical zone designated over the facilities protected by the zone. Due to the lack of a legal basis and, above all, for fear of liability for potential losses caused by the neutralisation of an unmanned aircraft, many CI operators have not installed systems to detect and neutralise these vessels. The amended law unambiguously identifies the pilot or operator of the aircraft performing the operation in violation of the law as responsible for the damage caused by the neutralisation of the aircraft³⁰.

When an unmanned aircraft:

- threatens or is likely to threaten the life or health of humans or animals,
- poses or is likely to pose a threat to protected facilities, equipment or areas,
- creates or may create a reasonable suspicion that it may be used as a means of a terrorist attack,
- poses or is likely to pose a threat to the safety of air traffic, the aircraft or the life or health of the crew or passengers on board,
- obstructs or is likely to obstruct air traffic or causes or is likely to cause its interruption or restriction,

officers of the Internal Security Agency, the Foreign Intelligence Agency, the Military Counterintelligence Service, the Military Intelligence Service, the Central Anticorruption Bureau, the Police, the Border Guard, the State

²⁸ Article 156ze(1), point 1 of the *Act of 3 July 2002 – Aviation Law*.

²⁹ Article 156ze(1), point 2 of the *Act of 3 July 2002 – Aviation Law*.

³⁰ Article 156ze(4) of the *Act of 3 July 2002 – Aviation Law*.

Protection Service, the Customs and Tax Service, the Prison Service, the Marshal Guard, inspectors of the Office for Internal Oversight, professional soldiers appointed to service positions in the Military Counterintelligence Service or the Military Intelligence Service, soldiers of the Military Police and the Armed Forces of the Republic of Poland, employees of airport security services, forest guards, security employees of specialised armed protection formations, as well as employees of internal protection services operating on the territory of organisational units subordinated to the Minister of National Defence or supervised by him are entitled to destroy, immobilise or take control of such vessel³¹.

The amended Act provides penalties for violations of the regulations on operations with unmanned aircraft. In Part XIa – Administrative fines – provisions have been added to allow a penalty to be imposed on anyone who carries out operations using an unmanned aircraft system contrary to the conditions for carrying out operations in a given geographical zone. The amount of such penalty is PLN 10 000 for each infringement.

Another important revision is the amendment of the Act of 24 May 2013 on means of direct coercion and firearms³². It extends the catalogue of direct coercive measures to include the destruction or immobilisation of an unmanned aircraft or taking control of its flight³³. The law has also been supplemented with an indication of the means of neutralising the UAV, which include:

- 1) a device that uses or interferes with radio waves,
- 2) an incapacitating net,
- 3) other UAVs,
- 4) non-penetrating projectiles or other objects propelled by means of devices designed for that purpose and by firearms and airsoft weapons,
- 5) devices emitting a cumulative beam of energy or electromagnetic waves³⁴.

The list of measures includes all currently known methods of neutralising UAVs.

³¹ Article 156ze(2) of the *Act of 3 July 2002 – Aviation Law*.

³² *Act of 24 May 2013 on means of direct coercion and firearms*.

³³ *Ibid.*, Article 11.

³⁴ *Ibid.*, Article 33a(2).

Recommendations of the Government Centre for Security on assessing the effectiveness of unmanned aircraft detection and neutralisation systems

With reports of unmanned platforms being used to paralyse the operation of technical systems responsible for the continuity of CI operations³⁵, disturbing facility staff³⁶ or even attacks with explosives³⁷, CI operators should consider building detection and neutralisation systems for drones.

The process of building a UAV detection and neutralisation system begins with a risk analysis of the system or facility for which the unmanned platforms are a threat source. If the CI operator considers that the system or facility it is protecting is vulnerable to attack, then building a detection and neutralisation system is essential.

Detection systems are made up of multiple devices using different methods to detect unmanned platforms³⁸. The simplest and seemingly most widely used detection method is the detection of communication between the flying platform and the ground station. It is versatile as both fixed and mobile detection devices can be used within this framework. Advanced devices using AI algorithms can determine the model of the aircraft based on the measurement of the characteristics of the communication signal³⁹. These easily constructed devices work on the principle of an indicator that emits an audible signal when a flying vessel is detected. Their disadvantage is the inability to detect unmanned vessels flying in radio silence, for example those controlled by fibre optic cable, and the inability to detect platforms whose communications are on frequencies not supported by the detection device.

Another detection method uses radar devices. It has the advantage of a wide radar range – its detection distance far exceeds the distances at which an unmanned aircraft can be detected by other methods. However,

³⁵ *Drones paralyzed Stockholm-Arlanda Airport...*; S. Lyngaas, *Drone at Pennsylvania electric substation...*

³⁶ H. Altman, *Nuclear Power Plants Report Massive Uptick In Drone Sightings*, The Warzone, 21.12.2024, <https://www.twz.com/news-features/massive-uptick-in-official-drone-sightings-by-nuclear-power-plants> [accessed: 21.02.2025].

³⁷ L. Kelly, *Ukrainian drone strikes trigger fires...*

³⁸ J. Łukasiewicz, M. Piekarski, M. Kluczyński, *Bezpieczeństwo infrastruktury krytycznej...*

³⁹ M.F. Al-Sa'd et al., *RF-based drone detection and identification using deep learning approaches: An initiative towards a large open-source drone database*, "Future Generation Computer Systems" 2019, vol. 100, pp. 86–97. <https://doi.org/10.1016/j.future.2019.05.007>.

the probability of detecting an aircraft depends on several factors, including the size of the object being detected and the altitude at which it is moving⁴⁰. Modern radar systems aided by AI algorithms can determine whether the tracked object is an unmanned platform or a bird. The method described also has the advantage of being able to detect the object regardless of the time of day or night. The disadvantage of radar detection is certainly the high cost of the device and the inability to detect a flying object if it is hiding behind terrain obstacles or flying very low to the ground.

The acoustic method is increasingly used⁴¹. The cost of an acoustic detector is lower than a radar detector and, more importantly, it is passive, i.e. it does not emit a signal in any form to make a detection. This method is becoming increasingly popular for drone detection systems in Ukraine, where the large platforms used to carry high explosive loads are powered by noisy internal combustion engines. The disadvantage of the acoustic method may be ineffective detection in a location where there are other noise sources than just the unmanned platform.

The final detection method is to analyse the image recorded by a camera operating in visible light or infrared⁴². Such a camera is equipped with AI algorithms to recognise the shape of a flying object. Infrared cameras analyse its temperature, which makes it possible to distinguish between the unmanned platform and the birds. The disadvantage of cameras operating in the visible area is the inability to record images in low-light conditions, such as at night. The disadvantage of infrared cameras, on the other hand, is the inability to detect the object when it is equipped with thermal insulators.

All the described methods used in the construction of the detection system allow for the detection of unmanned platforms in various conditions. The method for assessing the effectiveness of this system is described in a document prepared by the Government Centre for Security

⁴⁰ M. Ezuma et al., *Comparative Analysis of Radar Cross Section Based UAV Classification Techniques*, preprint, <https://arxiv.org/abs/2112.09774> [accessed: 21.02.2025]. <https://doi.org/10.48550/arXiv.2112.09774>.

⁴¹ H. Altman, T. Rogoway, *Ukraine's Acoustic Drone Detection Network Eyed By U.S. As Low-Cost Air Defense Option*, The Warzone, 24.07.2024, <https://www.twz.com/air/ukraines-acoustic-drone-detection-network-eyed-by-u-s-as-low-cost-air-defense-option> [accessed: 21.02.2025].

⁴² Y. Wu, Y. Sui, G. Wang, *Vision-Based Real-Time Aerial Object Localization and Tracking for UAV Sensing System*, "IEEE Access" 2017, vol. 5, pp. 23969–23978. <https://doi.org/10.1109/ACCESS.2017.2764419>.

as an annex to the National Critical Infrastructure Protection Program 2023 (NPOIK)⁴³. The method involves testing the probability of detection by individual devices in the system. This probability is determined from the counts of effective detections per 100 trials. These trials must take place under different conditions, i.e. the probability of detection for a given location under different weather conditions, under conditions of external sources of electromagnetic radiation, for different types of UAVs, for different attack scenarios, for different competences of security personnel is examined. Knowing the probability of detection of each device under given conditions, the total probability of detection by the entire system can be determined using the formula:

$$P_{\text{CALK_D}} = 1 - (1 - P_{1D})(1 - P_{2D})(1 - P_{3D})(1 - P_{4D}) \dots (1 - P_{ND})$$

in which:

$P_{\text{CALK_D}}$ – is the probability of detection by the whole system,

P_{1D} – is the probability of detection by the first detection device,

P_{2D} – is the probability of detection by the second detection device,

P_{3D} – is the probability of detection by the third detection device,

P_{ND} – is the probability of detection by the nth detection device.

The task of the CI operator is to build a detection system such that the probability value $P_{\text{CALK_D}}$ is higher than the threshold value assumed by the operator.

The construction of drone neutralisation systems also uses devices that operate on different principles to increase the likelihood of neutralisation. One of its most popular methods is the jamming of the communication signal between unmanned platform and ground station. The jamming is done by emitting an electromagnetic wave in the direction of the flying platform at the same frequency as that used for communication. The disadvantage of this solution is the increasingly common hopping mechanism, which involves changing the frequency of communication between the platform and the ground station during flight. The jamming device must therefore emit waves at different frequencies to jam the communication. Such

⁴³ *Standards for ensuring the smooth functioning of critical infrastructure – good practices and recommendations*, Annex 1 to the National Critical Infrastructure Protection Program, Government Centre for Security (RCB), 2023. The text of the Annex is available at: <https://www.gov.pl/web/rcb-en/national-critical-infrastructure-protection-program>.

a device is not effective against an unmanned platform flying in radio silence or in automatic or autonomous mode.

Another method is to jam or spoof the satellite navigation signal⁴⁴, which will result in the unmanned platform getting lost in the airspace or flying the platform to the location indicated by the falsified satellite navigation signal. This solution will prove ineffective if the unmanned platform uses counting navigation equipment, known as inertial navigation. In this case, the unmanned platform navigates on the basis of calculations, correcting its geographical position by periodic position readings from satellites.

A third method is the use of net systems that can be fired from special devices called *net guns*, which security personnel are equipped with, or devices carried by unmanned aircraft operated by security personnel⁴⁵. The disadvantage of this method is that the shot must be fired at close range from the attacking platform.

Another method of neutralisation is to destroy the UAV by emitting a high-energy electromagnetic pulse in its direction⁴⁶. Such a pulse destroys the semiconductor components of the electronics mounted on the platform. The disadvantage of this solution is that sensitive electronic components can be placed in what is known as a Faraday cage, a package that isolates electronic devices from the effects of external electromagnetic fields.

Laser systems are increasingly being used to combat unmanned systems. Lasers can be used as light sources that, by shining directly into the camera lens of the unmanned platform, prevent the pilot from controlling it properly. Lasers are also increasingly used as a device that physically destroys the illuminated platform by burning it⁴⁷. Laser systems

⁴⁴ M. Sahmoudi, M.G. Amin, *Robust tracking of weak GPS signals in multipath and jamming environments*, "Signal Processing" 2009, vol. 89, no. 7, pp. 1320–1333. <https://doi.org/10.1016/j.sigpro.2009.01.001>.

⁴⁵ D. Hambling, *Webslingers: How Net-Launching Drones Are Downing Russian Quadcopters*, Forbes, 12.12.2024, <https://www.forbes.com/sites/davidhambling/2024/11/12/webslingers-how-net-launching-drones-are-downing-russian-quadcopters/> [accessed: 21.02.2025].

⁴⁶ O.D. Razooqi, A.H. Ali, *Drones neutralized by utilize electromagnetic pulse (EMP) system*, in: *2022 5th International Conference on Engineering Technology and its Applications (IICETA)*, Al-Najaf 2022, pp. 487–492. <https://doi.org/10.1109/IICETA54559.2022.9888673>.

⁴⁷ J. Saballa, *Ukraine Announces Successful Use of First Laser Weapon on Battlefield*, The Defense Post, 6.02.2025, <https://thedefensepost.com/2025/02/06/ukraine-laser-weapon-battlefield/> [accessed: 21.02.2025].

are not popular because they require large and efficient energy sources, and their effectiveness is highly dependent on air transparency⁴⁸.

None of the described methods guarantees neutralisation, so, as mentioned, systems using different methods should be built. A proposal on how to evaluate the effectiveness of a system to neutralise unmanned platforms is described in the aforementioned annex to the NPOIK 2023⁴⁹. The method involves testing the probability of neutralisation using individual devices of the system. This probability is determined on the basis of the counts of successful neutralisations per 100 trials. These trials must take place under different conditions, i.e. the probability of neutralisation is tested for a given location under different weather conditions, for different types of UAVs, for different attack scenarios, for different competences of security personnel. Knowing the probability of neutralisation of each device of the system under given conditions, the total probability of neutralisation by the whole system can be determined using the formula:

$$P_{\text{CALK}_N} = 1 - (1 - P_{1N})(1 - P_{2N})(1 - P_{3N})(1 - P_{4N}) \dots (1 - P_{NN})$$

where:

P_{CALK_N} – is the probability of neutralisation by the whole system,
 P_{1N} – is the probability of neutralisation by the first neutralisation device,
 P_{2N} – is the probability of neutralisation by the second neutralisation device,
 P_{3N} – is the probability of neutralisation by the third neutralisation device,
 P_{NN} – is the probability of neutralisation by the nth neutralisation device.

The task of the CI operator is to build the neutralisation system in such a way that the probability value P_{CALK_N} is higher than the minimum threshold value assumed by the operator.

⁴⁸ R. Ceder, *US Navy hits drone with HELIOS laser in successful test*, Navy Times, 4.02.2025, <https://www.navytimes.com/news/your-navy/2025/02/04/us-navy-hits-drone-with-helios-laser-in-successful-test/> [accessed: 21.02.2025]; M. Knight, *Ukraine says it has a laser that can shoot down aircraft a mile away. It's called 'Tryzub'*, CNN, 18.12.2024, <https://edition.cnn.com/2024/12/18/europe/ukrainian-tryzub-laser-weapon-intl-latam/index.html> [accessed: 21.02.2025].

⁴⁹ *Standards to ensure smooth functioning...*

Summary

The amendment to the Polish Act – Aviation Law has been eagerly awaited by CI operators. It provides them with ample opportunities and a formal legal basis to combat drones that unauthorised violate the geographical zone designated over a CI facility. The new legislation clearly identifies the pilot of an unmanned platform in breach of the flight rules as the person who bears the consequences of a potential drone fall resulting in damage. The penalties introduced in this respect can be assessed as very severe. In addition, the amendment to the Act on direct coercive measures and firearms expands the catalogue of such measures to include devices that can be used to combat unmanned platforms. The amendment to the Aviation Law in question should be supplemented by an amendment to the Act on crisis management to oblige CI operators to conduct risk analyses of threats to facilities and, consequently, to build detection and neutralisation systems for unmanned aircraft.

In view of the rapid development of unmanned technology, the emergence of drone munitions, the increasingly widespread acquisition of UAV piloting skills, both EU institutions and Member States should encourage research institutions, laboratories, technology centres and private investors to invest in the research and development of modern detection and neutralisation systems for unmanned platforms. Based on the observation of the armed conflict in Ukraine, it can be concluded that current detection and neutralisation systems do not guarantee the security of protected facilities.

The technological gap between the ability of UAVs to attack CI facilities and the systems to detect and neutralise them is regularly widening. The same conclusion can be reached after comparing the cost of acquiring an unmanned aircraft capable of attacking a CI facility with the cost of acquiring, operating and servicing an anti-drone system that reduces the risk of attack to an acceptable level for the CI operator. This gap must not be allowed to widen. Increasing the resilience of CI facilities to attacks using unmanned aircraft systems depends on the actions of CI operators, who have received the legal and organisational framework that has been advocated for years.

Bibliography

Al-Sa'd M.F., Al-Ali A., Mohamed A., Khattab T., Erbad A., *RF-based drone detection and identification using deep learning approaches: An initiative towards a large open-source drone database*, "Future Generation Computer Systems" 2019, vol. 100, pp. 86–97. <https://doi.org/10.1016/j.future.2019.05.007>.

Ezuma M., Anjinappa C.K., Semkin V., Guvenc I., *Comparative Analysis of Radar Cross Section Based UAV Classification Techniques*, preprint, <https://arxiv.org/abs/2112.09774> [accessed: 21.02.2025]. <https://doi.org/10.48550/arXiv.2112.09774>.

Koulouris C., Dimitrios P., Al-Darraj I., Tsaramirsis G., Khadidos A.O., Khadidos A.O., Papageorgasi P., *A Survey Study and Comparison of Drones Communication Systems*, in: *Flexible Electronics for Electric Vehicles. Proceedings of the 3rd International Conference, FlexEV 2022*, S.K. Goyal, D.K. Palwalia, R. Tiwari, Y. Gupta (eds.), series: "Lecture Notes in Electrical Engineering", vol. 1065. Springer, Singapore. https://doi.org/10.1007/978-981-99-4795-9_33.

Łukasiewicz J., Piekarski M., Kluczyński M., *Bezpieczeństwo infrastruktury krytycznej wobec zagrożeń ze strony platform bezzałogowych* (Eng. Security of critical infrastructure in the face of threats from unmanned platforms), PTBN Report, vol. 2, Polskie Towarzystwo Bezpieczeństwa Narodowego 2021.

Razooqi O.D., Ali A.H., *Drones neutralized by utilize electromagnetic pulse (EMP) system*, in: *2022 5th International Conference on Engineering Technology and its Applications (IICETA)*, Al-Najaf 2022, pp. 487–492. <https://doi.org/10.1109/IICETA54559.2022.9888673>.

Sahmoudi M., Amin M.G., *Robust tracking of weak GPS signals in multipath and jamming environments*, "Signal Processing" 2009, vol. 89, no. 7, pp. 1320–1333. <https://doi.org/10.1016/j.sigpro.2009.01.001>.

Standards for ensuring the smooth functioning of critical infrastructure – good practices and recommendations, Annex 1 to the National Critical Infrastructure Protection Program, Government Centre for Security (RCB), 2023.

Szlachter D., *Terrorism in Poland and trends in its development. Survey results (summary report)*, "Terrorism – Studies, Analyses, Prevention" 2022, no. 2, pp. 335–363. <https://doi.org/10.4467/27204383TER.22.029.16349>.

Wu Y., Sui Y., Wang G., *Vision-Based Real-Time Aerial Object Localization and Tracking for UAV Sensing System*, "IEEE Access" 2017, vol. 5, pp. 23969–23978. <https://doi.org/10.1109/ACCESS.2017.2764419>.

Internet sources

Altman H., *Nuclear Power Plants Report Massive Uptick In Drone Sightings*, The Warzone, 21.12.2024, <https://www.twz.com/news-features/massive-uptick-in-official-drone-sightings-by-nuclear-power-plants> [accessed: 21.02.2025].

Altman H., Rogoway T., *Ukraine's Acoustic Drone Detection Network Eyed By U.S. As Low-Cost Air Defense Option*, The Warzone, 24.07.2024, <https://www.twz.com/air/ukraines-acoustic-drone-detection-network-eyed-by-u-s-as-low-cost-air-defense-option> [accessed: 21.02.2025].

Barrett B., *A Drone Tried to Disrupt the Power Grid. It Won't Be the Last*, Wired, 5.11.2021, <https://www.wired.com/story/drone-attack-power-substation-threat/> [accessed: 21.02.2025].

Ceder R., *US Navy hits drone with HELIOS laser in successful test*, Navy Times, 4.02.2025, <https://www.navytimes.com/news/your-navy/2025/02/04/us-navy-hits-drone-with-helios-laser-in-successful-test/> [accessed: 21.02.2025].

Cheap and They Don't Snitch: Drones Are the New Drug Mules, RUSI, 5.01.2024, <https://www.rusi.org/news-and-comment/in-the-news/cheap-and-they-dont-snitch-drones-are-new-drug-mules> [accessed: 21.02.2025].

Drone 'containing radiation' lands on roof of Japanese PM's office, The Guardian, 22.04.2015, <https://www.theguardian.com/world/2015/apr/22/drone-with-radiation-sign-lands-on-roof-of-japanese-prime-ministers-office> [accessed: 21.02.2025].

Faulconbridge G., Kelly L., *Ukrainian drone strikes trigger fires at major oil and gas facilities in Russia*, Reuters, 3.02.2025, <https://www.reuters.com/world/europe/ukraines-drone-attack-sparks-fire-forces-flight-suspensions-several-russian-2025-02-03/> [accessed: 21.02.2025].

Hambling D., *Webslingers: How Net-Launching Drones Are Downing Russian Quadcopters*, Forbes, 12.12.2024, <https://www.forbes.com/sites/davidhambling/2024/11/12/webslingers-how-net-launching-drones-are-downing-russian-quadcopters/> [accessed: 21.02.2025].

It is still unclear whose drone is blocking 6 flights at Sofia Airport, Fakti.bg, 9.02.2025, <https://fakti.bg/en/bulgaria/948414-it-is-still-unclear-whose-drone-is-blocking-6-flights-at-sofia-airport> [accessed: 21.02.2025].

Jam-Proof Fiber Optics for Drones: Revolutionizing Secure Communications, Linden Photonics Inc, 22.08.2024, <https://www.lindenphotonics.com/jam-proof-fiber-optics-for-drones-revolutionizing-secure-communications> [accessed: 21.02.2025].

Knight M., *Ukraine says it has a laser that can shoot down aircraft a mile away. It's called 'Tryzub'*, CNN, 18.12.2024, <https://edition.cnn.com/2024/12/18/europe/ukrainian-tryzub-laser-weapon-intl-latam/index.html> [accessed: 21.02.2025].

Lyngaas S., *Drone at Pennsylvania electric substation was first to 'specifically target energy infrastructure', according to federal law enforcement bulletin*, CNN, 4.11.2021, <https://edition.cnn.com/2021/11/04/politics/drone-pennsylvania-electric-substation/index.html> [accessed: 21.02.2025].

McKenzie S., Mezzofiore G., *Police hunt drone pilots in unprecedented Gatwick Airport disruption*, CNN, 20.12.2018, <https://edition.cnn.com/2018/12/20/uk/gatwick-airport-drones-gbr-intl/index.html> [accessed: 21.02.2025].

Saballa J., *Ukraine Announces Successful Use of First Laser Weapon on Battlefield*, *The Defense Post*, 6.02.2025, <https://thedefensepost.com/2025/02/06/ukraine-laser-weapon-battlefield/> [accessed: 21.02.2025].

Sweden drones: Sightings reported over nuclear plants and palace, BBC, 18.01.2022, <https://www.bbc.com/news/world-europe-60035446> [accessed: 21.02.2025].

Timeline: UAE under drone, missile attacks, Al Jazeera, 3.02.2022, <https://www.aljazeera.com/news/2022/2/3/timeline-uae-drone-missile-attacks-houthi-yemen> [accessed: 21.02.2025].

Ukrainians Made an FPV With Fiber-Optic Cord Stretching For 41 km, *Defence Express*, 26.01.2025, https://en.defence-ua.com/industries/ukrainians_made_an_fpv_with_fiber_optic_cord_stretching_for_41_km-13327.html [accessed: 21.02.2025].

Venezuela President Maduro survives 'drone assassination attempt', BBC, 5.08.2018, <https://www.bbc.com/news/world-latin-america-45073385> [accessed: 21.02.2025].

Wang B., *Ukraine's One Million FPV Drones Is Outnumbered by 5 Million Russian Drones*, *Next Big Future*, 27.01.2024, <https://www.nextbigfuture.com/2024/01/ukraines-one-million-fpv-drones-will-be-outnumbered-by-5-million-russian-drones.html> [accessed: 21.02.2025].

Legal acts

Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (EU Official Journal L 152/45 of 11.06.2019).

Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems (EU Official Journal L 152/1 of 11.06.2019).

Act of 24 January 2025 amending the Aviation Law and certain other acts (Journal of Laws of 2025, item 179).

Act of 24 May 2013 on means of direct coercion and firearms (Journal of Laws of 2024, item 383, as amended).

Act of 26 April 2007 on crisis management (Journal of Laws of 2023, item 122, as amended).

Act of 3 July 2002 – Aviation Law (Journal of Laws of 2023, item 2110, as amended).

Regulation of the Minister of Infrastructure of 27 December 2018 on the structure of Polish airspace and the detailed conditions and use of that space (Journal of Laws of 2019, item 619).

Guideline No. 4/2025 of the President of the Civil Aviation Authority of 21 February 2025 on the designation of geographical zones for unmanned aircraft systems.

Guideline No. 17/2023 of the President of the Civil Aviation Authority of 6 June 2023 on the designation of geographical zones for unmanned aircraft systems (Official Journal of the CAA of 2023, item 42).

Guideline No. 15/2023 of the President of the Civil Aviation Authority of 1 June 2023 on modalities of operations using unmanned aircraft systems in view of the entry into force of the provisions of Commission Implementing Regulation (EU) No. 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (Official Journal of the CAA of 2023, item 39).

Other documents

Government draft Act amending the Aviation Law and certain other acts, print no. 810, <https://www.sejm.gov.pl/sejm10.nsf/PrzebiegProc.xsp?nr=810> [accessed: 21.02.2025].

Jędrzej Łukasiewicz, PhD

Doctor of Physical Sciences. He is a former employee of the Poznań University of Technology, where he was employed as an assistant professor. Designer and pilot of unmanned aerial vehicles. Instructor at the drone pilot training centre of the Poznań University of Technology. He specialises in the security of critical infrastructure facilities for which unmanned aerial vehicles are a source of threats. Author of a method for assessing the effectiveness of detection and neutralisation systems for unmanned aerial vehicles. This method is described in Annex 1 to the National Critical Infrastructure Protection Program entitled *Standards for ensuring the efficient functioning of critical infrastructure - good practices and recommendations*. Author of scientific articles published in international journals. Participant in the work of departmental teams supporting the state administration in increasing the state's resilience to hybrid threats.

Contact: jedrzej.lukasiewicz@tlen.pl

Damian Szlachter, PhD

Editor-in-chief of the ISA (ABW) scientific journal "Terrorism – Studies, Analyses, Prevention". Member of the steering committee of the EU Protective Security Advisors group. National expert at the European Commission's Directorate-General for Migration and Home Affairs in the Policy Group on Public Spaces Protection. National auditor for quality control in civil aviation security (of the Civil Aviation Authority). Participant in the work of more than a dozen 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. Member of the team to investigate the challenges of engineering security of critical infrastructure buildings at the General Office of Construction Supervision. Author of nearly 40 scientific articles and co-author of several books and specialist reports on internal security.

Contact: d.szlachter@abw.gov.pl

Polish individual restrictive measures applied to economic entities in the context of the war in Ukraine and the situation in Russia and Belarus

MARIUSZ CICHOMSKI

Ministry of the Interior and Administration
Republic of Poland

 <https://orcid.org/0000-0003-3707-7856>

KONRAD KACZOR

Independent author

 <https://orcid.org/0009-0009-7182-4027>

Abstract

Poland, like several other European Union countries, adopted restrictive measures in response to the Russian Federation's aggression against Ukraine in 2022, as well as serious human rights violations against civil society and the democratic opposition in Russia and Belarus. The aim of this article is to characterise the economic entities subject to the restrictive measures applied in Poland. The type of activities carried out by these entities, the countries of their registration and their links with Russia or Belarus were taken into account as reasons for freezing their activities on the basis of the Polish sanctions list and the administrative decisions by which the list was entered. As an example, the authors analysed the case of an economic entity listed on the sanctions list, taking into account both the rationale for its inclusion and the established scope of restrictive measures, as well as additional legal mechanisms implemented to minimise the negative effects of these measures. The case analysis allowed for answering the question of the legitimacy of introducing individual restrictive measures at

the national level and whether the application of such measures can impact the security of energy resource supplies, the functioning of transmission infrastructure, and critical infrastructure.

Keywords

restrictive measures, sanctions list, sanctions, war in Ukraine

Restrictive measures in the European Union

The European Union's packages of restrictive measures introduced so far in connection with the aggression of the Russian Federation (RF) against Ukraine (16 packages at the time of preparing this article) and the support provided by Belarus to Russia in this regard, have their legal basis in Article 29 of the Treaty on European Union¹. It allows the Council of the EU to impose restrictive measures against non-EU governments, non-state actors such as economic operators, as well as individuals in order to bring about changes in their policies or actions. The second treaty-based foundation for the EU's application of restrictive measures is Article 215(2) of the Treaty on the Functioning of the European Union². According to this provision, the EU Council may adopt the necessary measures to implement decisions adopted under Article 29 of the Treaty on European Union, ensuring their uniform application across all Member States³. This refers to the possibility of applying restrictive measures of an economic (sectoral) nature, such as bans on the import of certain types of products or

¹ *Treaty on European Union* (consolidated version) – Title V – General provisions on the Union's external action and specific provisions on the common foreign and security policy – Chapter 2 – Specific provisions on the common foreign and security policy – Section 1 – Common provisions – Article 29 (former article 15 of the TEU).

² *The Treaty on the Functioning of the European Union* (consolidated version) – Part 5 – The Union's external action – Title IV – Restrictive measures – Article 215 (former article 301 of the Treaty Establishing the European Community).

³ See: M. Cichomski, *Between armed conflict and state terrorism – specific individual restrictive measures adopted in Poland in the context of the war in Ukraine and the situation in Belarus. Legal perspective*, "Terrorism – Studies, Analyses, Prevention" 2024, no. 5, pp. 314–315. <https://doi.org/10.4467/27204383TER.24.011.19399>; *General framework for EU sanctions*, The European Union, <https://eur-lex.europa.eu/PL/legal-content/summary/general-framework-for-eu-sanctions.html> [accessed: 20.02.2025].

raw materials from countries subject to these measures, as well as financial measures. These include, in particular, the freezing of financial assets and economic resources held or controlled by specific individuals or economic entities. A separate issue concerns diplomatic sanctions, including the suspension of official visits, bilateral or multilateral cooperation with the EU, and the boycott of events⁴.

The challenge does not lie in identifying economically significant vulnerabilities of the state targeted by restrictive measures. The depth of international interconnections is substantial enough to allow for a relatively straightforward assessment of which restrictions would exert the greatest pressure on the targeted state. However, the adoption of restrictive measures at the EU level necessitates agreement between Member States, which poses a significant challenge not only in political but also in economic terms. The implementation of both sectoral and individual restrictive measures requires each EU Member State to conduct a thorough analysis of the potential consequences of these measures⁵. The complexity and gradual nature of the sanctioning process are evidenced by the previously mentioned 16 so-called sanction packages⁶ introduced in response to the conflict in Ukraine. The basis for their introduction was the amendment of 3 main pieces of legislation in this area, namely the *Council Regulation (EC) No. 765/2006 of 18 May 2006 concerning restrictive measures in view of the situation in Belarus and the involvement of Belarus in the Russian aggression against Ukraine* (hereinafter: Regulation 765/2006), the *Council Regulation (EU) No. 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening*

⁴ General framework for EU sanctions...

⁵ See in more detail: M. Cichomski, *Between armed conflict and state terrorism...*, pp. 314–315; P. Pospieszna, *Sankcje Unii Europejskiej wobec Rosji: proces decyzyjny, trwałość i rola państw członkowskich*, „Rocznik Integracji Europejskiej” 2018, no. 12, pp. 311–321. <https://doi.org/10.14746/rie.2018.12.21>.

⁶ On the relationship between the concepts of sanctions, restrictive measures and retaliatory measures at EU level, see in more detail: M. Cichomski, *Between armed conflict and state terrorism...*, pp. 318–319; P. Kobza, *Środki restrykcyjne jako instrument Wspólnej Polityki Zagranicznej i Bezpieczeństwa Unii Europejskiej* (Eng. Restrictive measures as an instrument of the European Union's Common Foreign and Security Policy), „Studia Europejskie” 2006, no. 3, pp. 10–14. The topic of the origins of the concept of sanctions in the dimension of international law was addressed in the: M. Sulek, *Zachodnie sankcje wobec Rosji – sens i skuteczność* (Eng. Western sanctions against Russia – sense and effectiveness), „Rocznik Strategiczny” 2014/2015, vol. 20, pp. 398–400.

the territorial integrity, sovereignty and independence of Ukraine (hereinafter: Regulation 269/2014) and the Council Regulation (EU) No. 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine (hereinafter: Regulation 833/2014).

An example of the aforementioned gradual implementation of restrictive measures is the imposition of sanctions on Russian liquefied petroleum gas (LPG). It was only with *Council Regulation (EU) 2023/2878 of 18 December 2023 amending Regulation (EU) No. 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine* and constituting the 12. package of EU sanctions against the FR – that the import of LPG and its components from Russia was prohibited. The export of this raw material represents one of Russia's most significant sources of revenue and directly contributes to the enhancement of its military capabilities. At the same time, a transitional period was introduced, allowing for the import of Russian LPG until 20 December 2024, under acquired rights, meaning contracts concluded before the restrictive measures entered into force. As a result, the effective ban was implemented nearly 3 years after the outbreak of the full-scale armed conflict in Ukraine.

In this type of case, it is the capabilities or interests of the state to apply restrictions that influence the agreement to introduce certain restrictions, rather than the moderation of restrictive measures on the grounds of adequacy to the changing situation that gives rise to the restrictions (e.g. changes on the frontline and actions of the aggressor). In making this decision, the most important consideration is the level of a country's dependence on the supply of specific raw materials or goods from the country against which restrictive measures are to be applied. Lack of real diversification of supply sources may turn into a crisis situation (lack of resilience of the state in a given area). There may also be a reduction in the state revenue, as exemplified by the long-running discussion at the community level on the introduction of restrictions on diamond imports from the RF.

In view of the consensus of the Member States required to introduce restrictive measures, the limited effectiveness of these measures at the community level or the length of the decision-making process should not come as the surprise. This is due to the determinants of such consensus, which include both the particular economic interests of the states and their internal resilience to disruptions in the supply of specific raw materials or goods from a country subject to sanctions. Additionally, the distance

from a given country to the source of the restrictions (e.g. the location of the conflict or the country on which pressure is being exerted) plays a significant role. For obvious reasons, the perception of threat from the RF differs between Poland or Latvia and Spain or Portugal, just as the approach to threats from the African continent also varies among these states⁷. This discrepancy also translates into varying levels of willingness to bear the consequences of implementing restrictive measures. This difference in perception necessitates the identification of national restrictive measures that will complement the EU measures, allowing for the adaptation of solutions in a geopolitical context. For this reason, countries such as Poland, the Czech Republic⁸, and Latvia⁹ apply subsidiary restrictive measures in relation to the EU's.

The question arises as to what the relationship between community and national restrictive measures should be¹⁰. Reference to it is made in Article 4(2) of the Treaty on European Union, which states that the EU: (...) *shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.*

It is important to emphasise that the EU's competence in the field of Common Foreign and Security Policy, including adoption of restrictive measures, is not exclusive. Member States retain autonomous powers in these areas and have the right to adopt their own restrictive measures, independent of those at the EU level, as Poland, the Czech Republic and Latvia have done. The legal basis for such national competencies derives exclusively from domestic legislation. However, when adopting their own restrictive measures, Member States must ensure that such measures do not undermine the objectives pursued by the restrictive measures adopted at the EU level.

⁷ M. Cichomski, *Between armed conflict and state terrorism...*, p. 342.

⁸ *Zákon o omezujících opatřeních proti některým závažným jednáním uplatňovaných v mezinárodních vztazích (sankční zákon)*, https://www.mzv.cz/jnp/cz/o_ministerstvu/legislativa/pravni_predpisy_v_pusobnosti_mzv/zakon_c_1_2023_sb_o_omezujicich.html [accessed: 26.02.2025].

⁹ *Starptautisko un Latvijas Republikas nacionālo sankciju likums*, <https://likumi.lv/doc.php?id=280278> [accessed: 26.02.2025].

¹⁰ See in more detail: M. Cichomski, *Between armed conflict and state terrorism...*, pp. 321–326.

It is also worth mentioning the *Update on EU good practice in the effective implementation of restrictive measures*. The document states that Member States, in addition to the legislation adopted at the EU level, should also have legal mechanisms at the national level that enable them, where necessary, to freeze funds and financial assets, economic resources of individuals and entities subject to EU restrictive measures. Furthermore, national legislation should provide for the prohibition of making financial funds and economic resources available to these individuals and entities or for their benefit, including through administrative enforcement measures or judicial orders for asset freezing¹¹. It was explained that such measures should empower national authorities to order and enforce the freezing of financial funds and economic resources within the jurisdiction of a Member State, where such assets belong to, are owned by, controlled by, or held by the targeted individuals or entities. Additionally, these measures should also apply to EU-origin entities and individuals conducting their principal activities within the EU¹².

Polish solutions for the application of individual restrictive measures in connection with the conflict in Ukraine

The Polish legal framework governing the application of national individual restrictive measures in relation to the conflict in Ukraine is the *Act of 13 April 2022 on specific solutions to counteracting support for aggression against Ukraine and to protect national security* (hereinafter: Special Act). This legislation ensured the enforcement of EU Regulations 765/2006, 269/2014 and 833/2014. It introduced criminal or administrative sanctions for violations of the restrictive measures described in these regulations, designated the competent national authorities responsible for their implementation, and outlined the necessary procedures. Furthermore, it defined the framework for the application of national restrictive measures while taking into account the fundamental principles set forth in Regulations 765/2006 and 269/2014.

¹¹ *Update on EU good practice in the effective implementation of restrictive measures*, Brussels, 4.05.2018, document no. 8519/18, <http://data.consilium.europa.eu/doc/document/ST-8519-2018-INIT/pl/pdf> [accessed: 20.02.2025].

¹² Ibid.

The Act, in the dimension of the application of individual restrictive measures, is an autonomous piece of national legislation, merely making use of the mechanisms applied by the EU (by reference to them and not duplicating their content). This is clear from the wording of Articles 1(1) and (2) of the Special Act, referring to the Community restrictive measures set out in Article 2(1)-(3) of Regulation 765/2006 and Articles 2 and 9 of Regulation 269/2014. According to Article 2(2) of the Special Act, the measures imposed may not be duplicated: *The scope of the measures referred to in Article 1 applicable to listed persons and entities shall not duplicate the scope of the measures laid down in respect of those persons and entities in the lists set out in Regulation 765/2006 or Regulation 269/2014.*

The national solutions for determining individual restrictive measures were based on the list of persons and entities (hereinafter: the list) maintained by the minister responsible for internal affairs. This list is publicly available on the official website of the minister in the Bulletin of Public Information¹³. Prior to listing, the Minister shall issue a decision, individualised and appealable to the administrative court, on the introduction of individual restrictive measures against the person or entity concerned and on the scope of such measures.

The minister responsible for internal affairs makes a decision regarding the inclusion on the list of individuals and entities that hold financial assets, funds, and economic resources, as defined respectively by Regulation 765/2006 or Regulation 269/2014, and that directly or indirectly support:

- 1) the RF's aggression against Ukraine, initiated on 24 February 2022, or
- 2) serious human rights violations, repression against civil society and the democratic opposition, or activities that pose a serious threat to democracy or the rule of law in the RF or Belarus
 - or those directly linked to such individuals or entities, particularly due to personal, organisational, economic, or financial ties, or where there is a likelihood that their financial assets, funds, or economic resources could be used for such purposes¹⁴.

The fulfilment of any of the listed criteria must be demonstrated in the decision issued by the minister responsible for internal affairs

¹³ *List of sanctioned persons and entities*, Ministry of the Interior and Administration, <https://www.gov.pl/web/mswia/lista-osob-i-podmiotow-objetych-sankcjami> [accessed: 24.02.2025].

¹⁴ Article 3(2) of the Special Act.

regarding the inclusion on the list. For individuals and entities listed, the following measures apply:

- freezing of financial assets, funds, and economic resources in accordance with Article 2(1)–(3) of Regulation 765/2006 or Articles 2 and 9 of Regulation 269/2014. These measures include the freezing of financial assets, funds, and economic resources owned, held, controlled, or possessed by the natural or legal persons, entities, or bodies included in the sanctions list maintained by the minister responsible for internal affairs. This restrictive measure is accompanied by a prohibition on the direct or indirect provision of financial assets, funds, or economic resources to the sanctioned natural or legal persons, entities, or bodies, or for their benefit. Furthermore, it includes a ban on knowingly and intentionally participating in activities aimed at circumventing these measures, either directly or indirectly;
- exclusion from participation in public procurement procedures or competitions conducted under the *Act of 11 September 2019 – public procurement law*¹⁵.

Additionally, a restrictive measure may be applied to listed individuals in the form of their inclusion in the register of foreigners whose stay in the territory of Poland is considered undesirable (Article 434 of the *Act of 12 December 2013 on foreigners*).

The decision regarding inclusion on or removal from the list is issued by the minister responsible for internal affairs, either *ex officio* or upon a justified request submitted by legally designated entities. The authority to request inclusion on the list has been granted to special services, which are capable of gathering information on existing connections through both operational and reconnaissance activities as well as analytical and intelligence processes, including cooperation with partner services from other countries. Additionally, this authority has been conferred upon two law enforcement services, namely the Police and the Border Guard, entities possessing expertise in financial transactions and fund transfers, including the General Inspector of Financial Information (Poland's Financial Intelligence Unit), the Polish Financial Supervision Authority, the President of the National Bank of Poland, the Head of the National Revenue Administration, the Head of the National Prosecutor's Office, and the Chairman of the Committee of the Council of Ministers responsible

¹⁵ Article 1 of the Special Act.

for matters of security and state, due to the Committee's coordinating role in these matters¹⁶.

It is essential to emphasise that, similarly to the restrictive measures imposed by the EU, Poland's national restrictive measures are preventive in nature, rather than repressive or confiscatory¹⁷. Their primary objective is to prevent the flow of financial assets, funds, and economic resources to the RF or Belarus.

Subject-matter and material scope of the applied national individual restrictive measures

As of 31 January 2025, a total of **523 individuals and economic entities**¹⁸ were listed on the national restrictive measures list. Of the **428 individuals** listed: 379 were linked to Belarus (including Belarusian citizens, such as parliamentarians, propagandist journalists, security officials, prosecutors, and judges), 49 were associated with the RF (including 47 Russian citizens, 1 Moldovan citizen, and 1 Polish citizen).

Among the **95 economic entities** listed:

- 14 were linked to Belarus, registered in:
 - Poland – 6,
 - Belarus – 5,
 - Hungary – 1,
 - the United Arab Emirates – 1,
 - Cyprus – 1.
- 81 were linked to the RF, registered in:
 - Poland – 49,
 - the Russian Federation – 18,
 - Cyprus – 7,
 - Kazakhstan – 4,
 - Luxembourg – 1,
 - Turkey – 1,
 - Latvia – 1.

¹⁶ See in more detail: M. Cichomski, *Between armed conflict and state terrorism...*, pp. 327–332.

¹⁷ *Commission Opinion of 19 June 2020 on Article 2 of Council Regulation (EU) No. 269/2014*, Brussels, 19.06.2020, C (2020) 4117 final, p. 6. The same opinion in this respect was presented in paragraph 28 of the *Update on EU good practice...*

¹⁸ The distinctions in the text come from the authors (editor's note).

All listings to date have concerned a total of 535 individuals and entities (430 individuals and 105 entities). Since the adoption of the Special Act, a total of **12 de-listing decisions have been issued in relation to:**

- 2 individuals (1 person due to EU listing, 1 person due to the cessation of the grounds for restrictive measures),
- 10 entities (1 deletion was in connection with registration on the EU list, 9 were related to changes in the ownership structure and termination of cooperation with counterparties related to Russia or Belarus).

In connection with the issuance of a decision on entry into the list of restrictive measures, a total of 96 complaints were referred to the Voivodeship Administrative Court, of which 37 were dismissed (12 legally, including 3 after the judgments of the Supreme Administrative Court), 4 – repealed, 10 – rejected, 8 – discontinued, and 37 remain pending. Twenty-eight cassation appeals have been filed with the Supreme Administrative Court.

For the purposes of the analysis of the issue described, given the need to present the totality of the restrictive measures applied to date, the following section of the article considers both the economic entities that were on the list on 31 January 2025 and those removed from it by that date. This will allow the full spectrum of national restrictive measures applied to date to be presented.

As indicated, the application of restrictive measures at the EU level requires full consensus among Member States, which inherently prolongs the process of imposing these measures – from the identification of an entity to be subjected to restrictions to their actual implementation through an EU legal act. This also poses a significant challenge for the EU itself in the context of bilateral relations with third countries. The foreign policies of individual Member States are not uniform, as they are primarily guided by their national interests. The reasons for this divergence are manifold, ranging from geographical location (e.g. proximity to Russia and Belarus) to natural resources and economic assets (such as fossil fuel deposits and minerals, as well as the ability to quickly secure alternative supplies in the event of restrictive measures). Furthermore, another crucial factor is the capacity of states to ensure internal security in multiple dimensions (transmission infrastructure, public protection, and meeting essential societal needs).

The introduction of national restrictive measures by states provides a real opportunity for a faster response to evolving political and, more importantly, economic conditions. This enables a flexible adjustment of both the subjective and objective scope of the applied restrictive measures. At the same time, it facilitates more direct engagement with economic entities through domestic enforcement mechanisms such as tax audits, the banking system, and licensing regulations. However, implementing such measures presents a significant challenge for states. It requires careful consideration of a broad spectrum of risks that an EU Member State may face when deciding to introduce these measures. One of the primary concerns is the potential reduction in state revenue resulting from restrictions imposed on a given entity (or multiple entities, in the case of sectoral sanctions). This includes a decrease in tax revenues linked to the scale of business operations affected by the restrictive measures. Additionally, a reduction in the volume of certain products on the market – due to decreased business activity – may also lead to lower VAT revenues, as reduced purchasing power translates into lower tax collection.

The second area of risk relates to infrastructure owned by entities subject to restrictive measures. The application of such measures may cause disruptions to transmission lines used by these entities, e.g. natural gas, liquid fuels or power grids. This may lead, *inter alia*, to the cessation of production in production plants, non-delivery of fuel supplies to individual consumers (e.g. home heating), as well as to the cessation of operations of hospitals and other entities providing services to the population, the uninterrupted operation of which is necessary to ensure the proper functioning of the state and the security of its citizens.

Further threats to the state have to do with the employees of those subject to restrictive measures. The role of the state, for economic and social reasons, is to shape the market in such a way that its citizens can not only take up employment, but also that it is stable. Undoubtedly, the inclusion of a given operator in restrictive measures, despite their non-repressive nature, while limiting the possibility to continue operating, may result in a reduction of employment or delays in the payment of salaries or other employee benefits. The consequences of listing are therefore borne not only by the business owners, but also indirectly by the employees.

The Polish Special Act makes it possible to alleviate this inconvenience by introducing the institution of temporary compulsory administration (Article 6a). The task of the administration is to dispose of financial

resources, funds or economic resources within the meaning of Regulation 765/2006 or Regulation 269/2014, when this is necessary to ensure the functioning of an economic entity running an enterprise in the territory of the Republic of Poland in order to:

- 1) maintain jobs in that enterprise, or
- 2) maintain within the scope of activity of that enterprise the provision of services of general interest or the performance of other tasks of public character, or
- 3) protect the economic interest of the state.

Article 6b allows for the introduction of temporary compulsory administration to transfer ownership of financial assets, funds, or economic resources – within the meaning of Regulation 765/2006 or Regulation 269/2014 – to the State Treasury or another entity. This measure applies to assets belonging to persons or entities listed on the sanctions list if necessary to protect an important public interest, safeguard the state's economic interests or ensure its security. The temporary compulsory administrator is responsible for ensuring the continued operation of the economic entity until the financial assets, funds, or economic resources under administration are sold, thereby severing their connection with individuals and entities supporting the activities of the regimes in Russia and Belarus. The proceeds from the sale are frozen in the accounts of the sanctioned owners¹⁹.

To protect the public interest, specifically the interests of employees working for enterprises run by entities subject to restrictive measures, Article 6e of the Special Act introduces the possibility for such entities to apply for benefits from the Guaranteed Employee Benefits Fund to cover employee claims. If the employer fails to submit such an application, employees can also request the benefits individually.

These measures help ensure the continuity of operations for entities listed under the restrictions while safeguarding the rights of their employees. They also, to some extent, mitigate the risks assumed by the state imposing its own restrictions, which are inherently broader than EU measures. An example of such national solutions includes the exclusion from public procurement or competition procedures and the entry of certain foreign nationals into the register of individuals whose stay in Poland is considered undesirable.

¹⁹ See in more detail: M. Cichomski, *Between armed conflict and state terrorism...*, pp. 339–341.

The distribution of restrictive measures imposed by the Minister of Internal Affairs as of 31 January 2025, based on the country of registration of economic entities, was as follows (with the percentage share of the total number of entities subject to restrictive measures in parentheses):

- Poland – 64 entities (60.95%),
- the RF – 19 entities (18.10%),
- Cyprus – 8 entities (7.62%),
- Belarus – 5 entities (4.76%),
- Kazakhstan – 4 entities (3.81%).

Additionally, restrictive measures were applied to individual entities registered in Luxembourg, Turkey, the United Arab Emirates, Hungary, and Latvia, accounting for 4.76% of the total.

It is worth noting that Poland has listed not only entities registered in the RF and Belarus – consistent with the EU-wide objective of restricting the financing of the RF's aggression against Ukraine and the Belarusian regime under Alexander Lukashenko – but primarily entities registered in Poland itself.

The application of restrictive measures to economic entities registered in Poland should also be considered in the context of their ultimate beneficiaries and managing personnel. The fact that an entity is registered in Poland does not necessarily mean it has Polish capital. Due to the freedom of economic activity, this circumstance has no legal significance. Meeting the statutory requirements for registering a business entity – whether in the form of a company or a sole proprietorship – results in its inclusion in the National Court Register or the Central Register and Information on Economic Activity. As a result, a company registered in Poland does not have to be “Polish” in terms of its founding capital or operational funds. Consequently, there is flexibility in appointing its management personnel.

A similar situation applies to the ultimate beneficiaries of economic entities. According to the *Act of 1 March 2018 on counteracting money laundering and terrorist financing*, an ultimate beneficiary is any natural person who directly or indirectly exercises control over a company through rights arising from legal or factual circumstances. They enable decisive influence to be exerted over activities or actions undertaken by the company or any individual on whose behalf a business relationship is established or an occasional transaction is conducted. As a result, the beneficiaries of economic entities registered in Poland can be both business entities and natural persons associated with any country in the world or an economic

entity registered there. This means that individuals linked to the regimes in Russia or Belarus may also be beneficiaries. Consequently, this creates the possibility of unrestricted transfers of funds to these countries, which could then be used to support aggression against Ukraine or repression of the democratic opposition in Russia and Belarus.

The restrictive measures imposed by the Minister of Internal Affairs as of 31 January 2025, apply to economic entities operating in the following sectors (with the percentage share in the total number of entities subject to restrictive measures in parentheses):

- chemical industry (including production and distribution of fertilisers) – 17 entities (16.20%),
- transport and forwarding – 11 entities (10.48%),
- production, export, and distribution of natural gas (including owners of transmission infrastructure) – 9 entities (8.57%),
- production and distribution of construction chemicals – 8 entities (7.62%),
- production and distribution of software – 6 entities (5.71%),
- petrochemical industry – 5 entities (4.76%),
- organisation of mass events – 5 entities (4.76%),
- production and distribution of agricultural machinery – 5 entities (4.76%),
- production and distribution of industrial and medical gases – 4 entities (3.81%),
- trade in birch plywood – 4 entities (3.81%),
- import and distribution of coal – 3 entities (2.86%),
- metallurgical and mining industry – 3 entities (2.86%),
- sale of vehicles and automotive parts – 3 entities (2.86%),
- sale of electronic and telecommunication equipment – 3 entities (2.86%),
- production of hygiene products – 2 entities (1.90%),
- automotive industry – 2 entities (1.90%),
- machinery industry – 2 entities (1.90%),
- financial sector – 2 entities (1.90%),
- production and distribution of food products – 2 entities (1.90%).

Additionally, restrictive measures were applied to individual entities operating in the following sectors: sale of sports goods, electricity distribution, machinery production, online sales, battery production, production and distribution of salt, trade in industrial machinery, fuel

distribution settlements, and distribution of methyl alcohol. Together, they represent 8.57% of those subject to restrictive measures.

In the context of the subject matter of this study, specifically entities importing energy resources or possessing transmission infrastructure, further analysis of the Polish list of entities subject to restrictive measures shows that they were applied to (with the percentage share in the total number of entities subject to restrictive measures in parentheses):

- 5 entities importing energy resources, including 3 dealing with coal imports (4.76%),
- 5 entities possessing transmission infrastructure (4.76%).

The list also included 4 business entities that were in the initial stages of operating in the import and distribution of gas. The imposition of restrictive measures on these entities was preventive in nature and prevented them from developing full-scale operations.

One of the frozen companies listed did not own its own transmission networks, yet being listed on the sanctions list prevented it from engaging in wholesale electricity sales or purchases and from using the transmission networks of the owner of critical infrastructure (CI).

In relation to entities importing energy resources or possessing transmission infrastructure, regarding their place of registration, these restrictions were applied to (with the percentage share in the total number of entities subject to restrictive measures in parentheses):

- 9 entities registered in Poland, i.e. 3 dealing with coal imports, 2 importing natural gas, and 4 planning to start business operations in the import and distribution of gas (8.57%),
- 3 entities registered in the RF (2.86%).

Restrictive measures were applied to these 12 business entities under the provisions of Regulation 269/2014, which constitutes 13.79% of all 87 entities subject to the measures outlined in the regulation.

The entities mentioned are of significant importance for the functioning of the state and its infrastructure due to the nature of their activities, which are critical to ensuring the country's energy security. The application of restrictive measures to these companies posed a threat to the stability of energy and fuel supplies. On one hand, this highlights the risks assumed by a state when introducing such measures at the national level. On the other hand, it provides a real opportunity to exert pressure on the state against which these measures are applied. The application of individual restrictive measures may have an impact on

the security of energy resource supplies, the functioning of transmission infrastructure as well as CI, and should be judged from this perspective.

Case study

In the next section of the article, a case study of one of the entities listed on the national restrictive measures list is analysed. This analysis includes both a description of the premises for the listing and the scope of the restrictive measures applied, as well as additional legal mechanisms implemented to minimise the social and economic negative effects associated with listing this entity. The analysis was conducted based on the decisions of the Minister of the Interior and Administration published on the Ministry's website. In the article, authentic names of business entities have been omitted.

Company A had been operating on the Polish market for several years. Its main business profile involved the import and sale of LPG and liquefied natural gas (LNG), also in the European market. Additionally, the company was involved in the construction of LNG regasification installations, LNG refuelling stations, and the supply of liquefied natural gas. It owned LPG transshipment terminals and an LPG bottling plant. The company also supplied gas through its own transmission networks to several municipalities being gasified using LNG technology. The business profile of Company A, especially in the context of gas supply to individual entities, positioned it in the sector of entities crucial for ensuring the country's energy security, although it was not at a critical level.

Company A was a subsidiary within the B capital group, controlled by the Russian corporation C, from which it imported gas to Poland. Corporation C is one of the largest natural gas producers in Russia and one of the largest business entities in the RF, subject to restrictive measures imposed by the US government through OFAC (Specially Designated Nationals and Blocked Persons List, US Department of the Treasury's Office of Foreign Assets Control). Corporation C is linked to person X, who is subject to restrictive measures by the UK government under *the Sanctions and Anti-Money Laundering Act 2018* – No. 996. Additionally, a board member of corporation C was Y, one of Vladimir Putin's trusted associates, who is also subject to restrictive measures under Regulation 269/2014. Due

to the sector in which corporation C operated, as well as its size, it provided a significant source of revenue to the RF government.

These connections fully met the statutory grounds for the application of restrictive measures against Company A. As a result, the Minister of the Interior and Administration issued an administrative decision, and based on it, placed Company A on the list referred to in Article 2(1) of the Special Act, and initially applied the following measures to it:

- freezing of financial assets and economic resources within the meaning of Regulation 269/2014, owned by, held by, under the actual control of, or controlled by the entity, in full,
- prohibition of making available to the entity, or on its behalf – directly or indirectly – any financial assets or economic resources within the meaning of Regulation 269/2014,
- prohibition of knowingly and intentionally participating in actions aimed at or resulting in the circumvention of the above measures,
- exclusion from the public procurement or a competition conducted under the Public procurement law.

The justification for issuing the decision and applying the restrictive measures was the finding that Company A is an entity possessing financial assets and economic resources within the meaning of Regulation 269/2014, directly or indirectly supporting the RF's aggression against Ukraine. The factual grounds, on the other hand, are the personal, organisational, economic, and financial connections with the Russian entity (Corporation C), which provides the financial resources used to support the aggression against Ukraine. Additionally, individuals connected with Corporation C (both ownership and decision-making ties) are close associates of Putin and beneficiaries of decisions made by the RF government.

As indicated, Company A operated in Poland in the segment of importing natural gas and its subsequent distribution to end users (entities in the public and private sectors). Due to the critical importance of this activity, in order to ensure uninterrupted natural gas supply by the company, the Minister of the Interior and Administration took into account the need to counter the effects of a potential crisis situation²⁰ that could arise from the implementation of the measures specified in the initial decision regarding the inclusion of Company A on the list. He issued a decision in which he modified the scope of measures related to

²⁰ Within the meaning of Article 7a, point 1 of the *Act of 26 April 2007 on crisis management*.

the freezing of financial assets and economic resources of the company, as well as the prohibition of making them available, by excluding the scope related to activities carried out under the orders issued by the Prime Minister in accordance with Article 7a of the *Act of 26 April 2007 on crisis management*.

The purpose of issuing the indicated decision was to release the financial assets and economic resources held by the company, in order to allow their use to ensure the continuity of gas supply to recipients through the infrastructure owned by the company. It should be noted that the structure of the Special Act – and consequently the decision issued on its basis – means that the release of financial assets and economic resources of an entity subject to restrictive measures requires the prior approval of the Head of the National Revenue Administration. According to this law, the tasks and competences referred to in Article 4(1) of Regulation 269/2014 concerning individuals and entities on the list are carried out by the Head of the National Revenue Administration. Upon a justified request, the Head of the National Revenue Administration can agree to release certain frozen financial assets or economic resources or to make specific financial assets or economic resources available, with regard to individuals and entities subject to restrictive measures. However, considering the necessity of ensuring continuous gas supplies, submitting a request to the Head of the National Revenue Administration each time and waiting for a positive decision could disrupt the supply.

The consequence of issuing the aforementioned decision regarding the exclusion of the application of restrictive measures in relation to the company A was the issuance of a decision by the Prime Minister based on Articles 7a and 7b of the crisis management act. Under this decision, the Prime Minister instructed the company to provide specified economic entities engaged in gas fuel distribution with all documentation concerning the infrastructure owned and operated by the company for gas transmission, as well as documentation necessary to ensure uninterrupted gas supply to end consumers. Most notably, the company was required to transfer, on a free-of-charge loan basis, the networks and installations used for gas distribution. The designated economic entities, which were to take over the responsibilities of the company A, were, in turn, obligated to sell gas to the end consumers previously served by the company and to ensure the technical conditions necessary for carrying out these operations.

The actions taken ensured the uninterrupted and urgent delivery of gas to businesses, schools, kindergartens, and other public utility institutions that had previously received gas supplies from Company A. Moreover, despite the application of restrictive measures against the company – effectively prohibiting it from importing gas – no shortages of LPG were recorded in the Polish fuel market.

Company A, exercising the rights granted under the Special Act and administrative law regulations, filed complaints with the Voivodeship Administrative Court against the decisions issued by the Minister of the Interior and Administration. These complaints were dismissed by both the first-instance court and the Supreme Administrative Court. Additionally, the company submitted a request to the minister for removal from the sanctions list, which was denied. Consequently, the company filed a complaint, which was also dismissed by both the first- and second-instance courts.

Exercising his statutory powers, the Minister of Economic Development and Technology, at the request of the Head of the Central Anticorruption Bureau, imposed temporary compulsory administration on the company and defined the scope of financial resources, funds, and economic assets covered by it, including tangible fixed assets, intangible assets and legal rights, movable and immovable assets, as well as financial assets. The Minister considered that the application of this measure was necessary to ensure the operation of the entity in the provision of public services or the performance of other tasks of a public nature and to protect the economic interests of the state. The key task of the appointed administration, as specified in the decision, was to secure the company's assets to ensure the continuity of gas supply services. The temporary administrator initiated actions aimed at selling the company, which are still ongoing.

Summary

The presented analysis clearly indicates that the introduction of restrictive measures at the national level, regardless of those applied by the EU at the community level, is essential for effectively cutting off the revenues of states targeted by pressure. Of particular relevance in this respect is the sanctions policy of countries close to the state targeted by direct restrictive action. National restrictive measures serve as a valuable

complement to EU measures, offering greater flexibility and a stronger capacity for impact. Additionally, their significance lies in the ability to shorten response times to changing circumstances and in the scale of their influence within the territory of the state implementing them.

It should be noted that while the restrictive measures introduced by the EU predominantly target economic entities registered in the RF and Belarus, the measures implemented by Poland primarily affect entities registered in this country. The position of Poland, as a country bordering both the RF and Belarus, as well as Ukraine, where a full-scale war is ongoing, remains relevant in this context. This proximity results, on one hand, in a greater number of local economic ties, which may seem marginal from the perspective of EU objectives. On the other hand, it determines the introduction of restrictions. Poland in the context of the conflict in Ukraine, demonstrates that applying national restrictive measures to certain entities can be crucial for ensuring the security of energy supply, the functioning of transmission infrastructure, and CI.

The significance and effectiveness of national restrictive measures are also reflected in statistical data. According to the National Revenue Administration, the total value of assets frozen in Poland so far exceeds EUR 1.3 billion, including 885.4 million under national legislation²¹.

Bibliography

Cichomski M., *Between armed conflict and state terrorism – specific individual restrictive measures adopted in Poland in the context of the war in Ukraine and the situation in Belarus. Legal perspective*, "Terrorism – Studies, Analyses, Prevention" 2024, no. 5, pp. 311–350. <https://doi.org/10.4467/27204383TER.24.011.19399>.

Kobza P., *Środki restrykcyjne jako instrument Wspólnej Polityki Zagranicznej i Bezpieczeństwa Unii Europejskiej* (Eng. Restrictive measures as an instrument of the European Union's Common Foreign and Security Policy), „Studia Europejskie” 2006, no. 3, pp. 9–31.

²¹ Transcript of the meeting of the Parliamentary Public Finance Committee of 18 December 2024, <https://www.sejm.gov.pl/sejm10.nsf/biuletyn.xsp?documentId=EECD190CFA2CF2EFC1258C44004F3194> [accessed: 12.03.2025].

Pospieszna P., *Sankcje Unii Europejskiej wobec Rosji: proces decyzyjny, trwałość i rola państw członkowskich* (Eng. European Union sanctions against Russia: decision-making process, sustainability and the role of Member States), „Rocznik Integracji Europejskiej” 2018, no. 12, pp. 311–321. <https://doi.org/10.14746/rie.2018.12.21>.

Sulek M., *Zachodnie sankcje wobec Rosji – sens i skuteczność* (Eng. Western sanctions against Russia – sense and effectiveness), „Rocznik Strategiczny” 2014/2015, vol. 20, pp. 398–410.

Legal acts

Treaty on the Functioning of the European Union (consolidated version) – (Official Journal of the EU C 202/47 of 7.06.2016).

Treaty on European Union (consolidated version) – (Official Journal of the EU C 202/13 of 7.06.2016).

Council Regulation (EU) No. 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine (Official Journal of the EU L 229/1 of 31.07.2014).

Council Regulation (EU) No. 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine (Official Journal of the EU L 78/6 of 17.03.2014, as amended).

Council Regulation (EC) No. 765/2006 of 18 May 2006 concerning restrictive measures in view of the situation in Belarus and the involvement of Belarus in the Russian aggression against Ukraine (Official Journal of the EU L 134/1 of 20.05.2006, as amended).

Council Regulation (EC) No. 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism (Official Journal of the UE L 344/70 of 28.12.2001).

Commission Opinion of 19 June 2020 on Article 2 of Council Regulation (EU) No. 269/2014, Brussels, 19.06.2020, C (2020) 4117 final.

Act of 5 August 2022 amending the Act on Specific Solutions to Counteracting Support for Aggression against Ukraine and to Protect National Security and the Act on the National Revenue Administration (Journal of Laws of 2022, item 1713).

Act of 13 April 2022 on Specific Solutions to Counteracting Support for Aggression against Ukraine and to Protect National Security (Consolidated text of Journal of Laws of 2024, item 507, as amended).

Act of 11 September 2019 – Public Procurement Law (Consolidated text of Journal of Laws of 2024, item 1320).

Act of 1 March 2018 on counteracting money laundering and terrorist financing (Consolidated text of Journal of Laws of 2023, item 1124, as amended)

Act of 12 December 2013 on foreigners (Consolidated text of Journal of Laws of 2024, item 769, as amended).

Act of 26 April 2007 on crisis management (Consolidated text of Journal of Laws of 2023, item 122, as amended).

Starptautisko un Latvijas Republikas nacionālo sankciju likums, <https://likumi.lv/doc.php?id=280278> [accessed: 26.02.2025].

Zákon o omezujících opatřeních proti některým závažným jednáním uplatňovaných v mezinárodních vztazích (sankční zákon), https://www.mzv.cz/jnp/cz/o_ministerstvu/legislativa/pravni_predpisy_v_pusobnosti_mzv/zakon_c_1_2023_sb_o_omezujících.html [accessed: 26.02.2025].

Other documents

General framework for EU sanctions, The European Union, <https://eur-lex.europa.eu/PL/legal-content/summary/general-framework-for-eu-sanctions.html> [accessed: 20.02.2025].

List of sanctioned persons and entities, Ministry of the Interior and Administration, <https://www.gov.pl/web/mswia/lista-osob-i-podmiotow-objetych-sankcjami> [accessed: 24.02.2025].

Transcript of the meeting of the Parliamentary Public Finance Committee of 18 December 2024, <https://www.sejm.gov.pl/sejm10.nsf/biuletyn.xsp?documentId=EECD190CFA2CF2EFC1258C44004F3194> [accessed: 12.03.2025].

Update on EU good practice in the effective implementation of restrictive measures, Brussels, 4.05.2018, document no. 8519/18, <http://data.consilium.europa.eu/doc/document/ST-8519-2018-INIT/pl/pdf> [accessed: 20.02.2025].

Mariusz Cichomski

Lawyer, sociologist. He works on issues related to terrorism, organised crime, oversight of service activities, security legislation and issues related to the application of national restrictive measures. He is the author of more than 30 publications on security, particularly in the legal dimension, and on sociology.

Konrad Kaczor

A former police officer and former employee of the Ministry of the Interior and Administration. He has over thirty years of experience in combating economic and organised crime. He specialises in issues related to the international geopolitical situation.

The hybrid dimension of contemporary terrorism and critical infrastructure. Analysis of Europol's TE-SAT reports from 2021–2024

SEBASTIAN WOJCIECHOWSKI

 <https://orcid.org/0000-0002-7972-6618>

Adam Mickiewicz University in Poznań
Institute for Western Affairs in Poznań

Abstract

On the basis of Europol TE-SAT reports from 2021-2024, the author analyses contemporary manifestations of terrorism in the European Union, paying particular attention to its hybrid nature and its impact on the security of critical infrastructure (CI). The starting point of the considerations is the characterisation of the new – according to David Rapoport's typology – fifth wave of terrorism. It is characterised by, among other things, combining traditional and modern methods of operation, links between terrorists and organised crime and the special services of hostile states, as well as activity in the digital space. Analysis of TE-SAT reports reveals the changing dynamics of attacks and arrests in the EU, the different ideological motivations of the perpetrators (jihadist, separatist, right-wing, left-anarchist) and the rise of so-called "lone wolves". The author points to the growing role of countries such as Russia, Belarus and Iran in the use of proxy and cyber terrorist instrumentation and emphasises the need to redefine the EU's counter-terrorism policy, extend Europol's mandate (including state terrorism), intensify cooperation with NATO and develop the EU's multidimensional defence capabilities, including enhanced protection of European CI.

Keywords

terrorism, Europol, hybrid threats, critical infrastructure

A new wave of terrorist threat

Terrorism¹ is not only still present in the world, but is escalating again in different parts of the world, such as the Middle East, Africa and the European Union². The world is facing both its intensification and its evolution – so significant that it is justified to consider the hypothesis of a new wave of terrorism. According to the typology proposed by David Rapoport,³ this will be the fifth wave of the terrorist threat, after its earlier forms: anarchist, anti-colonial, leftist and religious era of jihad⁴. To a greater or lesser extent, it corresponds or even intertwines with its predecessors, for example in the context of the existence of jihadist ideology. It combines old and new aspects of tactics or strategy and has an exceptionally strong hybrid character. Hence its name – a hybrid wave of terrorism. Its main features are, among others:

1. The increasing use by terrorists of simple and easily accessible tools, including a knife or a car, on the one hand, and modern technologies on the other, e.g. drones or artificial intelligence (hybrid means), especially at the stage of planning an attack. This is accompanied by relatively easy access to firearms, massively smuggled from conflict-generating areas – in Africa, the Middle East or Europe (the case of the Balkans or Ukraine), and to weapons produced, including in 3D technology.

¹ On defining the concept of terrorism, see e.g.: A. Richards, *Defining terrorism*, in: *Routledge Handbook of Terrorism and Counterterrorism*, A. Silke (ed.), New York 2019; S. Wojciechowski, *The Hybridity of Terrorism: Understanding Contemporary Terrorism*, Berlin 2013.

² On the current escalation of terrorism see in more detail: R. Gunaratna, *Global Terrorism Threat Forecast 2025*, “RSIS Commentary” 2025, no. 002, <https://dr.ntu.edu.sg/bitstream/10356/182595/2/CO25002.pdf> [accessed: 9.03.2025]; *Security Council debates growing terrorism threat in Africa*, United Nations, 21.01.2025, <https://news.un.org/en/story/2025/01/1159246> [accessed: 5.03.2025]; Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2024*, <https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2024-eu-te-sat> [accessed: 4.02.2025]; Institute for Economics & Peace, *Global Terrorism Index 2025*, <https://www.economicsandpeace.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf> [accessed: 10.03.2025].

³ D. Rapoport, *Waves of Global Terrorism: From 1879 to the Present*, Columbia University Press 2022.

⁴ The concept of waves of terrorism provokes polemics. See e.g.: T. Parker, N. Sitter, *The Four Horsemen of Terrorism: It's Not Waves, It's Strains*, “Terrorism and Political Violence” 2016, vol. 28, no. 2, pp. 197–216. <https://doi.org/10.1080/09546553.2015.1112277>; D. Rapoport, *It Is Waves, Not Strains*, “Terrorism and Political Violence” 2016, vol. 28, no. 2, pp. 217–224. <https://doi.org/10.1080/09546553.2015.1112278>.

2. The formation of increasingly stronger connections in the triad: terrorist/terrorists – criminal groups – special services of hostile countries. This is another hybrid element, particularly dangerous in the case of state terrorism, when a state entity supports or uses this type of activity (from kinetic activities to operations conducted in cyberspace), combined, among others, with criminal terror, as exemplified by the actions of Russia, Belarus, Iran and North Korea (hybrid perpetrators).
3. Terrorists are increasingly effective in promoting their narrative online. The internet and other modern technologies, such as artificial intelligence, have become an important tool used for propaganda, recruitment, disinformation, or to raise funds and organise logistics facilities. They also serve to radicalise attitudes and promote hate speech (hybrid targets), which leads to an environment conducive to the growth of extremism in the targeted countries. The age of the perpetrators – called the generation of Tik-Tok terrorists – is getting lower and lower. For example, in August 2024, police arrested two teenagers, aged 19 and 17, who were planning attacks during Taylor Swift concert in Vienna. On the other hand, during Christmas in 2024, German police detained a 15-year-old terrorist who was planning an attack on a church in Berlin.
4. The combination of the above elements results in the emergence of new threats and modification of the existing ones, including threats to facilities that meet the criteria of national or European critical infrastructure (CI). These targets can be attacked both physically and with the use of cyberspace and in all domains: land, air, sea, cyber, space and cognitive⁵ (hybrid areas of operation). This is confirmed, among others by cases of destruction or disruption of underwater CI or communication infrastructure, as well as their land, air and even space counterparts.

The aim of the article is to analyse the terrorist threat in the EU in 2020–2023 based on Europol's annual reports entitled *European Union Terrorism Situation and Trend Report*. It covers several important categories, such as: attacks carried out, failed and foiled, the number of people arrested for

⁵ Quoted after: *Multi-Domain Operations in NATO – Explained*, NATO, 5.10.2023, <https://www.act.nato.int/article/mdo-in-nato-explained/> [accessed: 2.03.2025].

terrorist activities, court proceedings concerning arrests for committing terrorist offences in EU Member States, and forms of terrorism: jihadist, right-wing, left-wing and anarchist, ethno-nationalist and separatist. The most important point of reference is the analysis of terrorist threats concerning objects that can be classified as CI. A major limitation of the study is the scope of Europol's mandate. Against state-sponsored terrorism, it can only be engaged indirectly⁶. A direct diplomatic or military response to state terrorism falls under the jurisdiction of the EU or NATO foreign policy institution, not Europol. This also translates into its information activity and the data it collects, which are presented in the annual report. It is worth noting that some EU countries are currently taking the initiative to extend Europol's mandate to include issues of terrorism originating from state actors.

Terrorism in the European Union in 2020

Despite global restrictions resulting from the COVID-19 pandemic, there was no significant decrease in terrorist activity in the EU in 2020. According to the TE-SAT 2021 report⁷, the threat level in 2020 was comparable to that in 2019, and there was even a slight increase in the number of attacks and attempts to carry them out. In the EU (excluding the UK), there were 57 terrorist attacks (this number also includes foiled attacks), 2 more than in 2019.

In 2020, Italy had the highest number of terrorist attacks (24 cases), followed by France (15) and Spain (9). Further places were taken by Germany (6), Belgium (2) and Austria (1). Including data from the UK, the total number of attacks in Europe was 119. These data confirm that

⁶ The threat of terrorism has not only an internal dimension, but also a geopolitical one, because in the background there are state actors who can support or use terrorists for their own purposes. There is state terrorism on the territory of the EU, for example, Iran has been sponsoring armed groups (such as Hezbollah) for years and has been carrying out attacks on political opponents abroad. Russia, in turn, pursues an aggressive hybrid policy towards Western countries, for example, it supports extreme extremist movements in Europe through propaganda and finance, and its special services carry out terrorist activities (for example, they order the murder of dissidents in the EU).

⁷ Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2021*, <https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2021-te-sat> [accessed: 4.02.2025].

even during the period of general sanitary restrictions and these related to the possibility of movement, terrorist activity has not been stopped.

In the analysed period, 4 main ideological sources of extremist activities were identified. The attacks were based on the following themes: left-wing and anarchist (25 attacks), jihadist (14), separatist and ethno-nationalist (14) and right-wing (4). The continuing high number of left-wing and anarchist attacks confirms that this is a phenomenon with a relatively stable level of activity for several years.

Although the number of attacks inspired by jihadist ideology decreased in 2020 (from 18 in 2019 to 14 in 2020), according to Europol, they can still be considered the most dangerous. Their implementation was usually successful, which proves the increasing effectiveness of the perpetrators and increases the risk to the civilian population. The escalating potential of this threat has increased due to geopolitical events, including the withdrawal of international forces from Afghanistan and the rapid takeover of power by the Taliban. This success has been used by extremist circles to support the narrative of the durability and effectiveness of Islamist resistance. This could also have had an impact on the intensification of radical sentiments in extremist circles in Europe.

From the perspective of anti-terrorist activities, a noticeable decrease in the number of arrests of people suspected of links to terrorist activities was an important phenomenon – from over 700 cases in 2019 to less than 450 in 2020. However, it is debatable whether the lower number of arrests indicates less terrorist activity or perhaps the difficult work of the services in the conditions of the pandemic. Among the detainees, those suspected of links with jihadist terrorism dominated (57%), followed by people associated with left-wing and anarchist terrorism (12%), separatist terrorism (8%) and right-wing terrorism (7%). The characteristics of the perpetrators' methods of action reveal that the attacks were most often carried out by individuals acting independently, the so-called lone wolves, using easily available means, such as melee weapons or firearms.

The growing role of cyberspace as an area of operation for terrorists should be emphasised. The pandemic has increased online traffic, which extremists have used to spread ideology, recruit and consolidate their supporters. The report points out that terrorist messages increasingly included socially current themes, such as the pandemic, the ecological crisis or threats related to new technologies. The authors of this content tried to gain publicity and interest of new audiences in this way. The increase

in the importance of cyberspace may have several reasons, ranging from pandemic restrictions and difficulties, to the weakening of the logistical capabilities of terrorists, to instructions given, for example, by ISIS, to carry out attacks using the simplest means. It should be noted that due to difficult access to popular messengers, terrorists are constantly looking for new forms of communication. This applies not only to Islamists, but also to other strands of the terrorist threat.

Terrorism in the European Union in 2021

The TE-SAT 2022 report⁸ indicated that compared to previous years, 2021 brought a marked weakening of terrorist activity in Europe. Both the number of attacks – from over 50 in 2019 to 15 in 2021 – and the number of arrests have decreased significantly. The highest number of incidents was recorded in France – 5. There were 3 attacks in Germany, 2 in Sweden. Austria, Denmark, Hungary, Belgium and Spain reported 1 attack each.

Although the number of attacks linked to jihadist ideology was again lower than in previous years, this type of threat is still considered the most dangerous according to Europol. In 2021, of the 11 incidents of this type 3 were successful and 8 were successfully thwarted. The number of attempted right-wing attacks remained unchanged (3 cases), while the activity of extremist left-wing and anarchist movements almost completely decreased – only 1 case. It is worth noting the almost complete disappearance of separatist and ethno-nationalist terrorism, which was still a significant part of this phenomenon in 2020. This change may be partly due to the evolution of the classification criteria used by some Member States, as a result of which certain extremist activities are no longer classified as terrorism.

The dominant group of detainees in 2021 were people suspected of being linked to jihadism – 260 arrests, mainly in France, Spain and Austria. The second largest category were representatives of extreme right-wing currents (64 people). Smaller groups of those arrested were people associated with separatist and ethno-nationalist movements (26) and left-wing and anarchist terrorism (19).

⁸ Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2022*, <https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2022-te-sat> [accessed: 4.02.2025].

The authors of the report point out that the COVID-19 pandemic may have contributed significantly to the decline in physical terrorist activity, as it limited the mobility, communication and organisational capabilities of extremist groups. It also had an impact on changing the way terrorist organisations operate. On the other hand, activities carried out in the digital space – including in the field of recruitment, radicalisation, propaganda and fundraising – have intensified. This requires the security services to develop countermeasures adapted to the new conditions. However, the decline in physical terrorist activity should not be interpreted as a permanent disappearance of the threat. The increase in the number of attacks around the world, the reconstruction of ISIS and Al-Qaeda structures, the development of the extreme right, as well as new forms of terrorism – such as drone attacks, activities in cyberspace or cooperation between state structures and terrorist groups – indicate the evolutionary nature of the threat.

Terrorism in the European Union in 2022

As reported in the 2023 TE-SAT report⁹, in 2022, there were 28 events classified as terrorist attacks in EU countries. This number includes successful, unsuccessful and thwarted attacks (18). This is a significant percentage increase compared to 2021, when 15 such cases were recorded. At the same time, there were significantly fewer attacks in 2022 than in previous years (especially before the COVID-19 pandemic – 55 attacks were carried out in 2019¹⁰). The highest number of incidents occurred in Italy (12), followed by France (6), Greece (4) and Belgium (3), with isolated cases reported in Germany, Spain and Slovakia.

In terms of ideology, the most active were extreme left-wing and anarchist groups (18 incidents). Jihad-motivated actions accounted for 6 cases, and far-right ideology – 4 cases. As a result of these events, 4 people were killed: 2 as a result of Islamist attacks, 2 in connection with violence motivated by right-wing extremism.

⁹ Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2023*, <https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2023-te-sat> [accessed: 4.02.2025].

¹⁰ Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2022...*, pp. 8–9.

In the analysed period, law enforcement authorities of EU countries detained a total of 380 people suspected of terrorist activities. The highest number of arrests was in France (93), Spain (46), Germany (30), Belgium (22), Italy and the Netherlands (21 each). The vast majority of arrests were related to jihadist terrorism (266 people). 45 arrests were made in connection with right-wing terrorism, and 19 arrests were made on the left and anarchist lines. Also apprehended were 18 people associated with separatist and ethno-nationalist terrorism, 26 people associated with other forms of terrorism, and 6 people for whom the form of terrorism was not specified.

In 2022, 427 court proceedings related to terrorist offences were completed, slightly more than in the 2 previous years (in 2020 – 422 and in 2021 – 423). The largest number of trials took place in France (110). Next in line were: Belgium (81), Germany (54), Austria (48), Spain (42), Hungary, the Netherlands (26 each) and Italy (21). The conviction rate was high, with 100% for left- and right-wing terrorism cases and 84% for cases motivated by jihadist ideology. Separatist terrorism trials ended in conviction in 68% of cases.

An analysis of the methods used by the perpetrators shows that they most often chose primitive but effective means of attack. Left-wing and anarchist extremists used primarily improvised incendiary devices and homemade explosives. Jihadists mainly used knives and physical violence (e.g. strangulation), and perpetrators associated with right-wing extremism reached for firearms. Since the actions taken did not require either advanced resources or complex logistics, this made them difficult to predict and prevent.

The digital space has invariably been an important element of terrorist activity. The Internet was used by terrorists not only to spread propaganda and ideology, but also to recruit, raise funds and plan attacks. Popular social media platforms were used for this purpose, as well as closed discussion forums, encrypted messengers and video games. The increasing decentralisation of communication channels makes it difficult for security services to operate effectively, and the risk of radicalisation is therefore increasing.

Data from 2022 indicate that terrorism remains a significant threat to EU Member States. Although the number of arrests and convictions remains stable and the activity of organisations such as ISIS and Al-Qaeda is weakening in the EU, the threat is evolving. In addition to classic forms of violence, it is becoming increasingly important to monitor the digital space, where radicalisation occurs quickly, dispersed and often difficult

to detect. Security services must constantly adapt their activities to the changing dynamics of modern terrorism, and this is also a challenge for legal systems.

Terrorism in the European Union in 2023

In 2023, a total of 120 terrorist incidents were recorded in 7 EU Member States, of which 98 ended in an attack, 9 attempts were unsuccessful, and 13 were foiled by security services. Separatist groups, responsible for 70 attacks, and left-wing and anarchist groups, which carried out 32 attacks, were the most active. There were 14 jihadist attacks. As a result 6 people were killed and 12 injured. These were the events with the highest number of victims. In addition, 2 attacks planned by right-wing extremists were foiled.

Most attacks in 2023 were directed against: CI (15 incidents), private companies (7), civilians (4) and police officers (3). Among the reported forms of attacks, the most common were: arson (20), bombings (8), destruction of property (6), attacks with knives (6) and firearms (5).

The analysis of the TE-SAT 2024¹¹ report shows that the terrorist threat in the EU has various ideological backgrounds. In addition to jihadist terrorist groups, separatist, leftist, anarchist and right-wing organisations are active. The diversity of ideological motivations translates into diverse goals and methods of action, which makes it difficult to counteract and prevent it.

Terrorists are increasingly using modern technologies, including artificial intelligence and digital tools, to plan attacks, recruitment, and propaganda. There is a noticeable increase in interest in obtaining information on the production of weapons using 3D printers, as well as instructions on the use of drones, explosives and chemical weapons. Such actions are observed in environments focused around various ideologies, which means the need for a broad approach to monitoring and countering these threats.

The TE-SAT 2024 report indicates the significant impact of geopolitical events on the dynamics of terrorist threats in the EU. For example, Hamas's attack on Israel in October 2023 and the escalation of the conflict in the Gaza Strip have increased tensions and extremist activity in Europe. Such

¹¹ Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2024...*

events can lead to increased radicalisation and mobilisation of supporters of various extremist ideologies.

Terrorist threats in the European Union. Challenges and demands

Europol reports confirm that the EU area is one of the regions most threatened by terrorism. Among the European countries with an increased level of risk, it is necessary to point out both those that have already been frequently attacked, such as France, Italy or Germany, as well as others, such as Poland, the Czech Republic or the Baltic states. The Polish case – although the 2024 Europol report did not record any attempted attack in Poland and only 1 arrest due to terrorist activity – is important, among others, due to the increased interest of international public opinion in the Polish state. It results not only from his presidency of the EU Council or commitment to support Ukraine, but also from other political and diplomatic activities of Poland.

The intensification of the terrorist threat is confirmed by Europol data. In 2021, 18 attacks were recorded on the territory of EU Member States, in 2022 – 28, and in 2023 there were as many as 120, which means a more than fourfold increase compared to the previous year. Also noteworthy is the large disproportion in 2023 between the number of attacks carried out (98) and the number of foiled (13). Over 90% of all attacks in the year under review concerned 2 countries: France and Italy. This indicates, to some extent, the geographically limited occurrence of terrorist threats. The increase in the terrorist threat is also noticed by public opinion in the EU. According to a survey conducted in 2024 in the EU and the United Kingdom by the Bertelsmann Foundation, in which 26 000 people participated, terrorism is the second – according to the respondents – the greatest threat to peace and security. This answer was given by 21% of respondents. In the first place (25% of respondents) was indicated insufficient border protection¹².

With regard to the origins of terrorism in the EU, it should be noted that Europol reports highlight the diversity of the causes of terrorism in the EU. It is not only, as it is still quite often mistakenly believed, that it has an Islamist

¹² Survey: Border security and terrorism top threats for EU citizens, Yahoo, 20.11.2024, <https://www.yahoo.com/news/survey-border-security-terrorism-top-092813566.html> [accessed: 4.02.2025].

background. In 2023, for example, 70 separatist and ethno-nationalist attacks were recorded, 32 leftist and anarchist attacks, and 14 jihadist attacks. A further escalation of various strands of terrorism, state terrorism (inspired, for example, by Russia or Belarus) and non-state terrorism, fueled, among others, by the special services of hostile countries, for example in response to the intensified anti-Russian policy, support for Ukraine, or armament programmes implemented in the EU, is possible. This also generates the threat of more frequent attacks (physical and in the cybersphere) on objects related to the arms industry, including those classified as CI. The resurgence of ISIS and the accompanying operational and propaganda offensive in various parts of the world are also dangerous. This is due to various factors, including the spectacular success of the Islamists in Syria.

In recent years, CI has become a target with increased levels of vulnerability. Terrorists have noticed that a strike on power grids, transport or communication can paralyse the state as effectively as an attack on people, and it is sometimes easier to carry out. The TE-SAT 2024 report indicates that in 2023, as many as 15 terrorist attacks in the EU targeted CI (the most in the history of these reports). These were mainly attacks on transmission networks, arson attacks on telecommunications masts (traffic against 5G) or attempts to disrupt rail transport. Separatists and anarchists were behind most of these acts, for example, Corsican nationalists attacked facilities related to the functioning of the French government administration, and anarchists in Italy destroyed power stations and railway lines. Although attacks on CI rarely cause fatalities, their social impact is serious – interruptions in power, transport or communication cause chaos and economic losses. These are therefore very attractive targets from the perspective of terrorists who want to strike at society as a whole. Threats to CI are closely linked to the concept of hybrid threats. A terrorist attack on a gas network or financial system can be part of a broader terrorist campaign by a hostile state or group. The year 2023 has proven that CI will be at the heart of the EU's counter-terrorism strategy in the coming years (the new EU Counter-Terrorism Agenda will be launched in the second half of 2025). Many new or modified threats to CI facilities are related to the specificity of the fifth wave of terrorism described at the beginning of the article and to the formation of the triad: terrorist/terrorists – criminal groups – special services of hostile countries. This is particularly dangerous in the case of state terrorism, as exemplified by the actions of Russia, Belarus and Iran, among others. These countries use a wide range of operational

tools, including substitutes or intermediaries, to, inter alia cover their tracks. This is pointed out, among others, by the Finnish special service SUPO (Finnish: Suojelupoliisi) in a report covering 2024¹³.

It is worth highlighting the significant increase in crime in the EU. Europol points out directly that the main threat to the internal security of EU countries is the terror of criminal gangs. In Central and Eastern Europe, this applies especially to groups from the post-Soviet area, e.g. Ukrainian or Georgian. This threat may intensify with the end of the war in Ukraine, as it happened in the former Yugoslavia. We should take into account, among others, increased smuggling of weapons, explosives and cooperation of criminal groups with terrorists or special services of hostile countries. This is evidenced, for example, by the relations of Georgian gangs with Russian, and indirectly also with the local special services.

In conclusion, it should be emphasised that the EU needs not only a new look at the problem of the terrorist threat, but even a new anti-terrorist philosophy at the strategic level, as with the competitiveness compass and the EU's economic doctrine or the shaping of the current defence policy, including the production of armaments. The need for change results not only from the reports of Europol, Mario Draghi¹⁴ and Sauli Niinistö¹⁵, but above all from the re-escalation and evolution of the terrorist threat. This also entails new challenges in protecting CI from terrorist activity, indirectly supported by state actors hostile to the EU. TE-SAT reports indicate that Europol does not have a mandate to directly counter state terrorism. Therefore, it is necessary to revise the powers of EU agencies in this area and strengthen cooperation with NATO in the area of building the resilience of CIs to terrorist attacks supported by state actors.

¹³ SUPO, *National Security Overview 2025*, <https://katsaus.supo.fi/documents/62399122/236002257/National%20Security%20Overview%202025.pdf/a4480ede-834e-6cc3-3c08-f3b762d06253/National%20Security%20Overview%202025.pdf?t=1741941168438> [accessed: 4.02.2025].

¹⁴ M. Draghi, *The future of European competitiveness*, European Commission, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf [accessed: 4.02.2025].

¹⁵ S. Niinistö, *Safer Together. Strengthening Europe's Civilian and Military Preparedness and Readiness*, European Commission, https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf [accessed: 4.02.2025].

A new approach to security in the EU should address not only threats from Russia and its allies, solving the problem of migrants or energy security, but also many other issues, including effective combating terrorism. Effective countering the terrorist threat requires deepening cooperation (including intelligence, logistics, legal, and political) of all EU Member States and expanded cooperation with NATO and other allies in different parts of the world. The aim is to build resilience not only externally, but also internally.

A coherent EU anti-terrorist policy may be threatened by the particular interests of individual Member States, the ongoing political crisis in some of them, the rift in transatlantic relations, the lack of financial resources, or the economic collapse predicted by various specialists. Particular consideration should be given to the scenario assuming a reduction in intelligence cooperation between the US and European partners, which could, among others, significantly reduce the effectiveness of the EU's counter-terrorism efforts.

Bibliography

Parker T., Sitter N., *The Four Horsemen of Terrorism: It's Not Waves, It's Strains*, "Terrorism and Political Violence" 2016, vol. 28, no. 2, pp. 197–216. <https://doi.org/10.1080/09546553.2015.1112277>.

Rapoport D., *It Is Waves, Not Strains*, "Terrorism and Political Violence" 2016, vol. 28, no. 2, pp. 217–224. <https://doi.org/10.1080/09546553.2015.1112278>.

Rapoport D., *Waves of Global Terrorism: From 1879 to the Present*, Columbia University Press 2022.

Richards A., *Defining terrorism*, in: *Routledge Handbook of Terrorism and Counterterrorism*, A. Silke (ed.), New York 2019.

Wojciechowski S., *The Hybridity of Terrorism: Understanding Contemporary Terrorism*, Berlin 2013.

Internet sources

Gunaratna R., *Global Terrorism Threat Forecast 2025*, "RSIS Commentary" 2025, no. 002, <https://dr.ntu.edu.sg/bitstream/10356/182595/2/CO25002.pdf> [accessed: 9.03.2025].

Multi-Domain Operations in NATO – Explained, NATO, 5.10.2023, <https://www.act.nato.int/article/mdo-in-nato-explained/> [accessed: 2.03.2025].

Security Council debates growing terrorism threat in Africa, United Nations, 21.01.2025, <https://news.un.org/en/story/2025/01/1159246> [accessed: 5.03.2025].

SUPO, National Security Overview 2025, <https://katsaus.supo.fi/documents/62399122/236002257/National%20Security%20Overview%202025.pdf/a4480ede-834e-6cc3-3c08-f3b762d06253/National%20Security%20Overview%202025.pdf?t=1741941168438> [accessed: 4.02.2025].

Survey: Border security and terrorism top threats for EU citizens, Yahoo, 20.11.2024, <https://www.yahoo.com/news/survey-border-security-terrorism-top-092813566.html> [accessed: 4.02.2025].

Other documents

Draghi M., *The future of European competitiveness*, European Commission, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf [accessed: 4.02.2025].

Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2020*, <https://www.europol.europa.eu/publications-events/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020> [accessed: 4.02.2025].

Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2021*, <https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2021-te-sat> [accessed: 4.02.2025].

Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2022*, <https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2022-te-sat> [accessed: 4.02.2025].

Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2023*, <https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2023-te-sat> [accessed: 4.02.2025].

Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2024*, <https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2024-eu-te-sat> [accessed: 4.02.2025].

Institute for Economics & Peace, *Global Terrorism Index 2025*, <https://www.economicsandpeace.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf> [accessed: 10.03.2025].

Niinistö S., *Safer Together. Strengthening Europe's Civilian and Military Preparedness and Readiness*, European Commission, https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf [accessed: 4.02.2025].

Sebastian Wojciechowski, Professor

Head of the Department of Strategic Studies and International Security at the Faculty of Political Science and Journalism of Adam Mickiewicz University. Chief analyst at the Institute for Western Affairs in Poznań. Expert of the Organization for Security and Co-operation in Europe on security, including terrorism. Editor-in-chief of “Przegląd Strategiczny”. Recipient of two scholarships from the Foundation for Polish Science and the US State Department. Winner of the scientific award of the Prime Minister of the Republic of Poland and the scientific award funded by the European Union. Former Dean of the Faculty of Political Science and International Relations at the Higher School of Humanities and Journalism in Poznań. Member of, among others: the Commission on Balkan Studies of the Polish Academy of Sciences, the Scientific Board of the Terrorism Research Center at Collegium Civitas, the Programme Council of the Central Industrial District 2 (COP 2) Project. Author of many expert opinions and analyses prepared for Polish and foreign institutions, as well as publications in the field of international relations and internal and international security, with particular emphasis on the issues of: hard and soft threats to security, NATO, Polish and EU security policy, hybridity of terrorism. NATO DEEP eAcademy expert on internal and international security.

Contact: wojciechowski.s@wp.pl

Cyber threats as hybrid activity against the European Union in light of the current geopolitical situation

MONIKA STODOLNIK

Internal Security Agency

 <https://orcid.org/0009-0000-5319-7968>

Abstract

The article presents analysis of cyber threats as a manifestation of the hybrid threats facing Europe. The author analysed reports from European Union and NATO countries in terms of how the identified threats are presented by intelligence services, governments and national CERTs (Computer Emergency Response Teams) and CSIRTs (Computer Security Incident Response Teams). She also discussed the categorisation of cyber threats based on their source of origin and their purpose, including state-sponsored, hacktivist and cybercriminal groups. She pointed to the increasing frequency of cyber attacks, especially those conducted from Russia and China, and discussed their impact on the critical infrastructure and political stability of states. She presented the changing landscape of cyber threats in Europe, gave examples of cyber attacks and described the methods of reporting these incidents adopted in Denmark, Germany, Estonia, Lithuania, Latvia and Poland.

Keywords

hybrid threats, cyber attack, cyber security, disinformation, information operations

Introduction

The contemporary geopolitical situation makes hybrid threats one of the most serious challenges to Europe's security and stability. Hybrid threats represent a combination of conventional and unconventional tactics and aim, among other things, to destabilise the state, its democracy and undermine public confidence. Referring to Francis Fukuyama's definition, according to whom (...) *trust is a mechanism based on the assumption that other members of a given community are characterised by honest and cooperative behaviour based on professed norms*¹, it can be observed that manipulative psychological activities, disinformation violate this very mechanism and deepen divisions in society. In 2025, Europe is particularly vulnerable to such threats due to its close proximity to a potential adversary, as well as technological progress, the potential of which can be used for both defence and attack. Observations and lessons learned from the war in Ukraine point to possible vectors of activity of the Russian Federation (RF) in a situation where the conflict is extended to other European states. The dynamic development of artificial intelligence in recent years has supported hostile activity in cyberspace, in terms of generation of disinformation content and the development of tools to attack information and communication infrastructure.

The standard of living is increasing as technology advances. Due to the development of information and communication technologies (ICT) and growing dependence on automation of various industries, namely Industrial Control Systems (ICS), the society is at the all-time high risk of life threatening disruptions originating in the cyberspace. The energy sector, a key pillar of any modern country's economy, is particularly vulnerable to destructive actions². As EnergiCERT, the Danish energy sector computer incident response team, points out, the number of attacks on this sector in Europe between 2015 and 2022 had a steady upward trend³. Attacks on energy sector actors can paralyse a country – regardless of whether the perpetrators of the attack have financial, ideological or political motives. At the same time, the amount and character of official documents

¹ F. Fukuyama, *Zaufanie. Kapitał społeczny a droga do dobrobytu* (Eng. Trust. The social virtues and the creation of prosperity), Warszawa 1997, p. 38.

² *Cybersecurity of Critical Sectors – Energy*, ENISA, <https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/energy> [accessed: 8.04.2025].

³ *Cyber attacks against European energy & utility companies*, EnergiCERT, September 2022, <https://sektorcert.dk/wp-content/uploads/2022/09/Attacks-against-European-energy-and-utility-companies-2020-09-05-v3.pdf> [accessed: 8.04.2025].

and correspondence that is created and processed electronically make them the prime target for espionage operations that put the national security at risk.

This paper examines the multifaceted nature of hybrid threats facing Europe. This was done on the basis of a review of reports on cyber threats and cyber attacks as a manifestation of hybrid activity, produced from selected EU and NATO countries. The subject of the research was how such threats are presented by the intelligence services, governments and national CERTs and CSIRTs of Denmark, Germany, Estonia, Lithuania, Latvia and Poland – countries located in close proximity to the RF and of interest to Russian cyber offensive group.

Landscape of cyber threats as hybrid threats

As defined by NATO: *Hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace, and attempt to sow doubt in the minds of target populations. They aim to destabilise and undermine societies*⁴. The European Union in its *Joint framework on countering hybrid threats – a European Union response* by the European Commission, points out that *definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature*⁵. In turn, Hybrid CoE (The European Centre of Excellence for Countering Hybrid Threats) presents hybrid threats as activities (...) *used by authoritarian states and regimes, and by non-state actors (NSAs), which often act as proxies for authoritarian regimes. Examples of hybrid threat actors include Russia, China, and Iran. Non-state hybrid threat actors can include groups, movements or entities, which are used or co-opted to fulfil certain strategic objectives*⁶.

⁴ *Countering hybrid threats*, NATO, 7.05.2024, https://www.nato.int/cps/en/natohq/topics_156338.htm [accessed: 19.03.2025].

⁵ *Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response*, Brussels, 6.04.2016, JOIN(2016) 18 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016JC0018>, p. 2 [accessed: 19.03.2025].

⁶ *Frequently asked questions on hybrid threats*, Hybrid CoE, <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/> [accessed: 19.03.2025].

When considering cyber threats in this context, they can be divided into general categories depending on who is the source of the threat and the methods they use to achieve their chosen objective:

- Nation-state actors, often highly sophisticated and technologically advanced:
 - cyber espionage,
 - cyber sabotage,
 - cyber-enabled information operations.
- Hacktivist collectives, ideologically motivated:
 - disruption of IT systems and services (DDoS attacks),
 - cyber sabotage (attacks that alter parameters, damage, affect the provision of the service other than through unavailability),
 - defacement of page content,
 - hack-and-leak attacks.
- Cyber criminals, financially motivated:
 - money extortion via ransomware,
 - money extortion via threatening to disclose data.

Nation-state actors, also called state-sponsored groups, often equated to advanced persistent threat (APT) groups⁷, are government-backed entities, often units of special services, that conduct cyber offensive activities serving the state's interest⁸. Cyber espionage, being a natural extension to the traditional means of intelligence, are at the forefront of their activity, as the goal itself and also as a means for reconnaissance, necessary for staying unnoticed. Cyber espionage is often conducted by the means of phishing or spearphishing, that is by utilising social engineering through email in order to obtain certain information or infect workstation with malicious software. Other than phishing, cyber espionage can also be conducted by compromising a device or network using a vulnerability, that is a weakness of an IT system (a registered, well-known vulnerability, a zero-day vulnerability, a misused feature or a user error). Such attacks violate one element of the cybersecurity triad – confidentiality⁹. As for the integrity of data, such attacks are considered cyber sabotage – destructive in nature and with many more consequences.

⁷ APT groups – organised entities that carry out sophisticated and long-lasting attacks in cyberspace.

⁸ J. Kose, *Cyber Warfare: An Era of Nation-State Actors and Global Corporate Espionage*, "ISSA Journal" 2021, vol. 19, no. 4, pp. 12–15.

⁹ CIA triad: confidentiality, integrity, availability.

They have the potential to disrupt daily life of citizens when they affect CI and create blackouts or transport delays. More severely, when targeting navigation or health protection systems, they can be deadly.

Information operations are (...) *actions taken to affect adversary information and information systems while defending one's own information and information systems*¹⁰. Cyber-enabled information operations or influence campaigns – the terms being used interchangeably – (...) *sit at the nexus of intelligence-based deception and strategic-oriented delivered effects*¹¹. Their goal is a (...) *deliberate use of information by one party on an adversary to confuse, mislead, and ultimately to influence the choices and decisions that the adversary makes*¹². Such activity can involve compromising news media IT systems in order to publish crafted material in a reputable source, creating own websites and social media profiles, mass sending of messages via email or text messages.

Hacktivism as a term is a combination of the words *hacking* and *activism*, therefore is (...) *a combination of grassroots political protest with computer hacking*¹³. In the most recent times, on the forefront of hacktivists one will find pro-Russian and pro-Palestinian groups organising and communicating on Telegram application, conducting a range of cyber attacks with varied results. However, for some the “grassroots” character is questionable, as XakNet Team, Infocentr, Solntsepek and Cyber Army of Russia Reborn are assessed by some researchers to be cooperating with Russian Main Intelligence Directorate (GRU) and its affiliated cyber threat groups, namely APT28¹⁴ and APT44¹⁵.

¹⁰ D.T. Kuehl, *Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age*, “International Law Studies” 2022, vol. 76, p. 36.

¹¹ J. Vičić, R. Harknett, *Identification-imitation-amplification: understanding divisive influence campaigns through cyberspace*, “Intelligence and National Security” 2024, vol. 39, no. 5, pp. 897–914. <https://doi.org/10.1080/02684527.2023.2300933>.

¹² H. Lin, J. Kerr, *On Cyber-Enabled Information/Influence Warfare and Manipulation*, in: *The Oxford Handbook of Cyber Security*, P. Cornish (ed.), Oxford University Press 2021, pp. 251–272.

¹³ T. Jordan, P. Taylor, *Hacktivism and cyberwars. Rebels with a cause?*, London 2004, p. 1.

¹⁴ Mandiant Intelligence, *Hacktivists Collaborate with GRU-sponsored APT28*, Mandiant, 23.09.2022, <https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions> [accessed: 19.03.2025].

¹⁵ G. Roncone et al., *APT44: Unearthing Sandworm*, Mandiant, 17.04.2024, <https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf> [accessed: 19.03.2025].

The most well-known hacktivist groups' main *modus operandi* are *distributed denial-of-service* (DDoS) attacks with the goal of making the targeted websites or services unavailable for the general public. These groups also compromise infrastructure by unauthorised access. They are often not concerned with achieving some complex goal, but merely with demonstrating their technical capabilities. Along with the abovementioned, website *defacement* and *hack-and-leak* attacks are also tools used by the actors to spread their message. The former is used to replace the content of a website with a message from the hacker, while the latter is a form of attack where the data exfiltrated from the victim's networks and servers are shared publicly¹⁶.

With the hacktivism being activism in the cyberspace, similarly, cybercrime (...) *consists of criminal acts committed online by using electronic communications networks and information systems*¹⁷. Such acts include, for example, attacks on information systems as the most critical for the state, not the citizens themselves. The most widely reported incidents related to cybercrime have to do with ransomware, which (...) *has grown to be a dominant cybersecurity threat*¹⁸. Ransomware is a type of malicious software that is used to extort a ransom from the attacked party by denying access to systems and data. Most current ransomware attacks are double-extortion attacks, where the attacker encrypts the data and also exfiltrates it. In doing so, they demand a ransom not only for decryption, but also to prevent their sale or publication¹⁹. Such ransomware can disrupt an entity's operations and, due to the effects of service interruption and data leakage, including customer data, can cause a loss of trust on the part of potential cooperation partners.

Between 2014 and 2024, the frequency of hybrid attacks, especially in the cyberspace, increased. The RF is by far the largest perpetrator

¹⁶ D. Sancho, *Understanding Hacktivists. The Overlap of Ideology and Cybercrime*, Trend Micro, 4.02.2025, <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/understanding-hacktivists-the-overlap-of-ideology-and-cybercrime> [accessed: 19.03.2025].

¹⁷ *Cybercrime*, European Commission, 31.10.2024, https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en [accessed: 19.03.2025].

¹⁸ T. McIntosh et al., *Ransomware Reloaded: Re-examining Its Trend, Research and Mitigation in the Era of Data Exfiltration*, "ACM Computing Surveys" 2024, vol. 57, no. 1, p. 1. <https://doi.org/10.1145/3691340>.

¹⁹ *What is data exfiltration?*, IBM, <https://www.ibm.com/think/topics/data-exfiltration> [accessed: 19.03.2025].

of state-sponsored cyber attacks – including attacks by pro-Russian hacktivist – against European countries²⁰. These have mainly targeted governmental systems and websites, critical infrastructure, state-owned and private companies, think tanks, non-governmental organisations (NGOs), journalists and politicians. In 2022, hacktivist groups, acting on behalf of Russia, carried out 61% of cyber attacks worldwide²¹. The biggest catalyst of such activity has been the war in Ukraine. From the beginning of 2022, various actors declare support for Russia and act in their interest, conducting cyber espionage, cyber sabotage and information operations against EU and NATO countries²². In addition to these politically motivated acts, many cybercrime actors active in attacks against Europe and USA are also associated with Russia. Some of them are Hunters International²³, Hive²⁴ or Conti²⁵. Regardless of the attribution to an APT actor, hacktivist or cybercriminal collective, false-flag operations are also important to consider when it comes to Russian activity in the cyberspace. If one takes into account examples such as the activity of a group self-identifying as Cyber Berkut in 2014, the activities of Cyber Caliphate in 2015 and ransomware attacks in 2016 and 2017, all attributed to the Russian military

²⁰ Microsoft Digital Defense Report 2024, *The foundations and new frontiers of cybersecurity*, <https://go.microsoft.com/fwlink/?linkid=2290930&clid=0x409&culture=en-us&country=us>, p. 13 [accessed: 19.03.2025].

²¹ Thales Cyber Threat Intelligence, *From Ukraine to the whole of Europe: cyber conflict reaches a turning point*, Thales, 29.03.2023, https://www.thalesgroup.com/en/worldwide/security/press_release/ukraine-whole-europecyber-conflict-reaches-turning-point [accessed: 8.04.2025].

²² S.G. Jones, *Russia's Shadow War Against the West*, Center for Strategic & International Studies, 18.03.2025, <https://www.csis.org/analysis/russias-shadow-war-against-west> [accessed: 19.03.2025].

²³ R. Wolert, *RaaS group profile Hunters International*, CERT Orange, 28.10.2024, https://cert.orange.pl/wp-content/uploads/2024/11/CERTOPL_CTI_Hunters_International_en.pdf [accessed: 19.03.2025].

²⁴ *Russian National Charged with Ransomware Attacks Against Critical Infrastructure*, U.S. Department of Justice, 16.05.2023, <https://www.justice.gov/archives/opa/pr/russian-national-charged-ransomware-attacks-against-critical-infrastructure> [accessed: 19.03.2025].

²⁵ *Multiple Foreign Nationals Charged in Connection with Trickbot Malware and Conti Ransomware Conspiracies*, U.S. Department of Justice, 7.09.2023, <https://www.justice.gov/archives/opa/pr/multiple-foreign-nationals-charged-connection-trickbot-malware-and-conti-ransomware> [accessed: 19.03.2025].

intelligence service GRU²⁶, the reach of the Russian special services may be broader than one might have initially thought.

China, another important source of cyber threats, follows its political and ideological goals of greatness and a superpower status²⁷. Their hacking serves strategic economic goals. According to China's Military Strategy (...) *cyberspace has become a new pillar of economic and social development*²⁸. According to NATO experts (...) *Parts of the Chinese military have become useful tools for the government to conduct political and economic cyber espionage, and also to help reduce the PLA's [People's Liberation Army] own technological and strategic disadvantages relative to its competitors*²⁹. Thus the most vulnerable economic sectors of European states are: energy, telecommunications and transport³⁰.

Denmark

One of the most extensive cyber attacks against Danish CI happened in May 2023. The actor, not openly attributed to the GRU, but suspected by SektorCERT to be related to Sandworm group³¹, conducted thorough reconnaissance before the attack. It might have included, among cyber espionage, traditional means of collecting intelligence. SektorCERT reported, that the information about the vulnerable devices was not available on public services (such as Censys or Shodan) at the time

²⁶ A. Greenberg, *A Brief History of Russian Hackers' Evolving False Flags*, Wired, 21.10.2019, <https://www.wired.com/story/russian-hackers-false-flags-iran-fancy-bear/> [accessed: 19.03.2025].

²⁷ A.H. Cordesman, *China's Emergence as a Superpower*, Center for Strategic & International Studies, 15.08.2023, <https://www.csis.org/analysis/chinas-emergence-superpower> [accessed: 19.03.2025].

²⁸ *China's Military Strategy*, Ministry of National Defense of the People's Republic of China, 23.06.2021, <http://eng.mod.gov.cn/xb/Publications/WhitePapers/4887928.html> [accessed: 19.03.2025].

²⁹ M. Raud, *China and Cyber: Attitudes, Strategies, Organization*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn 2016, https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf, p. 21 [accessed: 19.03.2025].

³⁰ *Report on the state of Poland's cybersecurity in 2024*, in press.

³¹ *The attack against Danish, critical infrastructure*, SektorCERT, November 2023, <https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf>, p. 15 [accessed: 19.03.2025].

of the attack, proving that the attackers had obtained such information via other means³². The Zyxel edge device software vulnerability that was exploited in this attack (CVE-2023-28771) received a score of 9.8 out of 10. This makes it a critical vulnerability – one that is easy to exploit and allows for a security breach that has serious consequences. The vulnerable devices manufactured by Zyxel were at that time largely utilised by small Danish CI operators for their OT³³ environments. Altogether, 22 energy companies were successfully compromised and several of them noted disruptions in their operations.

The most recent assessment of Denmark on the hybrid threats from Russia is that it (...) *uses hybrid means both in the run-up to and during a direct military conflict (...) hybrid means include political, economic, informational and military tools, which can be used in coordination to maximize their impact*³⁴. Danish Defence Intelligence Service (Danish: Forsvarets Efterretningstjeneste) identifies that Russian hybrid operations involve both public authorities and private actors, with the former coordinating activities, which is often concealed as to who is behind it³⁵. Following similar outlook on the present situation regarding threat level and goals, Danish Centre for Cyber Security (Danish: Center for Cybersikkerhed) assesses that (...) *it is likely that state-sponsored Russian hackers conduct cyber espionage against Danish CI in preparation for destructive cyber attacks in the future*³⁶. At the same time China is also suspected to be conducting cyber espionage in order to gain information on technology and policies. Going further, this centre evaluates that the highest risk of cyber attacks, that result in death or injury, significant property damage or destruction or manipulation of information, data or software, comes from Russia, mainly state-sponsored groups.

³² Ibid., p. 10.

³³ Operational technology – systems and equipment used to monitor, control and manage technological processes, such as production machinery, pumps, measuring devices or traffic management systems.

³⁴ *Intelligence Outlook 2024*, Danish Defence Intelligence Service, 22.01.2025, https://www.fe-ddis.dk/en/produkter/Risk_assessment/riskassessment/Intelligenceoutlook2024/, p. 26 [accessed: 19.03.2025].

³⁵ Ibid.

³⁶ *Threat assessment: the cyber Threat against Denmark 2024*, Centre for Cyber Security, September 2024, <https://www.cfcs.dk/link/472c3cc8872446e59fa59eaf0f7ad945.aspx>, p. 8 [accessed: 19.03.2025].

Germany

In May 2023, Germany's Federal Minister of the Interior stated: *We will absolutely not be intimidated by the Russian regime*³⁷. These words were said in reference to cyber attacks conducted by the RF. The cause for such reaction was the announcement that the GRU and their threat group APT28 were behind the cyber attacks in January 2023. The targets of these attacks were the SPD party along with companies in the logistics, defense, aviation and IT sectors. The attack was possible due to a security gap in Microsoft Outlook, that made it possible for unauthorised actor to access email accounts of these entities. Germany stood behind the opinion that this attack was (...) *a serious interference with democratic structures*³⁸. In general, the Federal Ministry of the Interior and Community (German: Bundesministerium des Innern und für Heimat) assesses that the war in Ukraine has changed the security situation in Germany in such a way, that the country needs better protection and awareness of vulnerability to cyber attacks and Russian disinformation³⁹.

German intelligence services state that Russia's espionage activities concern government and administration as well as military, technology, research, business and industry. *Russian cyber attacks, whether directed at individuals, organisations or government institutions, are primarily aimed at gaining a steady source of intelligence. In addition to such espionage, these attacks may also be used for sabotage, influence operations, disinformation or propaganda purposes*⁴⁰.

On the issue of cyber threats from China, Germany believes that the actions of the intelligence services serve the Chinese Communist Party's goal of China's status as a global leader and world power⁴¹. Federal Office for the Protection of the Constitution (German: Bundesamt für

³⁷ *Cyber attacks traced to Russian military intelligence agency*, Federal Ministry of the Interior and Community, 3.05.2024, <https://www.bmi.bund.de/SharedDocs/kurzmeldungen/EN/2024/05/schutzmassnahmen-cyberangriffe-en.html> [accessed: 19.03.2025].

³⁸ Ibid.

³⁹ *Heightened security situation in Germany*, Federal Ministry of the Interior and Community, https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/ukrain/security_meldung.html [accessed: 19.03.2025].

⁴⁰ *Brief summary 2023 Report on the Protection of the Constitution (Facts and Trends)*, Bundesamt für Verfassungsschutz, <https://www.verfassungsschutz.de/SharedDocs/publikationen/EN/reports-on-the-protection-of-the-constitution/2024-06-brief-summary-2023-report-on-the-protection-of-the-constitution.pdf>, p. 60 [accessed: 19.03.2025].

⁴¹ Ibid.

Verfassungsschutz) directly points to groups APT15 and APT31 as notable due to their complex techniques and tools they use. In early 2023, Germany's IT service providers for government networks were targeted in a supply chain attack by a Chinese threat actor⁴². However, the report did not specify what the attack consisted of.

Estonia

The first cyber attack publicly attributed by Estonian authorities was conducted in 2020 by the military intelligence service of Russia – GRU, specifically Unit 29155. CERT-EE team, the incident handling unit of the Information System Authority of Estonia, reported that the computer systems of the Ministry of Economic Affairs and Communications were breached with a backdoor malware. This resulted in exfiltration of 350 GB of data, including sensitive internal information – strategic documents and working papers, personnel details, and correspondence with businesses⁴³. The same actor also attacked the Ministry of Foreign Affairs and the Health and Welfare Information Systems Centre. The public announcement and attribution only happened in late 2024 as a result of the Operation Toy Soldier by Estonia and several other countries, linking Unit 29155 to multiple cyber attacks against Ukraine, NATO and EU countries. *The objectives of GRU's cyber cell, Unit 29155, include gathering intelligence, causing reputational damage through the theft and leak of sensitive information, and systematic sabotage by destroying data and computer systems*⁴⁴.

In 2023, CERT-EE also published a thorough analysis of hacktivist-lead DDoS attacks that were carried out in 2022 and targeted public, transport and financial sector websites of Estonia. The attacks were increasing in relation to certain events, such as moving of the Soviet monuments in Narva or declaration by Estonian parliament Riigikogu that the Russian regime is terrorist⁴⁵. CERT-EE announced that the impact of those attacks

⁴² Ibid., p. 62.

⁴³ *Cyber Security in Estonia 2025*, Republic of Estonia Information System Authority, <https://www.ria.ee/en/cyber-security-estonia-2025> [accessed: 19.03.2025].

⁴⁴ Ibid.

⁴⁵ *Cyber Security in Estonia 2023*, Republic of Estonia Information System Authority, <https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf>, p. 17 [accessed: 19.03.2025].

was marginal, sending the message that Estonia does not consider them as a serious threat, but rather as a nuisance. Most importantly, CERT-EE did not attribute these attacks to the Russian state, but to ideologically motivated hackers for whom the war was the catalyst. The attacks were often the result of actions not in line with the official Russian narration.

Presenting a general perception of sponsored threats in cyberspace, the Estonian Internal Security Service (Estonian: Kaitsepolitseiamet, KAPO) stated that hostile cyber intelligence activities (...) *are usually carried out by hostile nations' military and special services' cyber intelligence units that persistently work to advance their country's interests*⁴⁶. According to KAPO (...) *both state institutions and companies providing critical services must recognise that their status as such renders them potential targets for [cyber sabotage] attacks*⁴⁷. *KAPO considers it highly likely that the Russian special services will continue to attempt to gain illegal access to the computer networks of Estonia's critical service providers and key transport and logistics companies in order to gather information and be prepared to disrupt their operations with cyber measures if necessary*⁴⁸.

An important observation to public attitude and perception towards non-state actors such as cybercriminals or hacktivists is that (...) *Russian special services also use hackers who are indirectly related to them and appear to operate independently*⁴⁹. KAPO assesses that such low-level, low-impact attacks, as opposed to APT groups directly tied to special services, enable Russia to generate an illusion of strong support and high capabilities⁵⁰.

Estonia also draws attention to threats from China. KAPO points out that technology produced there may contain malware and hardware backdoors, allowing for unauthorised access to Estonian networks and devices by the Chinese⁵¹. Therefore, despite the competitive prices of these technologies, it is important to consider Chinese-origin solutions as

⁴⁶ *Annual review 2023–2024*, Estonian Internal Security Service, https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2023-2024.pdf, p. 26 [accessed: 19.03.2025].

⁴⁷ Ibid.

⁴⁸ *Annual review 2022–2023*, Estonian Internal Security Service, https://kapo.ee/sites/default/files/content_page_attachments/Annual%20Review%202022-23_0.pdf, p. 22 [accessed: 19.03.2025].

⁴⁹ *Annual review 2023–2024...*, p. 26.

⁵⁰ Ibid., p. 27.

⁵¹ *Annual review 2022–2023...*, p. 24.

a potential threat to the information processed in the targeted systems and to carry out an analysis of the risks arising from their use on a case-by-case basis.

Lithuania

Preceding the war in Ukraine, Lithuania had been one of the prime targets of the “Ghostwriter” campaign, attributed to group UNC1151 and at that time associated with Russia⁵². This activity, which continues, albeit on a smaller scale, combines two spheres – cyber attacks and information operations, where compromised infrastructure is used to spread disinformation to the public. Numerous operations were mostly related to relations between Lithuania and Poland, e.g. information operations under the heading “Radioactive waste leaked from Lithuanian nuclear plant poses danger to Poles living near border” or “Poland trained extremists to destabilise Lithuania”, but also between Lithuania and Germany or the US⁵³. In a statement on 23 September 2021, Vice Minister of National Defence Margiris Abuševičius said that *Lithuania firmly supports the joint European Union Declaration issued in a rigorous condemnation of the Ghostwriter cyber-information attacks associated with Russia that target democratic processes, institutions, politicians, media representatives and, generally, societies, of EU member states*⁵⁴. In 2023, Lithuanian intelligence services – The Second Investigation Department under the Ministry of National Defence (Lithuanian: Antrojo Operatyvinių Tarnybų Departamento, AOTD) and State Security Department (Lithuanian: Valstybės Saugumo Departamentas, VSD) reported that cyber-enabled information operations against Lithuania by the Ghostwriter have subsided due to its redirected effort towards Ukraine.

⁵² The current assessment of experts on the subject is that the group is equally likely to have ties to either Russia or Belarus. A false flag operation is also possible.

⁵³ *GhostWriter Update: Cyber Espionage Group UNC1151 Likely Conducts GhostWriter Influence Activity*, Mandiant, 28.04.2021, https://services.google.com/fh/files/misc/ghostwriter_update_report.pdf, pp. 12–14 [accessed: 19.03.2025].

⁵⁴ *Lithuania supports the EU declaration condemning Ghostwriter malicious cyber activities and calls to use more political tools*, Ministry of National Defence of the Republic of Lithuania, 23.09.2021, <https://kam.lt/en/lithuania-supports-the-eu-declaration-condemning-ghostwriter-malicious-cyber-activities-and-calls-to-use-more-political-tools/> [accessed: 8.04.2025].

Lithuanian intelligence services assess that due to mass expulsions of Russian diplomats, or rather Russian intelligence officers under diplomatic cover, Russia will seek other means for information gathering and thus resort to, among others, cyber espionage. AOTD and VSD evaluated attacks as increasingly prevalent, mostly targeting governmental organisations and CI.

Lithuania, like Estonia, points to the cooperation of cyber criminals and non-state-supervised hackers with Russian special services. Criminals benefit financially and have technological support through this cooperation, while states gain from the fact that attribution becomes more difficult⁵⁵.

In 2024 Lithuania focused their reporting on the threat posed by China. It was pointed, that (...) *their activity in Lithuanian cyberspace has increased especially since 2021, when Lithuania announced the opening of the Taiwanese Representative Office*⁵⁶. The most recent switch in targeting happened from the private sector to governmental institutions for internal affairs and foreign policy. Tactics have evolved towards social engineering, activities are conducted via social networks.

Latvia

Latvian government is not very open to naming perpetrators of cyber attacks, while still presenting the sectors that are the most targeted – in 2022 the same actors behind attacks on Ukrainian infrastructure tried to attack entities in telecommunication and energy sectors. The names or affiliation of the attackers were not disclosed due to security reasons⁵⁷. As predicted by Latvian State Security Service (Latvian: Valsts drošības dienests, VDD)

⁵⁵ *National Threat Assessment 2023*, <https://kam.lt/wp-content/uploads/2023/03/Assessment-of-Threats-to-National-Security-2022-published-2023.pdf>, p. 55 [accessed: 19.03.2025].

⁵⁶ *National Threat Assessment 2024*, <https://www.vsd.lt/wp-content/uploads/2024/03/GR-2024-02-15-EN-1.pdf>, p. 57 [accessed: 19.03.2025].

⁵⁷ D. Antoniuk, *Latvia's cyberspace faces new challenges amid war in Ukraine*, The Record, 28.10.2022, <https://therecord.media/latvias-cyberspace-faces-new-challenges-amid-war-in-ukraine> [accessed: 19.03.2025].

in 2022⁵⁸ and manifested in 2023⁵⁹ and 2024⁶⁰, state-supported groups originating in Russia were behind supply chain attacks using malware-laced hardware or software as well as updates or maintenance services. According to the Constitution Protection Bureau (Latvian: Satversmes aizsardzības birojs, SAB), such supply chain attacks targeted, for one, a TV satellite of Tet, a Latvian telecom company, which resulted in brief Russian propaganda broadcast. Similarly, the hackers managed to obtain access to outsourced Balticom servers in Bulgaria and broadcast a Russian military parade⁶¹ – in neither case the infrastructure was located in Latvia⁶². Nevertheless, Latvia's CERT.LV team emphasised that (...) *it is essential to prevent the involvement of Latvia's IT infrastructure in cyberattacks and the possibility of attacks from within the country, as Russian-linked telecommunications companies are deliberately building a presence in Latvia and other EU member states*⁶³.

The attacks that compromise transmission infrastructure for broadcasting propaganda blur the boundaries between a cyber attack and an information operation, where an entity gets breached in order to use its reach and reputation for distribution of disinformation. Compared to other means of such activity, cyber-enabled information operations can much more quickly reach the intended audience, thus making them an attractive vector for the perpetrators.

Similarly to other European countries, Latvia also supports the belief, that pro-Russian hacktivists are (...) *likely coordinated and financed to achieve the objectives of Russia's domestic and foreign policy influence operations*⁶⁴.

⁵⁸ *Annual Report on the activities of Latvian State Security Service (VDD) in 2022*, <https://vdd.gov.lv/uploads/materials/33/en/annual-report-2022.pdf>, pp. 13–14 [accessed: 19.03.2025].

⁵⁹ *Annual Report on the activities of Latvian State Security Service (VDD) in 2023*, <https://vdd.gov.lv/uploads/materials/37/en/annual-report-2023.pdf>, p. 15 [accessed: 19.03.2025].

⁶⁰ *Annual report on the activities of Latvian State Security Service (VDD) in 2024*, <https://vdd.gov.lv/uploads/materials/40/en/annual-report-2024.pdf>, p. 17 [accessed: 19.03.2025].

⁶¹ *Latvia mulls tightening security after recent TV propaganda hacks*, LSM+, 20.05.2024, <https://eng.lsm.lv/article/society/crime/20.05.2024-latvia-mulls-tightening-security-after-recent-tv-propaganda-hacks.a554618/> [accessed: 19.03.2025].

⁶² *2024 Annual Report*, Republic of Latvia Constitution Protection Bureau, https://www.sab.gov.lv/files/uploads/2025/02/SAB-gada-parskats_2024_ENG.pdf, p.36 [accessed: 19.03.2025].

⁶³ *Latvian Cybersecurity and CERT.LV Technical Activities Annual Report 2023*, 26.07.2024, https://cert.lv/uploads/eng/Annual_Report_CERT-LV_2023.pdf, pp. 4–5 [accessed: 19.03.2025].

⁶⁴ *Ibid.*, p. 6.

At the same time, reflecting on the events of 2022, VDD verified that the information published by such groups on their channels on Telegram is disinformation, as the damage they report did not actually occur⁶⁵.

In regards to Chinese intelligence, VDD assesses that China continues to consider Latvia primarily as a part of NATO and the EU, which it sees as the main rivals in the competition for global influence⁶⁶. With this in mind, their goal is clear – collecting intelligence on strategic decisions and policy regarding relations between China and opponent countries. Latvia's intelligence services observe attempts from Chinese representatives to create and strengthen positive relations and influence with Latvian politicians, academics and researchers, which confirms their interest in new technologies, innovations and policies. This interest translates into cyber matters, where Chinese cyber units show their hacking activity.

Poland

Polish state security institutions do not make information available in the form of periodic reports on strategic or operational issues (only reports on technical issues), so in order to assess the government's position on hybrid threats it was necessary to reach for ad hoc announcements from spokespersons or publications appearing on the official government website gov.pl.

Such was the official statement of the Government Plenipotentiary for the Security of Information Space of the Republic of Poland in late 2022, where several cyber attacks were attributed to Russian hackers: (...) *through hostile operations in cyberspace Russia wants to exert pressure on Poland, as a frontline country and a key Ukraine's ally on the NATO eastern flank*⁶⁷. Those included DDoS attacks carried out by the pro-Russian hacktivist group NoName057(16) as a response to a resolution of the Polish Parliament

⁶⁵ *Annual Report on the activities of Latvian State Security Service (VDD) in 2022...*, p. 13.

⁶⁶ Ibid.

⁶⁷ *Russian cyberattacks*, Serwis Rzeczypospolitej Polskiej, 30.12.2022, <https://www.gov.pl/web/special-services/russian-cyberattacks> [accessed: 19.03.2025].

of December 2022 recognising Russia as a state sponsor of terrorism⁶⁸, as well as the creation of data collection websites through phishing.

Similarly, the Spokesman for Poland's Minister-Special Services Coordinator stated in mid-2022 that (...) *intelligence operations involving hacking attacks, taking over information resources and using them to manipulate public opinion have been used by the Kremlin in recent years in its fight against NATO*⁶⁹. He therefore clearly attributed these actions to Russia.

The year 2024 was the first year that the Report of the Government Plenipotentiary for Cybersecurity for the previous year was presented publicly⁷⁰. Previously, it was a fully classified document. This thus served, along with CERT Polska and CSIRT GOV annual reports, as the only official resources for an overview of 2023.

During several months preceding the parliamentary elections in 2023, hacking group UNC1151 continued to carry out their personalised spearphishing activity against politicians, military personnel, journalists, lawyers, and various other people that might have a connection to Russia and Belarus. Such campaigns had the goal of cyber espionage and disinformation. In the Report on the state of Poland's cybersecurity in 2023 they were attributed to Belarus. The same group is thought to be behind a cyber-enabled information operation directly preceding the elections, where emails, text messages and mail info screens were utilised for spreading disinformation⁷¹.

No direct attribution, but hints to the Russian provenience, were given by the Minister of Digital Affairs regarding the cyber attack on the Polish

⁶⁸ *Sejm uznał Rosję za państwo wspierające terroryzm* (Eng. The Sejm recognised Russia as a state supporting terrorism), Sejm Rzeczypospolitej Polskiej, 14.12.2022, <https://www.sejm.gov.pl/sejm9.nsf/komunikat.xsp?documentId=4774505381CECC10C1258918007022FA> [accessed: 8.04.2025].

⁶⁹ *Ataki hakerskie na RP operacją rosyjskich służb* (Eng. Hacker attacks in the Republic of Poland as an operation of Russian services), Serwis Rzeczypospolitej Polskiej, 20.07.2022, <https://www.gov.pl/web/special-services/hacker-attacks-on-the-republic-of-poland-as-an-operation-of-russian-services> [accessed: 19.03.2025].

⁷⁰ *Sprawozdanie Pełnomocnika Rządu do spraw Cyberbezpieczeństwa za 2023 rok* (Eng. Report of the Government Plenipotentiary for Cyber Security for 2023), Ministerstwo Cyfryzacji (Eng. Ministry of Digital Affairs), 11.04.2024, <https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni> [accessed: 8.04.2025].

⁷¹ *Report on the state of Poland's cybersecurity in 2024*, CSIRT GOV, <https://csirt.gov.pl/download/3/220/RaportostaniebezpieczenstwacyberprzestrzeniRPw2023.pdf>, p. 6 [accessed: 19.03.2025].

Press Agency and a false dispatch about a partial mobilisation in Poland that was published on the PAP website as a result of a hack. The minister stated about this event that its goal was (...) *to spread disinformation before the elections and to 'paralyse' society*⁷². It was about the European Parliament elections in 2024.

Reporting in Poland focuses more on the incidents themselves, such as various examples of phishing emails distributed by Russia-affiliated APT groups like APT28, APT29 or Gamaredon for the purpose of cyber espionage. Such reports are presented by the national CSIRTs. In Poland, little is said about the overall hybrid threat landscape from a counterintelligence perspective despite one national CSIRT team operating within the structures of the Internal Security Agency.

There is very little information published on threats originating from China in Poland. Only a few examples of such incidents can be found in the government sources. The assessment of the situation in 2023 was that due to the level of propaganda cooperation between China and Russia, (...) *it should be expected that the interests and activity of Chinese intelligence will not change, mainly due to the scale of support that the Republic of Poland provides to Ukraine in repelling Russian aggression, Warsaw's alliance with Washington, and the situation around Taiwan*⁷³.

Conclusions

The results of presented research as a whole provide an in-depth overview of the current cyber threats faced by the European Union. The position of the countries analysed is that the attacks originating in Russia have been on the rise since the beginning of the war in Ukraine in 2022. There are no signs suggesting that they might subside. On the contrary, the capabilities of the threat actors are evolving with their experience and the attacks are becoming more covert and sophisticated. In regards to China, the unanimous opinion is that the threats originating from this country are intensifying and may evolve from intelligence gathering into destructive.

⁷² *Fake PAP report looks like cyberattack, says gov't official*, Polska Agencja Prasowa, 31.05.2024, <https://www.pap.pl/en/news/fake-pap-report-looks-cyberattack-says-govt-official> [accessed: 19.03.2025].

⁷³ *China's propaganda offensive*, 17.02.2023, <https://www.gov.pl/web/special-services/Chinas-propaganda-offensive> [accessed: 19.03.2025].

The other two states from the Big Four⁷⁴, that is Iran and North Korea, are rarely mentioned in relation to cyber threats.

The strategies for reporting and attributing the attacks adopted in the countries analysed can be divided into 3 categories: minimal, cautious and direct. Latvia, in the case of attacks on its telecommunications and energy sectors, only reported that the same actor was behind the attacks in Ukraine. It led the public to believe that this actor was linked to Russia, but did not name them directly. Denmark was careful to identify the name of the group potentially behind the critical infrastructure attack, while emphasising the high uncertainty and circumstantiality of the attribution. Germany however directly attributed the attacks against various sectors to a GRU-lead group APT28, openly speaking about Russian activity. At the same time, questions arise about how many similar attacks have not been made public? How many disruptions reported as accidents and malfunctions were in fact serious cyber attacks of foreign actors?

Each report on the technicalities of attacks is an important source of information for cyber security analysts and each report of intelligence services broadens the horizon of knowledge of security researchers, allowing for a better understanding of the threat landscape not only in one country, but also a whole region. It is imperative for Europe to build a unified and coherent stance on cyber treats for the common good.

Bibliography

Fukuyama F., *Zaufanie. Kapitał społeczny a droga do dobrobytu* (Eng. Trust. The social virtues and the creation of prosperity), Warszawa 1997.

Jordan T., Taylor P., *Hactivism and Cyberwars. Rebels with a cause?*, London 2004.

Kose J., *Cyber Warfare: An Era of Nation-State Actors and Global Corporate Espionage*, "ISSA Journal" 2021, vol. 19, no. 4, pp. 12–15.

Kuehl D.T., *Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age*, "International Law Studies" 2022, vol. 76, pp. 35–58.

⁷⁴ The Big Four state actors, i.e. China, Russia, North Korea, Iran, are a group of states identified by cyber security analysts as the biggest sources of cyber threats.

Lin H., Kerr J., *On Cyber-Enabled Information/Influence Warfare and Manipulation*, in: *The Oxford Handbook of Cyber Security*, P. Cornish (ed.), Oxford University Press 2021, pp. 251–272. <https://doi.org/10.1093/oxfordhb/9780198800682.013.15>.

McIntosh T. et al., *Ransomware Reloaded: Re-examining Its Trend, Research and Mitigation in the Era of Data Exfiltration*, “ACM Computing Surveys” 2024, vol. 57, no. 1. <https://doi.org/10.1145/3691340>.

Vičić J., Harknett R., *Identification-imitation-amplification: understanding divisive influence campaigns through cyberspace*, “Intelligence and National Security” 2024, vol. 39, no. 5, pp. 897–914. <https://doi.org/10.1080/02684527.2023.2300933>.

Internet sources

Antoniuk D., *Latvia's cyberspace faces new challenges amid war in Ukraine*, The Record, 28.10.2022, <https://therecord.media/latvias-cyberspace-faces-new-challenges-amid-war-in-ukraine> [accessed: 19.03.2025].

Ataki hakerskie na RP operację rosyjskich służb (Eng. Hacker attacks in the Republic of Poland as an operation of Russian services), Serwis Rzeczypospolitej Polskiej, 20.07.2022, <https://www.gov.pl/web/sluzby-specjalne/ataki-hakerskie-na-rp-operacja-rosyjskich-sluzb> [accessed: 19.03.2025].

Brief summary 2023 Report on the Protection of the Constitution (Facts and Trends), Bundesamt für Verfassungsschutz, <https://www.verfassungsschutz.de/SharedDocs/publikationen/EN/reports-on-the-protection-of-the-constitution/2024-06-brief-summary-2023-report-on-the-protection-of-the-constitution.pdf> [accessed: 19.03.2025].

China's propaganda offensive, 17.02.2023, <https://www.gov.pl/web/special-services/Chinas-propaganda-offensive> [accessed: 19.03.2025].

Cordesman A.H., *China's Emergence as a Superpower*, Center for Strategic & International Studies, 15.08.2023, <https://www.csis.org/analysis/chinas-emergence-superpower> [accessed: 19.03.2025].

Countering hybrid threats, NATO, 7.05.2024, https://www.nato.int/cps/en/natohq/topics_156338.htm [accessed: 19.03.2025].

Cyber attacks against European energy & utility companies, EnergiCERT, September 2022, <https://sektorcert.dk/wp-content/uploads/2022/09/Attacks-against-European-energy-and-utility-companies-2020-09-05-v3.pdf> [accessed: 8.04.2025].

Cyber attacks traced to Russian military intelligence agency, Federal Ministry of the Interior and Community, 3.05.2024, <https://www.bmi.bund.de/SharedDocs/kurz-meldungen/EN/2024/05/schutzmassnahmen-cyberangriffe-en.html> [accessed: 19.03.2025].

Cybercrime, European Commission, 31.10.2024, https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en [accessed: 19.03.2025].

Cybersecurity of Critical Sectors – Energy, ENISA, <https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/energy> [accessed: 8.04.2025].

Fake PAP report looks like cyberattack, says gov't official, Polska Agencja Prasowa, 31.05.2024, <https://www.pap.pl/en/news/fake-pap-report-looks-cyberattack-says-govt-official> [accessed: 19.03.2025].

Frequently asked questions on hybrid threats, Hybrid CoE, <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/> [accessed: 19.03.2025].

Greenberg A., *A Brief History of Russian Hackers' Evolving False Flags*, Wired, 21.10.2019, <https://www.wired.com/story/russian-hackers-false-flags-iran-fancy-bear/> [accessed: 19.03.2025].

Heightened security situation in Germany, Federal Ministry of the Interior and Community, https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/ukrain/security_meldung.html [accessed: 19.03.2025].

Intelligence Outlook 2024, Danish Defence Intelligence Service, 22.01.2025, https://www.fe-ddis.dk/en/produkter/Risk_assessment/riskassessment/Intelligenceoutlook2024/ [accessed: 19.03.2025].

Jones S.G., *Russia's Shadow War Against the West*, Center for Strategic & International Studies, 18.03.2025, <https://www.csis.org/analysis/russias-shadow-war-against-west> [accessed: 19.03.2025].

Latvia mulls tightening security after recent TV propaganda hacks, LSM+, 20.05.2024, <https://eng.lsm.lv/article/society/crime/20.05.2024-latvia-mulls-tightening-security-after-recent-tv-propaganda-hacks.a554618/> [accessed: 19.03.2025].

Lithuania supports the EU declaration condemning Ghostwriter malicious cyber activities and calls to use more political tools, Ministry of National Defence of the Republic of Lithuania, 23.09.2021, <https://kam.lt/en/lithuania-supports-the-eu-declaration-condemning-ghostwriter-malicious-cyber-activities-and-calls-to-use-more-political-tools/> [accessed: 8.04.2025].

Mandiant Intelligence, *GhostWriter Update: Cyber Espionage Group UNC1151 Likely Conducts GhostWriter Influence Activity*, Mandiant, 28.04.2021, https://services.google.com/fh/files/misc/ghostwriter_update_report.pdf [accessed: 19.03.2025].

Mandiant Intelligence, *Hacktivists Collaborate with GRU-sponsored APT28*, Mandiant, 23.09.2022, <https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions> [accessed: 19.03.2025].

Microsoft Digital Defense Report 2024, *The foundations and new frontiers of cybersecurity*, <https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024> [accessed: 19.03.2025].

Multiple Foreign Nationals Charged in Connection with Trickbot Malware and Conti Ransomware Conspiracies, U.S. Department of Justice, 7.09.2023, <https://www.justice.gov/archives/opa/pr/multiple-foreign-nationals-charged-connection-trickbot-malware-and-conti-ransomware> [accessed: 19.03.2025].

Raud M., *China and Cyber: Attitudes, Strategies, Organization*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn 2016, https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf [accessed: 19.03.2025].

Roncone G. et al., *APT44: Unearthing Sandworm*, Mandiant, 17.04.2024, <https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf> [accessed: 19.03.2025].

Russian cyberattacks, Serwis Rzeczypospolitej Polskiej, 30.12.2022, <https://www.gov.pl/web/special-services/russian-cyberattacks> [accessed: 19.03.2025].

Russian National Charged with Ransomware Attacks Against Critical Infrastructure, U.S. Department of Justice, 16.05.2023, <https://www.justice.gov/archives/opa/pr/russian-national-charged-ransomware-attacks-against-critical-infrastructure> [accessed: 19.03.2025].

Sancho D., *Understanding Hacktivists. The Overlap of Ideology and Cybercrime*, Trend Micro, 4.02.2025, <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/understanding-hacktivists-the-overlap-of-ideology-and-cybercrime> [accessed: 19.03.2025].

Sejm uznał Rosję za państwo wspierające terroryzm (Eng. The Sejm recognised Russia as a state supporting terrorism), Sejm of the Republic of Poland, 14.12.2022, <https://www.sejm.gov.pl/sejm9.nsf/komunikat.xsp?documentId=4774505381CECC10C1258918007022FA> [accessed: 8.04.2025].

Thales Cyber Threat Intelligence, *From Ukraine to the whole of Europe: cyber conflict reaches a turning point*, Thales, 29.03.2023, https://www.thalesgroup.com/en/world-wide/security/press_release/ukraine-whole-europecyber-conflict-reaches-turning-point [accessed: 8.04.2025].

The attack against Danish, critical infrastructure, SektorCERT, November 2023, <https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf> [accessed: 19.03.2025].

What is data exfiltration?, IBM, <https://www.ibm.com/think/topics/data-exfiltration> [accessed: 19.03.2025].

Wolert R., *RaaS group profile Hunters International*, CERT Orange, 28.10.2024, https://cert.orange.pl/wp-content/uploads/2024/11/CERTOPL_CTI_Hunters_International_en.pdf [accessed: 19.03.2025].

Other documents

2024 Annual Report, Republic of Latvia Constitution Protection Bureau, https://www.sab.gov.lv/files/uploads/2025/02/SAB-gada-parskats_2024_ENG.pdf [accessed: 19.03.2025].

Annual Report on the activities of Latvian State Security Service (VDD) in 2022, <https://vdd.gov.lv/uploads/materials/33/en/annual-report-2022.pdf> [accessed: 19.03.2025].

Annual Report on the activities of Latvian State Security Service (VDD) in 2023, <https://vdd.gov.lv/uploads/materials/37/en/annual-report-2023.pdf> [accessed: 19.03.2025].

Annual report on the activities of Latvian State Security Service (VDD) in 2024, <https://vdd.gov.lv/uploads/materials/40/en/annual-report-2024.pdf> [accessed: 19.03.2025].

Annual review 2022–2023, Estonian Internal Security Service, https://kapo.ee/sites/default/files/content_page_attachments/Annual%20Review%202022-23_0.pdf [accessed: 19.03.2025].

Annual review 2023–2024, Estonian Internal Security Service, https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2023-2024.pdf [accessed: 19.03.2025].

China's Military Strategy, Ministry of National Defence of the People's Republic of China, 23.06.2021, <http://eng.mod.gov.cn/xb/Publications/WhitePapers/4887928.html> [accessed: 19.03.2025].

Cyber Security in Estonia 2023, Republic of Estonia Information System Authority, <https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf> [accessed: 19.03.2025].

Cyber security in Estonia 2025, Republic of Estonia Information System Authority, <https://www.ria.ee/en/cyber-security-estonia-2025> [accessed: 19.03.2025].

Latvian Cybersecurity and CERT.LV Technical Activities Annual Report 2023, 26.07.2024, https://cert.lv/uploads/eng/Annual_Report_CERT-LV_2023.pdf [accessed: 19.03.2025].

National Threat Assessment 2023, <https://kam.lt/wp-content/uploads/2023/03/Assessment-of-Threats-to-National-Security-2022-published-2023.pdf> [accessed: 19.03.2025].

National Threat Assessment 2024, <https://www.vsd.lt/wp-content/uploads/2024/03/GR-2024-02-15-EN-1.pdf> [accessed: 19.03.2025].

Report on the state of Poland's cybersecurity in 2023, CSIRT GOV, <https://csirt.gov.pl/download/3/220/RaportostaniebezpieczenstwacyberprzestrzeniRPw2023.pdf> [accessed: 19.03.2025].

Report on the state of Poland's cybersecurity in 2024, in press.

Sprawozdanie Pełnomocnika Rządu do spraw Cyberbezpieczeństwa za 2023 rok (Eng. Report of the Government Plenipotentiary for Cyber Security for 2023), Ministerstwo Cyfryzacji (Eng. Ministry of Digital Affairs), 11.04.2024, <https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni> [accessed: 8.04.2025].

Threat assessment: the cyber Threat against Denmark 2024, Centre for Cyber Security, September 2024, <https://www.cfcs.dk/link/472c3cc8872446e59fa59eaf0f7ad945.aspx> [accessed: 19.03.2025].

Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response, Brussels, 6.04.2016, JOIN(2016) 18 final, <https://eur-lex.europa.eu/legal-content/PL/TEXT/PDF/?uri=CELEX:52016JC0018> [accessed: 19.03.2025].

Monika Stodolnik

Internal Security Agency officer.

Contact: monika.stodolnik@abw.gov.pl

Results of the survey on the perception of terrorist and sabotage threats among the experts of the EU Protective Security Advisors

KAROLINA WOJTASIK

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

 <https://orcid.org/0000-0002-1215-5005>

DAMIAN SZLACHTER

Internal Security Agency

 <https://orcid.org/0000-0003-2763-9325>

Abstract

This article presents the results of a survey on the perception of terrorist and sabotage threats by experts participating in the European Commission's (DG Home) initiative EU Protective Security Advisors (EU PSA). The survey was conducted in February 2025 on a sample of 50 individuals representing EU PSA, EU institutions, and strategic project partners. The questionnaire covered several key aspects of terrorist and sabotage threats, including the types of potential targets, attack methods, and expected developments in hybrid threats. Respondents were also asked to assess which critical infrastructure systems require the highest priority in resilience-building efforts, as well as which counter-terrorism measures should be prioritised at the EU level. Additionally, the survey explored factors that could improve the security of protected facilities and identified the most likely perpetrators of attacks on EU critical infrastructure. The survey results provide valuable insights for shaping counter-terrorism and counter-sabotage policies at

the EU level. The authors emphasise the necessity of standardising physical security measures and developing educational initiatives to build a security culture.

Keywords

critical infrastructure, public space, terrorism, sabotage, resilience, soft targets, hard targets, European Commission, DG HOME, EU PSA, critical infrastructure protection, hybrid threats, hybrid warfare

Introduction

The protection of public spaces and critical infrastructure (CI) is a fundamental duty of the Member States of the European Union. In response to increasing terrorist threats, the EU undertakes initiatives to support Member States in their efforts to protect citizens and CI. One such initiative is the EU Protective Security Advisors (EU PSA)¹, created by the Directorate-General for Migration and Home Affairs (DG HOME) of the European Commission.

The EU PSA initiative has its roots in the EU's work on the protection of public spaces, which began in 2012. The impetus for these efforts was the expert support provided in Poland during the UEFA Euro 2012 European Football Championship. The positive experiences from this event led to further invitations to support security at high-level political events and large public gatherings. A significant milestone in the development of the EU's public space protection policy was the adoption of an action plan in October 2017 dedicated to these issues. As part of its implementation, the EU developed a threat vulnerability assessment tool. This ultimately led to the creation of a group of specialists and the establishment of the EU PSA programme. The EU PSA expert group consists of approx. 130 specialists from the European Commission and EU Member States. These experts have professional experience in public space protection and specialised knowledge in various security fields. Implementation of the EU PSA

¹ *EU Protective Security Advisors (EU PSA)*, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/eu-protective-security-advisors-eu-psa_en [accessed: 26.02.2025].

initiative into the official EU anti-terrorism acquis took place in December 2020, with the publication of the EU Counter-Terrorism Agenda.

The EU PSA programme aims to provide support to EU's Member States upon request. The activities carried out under this initiative include:

- raising awareness of vulnerabilities in public spaces and CI by providing a common security assessment system,
- sharing best practices and encouraging knowledge exchange to eliminate identified security weaknesses,
- providing guidance to Member States on organising mass events and protecting high-risk sites,
- building a network of experts by organising international training sessions and initiatives that contribute to developing a shared security culture in the EU.

The EU PSA programme covers the protection of public spaces and CI, including:

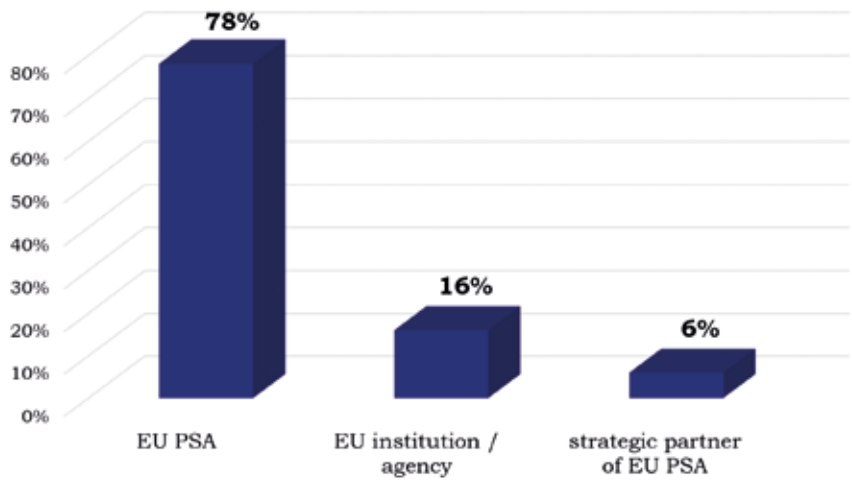
- places of worship and religious institutions,
- cultural events, such as large music festivals,
- VIP events, such as EU summits,
- large infrastructure facilities not included in CI,
- airports, seaports, energy sector facilities and other facilities included in CI.

Given the growing recognition of the EU PSA programme among Member State authorities and the unstable geopolitical situation, interest in its activities is expected to increase. Member States have expressed their intention to invite EU PSA experts to assess national CI facilities, particularly in the context of the EU Directive on the resilience of critical entities. The EU PSA programme is a key EU initiative supporting Member States in protecting public spaces and CI against terrorist threats. By raising awareness, sharing best practices, and providing expert support, EU PSA contributes to improving the security of citizens and infrastructure across the EU. This was the rationale behind the article's authors' decision to conduct a survey on terrorist and sabotage threat perceptions among the EU PSA community. It consists of EU PSA members, representatives of the EU institutions and agencies working with the EU PSA and the initiative's strategic partner.

Results of the survey

The survey was conducted in February 2025, using a standardised questionnaire consisting of 8 questions². It was anonymous in nature. Fifty people took part in the survey³. Respondents represented: the EU PSA (78%), the EU institutions and agencies supporting the above-mentioned initiative (16%) and the EU PSA project’s strategic partner (6%). The division of respondents is shown in Chart 1.

Chart 1. Division of respondents according to the environment they represent.



Question 1 of the survey was: *What objects are terrorists/saboteurs interested in when planning their activities in the European Union?*

Respondents were asked to rank their answers in order from 1st to 10th place, with 1st place indicating the object in which terrorists/saboteurs are most interested, 10th – the least⁴. Respondents were given the following facilities: buildings of state and EU offices, CI facilities, military bases, symbolic tourist landmarks, sport and entertainment facilities, places

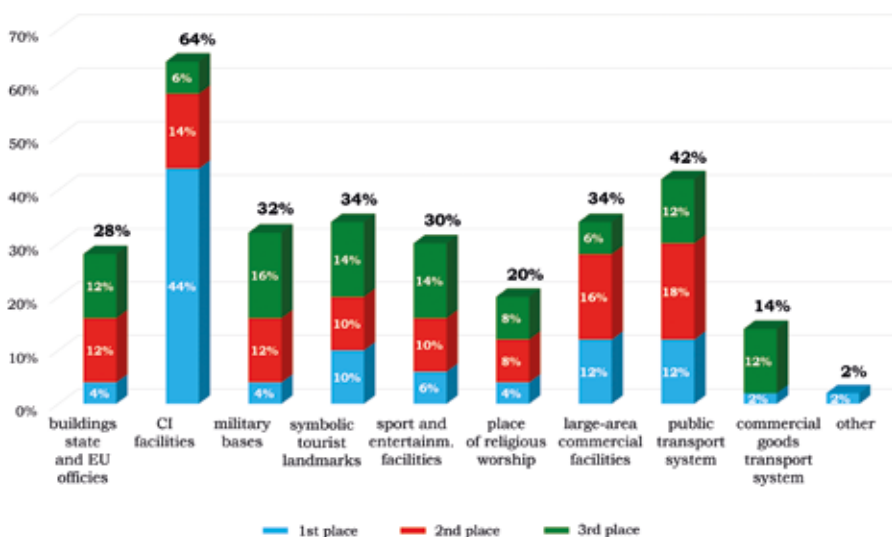
² Attachment: template of the research questionnaire.
³ This represents approx. 40% of the number of EU PSA members.
⁴ For questions where respondents were asked to rank their answers, the results are presented only for positions 1 to 3. Therefore, the data in the charts displaying these results do not sum up to 100%.

of religious worship, large-area commercial facilities, public transport system, commercial goods transport system and others.

Within the group of facilities that respondents singled out for 1st place, CI facilities (44%), large-area commercial facilities and the public transport system (both 12% each) as well as symbolic tourist landmarks (10%) were most frequently indicated. There is therefore a marked difference in the frequency of indications for CI and subsequent facilities. Among the facilities to which survey participants assigned 2nd place, the public transport system (18%), large-area commercial facilities (16%) and critical infrastructure facilities (14%) were most frequently indicated. Among the facilities that respondents ranked 3, the most common response was military bases (16%). The results for subsequent facilities were the same – symbolic tourist landmarks as well as sport and entertainment facilities were indicated by 14% of the respondents. In the case of the objects that the respondents indicated in 2nd and 3rd place, therefore, no clear predominance of one of them could be established.

The results from places 1st–3rd for the individual responses were added up and it was checked which facilities were most frequently indicated by respondents within the top three. The data obtained shows that these are: CI facilities (64%), public transport system (42%) and ex aequo symbolic tourist landmarks and large-area commercial facilities (34% each). Detailed results are shown in Chart 2.

Chart 2. Facilities of interest to terrorists/saboteurs planning operations in the EU.

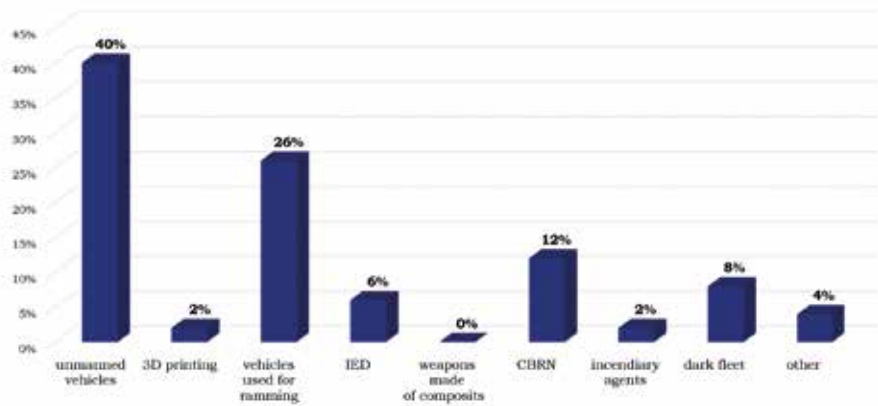


Question 2 of the survey was: *What methods of attack and sabotage can be the greatest challenge for law enforcement authorities and institutions which ensure the security of people and facilities?*

Respondents were able to select one answer from the following categories: unmanned vehicles (air, land, water), 3D printing, vehicles used for ramming the target, improvised explosive devices (IED), weapons made of composites, CBRN, incendiary agents, so called *shadow fleet/dark fleet*, others.

The largest number of respondents (40%) indicated unmanned vehicles (air, land, water). In 2nd place, respondents indicated vehicles used for ramming (26%), followed by CBRN (12%). All results are shown in Chart 3.

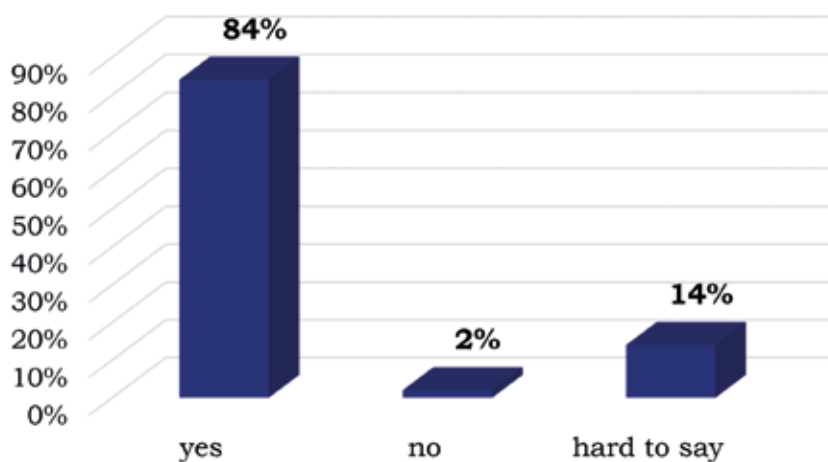
Chart 3. Methods of attack and sabotage that are likely to pose the greatest challenge to law enforcement and institutions providing security for people and facilities.



Question 3 of the survey was: *Should we expect, in a 3-year perspective, the use of terrorist/sabotage activity as part of hybrid threats undertaken on the territory of the EU by a foreign state?*

Respondents could choose one answer from the following options: yes, no, or hard to say. A total of 84% of respondents answered affirmatively, 14% did not take a clear stance, and only 2% provided a negative response. The results are presented in Chart 4.

Chart 4. Could terrorist/sabotage activities be used as a tool of hybrid operations in the EU within the next 3 years?



Question 4 of the survey was: *Which facilities, in a 3-year perspective, will be characterised by the highest level of terrorist/sabotage attack threat in the EU?*

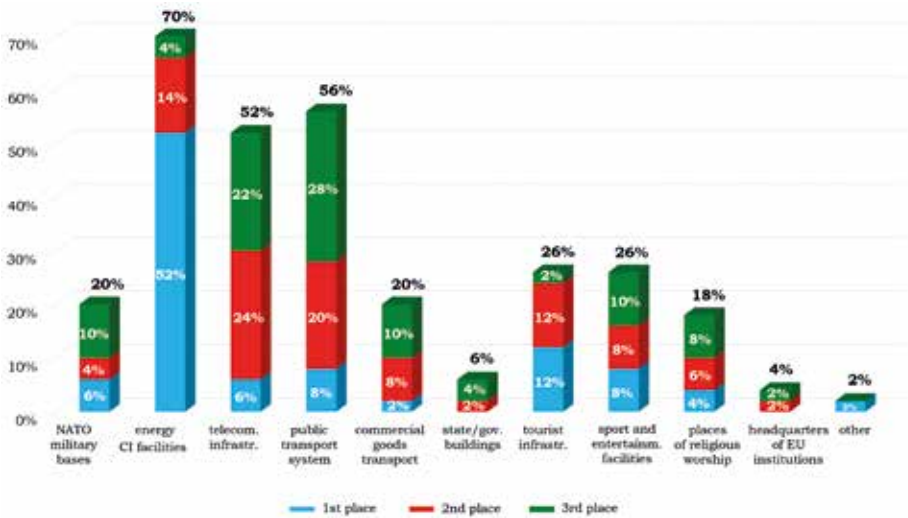
Respondents were asked to rank the provided options from 1st to 11th, with 1st indicating the facility facing the highest level of terrorist/sabotage threat and 11th – the lowest. The following facilities were listed: NATO military bases, energy CI facilities, telecommunications infrastructure, public transport system, commercial goods transport system, government offices, tourist infrastructure, sport and entertainment facilities, places of religious worship, headquarters of EU institutions and agencies, and others.

Among the facilities that respondents ranked in 1st place, the most frequently indicated were energy CI facilities (52%), tourist infrastructure (12%), and sport and entertainment facilities (8%). It is important to highlight the significant dominance of CI, as the next facilities in the ranking received considerably fewer votes. For the facilities ranked in 2nd place, the most commonly selected were: telecommunications infrastructure (24%), public transport system (20%), and energy CI facilities (14%). Among the facilities ranked in 3rd place, the most frequent responses were: public transport system (28%), telecommunications infrastructure (22%), and NATO military bases, commercial goods transport system, and sport and entertainment facilities (each receiving 10%). Therefore, in the case

of 2nd and 3rd place, the phenomenon of dominance of one type of object did not occur.

The results from rankings 1st–3rd were summed for each response to determine which facilities were most frequently placed in the top three by respondents. The data indicate that these are: energy CI facilities (70%), public transport system (56%), and telecommunications infrastructure (52%). Detailed results are presented in Chart 5.

Chart 5. Facilities expected to face the highest level of terrorist/sabotage threats.



Question 5 of the survey was: *Which critical infrastructure systems, in the 3-year perspective, should be treated as a priority in terms of building their resistance to hybrid threats?*

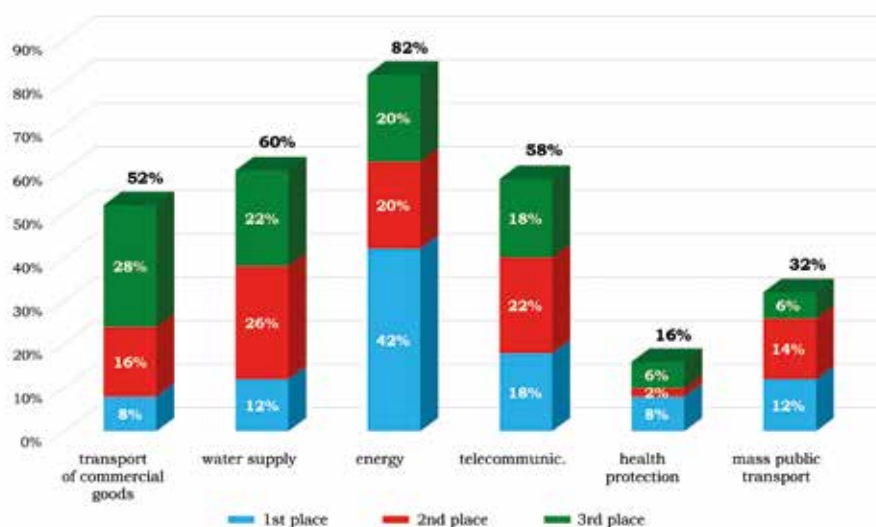
Respondents were tasked with ranking the given systems from 1st to 7th, where 1st place indicated the CI system with highest priority and 7th place. The respondents were provided with the following systems: transport of commercial goods (communication routes and transshipment hubs), water supply, energy, telecommunications, health protection, mass public transport, others.

Among the CI systems ranked 1 by respondents, the energy system was the most frequently selected (42%), followed by telecommunications system (18%) and both the water supply system and mass public transport system (each with 12%). For the 2nd and 3rd places, the responses were more

evenly distributed. The systems most frequently ranked 2 were: water supply system (26%), telecommunications system (22%), and energy (20%). Among the systems ranked 3, the most common choices were: transport of commercial goods (28%), water supply (22%), and energy (20%).

The results from positions 1st–3rd for each response were summed up to determine which CI systems were most frequently ranked in the top three by respondents. The data show that these are the energy system (82%), the water supply system (60%), and the telecommunications system (58%). Detailed results are presented in Chart 6 (the answer “others” was not given).

Chart 6. Priority CI systems in building resistance to hybrid threats.



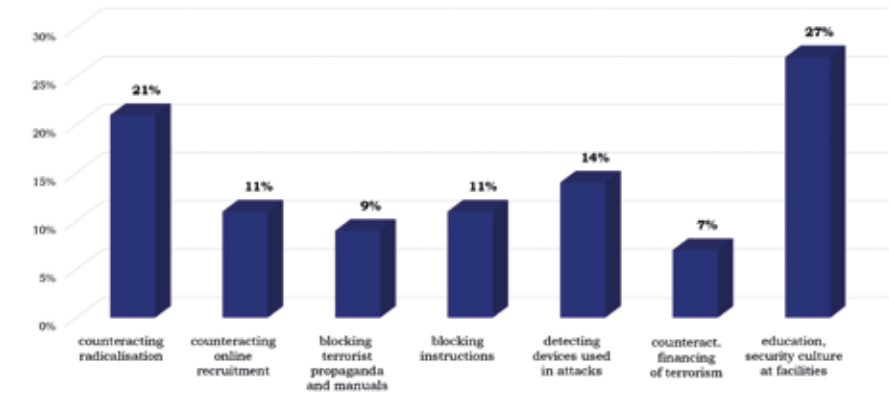
Question 6 of the survey was: *Which of the areas of counteracting terrorist activities require priority treatment on the EU level today?*

Respondents could choose one answer from the following options: counteracting radicalisation leading to terrorist activities, counteracting online recruitment for terrorist/sabotage actions, detecting and blocking terrorist propaganda, detecting and blocking terrorist/sabotage manuals published online, developing technologies for detecting devices used in terrorist attacks, counteracting the financing of terrorism, educational

initiatives concerning security culture for facilities vulnerable to terrorist/sabotage attacks, and other.

Responses to this question were divided. The largest share of respondents indicated educational initiatives and building a security culture in facilities that could be potential targets of terrorist or sabotage activities (27%). The 2nd most selected option was preventing radicalisation leading to terrorist activities (21%), followed by developing technologies for detecting devices used in terrorist attacks (14%). All results are presented in Chart 7.

Chart 7. Priorities in counteracting terrorism.

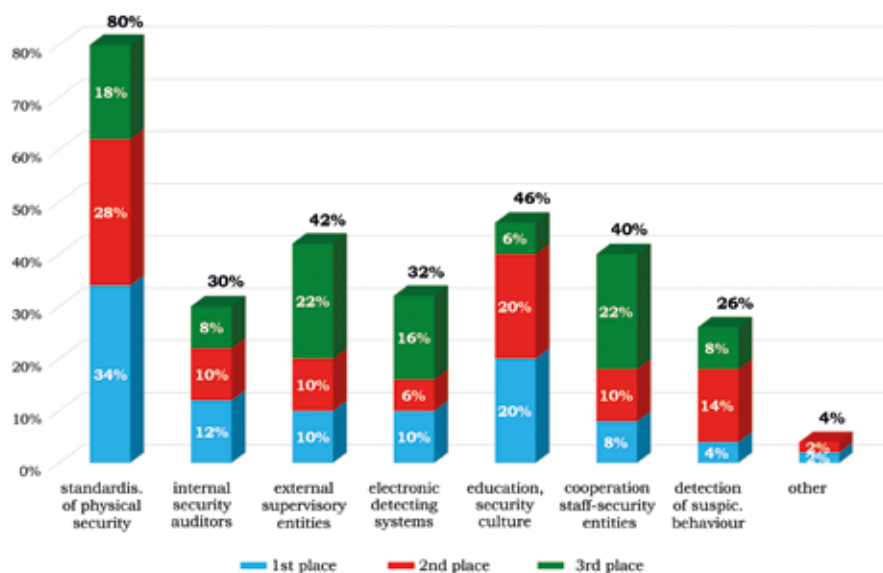


Question 7 of the survey was: *What can increase the level of resistance to terrorist attacks and sabotage activities in protected facilities?*

The respondents were tasked with ranking the given actions from 1st to 8th place, where 1st place represented the most important activities and 8th place – the least important. The provided options were: standardisation of physical security (also security personnel procedures), tasks performed by internal security auditors, external security control tests by external supervisory entities (such as: EU institutions, state control authorities), development of intelligent electronic systems for detecting security incidents, development of anti-terrorist prevention initiatives as part of the security culture of the facility (education for security), improving cooperation between CI entities and entities responsible for security, detection of suspicious behaviour carried out by trained security personnel, and others.

Among the actions ranked 1 by respondents, the most frequently selected were: standardisation of physical security (34%), development of anti-terrorist prevention initiatives (20%), and tasks performed by internal security auditors (12%). The difference between the next-ranked actions – security control tests conducted by external supervisors (such as: EU institutions, state control authorities) and development of intelligent electronic systems for detecting security incidents – was minimal, with both receiving 10% of the respondents. Among the actions ranked 2, the most frequently chosen were: standardisation of physical security (28%), development of initiatives related to terrorism prevention (20%), and detection of suspicious behaviour by trained security personnel (14%). For actions ranked 3, the most common responses were security control tests conducted by external supervisory entities and improving cooperation between CI entities and security organisations (both at 22%). The next most frequently selected action was standardisation of physical security (18%). The results from positions 1st–3rd for each response were summed up to determine which actions were most frequently ranked in the top three by respondents. The data show that these are: standardisation of physical security (80%), development of anti-terrorist prevention initiatives (46%), security control tests conducted by external entities (42%). Detailed results are presented in Chart 8.

Chart 8. Projects aimed at increasing the resilience of protected objects.

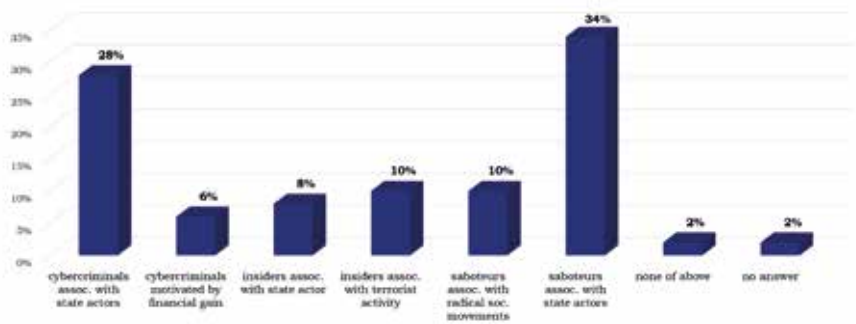


Question 8 of the questionnaire concerned the perpetrators of attacks on CI.

Respondents could choose one answer from the following options: cybercriminals associated with a state actor, cybercriminals who are motivated only by the desire for financial gain, activities of the so-called insiders associated with a state actor, activities of the so-called insiders associated with terrorist activity, saboteurs associated with the activity of radical social movements, saboteurs associated with a state actor, none of the above.

The largest share of respondents (34%) indicated saboteurs affiliated with a state actor. The 2nd most selected option was state-associated cybercriminals (28%), followed by insiders linked to terrorist activities and saboteurs associated with radical social movements (both at 10%). All results are presented in Chart 9.

Chart 9. Potential perpetrators of attacks on CI facilities.



Summary of survey results

Experts involved in the EU PSA indicated CI facilities (64% of all responses), public transport system (42%) and symbolic tourist landmarks as well as large-area commercial facilities (both 34%) as the most potential targets for a terrorist/sabotage attack within the EU. It should be emphasised that when constructing the survey questionnaire, the authors of the article focused primarily on the purpose of the attack rather than the method. The conclusions drawn from the survey research do not differ from other data. The latest TE-SAT report provides data on terrorist attacks that

took place in 2023. In 45 out of 120 cases, more detailed information was provided, which shows that in 1/3 of them the target was CI⁵.

As for the methods of attack and sabotage that today pose the greatest challenge for the law enforcement agencies, authorities and institutions responsible for ensuring the physical security, respondents indicated unmanned vehicles (air, land, water) – 40% of responses. Recent years have been a time of intensive development of drones, they are increasingly used to commit crimes. It is worth emphasising that underwater drones may pose a serious threat to maritime CI in the future. In TE-SAT report it was also indicated, that individuals from a variety of ideological backgrounds who may pose a threat are actively seeking online training material and instruction manuals that contain attack tactics and information on how to make weapons, drones, bombs or chemical weapons⁶. In second place, respondents indicated vehicles used for ramming (26%), which is probably related to recent events (attack in Magdeburg in December 2024 and in Mannheim in March 2025)⁷. A total of 84% of respondents believe that in the 3-year perspective, terrorist and sabotage activities will be used as part of hybrid threat scenarios undertaken on EU territory by a foreign country.

As for the types of facilities that in the next 3 years in the EU will be characterised by the highest level of threat of a terrorist/sabotage attack, the respondents most often selected: energy CI facilities (70%), the public transport system (56%) and the telecommunications infrastructure (52%). Attacks, mostly cyberattacks, on energy and telecommunications

⁵ *European Union Terrorism Situation and Trend Report (EU TE-SAT) 2024*, <https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf>, p. 12 [accessed: 26.02.2025].

⁶ *Ibid.*, p. 7.

⁷ Attack in Magdeburg – on 20 December 2024, a driver drove into a crowd at a Christmas market, killing 6 people and injuring over 100. The perpetrator was a 50-year-old doctor of Saudi origin who had been living in Germany since 2006. Attack in Mannheim – on 3 March 2025, a 40-year-old German citizen drove a car into a group of people on a pedestrian street, killing 2 and injuring several others. The perpetrator was arrested by the police shortly after the incident.

infrastructure have been on the rise⁸, becoming a staple of hybrid warfare. Attacks on public transport are a common tactic used by jihadist groups⁹.

Majority of the respondents indicated that the CI system, that should be treated as a priority in terms of building resistance to hybrid threats in the 3-year perspective, is the energy system (82%). The efficient functioning of the energy infrastructure is a condition for the functioning of modern society. The effects of an attack on the energy system are multi-level. Therefore, the energy system is considered the most vulnerable to attacks.

In the case of the question about the area of counteracting terrorist activity, which today requires priority treatment by the EU, the respondents' opinions were divided, the majority of respondents (27%), however, indicated to educational activities and building a security culture at facilities that could be targeted. This will be a significant challenge for CI operators and the institutions supervising them.

The projects most likely to increase the level of resistance to terrorist attacks in protected facilities are: standardisation of physical security (80%), development of anti-terrorist prevention initiatives as part of the security culture of the facility (46%) and use of security control tests by external entities (42%).

Most respondents believe that the perpetrators of current attacks on CI systems are saboteurs linked to a state actor (34%) or cybercriminals linked to a state actor (28%).

The results of the survey clearly indicate the threat of terrorist and sabotage attacks, targeting in particular CI, mass public transport

⁸ B. Nieróbca, *Energetyka w sieci cyberzagrożeń* (Eng. Energy sector in the Network of Cyber Threats), EY, 14.08.2024, https://www.ey.com/pl_pl/insights/cybersecurity/energetyka-w-siecicyberzagrozen [accessed: 26.02.2025]; *Raport: cyberbezpieczeństwo w energetyce* (Eng. Report: Cybersecurity in the Energy Sector), https://www.inteligentnaenergetyka.pl/enereka/wp-content/uploads/2024/02/Raport_Cyberbezpiecze%C5%84stwo-w-energetyce_ARTSMART_29.02.2024.pdf [accessed: 26.02.2025]; K. Pohoska, *Cyberprzestępczość – prognozy na 2025 rok* (Eng. Cybercrime – Predictions for 2025), Stołeczny Magazyn Policyjny, 3.03.2025, <https://magazyn-ksp.policja.gov.pl/mag/technologie/137761,Cyberprzestepczosc-prognozy-na-2025-rok.html> [accessed: 20.03.2025].

⁹ *The Tactics and Targets of Domestic Terrorists*, Center for Strategic and International Studies, 30.07.2020, <https://www.csis.org/analysis/tactics-and-targets-domestic-terrorists> [accessed: 26.02.2025]; B.M. Jenkins, B.R. Butterworth, K.S. Shrum, *Terrorist Attacks On Public Bus Transportation: A Preliminary Empirical Analysis*, <https://transweb.sjsu.edu/research/Terrorist-Attacks-Public--Bus-Transportation-Preliminary-Empirical-Analysis> [accessed: 26.02.2025].

system and telecommunications system. Respondents, representing the community of security experts, stressed the need to prioritise activities aimed at strengthening the resilience of facilities of key importance for the functioning of the state and society.

Based on the analysis of the survey results, it can be noted that in the coming years it will be necessary to further develop measures to prevent attacks, including: standardisation of physical protection, implementation of modern threat detection technologies and educational initiatives in the field of terrorist prevention. In addition, cooperation between CI operators and security authorities will be important to better coordinate actions and respond to incidents more effectively.

The study also confirms that terrorist and sabotage threats are increasingly part of hybrid strategies by state and non-state actors. In the face of rapidly changing security environment, EU Member States should strive to implement comprehensive protection strategies, taking into account both physical and cybersecurity aspects.

Bibliography

EU Protective Security Advisors (EU PSA), https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/eu-protective-security-advisors-eu-psa_en [accessed: 26.02.2025].

Jenkins B.M., Butterworth B.R., Shrum, K.S., *Terrorist Attacks On Public Bus Transportation: A Preliminary Empirical Analysis*, <https://transweb.sjsu.edu/research/Terrorist-Attacks-Public-Bus-Transportation-Preliminary-Empirical-Analysis> [accessed: 26.02.2025].

Nieróbca B., *Energetyka w sieci cyberzagrożeń* (Eng. Energy sector in the Network of Cyber Threats), EY, 14.08.2024, https://www.ey.com/pl_pl/insights/cybersecurity/energetyka-w-siecicyberzagrozen [accessed: 26.02.2025].

Pohoska K., *Cyberprzestępczość – prognozy na 2025 rok* (Eng. Cybercrime – Predictions for 2025), Stołeczny Magazyn Policyjny, 3.03.2025, <https://magazyn-ksp.policja.gov.pl/mag/technologie/137761,Cyberprzestepczosc-prognozy-na-2025-rok.html> [accessed: 20.03.2025].

The Tactics and Targets of Domestic Terrorists, Center for Strategic and International Studies, 30.07.2020, <https://www.csis.org/analysis/tactics-and-targets-domestic-terrorists> [accessed: 26.02.2025].

Other documents

European Union Terrorism Situation and Trend Report (EU TE-SAT) 2024, <https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf> [accessed: 26.02.2025].

Raport: cyberbezpieczeństwo w energetyce (Eng. Report: Cybersecurity in the Energy Sector), https://www.inteligentnaenergetyka.pl/enereka/wp-content/uploads/2024/02/Raport_Cyberbezpiecze%C5%84stwo-w-energetyce_ARTSMART_29.02.2024.pdf [accessed: 26.02.2025].

Attachment

Template of the research questionnaire used in February 2025

The EU PSA SURVEY 2025

This survey is conducted among representatives of EU Member States and the European Commission participating in the project of building resistance to terrorist attacks in public spaces – EU PSA (Protective Security Advisors) at DG HOME European Commission. The survey is anonymous, and the survey results will be collected in a way that makes it impossible to identify the person completing it.

The purpose of the survey is to obtain respondents' opinions on the most probable ways of development of terrorist/sabotage threats in the EU.

The results of the survey will be published in a special issue of the scientific journal "Terrorism – Studies, Analyses, Prevention" which will be devoted to terrorist and hybrid threats to critical infrastructure. The special issue will be published in May 2025 and will be distributed at meetings of the EU Council working parties: TWP, PROCIV-CER as part of the Polish Presidency of the EU Council.

In our opinion, the results of this survey could contribute to the discussion about the development of antiterrorist and counter-sabotage initiatives, including risk prevention and awareness-raising at the EU level and in the Member States.

The beginning of the research survey

1. What objects are terrorists/saboteurs interested in when planning their activities in the European Union?

When you use your mobile phone to fill in the questionnaire: drag the option and drop it to arrange the order.

When you use your computer to fill in the questionnaire: number the options using the button on the left or drag the option and drop it to arrange the order.

- buildings of state offices and EU institutions,
 - critical infrastructure facilities,
 - military bases,
 - symbolic tourist landmarks,
 - sports and entertainment facilities,
 - places of religious worship,
 - large-area commercial facilities,
 - public transport system,
 - commercial goods transport system,
 - others.
2. What methods of attack and sabotage can be the greatest challenge for law enforcement authorities and institutions which ensure the security of people and facilities?

Choose one answer:

- unmanned vehicles (air, land, water),
- 3D printing,
- vehicles used for ramming the target,
- improvised explosive devices,
- weapons made of composites,
- CBRN,
- incendiary agents,
- so called shadow fleet/dark fleet,
- others.

3. Should we expect, in a 3-year perspective, the use of terrorist/sabotage activity as part of hybrid threats undertaken on the territory of the EU by a foreign state?

Choose one answer:

- yes,
- no,
- hard to say.

4. Which facilities, in the 3-year perspective, will be characterised by the highest level of terrorist/sabotage attack threat in the EU?

When you use your mobile phone to fill in the questionnaire: drag the option and drop it to arrange the order.

When you use your computer to fill in the questionnaire: number the options using the button on the left or drag the option and drop it to arrange the order.

- NATO military bases,
- critical energy infrastructure facilities,
- telecommunications infrastructure,
- public transport system,
- commercial goods transport system,
- government offices,
- tourist infrastructure,
- sport and entertainment facilities,
- places of religious worship,
- headquarters of EU institutions and agencies,
- others.

5. Which critical infrastructure systems, in the 3-year perspective, should be treated as a priority in terms of building their resistance to hybrid threats?

When you use your mobile phone to fill in the questionnaire: drag the option and drop it to arrange the order.

When you use your computer to fill in the questionnaire: number the options using the button on the left or drag the option and drop it to arrange the order.

- transport of commercial goods (communication routes and transshipment hubs),
- water supply,
- energy,
- telecommunications,
- health protection,
- mass public transport,
- others.

6. Which of the areas of counteracting terrorist activities require priority treatment on the EU level today?

Choose one answer:

- counteracting radicalisation leading to terrorist activities,
- counteracting online recruitment for terrorist/sabotage activities,
- detecting and blocking terrorist propaganda,
- detecting and blocking terrorist/sabotage manuals published on-line,
- detection technologies for devices used to carry out terrorist attacks,
- counteracting the financing of terrorism,
- educational initiatives concerning security culture for facilities vulnerable to terrorist/sabotage attacks,
- others.

7. What can increase the level of resistance to terrorist attacks and sabotage activities in protected facilities?

When you use your mobile phone to fill in the questionnaire: drag the option and drop it to arrange the order.

When you use your computer to fill in the questionnaire: number the options using the button on the left or drag the option and drop it to arrange the order.

- standardisation of physical security (also security personnel procedures),
- tasks performed by internal security auditors,
- the use of security control tests by external supervisory entities (such as: EU institutions, state inspection authorities),

- development of intelligent electronic systems for detecting security incidents,
- development of anti-terrorist prevention initiatives as part of the security culture of the facility (education for security),
- improving cooperation between CI entities and entities responsible for security,
- detection of suspicious behaviour carried out by trained security personnel,
- others.

8. Attacks on critical infrastructure are currently carried out by:

Choose one answer:

- cybercriminals associated with a state actor,
- cybercriminals who are motivated only by the desire for financial gain,
- activities of the so-called insiders associated with a state actor,
- activities of the so-called insiders associated with terrorist activity,
- saboteurs associated with the activity of radical social movements,
- saboteurs associated with a state actor,
- none of the above.

COMPLETE THE INFORMATION

Choose one answer:

- EU Member State representative,
- representative of the EU institution or agency,
- representative of a country that is a strategic partner of the EU PSA.

The end of the research survey

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

Damian Szlachter, PhD

Editor-in-chief of the ISA (ABW) scientific journal “Terrorism – Studies, Analyses, Prevention”. Member of the steering committee of the EU Protective Security Advisors group. National expert at the European Commission’s Directorate-General for Migration and Home Affairs in the Policy Group on Public Spaces Protection. National auditor for quality control in civil aviation security (of the Civil Aviation Authority). Participant in the work of more than a dozen 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. Member of the team to investigate the challenges of engineering security of critical infrastructure buildings at the General Office of Construction Supervision. Author of nearly 40 scientific articles and co-author of several books and specialist reports on internal security.

Contact: d.szlachter@abw.gov.pl



EXPERT MATERIALS

The role of standardisation and conformity assessment in ensuring security and building resilience of critical infrastructure to hybrid threats

Adam Tatarowski

The Technical Property Protection Development Institute TECHOM

 <https://orcid.org/0009-0007-5503-6819>

Introduction

The approach to understanding security has been dynamically evolving in Poland since the 1989 transition period. It was only then that the needs of the market and the state administration for security and safety services began to take shape. Until the enactment of the *Act of 22 August 1997 on the protection of persons and property*, which is still in force today, the security and safety sector in Poland functioned without dedicated statutory regulations. It developed on a market basis and was subject to both positive and negative bottom-up influences – intra-market, as well as top-down influences – from the state administration and from the outside.

An obstacle to the creation of a coherent and transparent legal system that would provide the security and safety sector with a stable foundation

was the lack of a clear vision and decision-making of state regulatory institutions at the level of creating detailed requirements. The development of coherent solutions was further complicated by the conflicting interests of various influential groups whose activities had adverse impact on legislative process. The potential of the standardisation *acquis* was not realised. Successive legislative initiatives, although necessary and often inspired by European solutions, did not create a coherent structure – they left significant gaps, hampering the growth of competitiveness, transparency and quality of services and organisational as well as technical solutions provided. An example of a much-needed normative act, which, however, did not take into account systemic solutions concerning quality assurance and compliance, was the *Regulation of the Council of Ministers of 24 June 2003 on facilities of particular importance for the security and defence of the state and their special protection*, specifying the issues of protection of these facilities in a situation of a threat to state security.

Alongside the legal ‘mainstream’ focused on the Act on the protection of persons and property, the need to create a unified approach to protecting and ensuring security for critical infrastructure (CI) began to be recognised in Poland. Although it was understood that certain systems and facilities – such as power grids, telecommunications infrastructure or transport systems – were fundamental to the functioning of the state, for a long time there was a lack of regulations that comprehensively addressed their protection. The Polish legal system lacked the very concept of CI. As Tomasz Szewczyk and Maciej Pyznar point out¹, the Polish state administration encountered this concept mainly in the framework of international cooperation, within the structures of NATO and the European Union. The regulations created at that time focused on selected sectors or referred to the protection of individual objects, but did not create a uniform security system. As a result, activities undertaken in the field of CI protection were dispersed, and issues of administrative responsibility for its security were not clearly defined.

For many countries, the US approach at the turn of the 20th century became a model in trying to sort out this issue. A turning point in this regard was the entry into force of Presidential Decision Directive 63 of 22 May

¹ T. Szewczyk, M. Pyznar, *Ochrona infrastruktury krytycznej a zagrożenia asymetryczne* (Eng. Critical infrastructure protection and asymmetric threats), „Przegląd Bezpieczeństwa Wewnętrznego” 2010, no. 2, p. 54.

1998², which introduced the concept of *critical infrastructure* as the systems necessary to ensure the basic functioning of the economy and government. According to it, these are systems, physical and digital, the destruction or disruption of which could lead to serious socio-economic and political consequences. The novelty was the recognition that protecting these systems required a coordinated effort by both government and the private sector, which owned most of the assets deemed critical to the functioning of the state. The directive required individual US federal agencies to develop plans for the protection of CI and to establish mechanisms for information sharing between public and private sectors.

Influenced by the American standards, work on the creation of a unified framework for the protection of CI has started in the EU. In Poland, the initial activities of the state administration in this area focused on selected sectors. There was still a lack of an approach that would integrate the various aspects of infrastructure security in the same management model.

A turning point in the shaping of the Polish CI protection system was the enactment of the *Act of 26 April 2007 on crisis management*, which in Article 3(2) for the first time introduced a definition of CI into the Polish legal order, understood as:

(...) systems and their functionally related facilities, including buildings, equipment, installations, services that are critical to the security of the state and its citizens and to the smooth functioning of public administration bodies, as well as institutions and businesses.

CI includes systems:

- a) energy, energy raw materials and fuels supply,
- b) communications,
- c) ICT networks,
- d) finance,
- e) food supply,
- f) water supply,
- g) health care,
- h) transport,
- i) rescue services,
- j) ensuring continuity of public administration,

² *Presidential Decision Directive/Nsc-63*, The White House, 22.05.1998, <https://irp.fas.org/offdocs/pdd/pdd-63.htm> [accessed: 5.03.2025].

- k) production, storage, warehousing and use of chemical and radioactive substances, including pipelines for hazardous substances.

The Act also defined the concept of CI protection, i.e. (...) *actions aimed at ensuring the functionality, continuity and integrity of critical infrastructure in order to prevent threats, risks or vulnerabilities, and to limit and neutralise their effects, as well as the rapid restoration of this infrastructure in the events of failures, attacks or other events that disrupt its proper functioning* (Article 3(3)).

In addition, the Act created the Government Centre for Security (RCB), a supra-ministerial structure, reporting directly to the Prime Minister, responsible for planning and programming activities in the field of CI protection (Article 10(1)).

Developing of European regulations and their impact on Polish legislation

At EU level, a breakthrough occurred with the entry into force of *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*. Under this directive, CI is defined more generally as (...) *an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions* (Article 2). The Directive introduced and further defined the 'object-oriented' approach to the protection of CI, as it focused on the protection of facilities and installations the damage of which could have serious consequences for the functioning of the state. The Polish implementation of the Directive took into account this model more comprehensively. This was due to an awareness of the growing interdependence between public administration and the private sector and the dynamic changes in the global security environment. The solutions adopted in Poland not only strengthened the protection of facilities, but also laid the foundation for overcoming future challenges in maintaining continuity of services.

The Act on crisis management required the RCB to create and systematically update the National Critical Infrastructure Protection Program (NPOIK), which defined in detail the process of identifying CI and protecting it. It added an annex entitled *Standards for ensuring the smooth functioning of critical infrastructure – good practices and recommendations*.

As a whole, it laid the foundation for the standardisation of CI protection, based on the so-called six-pack concerning:

- 1) physical protection,
- 2) technical protection,
- 3) personal protection,
- 4) information and communication security,
- 5) legal protection,
- 6) aspects related to recovery plans.

The Act and the set of documents that complement it, including the NPOIK, have evolved over the years. During this time, a rather complex process for identifying CI has been established, consisting of three stages. The first establishes which system a potential CI site belongs to. Next, it is checked whether the site performs the function referred to in the statutory definition. Finally, it is analysed whether the possible consequences of the destruction or discontinuation of the potential CI will meet the cross-cutting criteria relating to the social impact of the destruction or discontinuation of the facility, equipment, installation or service. These criteria include:

- casualties,
- financial implications,
- the need to evacuate,
- loss of service,
- recovery time,
- international effect,
- uniqueness (in terms of the impossibility of replacing and reconstructing the damaged facility, equipment or installation)³.

Since the implementation of the NIS Directive⁴ in Poland by the *Act of 5 July 2018 on the national cybersecurity system*, parallel to the ‘object-based’ approach, there is a ‘service-oriented’ system for selecting operators of essential services, i.e. those that are important to maintaining critical

³ See in more detail: A. Tatarowski, *Building resilience of critical infrastructure in the light of asymmetric threats and terrorism. Legislative trends in the Polish implementation of the CER Directive with particular reference to aspects of standardisation and certification of organisational and technical solutions*, “Terrorism – Studies, Analyses, Prevention” 2024, no. 5, pp. 391–409, <https://doi.org/10.4467/27204383TER.24.014.19402>.

⁴ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security for network and information systems across the Union.

social or economic activity and are mentioned in the list of important services issued under the Act. In turn, a decision recognising an entity as essential service operator is issued when:

- entity provides essential service,
- provision of this service depends on information systems,
- incident would have a significant effect resulting in disruption to the provision of the essential service by that operator⁵.

The coexistence of ‘object-oriented’ and ‘service-oriented’ approaches has led to inconsistencies in the overall CI management system. The ‘object-oriented’ model, based on classic infrastructure protection, did not encompass a system perspective and did not take into account important interdependencies between sectors. In contrast, the ‘service’ approach, developed within the framework of cyber security regulation, was limited in scope. This dualism was particularly evident in EU policies, in which two separate directives were in place: the Council Directive 2008/114/EC, mandating the protection of physical infrastructure, and the NIS Directive, focusing on ensuring the resilience of information systems and digital services.

Towards a new model for critical infrastructure protection

Over the years, there has been a growing understanding that the CI protection model, focused solely on physical facilities, is insufficient. It has been influenced both by the scientific analysis carried out and by events that have revealed significant gaps in the existing risk management system. Experiences from terrorist attacks (e.g. 11 September 2001), the COVID-19 pandemic, cyber attacks and natural disasters (e.g. Hurricane Sandy)⁶ have highlighted that it is not so much the protection of individual facilities, systems or installations that is important, but ensuring the uninterrupted operation of services that are vital for the stability of the state and the security of citizens. A disruption of one service, e.g. fuel supply, can have a knock-on effect and lead to transport problems, food shortages or limited availability of medical care. An interesting concept that has influenced the development of this approach in Poland and the EU is the ‘Six Ways

⁵ See in more detail: A. Tatarowski, *Building resilience of critical infrastructure...*, p. 394.

⁶ M. Wiśniewski, K. Szwarz, W. Skomra, *Continuity of Essential Services as an Emerging Challenge for Societal Resilience*, “IEEE Access” 2023, vol. 11, pp. 44615. <https://doi.org/10.1109/ACCESS.2023.3271751>.

to Die'⁷. Its most important premise is that the goal of protection should not be the 'physical' CI itself, but ensuring uninterrupted access to services on which the security of citizens depends at 3 levels: individual, social and state. It identifies 6 fundamental threats that can lead to individual death and social and economic destabilisation: lack of food, lack of water, disease, injury, extreme cold and extreme heat.

The US was the first to widely implement a 'service' model of protection. The US Cybersecurity and Infrastructure Security Agency (CISA) produced the *National Critical Functions Set* (NCFS)⁸, which defines critical functions as activities and processes necessary to maintain national security, economic stability and the basic functioning of society. The document distinguishes 4 main areas in which 55 critical functions have been identified:

- 1) connect – ensuring the smooth functioning of telecommunications systems, the internet, data transmission and postal services,
- 2) distribute – maintaining the continuous movement of people, goods and resources essential to the functioning of the economy and infrastructure,
- 3) supply – securing key resources including energy, potable water, industrial raw materials and production systems,
- 4) manage – protection of public administration systems (e.g. important in the US election protection), financial stability, capital markets and crisis management.

Thus, in the NCFS model, it is not individual facilities or systems that are protected, but services, which implies, for example, the need to implement complex solutions to ensure fault tolerance and resource redundancy.

A consequence of the actions described above was the adoption (14 December 2022) in the EU of the groundbreaking CER Directive on the resilience of critical entities⁹. The CER Directive ends the division between 'facility' and 'service' approaches. It formalises a modern approach to infrastructure protection, with a focus on ensuring

⁷ M. Bennett, V. Gupta, *Dealing in Security Understanding Vital Services and How They Keep You Safe*, 2010, http://resiliencemaps.org/files/Dealing_in_Security.July2010.en.pdf [accessed: 22.06.2022].

⁸ *National Critical Functions Set*, CISA, <https://www.cisa.gov/national-critical-functions-set> [accessed: 24.06.2022].

⁹ *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*.

the resilience of those providing essential services to society. It introduces a comprehensive risk management model at a system level, taking into account interdependencies between sectors and with a focus on the resilience of entire supply chains. Significantly, the NIS 2 Directive¹⁰ on cyber security was adopted at the same time. The two directives are compatible with each other and, as such, should be implemented in the legal systems of individual Member States.

The groundbreaking role of the CER Directive – the Polish perspective

For Poland, the implementation of the CER Directive is not only another legislative requirement, but also a natural step towards adopting a systemic approach to national security. The experience of CI protection, gained both at the national level and in international cooperation (e.g. within NATO and the EU), is valuable in this regard. Poland has been developing its own methods of risk management and CI protection for years, including the implementation of NPOIK, building cyber security, introducing mechanisms to protect the population¹¹ and civil defence or enhancing military capabilities¹². These are solid foundations on which the new architecture of critical entities resilience and the services they provide will be based.

Moreover, Poland has a unique competence to shape the standards of CI protection at the European level. Many years of experience in bringing together the public and private sectors in the area of security, taking into account awareness of new threats and their continuous evolution as well as understanding of the broad socio-technological context, make Poland an important participant in the process of improving resilience mechanisms. The Polish Presidency of the Council of the EU, which runs from 1 January to 30 June 2025, focuses on strengthening 7 dimensions of European security. These are:

- defence and security,
- protection of people and borders,
- resistance to foreign interference and disinformation,

¹⁰ 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).

¹¹ Act of 5 December 2024 on civil protection and civil defence.

¹² Act of 11 March 2022 on the defence of the Homeland.

- ensuring security and freedom of business,
- energy transition,
- competitive and resilient agriculture,
- health security¹³.

In Poland, the RCB is responsible for all substantive work related to the implementation of the CER Directive into the Act on crisis management.

A new phase in critical infrastructure protection for the European Union and its Member States

The implementation of the CER Directive is one of the biggest legislative and operational challenges for EU Member States. It is a milestone in building European resilience to systemic threats – from cyber attacks through infrastructure sabotage to energy, health and other crises involving unknown risks. It is also a clear signal that Member States recognise the need to evolve the CI protection model in a unified, modern direction. The new regulation will allow for more effective countering of current and future threats and enhance resilience at both national and EU-wide levels. The European Commission has set October 2024 as the deadline for its full implementation, but by March 2025, only 9 countries had completed the process of transposing the regulations into national law, while the others – including Poland – are working intensively to finalise them. It is worth mentioning that the concerted efforts of Member States in implementing the CER Directive represent a shift to a new level of integration and solidarity in terms of security. This gives the EU a more resilient, flexible and coordinated security system to respond effectively to the dynamically changing threats of the 21st century.

Ideas behind the Polish implementation of the CER Directive

Conceptual work on the Polish law implementing the CER Directive began within the RCB in the first half of 2023¹⁴, the results of which were discussed

¹³ *The Polish presidency of the Council of the EU*, European Council, Council of the European Union, <https://www.consilium.europa.eu/pl/council-eu/presidency-council-eu/> [accessed: 28.02.2025].

¹⁴ Draft act amending the Act on crisis management and certain other acts, <https://legislacja.rcl.gov.pl/docs/2/12386961/13069020/13069024/dokument711601.pdf> [accessed: 6.04.2025].

at the 10th National Forum for Critical Infrastructure Protection (2023), and aspects of standardisation and conformity assessment were presented by the article's author¹⁵. In Q1 2024, formal decisions were taken on the RCB's commitment as executor of the draft amendment. In March 2024, the first draft was circulated for consultation, and its innovative solutions won the appreciation of both the state administration and market stakeholders, especially CI operators. At the current stage of legislative work (March 2025), most of the solutions have already been refined. The law itself is waiting to enter the parliament.

One of the most important areas in the implementation of the CER Directive is to ensure consistent and effective standardisation and conformity assessment mechanisms that will enable a uniform approach to the resilience requirements of critical entities and business continuity of essential services.

The purpose of this article is to contribute to the discussion conducted under the Polish Presidency of the Council of the EU, particularly in the context of the work of the Working Party on Civil Protection – Critical Entities Resilience (PROCIV-CER), the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats and the Working Party on Terrorism (TWP). The paper shows how the European regulations have been translated in the draft Polish law into concrete solutions for risk assessment, standardisation of organisational and technical solutions and services provided to critical entities, as well as conformity assessment (auditing and certification). The author of this paper, as a co-author of the concept of standardisation system in the Polish implementation of the CER, presented the genesis and justification of the adopted solutions and their practical consequences for CI operators and public administration.

National Critical Infrastructure Protection Program as a foundation for ensuring the security of critical infrastructure and a source of inspiration

In the National Critical Infrastructure Protection Program (NPOIK), which has evolved over the years, the CI protection regime is based on

¹⁵ A. Tatarowski, *Standaryzacja i certyfikacja rozwiązań wynikających z Dyrektywy CER* (Eng. Standardisation and certification of solutions under the CER Directive), *10th National Forum for Critical Infrastructure Protection*, Warszawa 2023, <https://www.gov.pl/web/rcb/x-krajowe-forum-ochrony-infrastruktury-krytycznej-za-nami> [accessed: 28.02.2025].

the aforementioned so-called six-pack. For the sake of order, the current (2023)¹⁶ description of these assumptions will be quoted, which include:

- 1) ensuring physical security – a set of organisational and technical measures aimed at minimising the risk of disrupting CI operations as a result of actions taken by persons who have attempted to enter or have entered CI in an unauthorised manner;
- 2) ensuring technical security – a set of organisational and technical measures aimed at minimising the risk of disrupting CI operations as a result of disturbances to ongoing technological processes;
- 3) ensuring personal security – a set of organisational and technical measures aimed at minimising the risk of disrupting CI operations as a result of actions taken by persons who have authorised access to CI;
- 4) ensuring information and communication security – a set of organisational and technical actions aimed at minimising the risk of disrupting CI operations as a result of unauthorised interference with control apparatus and information and communication systems and networks;
- 5) ensuring legal security – a set of organisational and technical actions aimed at minimising the risk of disrupting CI operations as a result of legal actions of external entities;
- 6) business continuity and restoration plans, understood as a set of organisational and technical actions leading to the maintenance and restoration of functions performed by CI¹⁷.

This regime corresponds to Article 13 of the CER Directive, concerning resilience measures to be put in place by critical entities. It is worth recalling the first paragraph of this provision:

- 1) Member States shall ensure that critical entities take appropriate and proportionate technical, security and organisational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:

¹⁶ *National Critical Infrastructure Protection Program*, Government Centre for Security, 2023. The text of the programme is available at: <https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej>.

¹⁷ *National PCritical Infrastructure Protection Program*, pp. 30–31.

- a) prevent incidents from occurring, duly considering disaster risk reduction and climate adaptation measures;
- b) ensure adequate physical protection of their premises and critical infrastructure, duly considering, for example, fencing, barriers, perimeter monitoring tools and routines, detection equipment and access controls;
- c) respond to, resist and mitigate the consequences of incidents, duly considering the implementation of risk and crisis management procedures and protocols and alert routines;
- d) recover from incidents, duly considering business continuity measures and the identification of alternative supply chains, in order to resume the provision of the essential service;
- e) ensure adequate employee security management, duly considering measures such as setting out categories of personnel who exercise critical functions, establishing access rights to premises, critical infrastructure and sensitive information, setting up procedures for background checks in accordance with Article 14 and designating the categories of persons who are required to undergo such background checks, and laying down appropriate training requirements and qualifications;
- f) raise awareness about the measures referred to in points (a) to (e) among relevant personnel, duly considering training courses, information materials and exercises.

For the purposes of the first subparagraph, point (e), Member States shall ensure that critical entities take into account the personnel of external service providers when setting out categories of personnel who exercise critical functions.

The above provisions were the starting point for work on a new framework for standardisation in ensuring security and building resilience of CI in Poland. The CER Directive, under Article 3, is based on the principle of minimum harmonisation, meaning that it only sets out a basic regulatory framework and leaves it to the Member States to introduce solutions adapted to national realities, including more stringent ones. Such an approach provides flexibility and the ability to take into account specific national circumstances and allows for a CI protection regime that corresponds to actual threats and operational requirements. The Polish implementation takes advantage of this margin of freedom and designs solutions that not only fully implement the EU guidelines, but also integrate national experiences and lessons learned from existing CI security regulations and practices.

Normalisation as a basis for implementing optimal standardisation

Standardisation, understood as an activity aimed at achieving an optimum degree of order in a particular area by setting out provisions intended to be universally reusable¹⁸, is fundamental to the smooth functioning of societies and economies, and its importance dates back to the beginning of civilisation¹⁹.

Standards organise reality and ensure predictability and coordination of activities on a global scale. From energy production and distribution systems, through transport and telecommunications, to cyber security and risk management, standardisation underpins interoperability and stability. In an era of dynamic technological change and increasing security threats, its role is even more important, as it provides a coherent framework for the functioning of countries, economies and institutions in an increasingly complex world.

Today, standardisation provides important support to EU legislation. A landmark moment in the anchoring of standardisation in the EU socio-economic ecosystem was the adoption and publication on 7 May 1985 of the EC Council Resolution²⁰ on a new approach to technical harmonisation and standards. According to Teresa Idzikowska and Krzysztof Banaszek, (...) *giving a particularly high priority to the standards and technical specifications that are the product of standardisation activity, in the creation of rules for the free movement of goods and the elimination of barriers to trade, meant a radical change in the status of standards at both*

¹⁸ J. Łunarski, *Normalizacja i standaryzacja* (Eng. Normalisation and standardisation), Rzeszów 2014, Oficyna Wydawnicza Politechniki Rzeszowskiej.

¹⁹ Already in the ancient world, efforts to standardise units of measurement, systems of weights, building and organisational standards were important not only for the development of trade and administration, but also for ensuring the effectiveness of military operations and public safety. Ancient Egypt used precise measurements in the construction of monumental structures such as the pyramids, and in Mesopotamia, uniform systems of weights allowed the economy and exchange of goods to function efficiently. Ancient Rome, on the other hand, developed a system of standardisation in a way that shaped social and military organisation for many centuries. The standardisation of armament and equipment for legionaries provided an operational advantage on the battlefield and increased the efficiency of military logistics. The Romans also applied standards in construction – standardised methods of building roads, aqueducts and military forts enabled the efficient expansion and maintenance of the empire. The Romans also developed the first standardised forms of municipal guards and sewerage systems that minimised health risks in cities.

²⁰ *Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards.*

*national and international level*²¹. The model adopted was that legislation should specify only the basic safety and quality requirements, while detailed technical guidelines should be developed within the framework of voluntary European standards. In practice, this allowed the requirements to be flexibly adapted to changing market and technological conditions, while harmonising the most important standards across the European Community.

Since 1 January 2004, the Polish Committee for Standardisation (PKN) has been a member of the European standardisation organisations: European Committee for Standardisation and European Committee for Electrotechnical Standardisation. These are private, non-profit associations, operating under Belgian law. They are not EC bodies. The European standardisation system is distinguished by the fact that European Standards are agreed by all Member States, and each Member State, regardless of its involvement in their development, is obliged to assess and implement them. As a result, there is one European Standard in Europe, available only as an implementation of national standards²². For the record, it should be mentioned that a standard has many converging definitions²³. Quite comprehensible is the one included in the *Act of 12 September 2002 on standardisation*, according to which it is (...) *a document adopted by consensus and approved by an authorised organisational unit, establishing – for general and repeated use – principles, guidelines or characteristics relating to various activities or their results, and aimed at achieving an optimal degree of order in a specified scope* (Article 2(4)).

Awareness of the role played by standardisation as an instrument to support risk and security management was reflected in the CER Directive, which allowed Member States to take into account standards applicable to critical entities. In accordance with recital 34 of the Directive (...) *standardisation should remain primarily a market-driven process. However, there may still be situations in which it is appropriate to require compliance with*

²¹ T. Idzikowska, K. Banaszek, *Rola i znaczenie normalizacji w bezpieczeństwie transportu* (Eng. The role and importance of standardisation in transport safety), „Logistyka” 2010, vol. 4.

²² T. Schweitzer, E. Zielińska, *Działalność normalizacyjna* (Eng. Standardisation activity), in: *Normalizacja*, T. Schweitzer (ed.), Warszawa 2013, Polski Komitet Normalizacyjny, pp. 15–18.

²³ *A World Built on Standards: A Textbook for Higher Education*, S.A. Bøgh (ed.), Nordhavn 2015, Danish Standards Foundation.

specific standards. In turn, Article 16 indicates that (...) in order to promote the convergent implementation of this Directive, Member States shall, where useful and without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European and international standards and technical specifications relevant to the security and resilience measures applicable to critical entities.

The proposal for the Polish implementation of the CER Directive fully meets these objectives. It takes into account both the European standardisation acquis and national experience in standardisation of security systems in CI (NPOIK with annexes).

Incorporating standards into legislation – the Polish specificity

The possibility to refer to standards in legislation derives from the aforementioned Act on standardisation. Pursuant to Article 5(4): *Polish Standards may be referred to in legal regulations after they have been published in the Polish language*, and the method of citation taking into account accuracy (dated, undated, general citation) and strength (exclusive or indicative) is defined in PN-EN 45020:2009 *Standardisation and related activities. General vocabulary*. Legislative work to achieve the objectives set by the CER Directive obviously also had to take into account the broadly understood voluntary use of standards, resulting not so much from the Act itself, but from the adopted system of European standardisation. According to the position of PKN, the reference to Polish Standards in a legal provision does not change its voluntary status, unless the legislator wants to change this status, which is only possible by explicitly indicating it in the provisions of another law²⁴. This position was used in the first draft of the implementation, in which the standards were referred to. During the first phase of inter-ministerial agreement, opinion and public consultation, the RCB accepted the argumentation of the Government Centre for Legislation (RCL) that standards, as payable standards, should not be referred to in the Act as mandatory for use. Moreover, despite PKN's clear position on the change of the status of a standard from voluntary to mandatory within the meaning of the act in which it is referenced, the principle of voluntary application of standards could be violated. Therefore, an alternative solution was decided upon – standards

²⁴ *Dobrowolność stosowania norm* (Eng. Voluntary application of standards), Polski Komitet Normalizacyjny, <https://wiedza.pkn.pl/web/wiedza-normalizacyjna/stanowisko-pkn-w-sprawie-dobrowolnosci-pn> [accessed: 28.02.2025].

will be directly referred to not in the Act, but in the implementing acts or in the official lists published in the Bulletin of Public Information (BIP) of the relevant institutions. This approach strikes a balance between ensuring access to standards and respecting the principles of standardisation and regulation. Furthermore, in consultation with the RCL, a construction of the regulations has been developed. It takes into account the existing arrangements while fully complying with the existing regulations on standardisation and the principles of the standardisation system. It was specified that the solutions referred to in the following paragraphs (...) *should meet the requirements set out in the standards, indicated in the implementing act*. This way of writing indicates the need to meet the requirements set out in the standard, but does not impose the standard as a mandatory document to be used.

Mentality and system barriers – the genesis of the problems.

The need for a tough approach to the use of standards

The experience of state regulatory institutions, in particular the RCB, CI operators and the market as a whole (including other ordering parties – investors, service providers, suppliers of various organisational and technical solutions, etc.) clearly shows that the protection of CI in Poland has been limited for years by systemic barriers, the sources of which date back to the beginning of the political transformation. They led to a situation where ensuring adequately high security standards was difficult, and in some cases even impossible.

One of the most important problems became the misinterpretation of the legal regulations governing public procurement (EU and Polish) – the lowest price was the dominant and sometimes the only criterion considered. In many cases, the formulation of requirements concerning the quality of equipment or services encountered difficulties both at the level of the contracting authorities and the controlling institutions. The substantive cells at CI operators, responsible for defining security needs, often formulated requirements corresponding to real threats and using proven standards (e.g. NPOIK) and norms. However, at the next stage, at the formal level, these requirements were reduced by procurement departments (or management boards!) which, citing regulations and unwritten rules to eliminate unnecessary costs, removed additional technical or organisational requirements and left only those explicitly included in the law.

The situation was further complicated by inspection bodies, which often equated requirements that went beyond the absolute legal minimum with a breach of the principles of economy. On more than one occasion, control actions were taken against units that had introduced stricter security requirements. As a result, those responsible for procurement did not formulate high standards for fear of accusations of mismanagement or even corruption. In cases where higher requirements were successfully pushed through, external audits may have found them to be unwarranted expenditure, raising suspicions. This systemic arrangement led to a vicious circle:

- CI operators formulate high requirements for CI security based on standards and good practices,
- procurement cells (or boards) reject these requirements citing the need to reduce costs and avoid potential accusations of mismanagement,
- controlling authorities act in a way that de facto favours the lowest price, ignoring real security needs,
- providers of high quality services, equipment and other solutions cannot compete effectively because they have no other arguments than price,
- providers of low quality services and equipment win contracts by offering solutions of questionable effectiveness and origin.

In this situation, it became necessary to introduce regulations that would make the quality and safety requirements for CI impossible to circumvent. The CER Directive, in Article 16 and Recital 34, clearly indicates that Member States should encourage the use of standards, which in the case of Poland required a firmer approach. The adoption of the minimum harmonisation model has allowed the development of mechanisms to eliminate the possibility of circumventing quality requirements and thus close the systemic gaps that have hindered the application of high security standards for years.

Moreover, the draft implementation of the CER Directive takes into account the provisions of the *Act of 5 August 2010 on the protection of classified information* as the most important for ensuring an adequate level of protection of the documentation produced and the solutions used. In addition, the application of these provisions makes it possible to take advantage of the regulations provided for in Article 12 of the *Act of 11 September 2019 – Public procurement law*, which, in certain cases, allows

for the implementation of orders in a mode other than that provided for in the Act. This solution, resulting from the need to adapt the procedures to the specifics of CI, is part of the concept of raising security standards and shaping requirements for services and organisational and technical solutions.

Standardisation of organisational and technical solutions and requirements for services and persons in the Polish proposal for implementation of the CER Directive

CI security standardisation is a process of systemic unification of requirements for CI protection that draws on both international and European standards, as well as national standards, guidelines or recommendations such as NPOIK. It is a process that draws on standardisation, but also precisely defines requirements, unifies them and adapts them to the specifics of CI, taking into account specific threats and growing sectoral interdependencies. It encompasses the entire ecosystem of stakeholders: CI operators, critical actors, service providers, public administrations, supervisory and control bodies, as well as entities or persons conducting validation (audits and certifications) of the solutions used. The main objectives of standardisation are: to ensure consistent and effective protection measures, reduce risks and build systemic resilience to different types of threats.

This process takes the dynamically changing security challenges into account. It requires a flexible approach to updating and improving security measures. The introduction of uniform standards allows for a more effective risk management system, the elimination of its weaknesses and the strengthening of interoperability between those responsible for the security of CI. Consequently, standardisation provides not only a higher level of protection, but also transparency and predictability in terms of requirements and delivery mechanisms.

CI operators and critical entities

The Polish proposal to implement the CER Directive describes the requirements for CI operators and critical entities. According to the draft law, a CI operator is (...) *the owner or holder of a facility, equipment, installation, network, system and service or functionally interconnected*

facilities, equipment, installations, networks, systems and services on the list of critical infrastructure, while a critical entity (i.e. an entity identified under the CER Directive) is (...) a CI operator included in the list of critical entities, providing at least one essential service, operating in a sector or sub-sector listed in the Annex to the Act and conducting activity on the territory of the Republic of Poland or in maritime areas of the Republic of Poland, referred to in the Act of 21 March 1991 on maritime areas of the Republic of Poland and maritime administration. Critical infrastructure, in turn, is defined as:

- (...) facility, equipment, installation, network, system and service or functionally interconnected facilities, equipment, installations, networks, systems and services necessary for:
- a) the pursuit of important state interests, including ensuring the functioning of public administration bodies,
 - b) ensuring the functioning of enterprises,
 - c) satisfying and maintaining the needs of citizens, including those of a local nature,
 - d) ensuring the provision of essential services.

A critical entity is a CI operator that provides at least 1 essential service and the occurrence of a so-called 'significant incident' could cause a major disruption to its provision. The inclusion in the list of critical entities is based on an analysis of the thresholds of materiality of the disruptive effect, which will be defined in an implementing act of the Council of Ministers. The assessment of the materiality of the disruptive impact shall take into account, among other things: the number of users dependent on the service in question; the interconnectedness between sectors; the impact of the incident on the economy, society, public safety and the environment; the market share of the entity in question; the geographical area affected by the possible incident; and the availability of alternative means of providing that service.

Standardisation of requirements for CI operators.

Statutory requirements and minimum safety standards

The draft implementation of the CER Directive introduces new obligations for CI operators, including a systematic risk analysis and the implementation of appropriate solutions adapted to the results, in line with the so-called NPOIK six-pack.

Legislative work has succeeded in developing an approach that will oblige CI operators to implement the minimum requirements to the extent

indicated. This is a game changer to address the system and operational problems described in the previous chapter, which have so far prevented the implementation of appropriate solutions despite the existence of NPOIK, norms and many other standards. The minimum standards will be set by regulation and will apply to the entire so-called six-pack. They will be developed taking into account recommendations of a specialist nature on the protection of CI, necessary for the implementation of CI security solutions, its location and characteristics and the need to take measures to ensure its security. The author of this article is a co-author of these standards (they are in an approval process). They provide a tool to ensure a consistent and uniform approach to the protection of CI, in line with the requirements set out in the draft Act. This document may have a broad impact on the entire security industry in Poland and Europe and to be a source of knowledge and inspiration not only for CI operators. It is therefore worth describing it in more detail, with a particular focus on physical security, so much emphasised in the CER Directive.

The standards flesh out the concept of CI protection as a process divided into the following stages:

- 1) identification of the scope of activities, the objectives to be achieved in the protection of CI and the addressees of these activities,
- 2) identification of critical resources, functions and identification of the network of relationships (dependencies) with other CI sectors, including entities and bodies,
- 3) identification of roles and responsibilities of participants in the CI protection process,
- 4) risk estimation,
- 5) identification of priorities for action and their prioritisation depending on the results of the risk assessment,
- 6) development and implementation of the CI protection system, including:
 - identification of design criteria and installation of technical security systems in CI facilities,
 - development, application and ongoing updating of CI protection documentation,
- 7) testing (through exercises) and reviewing (through self-assessment and audit or certification) of the CI protection system and measuring progress towards the goal,

- 8) improvement understood as introducing modifications and corrections as a result of tests, reviews, measurements and the use of intelligent solutions, which should include the protected assets, the threats to these assets and their levels of protection against identified threats.

The stages that require special attention and care are the risk assessment and the development and implementation of a CI protection system. This system should apply to all types of identified threats, both natural and intentional and technical, and be prepared to restore the functions performed by the CI as quickly as possible. Accordingly, the measures taken to ensure security are aimed at minimising the risk of disruption to the functioning of CI by:

- reducing the likelihood of a risk occurring,
- reducing vulnerability to risks,
- minimising the impact of the risk.

The standards introduce consolidated definitions of terms relevant to the implementation of all scopes from the so-called six-pack. For example, risk-related terms are defined as follows:

- risk – the likelihood of a hazard occurring with its consequences,
- sources of risk – elements or factors that may lead to the occurrence of risk, may arise from hazards, vulnerabilities, characteristics and type of assets, organisational or technical environment, behaviour, actions or mistakes of individuals,
- risk criteria – a set of principles and benchmarks defining the acceptability of risks, established taking into account the objectives of the organisation, the internal and external context and applicable laws, regulations and standards,
- risk identification – the process of finding, identifying and describing risks, including the identification of resources subject to risk, the identification of their sources and potential consequences,
- risk analysis – the process of determining the level of risk by assessing the likelihood of events arising from risks and their potential consequences, taking into account existing vulnerabilities and safeguards,
- risk assessment – the process of comparing the results of a risk analysis with accepted risk criteria to determine the acceptability of the risk and the need for remedial action,

- risk evaluation – the overall process of identifying, analysing and evaluating risks.

The definitions have been developed taking into account a number of standards from the risk field and the context of their application in the standards being developed²⁵. It is worth recalling that the risk-based approach has been the philosophy for ensuring CI safety in Poland for many years and has been reinforced by the objectives set by the CER Directive. This approach allows CI operators to use a range of solutions, depending on their own risk assessment. For example, technical security systems (i.e. intrusion detection systems, access control systems and CCTV systems) should, once installed, meet the requirements of the Polish Standard relevant to the technical security system in a degree of security appropriate to the risk assessment, with a degree of security no lower than level three being recommended²⁶. The standards describe in great detail the minimum technical parameters that should be used for CI protection equipment.

The draft law also includes a provision that forces operators to request certificates from service providers (when developing and concluding contracts to ensure implementation of the so-called ‘six-pack’). In the absence of these, other documents specific to particular solutions, confirming relevant competences of service providers and authorisations necessary for implementation of these solutions, are also taken into account, in accordance with EU mutual recognition rules. In terms of physical security, in the context of the design, installation and maintenance of technical security systems, this can be expected to be a certificate of conformity with the PN-EN 16763 *Services for fire safety systems and security systems*.

²⁵ PN-ISO 31000:2018-08 *Risk management – Guidelines*; PN-ISO 31000:2012 *Risk management – Principles and Guidelines*; PN-EN ISO/IEC 27005:2025-01 *Information security, cybersecurity and privacy protection – Guidelines on managing information security risk*; PN-ISO/IEC 27005:2014-01 *Information technology – Security techniques – Information security risk management*; PN-EN IEC 31010:2020-01 *Risk management – Risk assessment techniques*; PKN-ISO Guide 73:2012 *Risk management – Vocabulary*.

²⁶ Pursuant to: PN-EN 50131-1 *Alarm systems – Intrusion and hold-up systems – Part 1: System requirements*; PN-EN 60839-11-1 *Alarm and electronic security systems – Part 11-1: Electronic access control systems – System and components requirements*; PN-EN 62676-1-1 *Video surveillance systems for use in security applications – Part 1-1: System requirements – General*.

The original idea of standardising requirements for critical entities – security management system, auditing and certification

The original idea behind the implementation of Article 13 of the CER Directive was to establish a security management system for critical entities, which would complementarily cover aspects relating to risk assessment, quality of service, the organisational-technical solutions used and the assessment of their compliance, as well as those relating, for example, to the implementation of other requirements under sectoral EU legislation. The organisational and technical solutions were based on an information security management system compliant with PN-EN ISO/IEC 27001, taking into account the hard requirements for technical security systems, which were to be installed in accordance with PN-EN 50131 and/or PN-EN 60839 and/or PN-EN 62676. The most important element also became the establishment of a business continuity management system compliant with PN-EN ISO 22301 to the extent necessary to maintain the provision of the essential service.

The culmination of this idea was to formalise audits of the security management system of critical entities and to provide for the possibility of using certification as an alternative to audit. This was based on Article 21 of the CER Directive, which allows Member States to specify requirements for assessing the conformity of the organisational and technical arrangements implemented and to oblige critical entities to apply appropriate security measures. In this way, the security management system proposed in the draft implementation was intended to be a coherent, standardised whole and to address both the problems associated with the lack of uniform requirements and the long-standing difficulties in ensuring high quality security at CI.

The audit commitment covered 3 key pillars: the information security management system, the business continuity management system and the technical security systems. Critical entities were able to perform these audits in a flexible manner, adapted to their specific characteristics and organisational structure. The proposed solution allowed audits to be conducted in an integrated manner, then covering all 3 pillars simultaneously, or in a disconnected manner, e.g. by certifying the information security management system, auditing technical safeguards at the same time and conducting a separate business continuity audit. This model allowed for more freedom in the selection of auditors or certification bodies and also gave the possibility to involve internal auditors to a certain extent. More specifically, some of the organisational and

technical arrangements could be subject to an internal audit, carried out by qualified auditors who were employees of the entity, while some could be certified by external certification bodies. The introduction of mandatory audits and the possibility of certification for compliance with Polish Standards was intended to ensure the unification of requirements and their enforcement, as well as to increase transparency and predictability in terms of the control mechanisms applied. What is more, it became a very important element of the system to oblige the critical entity to demand appropriate competences confirmed by a certificate from service providers who are to implement various organisational and technical solutions for the entity. Thus, already the initial stage of the whole process of implementing the security management system has been secured in terms of quality and compliance with the described requirements. The use of such tools in the Polish implementation of the CER Directive was intended not only to facilitate the implementation of effective security management measures by critical entities, but also to break the vicious circle that had been hindering the raising of CI protection standards for years. The concept described in the course of inter-ministerial arrangements, opinions and a number of public consultations has gained recognition and evolved in the right direction.

Standardisation of requirements for critical entities – an evolved concept, included in the current draft implementation of the CER Directive

The critical entity under the draft law will be required to implement an integrated safety management system for the provision of the essential service. A pillar of this system is to conduct a systematic risk assessment taking into account:

- a) threats and associated risks listed in the National Risk Assessment and other risks specific to the essential service provided, including antagonistic threats,
- b) the degree of dependence of other sectors or sub-sectors identified in the Annex to the Act on the essential service provided by the critical entity, and the degree of dependence of that critical entity on essential services provided by other entities in other sectors, including, where applicable, neighbouring Member States of the European Union and third countries,
- c) the identification of alternative supply chains for the re-establishment of the essential service,
- d) risk assessments carried out under separate legislation.

The standardisation of the approach to risk assessment is one of the objectives of the CER Directive, which has been realised in a complementary manner in the Polish proposal. In particular, it is worth citing that the National Risk Assessment, a document for which the RCB will be responsible, will include:

- 1) identified significant threats, in particular:
 - a) constituting a natural disaster or technical failure within the meaning of the provisions of the Act of 18 April 2002 on the state of natural disaster (Journal of Laws of 2017, item 1897),
 - b) hybrid,
 - c) cyber security,
 - d) of a terrorist nature,
 - e) that may cause unavailability of essential services,
 - f) others that may cause significant adverse effects on the population, economy or cultural assets;
- 2) threats not clearly identified that may occur in the future;
- 3) an assessment of the risk of occurrence of identified significant threats.

In carrying out the risk assessment, the critical actor should not only use the 'classic' risk standards mentioned earlier, but also the new technical specification ISO/TS 31050 *Risk management – Guidelines for managing an emerging risk to enhance resilience*, according to which it is important to develop an approach to managing new, hitherto unknown risks, such as those related to the development of artificial intelligence²⁷.

A further element of the integrated security management system for the provision of the essential service will be the implementation by the critical entity of organisational and technical arrangements that are appropriate and proportionate to the results of the risk assessment, in particular:

- a) risk management policies,
- b) physical security, including physical protection of the critical entity's buildings and premises and technical safeguards, including access control,
- c) protection of critical infrastructure necessary for the provision of the essential service, in accordance with the critical infrastructure

²⁷ See in more detail: A. Tatarowski, *Building resilience of critical infrastructure...*

- protection requirements referred to in the provisions of Chapter 7 of the Act,
- d) personal security regarding employees and external suppliers,
 - e) cyber security, in accordance with the requirements for key entities referred to in the provisions of the Act of 5 July 2018 on the national cybersecurity system,
 - f) legal security of the provision of the essential service,
 - g) business continuity and recovery, including maintaining its own back-up systems to ensure security and sustain the operation of the provision of the essential service until it is fully recovered,
 - h) the ability to protect classified information to the extent necessary for the provision of the essential service,
 - i) training and exercises of staff to prepare them for various types of threats and incidents,
 - j) performance of periodic audits and certification.

The above provisions contained in the form of detailed tasks, prepared in accordance with the formal requirements of Article 91(1) of the *Constitution of the Republic of Poland of 2 April 1997*, correspond to the normative assumptions of the information security management system and the business continuity management system, taking into account aspects relating to physical security and technical safeguards, and are therefore elements to meet the requirements set out in the standards to be indicated in the implementing act. The RCB concept envisages the identification of at least the following standards:

- 1) EN ISO/IEC 27001 *Information security, cybersecurity and privacy protection. Information security management systems. Requirements*,
- 2) PN-EN ISO 22301 *Security and resilience. Business continuity management systems. Requirements*,
- 3) PN-EN 50131-1 *Alarm systems. Intrusion and hold-up systems. Part 1: System requirements*,
- 4) PN-EN 62676-1-1 *Video surveillance systems for use in security applications. Part 1-1: System requirements. General*,
- 5) PN-EN 60839-11-1 *Alarm and electronic security systems. Part 11-1: Electronic access control systems. System and components requirements*.

This implementing act will be complemented by the possibility for a critical entity authority (i.e. a sector-specific minister or other authority, such as the Chairman of the Financial Supervision Authority) to develop and make available an additional list of standardisation documents (i.e. standards, technical specifications or other documents setting out principles, guidelines or characteristics). This list, published on the entity's

BIP website, will provide a tool for updating and clarifying the necessary requirements. Consequently, the critical entity will be obliged to take into account both the provisions of the implementing act and the complementary list when implementing the relevant organisational and technical solutions, thus allowing for greater flexibility in the context of a dynamically changing regulatory and technological environment. A good example illustrating the rationale for this is the requirements for external security systems. Currently, the technical specification²⁸ adopted by PKN operates in English, which makes it impossible to refer to it in legal acts. Once it is translated into Polish, which can be expected at the earliest in 2026, it will be easier and much quicker to incorporate it into requirements that will furthermore be targeted at a specific sector or subsector.

As a success may be considered the introduction in the draft act of an obligation for critical entities (translated 1 to 1 of the obligations defined for CI operators) to require from service providers – when developing and concluding contracts ensuring the implementation of organisational and technical solutions – *certificates, taking into account equivalent ones, in accordance with the principles of mutual recognition in the European Union or, in the absence thereof, other documents appropriate for particular solutions, confirming the possession of appropriate competences and authorisations necessary for their implementation*. Conceptually, the list of certificates was to be included in an implementing act, but due to the evolution of organisational and technical solutions and ways of defining competences, it is impossible to publish a list satisfactory to all stakeholders. It was decided that the optimal solution would be for the critical entity authorities to compile and publish such a list on their respective BIPs. In this case, the critical entity authority is obliged – before publishing the list – to consult the relevant sectoral competence council referred to in Article 4c(1)(2) of the *Act of 9 November 2000 on the establishment of the Polish Agency for Enterprise Development*. The same mechanism is applied to CI operators. In the area of physical security, which includes technical security systems, there are various options for confirming competences and qualifications. One example is the certification for compliance with PN-EN 16763, which covers, among other things, the design, installation and maintenance of technical security systems. This standard, published in Polish, has

²⁸ PKN-CLC/TS 50661-1:2024-10 *Alarm systems – External perimeter security systems – Part 1: System requirements*.

been discussed at many conferences (including those on CI organised by the RCB) and industry training courses, and the market (technical security companies) is adapted to certification for compliance with it. Such certification could be indicated in the originally planned implementing act. On the other hand, the standards on private security services for CI²⁹, which offer the possibility of certification, could not be used in the regulation as reference documents for assessing the competence of service providers delivering security services due to the lack of their Polish translation.

These standards are gaining increasing interest within the EU itself as well as in Member States. According to a presentation by the Confederation of European Security Services to the PROCIV-CER group, these standards should play a fundamental role in translating the security principles of the CER Directive into concrete operational requirements. It emphasised that private security service providers are an integral part of the security chain and its effectiveness depends on the quality of each link. In this context, the standards were identified as a key tool to enhance the quality of protection of critical entities and increase their resilience to threats. It was also indicated that the use of these standards is a recommended pathway to ensure high standards in the area of CI protection and supports the objectives of the CER Directive³⁰. Thus, it should be emphasised that Polish legislative solutions are distinguished by pragmatism and flexibility. They enable the smooth implementation of standards as a tool for enhancing the quality of services. The consultation mechanism, taking into account the opinions of the sectoral competence councils, is an important support for the bodies for critical subjects. As a body representing an entire sector (e.g. the Security and Safety of Property and Persons sector), the sector council gathers information from key stakeholders, allowing for the ongoing identification of needs and the adaptation of competence requirements to changing market and regulatory realities.

Thanks to this mechanism, the various standardisation documents can be incorporated into market practice through the publication of reference

²⁹ PN-EN 17483-1:2021-11 *Private security services – Protection of critical infrastructure – Part 1: General requirements*; PN-EN 17483-2:2024-03 *Private security services – Protection of critical infrastructure – Part 2: Airport and aviation security services*; PN-EN 17483-3:2024-03 *Private security services – Protection of critical infrastructure – Part 3: Maritime and port security services*.

³⁰ Confederation of European Security Services, *How standards drive quality and resilience in critical entities security*, 5.02.2025, EU Council PROCIV-CER Working Party.

statements on BIP websites. This solution avoids formal barriers that could inhibit the implementation of organisational and technical solutions by competent service providers and make it difficult to adapt requirements to evolving security challenges. At the same time, the obligation to consult the sector council ensures that the compilations reflect the actual needs of the market, taking into account both operational practice and international standardisation trends. Sectoral competence councils play an important role in shaping qualification and competence standards in specific areas of the economy. They are advisory bodies, brought into existence on the basis of the Act on the establishment of the Polish Agency for Enterprise Development, whose task is to identify competence gaps, recommend educational solutions and support the processes of certification and validation of professional skills. Their particular value is the broad representation of key stakeholders – public administration, educational institutions, industry organisations and enterprises – which allows for effective adaptation of competences to real market needs.

The solutions presented show that the Polish implementation of the CER Directive not only meets its objectives, but also sets out modern legislative solutions, thanks to which the application of standards becomes a real mechanism for improving the quality of services provided to critical entities.

The standardisation of the integrated safety management system for the provision of the essential service is encapsulated by the obligation for critical entities to audit this system, at least once every 3 years, at their own expense. The audit will cover the following:

- 1) information security management;
- 2) business continuity management of the essential service;
- 3) physical security, including physical protection of the critical entity's buildings and premises and technical security, including access control.

The audit would be conducted by:

- 1) a certification body appropriate to the scope,
- 2) at least 2 auditors, 1 of whom has completed lead auditor training, are certified as specified in the implementing act and meet the personal and industrial security requirements for access to information classified 'confidential'.

The general premise of an audit is to assess compliance now and in the past; an audit can have a legal and normative purpose and should fulfil a business need. It is based on 7 principles, listed in the relevant standard³¹:

- 1) integrity as a basis for professionalism,
- 2) honesty in the presentation of results,
- 3) professional due diligence,
- 4) confidentiality,
- 5) independence,
- 6) an evidence-based approach,
- 7) a risk-based approach.

The idea that certification bodies should conduct audits (which, after all, do not have to end in a certificate, just an audit report) had already emerged and was adapted from the Act on the National cybersecurity system. Indeed, certification bodies are institutions whose competences, rules and ethics are defined by regulations stemming from the European conformity assessment system (described in the next chapter). An alternative to a certification body are auditors, who will be competent and give a guarantee of secrecy, confirmed by an appropriate security clearance.

The manner of verification of auditors' qualifications (including their competence) will be specified in the implementing act and will take into account the list of certificates authorising the performance of audits, as well as the scope of expertise and experience of the auditors. In the case of the information security management system and the business continuity management system, it can be expected to refer to the certificates of the lead auditor in a given scope, which are, incidentally, very popular on the market. It can be assumed that for technical security systems, on the other hand, certification of a lead auditor for an information security management system in the specialisation of technical security systems will be required, as there is no standard in the field of security systems that would allow certification of lead auditors. Thus, the certification of a lead auditor for this field draws from the established methodology in the market for auditing information security management systems.

Audits would be allowed to be conducted by internal auditors – employees of the critical entity, who are not subject to a security clearance, but the critical entity may conduct a background check on them. It shall

³¹ PN-EN ISO 19011:2018 *Guidelines for auditing management systems*.

in particular take into account information obtained from criminal records (the National Criminal Register and analogous registers in EU countries). The terms of reference are uniform for auditors who are employees of the critical entity and external auditors, so an internal auditor must have the competence of a lead auditor in order to conduct an audit under the Act.

The audit may be replaced by certification of the organisational and technical arrangements by an approved body. In such a case, the holding of a certificate by the critical entity in the relevant scope shall be considered equivalent to the fulfilment of the audit obligation.

The CER Directive also sets objectives for the control and punishment of critical entities, which are also implemented in the Polish proposal. Critical entities will be subject to fines in cases where:

- do not carry out a systematic risk assessment,
- do not implement organisational and technical solutions,
- do not keep records of the solutions implemented,
- do not follow up on audit recommendations,
- and others.

Inspiration for auditing and certification in the implementation of the CER Directive. Mandatory and voluntary conformity assessment

The intention of the European Community countries was to develop such a model of conformity assessment system, which would harmonise the requirements for products within the common European market. This goal was guided by the principle of mutual recognition, known in the literature as the *Cassis de Dijon*³², according to which goods legally manufactured and marketed in one EU country should be allowed to enter the markets of other Member States³³. In view of the objectives of removing barriers to trade while ensuring safety for its consumer and user, the manufacturer of a product or the manufacturer's authorised representative or importer of that product is involved in the conformity

³² The name refers to the European Court ruling on the introduction of a liqueur of that name on the German market.

³³ Judgment of the Court of 20 February 1979 – Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein. – Reference for a preliminary ruling: Hessisches Finanzgericht – Germany. – Measures having an effect equivalent to quantitative restrictions. – Case 120/78, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?isOldUri=true&uri=CELEX:61978CJ0120> [accessed: 28.02.2025].

assessment system in a differentiated manner (mandatory or voluntary area), depending on the type of product in question. In a nutshell, the entire scope of EU legislation on conformity assessment relates primarily to the safety of products and their authorisation to be placed on the market. The EU legislation introduces a framework for the market surveillance of products to ensure that these products meet high requirements in terms of protecting public interests such as general health and safety, health and safety in the workplace, consumer protection, environmental protection and public security³⁴. A general framework of rules and principles has been defined in relation to accreditation and market surveillance:

- 1) 'accreditation' means an attestation by a national accreditation body that a conformity assessment body meets the requirements set out in harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes needed for the performance of specific conformity assessment activities;
- 2) 'national accreditation body' means the sole authoritative body in a Member State that performs accreditation with authority derived from the State;
- 3) 'conformity assessment' means the process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled;
- 4) 'conformity assessment body' means a body that performs conformity assessment activities including calibration, testing, certification and inspection³⁵.

In Polish legislation, the conformity assessment system is regulated by the *Act of 13 April 2016 on conformity assessment and market surveillance systems*, which primarily defines the principles of operation of the conformity assessment system in Poland and the principles of operation of the control system for products placed on the market. Its two main objectives are:

³⁴ Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.

³⁵ Ibid. See also: Regulation (EU) 2019/515 of the European Parliament and of the Council of 19 March 2019 on the mutual recognition of goods lawfully marketed in another Member State and repealing Regulation (EC) No 764/2008; Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC; Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety.

- elimination of risks to the life or health of users and consumers posed by products, as well as risks to the environment,
- creation of conditions for reliable assessment of products through their testing, inspection and certification by competent and independent bodies.

The infrastructure of the conformity assessment system consists of notified, certifying, testing (research and calibration laboratories), inspection and accreditation bodies. In Poland, the national accreditation body is the Polish Centre for Accreditation.

The aforementioned Act, like the European legislation, focuses on mandatory conformity assessment, which is evident in the very definitions cited in the Act, where, for example, a certificate is understood as (...) *or product manufacturing process complies with the requirements* (Article 4, point 4). A notified body, in turn, is a conformity assessment body (i.e., in accordance with Article 4(11), one as referred to in Article 2(13) of Regulation (EC) No. 765/2008) operating in the regulated area – in accordance with Article 4(12). As Anna Stankowska, Adam Muszyński and Sławomir Wilczyński write³⁶:

(...) where the law lays down requirements with regard to the subject matter, conformity assessment shall be obligatory and the conformity assessment bodies/organisations which by law undertake such assessment shall be identified where the law so requires. The conformity assessment body (third party) designated in the directive to participate in the conformity assessment must be notified. Notification serves to formally demonstrate the competence of that body to carry out specific conformity assessment tasks.

Patterns from the mandatory conformity assessment system, developed at the EU level and clarified in Poland, were an important point of reference when formulating legislative solutions for auditing and certification of organisational and technical solutions implemented by critical entities. It should be emphasised that the standards applicable to these solutions are not subject to mandatory certification, but it is possible to assess compliance with them on a voluntary basis. For the purposes of the draft law, the following definitions have therefore been adopted.

³⁶ A. Stankowska, A. Muszyński, S. Wilczyński, *System oceny zgodności* (Eng. Conformity assessment system), in: *Normalizacja*, T. Schweitzer (eds.), Warszawa 2013, Polski Komitet Normalizacyjny, p. 169.

The certification body was defined as (...) *a conformity assessment body accredited in accordance with the provisions of the Act of 13 April 2016 on conformity assessment and market surveillance systems* (Journal of Laws of 2022, item 1854) *or authorised to certify pursuant to the provisions of the Act of 12 September 2002 on standardisation* (Journal of Laws of 2015, item 1483), which not only takes into account the provisions of Regulation (EC) No 765/2008 of the European Parliament and of the Council, but also provides opportunities for certification bodies that are not accredited. Indeed, accreditation, it should be emphasised, is required for the scopes set out in the said Regulation and the Act on conformity assessment and market surveillance systems. On the other hand, entities authorised to certification in accordance with the provisions of the Standardisation Act do not operate in the regulated area, but in a voluntary one, and have the possibility to use the only voluntary certification mark in Poland which is legally authorised, i.e. the PN mark³⁷.

A certificate is described as (...) *a document issued by a certification body confirming that a product, installation, system, process, service or person complies with the relevant requirements*. This is a very important definition, as the use of the term certificate is often colloquial and misused. There are also common cases – whether intentional or not – of directing interested parties to the definition set out in the Act on conformity assessment and market surveillance systems, which – when the context is not taken into account – is misleading and has great potential for manipulation and misinformation. This was particularly noticeable in the technical security systems industry. Certification, on the other hand, means (...) *the actions of a certification body demonstrating that a product, installation, system, process, service or person complies with the relevant requirements*.

The draft implementation of the CER Directive adapted the existing accreditation and authorisation mechanisms in the European and Polish legal framework as tools for validating the competence of conformity assessment bodies against standards relating to information security management system, business continuity management system and technical security systems. Taking these mechanisms into account allowed for a smooth insertion of the auditing and certification system into the well-

³⁷ Regulation of the Council of Ministers of 11 October 2010 on the method of granting and using the mark of conformity with the Polish Standard.

established legal framework, already regulating the principles of verifying the competence of conformity assessment bodies.

The primary objective was to ensure a high level of reliability and credibility of the conformity assessment process, while avoiding the introduction of overly complex, novel legal mechanisms that could generate difficulties of interpretation and implementation. Accreditation, as a recognised form of formal attestation of the competence of certification bodies, is a guarantee of independence, quality, the highest substantive and organisational level and the application of ethical principles. The analogy is with the mandate pointed in Article 7 (3) of the act of standardisation, which opens a path for entities wishing to operate in the area of certification on a voluntary basis. These solutions correspond to the market, ensure the flexibility of the system and allow it to function smoothly. An important element that completes the above explanations is the certificates operating in the market.

Summary

The year 2025 will be a landmark year for EU Member States as they finalise the transposition of the CER Directive into their national legal systems. Poland, as one of the countries most involved in this process, is setting high standards for CI protection. The proposed legislative solutions, based on normalisation, combining standardisation and conformity assessment, can set a benchmark for the other Member States, especially in the context of growing antagonistic and hybrid threats – and these are one of the biggest challenges for CI security today. In a report on the security and safety of property and persons sector in Poland, Anna Araminowicz, Piotr Klatta, Tomasz Radochoński and Magda Sierżyńska write: *At the local level, successful sabotage can reduce economic potential, causing loss of life and property, as well as endangering the life and health of residents and the environment (e.g. arson attacks on landfill sites). At the national level, any such act, due to its publicity in traditional and electronic media, can cause social unrest, panic, and the impression of chaos in the state. All these effects are targets for action in a hybrid conflict*³⁸.

³⁸ A. Araminowicz, P. Klatta, T. Radochoński, M. Sierżyńska, *Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania* (Eng. Protection and Security of Property and Persons – analysis of the sector. Survey report), Kraków 2024, MABEA sp. z o.o., p. 106.

The Polish implementation proposal stands out for its comprehensive approach to the protection of CI, as it integrates the security management system for the provision of essential service, normative requirements and auditing and certification mechanisms. Most important is the obligation to verify the competence of suppliers and service providers by recognised conformity assessment systems, thus eliminating the risks associated with poor quality organisational and technical solutions.

The geopolitical location and experience resulting from the immediate vicinity of the region of war strengthen Poland's position as a state that shapes CI security policy at the European level. The solutions adopted may become the foundation for future initiatives strengthening the resilience of strategic sectors of the economy across the EU.

Bibliography

Araminowicz A., Klatta P., Radochoński T., Sierżyńska M., *Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania* (Eng. Protection and Security of Property and Persons – analysis of the sector. Survey report), Kraków 2024, MABEA sp. z o.o.

A World Built on Standards: A Textbook for Higher Education, S.A. Bøgh (ed.), Nordhavn 2015, Danish Standards Foundation.

Confederation of European Security Services, *How standards drive quality and resilience in critical entities security*, 5.02.2025, EU Council PROCIV–CER Working Party.

Idzikowska T., Banaszek K., *Rola i znaczenie normalizacji w bezpieczeństwie transportu* (Eng. The role and importance of standardisation in transport safety), „Logistyka” 2010, vol. 4.

Łunarski J., *Normalizacja i standaryzacja* (Eng. Normalisation and standardisation), Rzeszów 2014, Oficyna Wydawnicza Politechniki Rzeszowskiej.

Schweitzer T., Zielińska E., *Działalność normalizacyjna* (Eng. Standardisation activity), in: *Normalizacja*, T. Schweitzer (ed.), Warszawa 2013, Polski Komitet Normalizacyjny.

Stankowska A., Muszyński A., Wilczyński S., *System oceny zgodności* (Eng. Conformity assessment system), in: *Normalizacja*, T. Schweitzer (ed.), Warszawa 2013, Polski Komitet Normalizacyjny.

Szewczyk T., Pyznar M., *Ochrona infrastruktury krytycznej a zagrożenia asymetryczne* (Eng. Critical infrastructure protection and asymmetric threats), „Przegląd Bezpieczeństwa Wewnętrznego” 2010, no. 2, pp. 53–59.

Tatarowski A., *Building resilience of critical infrastructure in the light of asymmetric threats and terrorism. Legislative trends in the Polish implementation of the CER Directive with particular reference to aspects of standardisation and certification of organisational and technical solutions*, “Terrorism – Studies, Analyses, Prevention” 2024, no. 5, pp. 391–409. <https://doi.org/10.4467/27204383TER.24.014.19402>.

Tatarowski A., *Standaryzacja i certyfikacja rozwiązań wynikających z Dyrektywy CER* (Eng. Standardisation and certification of solutions under the CER Directive), *10th National Forum for Critical Infrastructure Protection*, Warszawa 2023, <https://www.gov.pl/web/rcb/x-krajowe-forum-ochrony-infrastruktury-krytycznej-za-nami>.

Wiśniewski M., Szwarc K., Skomra W., *Continuity of Essential Services as an Emerging Challenge for Societal Resilience*, “IEEE Access” 2023, vol. 11, pp. 44615. <https://doi.org/10.1109/ACCESS.2023.3271751>.

Internet sources

Bennett M., Gupta V., *Dealing in Security Understanding Vital Services and How They Keep You Safe*, http://resiliencemaps.org/files/Dealing_in_Security.July2010.en.pdf [accessed: 22.06.2022].

Dobrowolność stosowania norm (Eng. Voluntary application of standards), Polski Komitet Normalizacyjny, <https://wiedza.pkn.pl/web/wiedza-normalizacyjna/stanowisko-pkn-w-sprawie-dobrowolnosci-pn> [accessed: 28.02.2025].

Narodowy Program Ochrony Infrastruktury Krytycznej (Eng. National Critical Infrastructure Protection Program), Rządowe Centrum Bezpieczeństwa, 2023.

National Critical Functions Set, CISA, <https://www.cisa.gov/national-critical-functions-set> [accessed: 24.06.2022].

The Polish presidency of the Council of the EU, European Council, Council of the European Union, <https://www.consilium.europa.eu/pl/council-eu/presidency-council-eu/> [accessed: 28.02.2025].

Legal acts

Regulation (EU) 2019/515 of the European Parliament and of the Council of 19 March 2019 on the mutual recognition of goods lawfully marketed in another Member State and repealing Regulation (EC) No 764/2008 (Official Journal of the EU L 91/1 of 29.03.2019).

Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (Official Journal of the EU L 218/30 of 13.08.2008).

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 Directive 2) – (Official Journal of the EU L 333/80 of 27.12.2022).

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security for network and information systems across the Union (Official Journal of the EU L 194/1 of 19.07.2016).

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Official Journal of the EU L 345/75 of 23.12.2008).

Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (Official Journal of the EU L 11/4 of 3.12.2002).

Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards (Official Journal of the EU C 136/1 of 4.06.1985).

Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC (Official Journal of the EU L 218/82 of 13.08.2008).

Act of 5 December 2024 on civil protection and civil defence (Journal of Laws 2024, item 1907).

Act of 11 March 2022 on defence of the Homeland (Journal of Laws 2024, item 248, as amended).

Act of 11 September 2019 – Public Procurement Law (Journal of Laws 2024, item 1320).

Act of 5 July 2018 on the national cybersecurity system (Journal of Laws 2024, item 1077, as amended).

Act of 13 April 2016 on conformity assessment and market surveillance systems (Journal of Laws 2022, item 1864, as amended).

Act of 5 August 2010 on the protection of classified information (Journal of Laws 2024, item 632, as amended).

Act of 26 April 2007 on crisis management (Journal of Laws 2023, item 122, as amended).

Act of 12 September 2002 on standardisation (Journal of Laws 2015, item 1483).

Act of 9 November 2000 on the establishment of the Polish Agency for Enterprise Development (Journal of Laws 2025, item 98).

Act of 22 August 1997 on the protection of persons and property (Journal of Laws 2021, item 1995, as amended).

Act of 21 March 1991 on maritime areas of the Republic of Poland and maritime administration (Journal of Laws 2024, item 1125).

Regulation of the Council of Ministers of 11 October 2010 on the method of granting and using the mark of conformity with the Polish Standard (Journal of Laws 2010 No. 198, item 1316).

Regulation of the Council of Ministers of 24 June 2003 on facilities of particular importance for state security and defence and their special protection (Journal of Laws 2003 No. 116, item 1090).

Presidential Decision Directive/Nsc-63, The White House, 22.05.1998, <https://irp.fas.org/offdocs/pdd/pdd-63.htm> [accessed: 5.03.2025].

Case law

Judgment of the Court of 20 February 1979. – Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein. – Reference for a preliminary ruling: Hessisches Finanzgericht – Germany. – Measures heaving an effect equivalent to quantitative restrictions. – Case 120/78, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?isOldUri=true&uri=CELEX:61978CJ0120> [accessed: 28.02.2025].

Other documents

ISO/TS 31050 *Risk management – Guidelines for managing an emerging risk to enhance resilience.*

PKN-CLC/TS 50661-1:2024-10 *Systemy alarmowe – Zewnętrzne perymetryczne systemy zabezpieczeń – Część 1: Wymagania systemowe.* (Eng. Alarm systems – External perimeter security systems – Part 1: System requirements).

PKN-ISO Guide 73:2012 *Zarządzanie ryzykiem – Terminologia.* (Eng. Risk management – Vocabulary).

PN-EN 16763 *Usługi w zakresie systemów ochrony przeciwpożarowej i systemów zabezpieczeń technicznych* (Eng. Services for fire safety systems and security systems).

PN-EN 17483-1:2021-11 *Prywatne usługi ochrony – Zabezpieczenie infrastruktury krytycznej – Część 1: Wymagania ogólne.* (Eng. Private security services – Protection of critical infrastructure – Part 1: General requirements).

PN-EN 17483-2:2024-03 *Prywatne usługi ochrony – Zabezpieczenie infrastruktury krytycznej – Część 2: Usługi ochrony portów lotniczych i lotnictwa.* (Eng. Private security services – Protection of critical infrastructure – Part 2: Airport and aviation security services).

PN-EN 17483-3:2024-03 *Prywatne usługi ochrony – Zabezpieczenie infrastruktury krytycznej – Część 3: Usługi ochrony morskiej i portowej.* (Eng. Private security services – Protection of critical infrastructure – Part 3: Maritime and port security services).

PN-EN 45020:2009 *Normalizacja i dziedziny związane. Terminologia ogólna.* (Eng. Standardisation and related activities. General vocabulary).

PN-EN 50131-1 *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Część 1: Wymagania systemowe.* (Eng. Alarm systems – Intrusion and hold-up systems – Part 1: System requirements).

PN-EN 60839-11-1 *Systemy alarmowe i elektroniczne systemy zabezpieczeń – Część 11-1: Elektroniczne systemy kontroli dostępu – Wymagania dotyczące systemów i komponentów.* (Eng. Alarm and electronic security systems – Part 11-1: Electronic access control systems – System and components requirements).

PN-EN 62676-1-1 *Systemy dozoru wizyjnego stosowane w zabezpieczeniach – Część 1-1: Wymagania systemowe – Postanowienia ogólne.* (Eng. Video surveillance systems for use in security applications – Part 1-1: System requirements – General).

PN-EN IEC 31010:2020-01 *Zarządzanie ryzykiem – Techniki oceny ryzyka*. (Eng. Risk management – Risk assessment techniques).

PN-EN ISO 19011:2018 *Wytyczne dotyczące audytowania systemów zarządzania*. (Eng. Guidelines for auditing management systems).

PN-EN ISO 22301 *Bezpieczeństwo i odporność. Systemy zarządzania ciągłością działania. Wymagania* (Eng. Security and resilience. Business continuity management systems. Requirements).

PN-EN ISO/IEC 27001 *Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności. Systemy zarządzania bezpieczeństwem informacji. Wymagania* (Eng. Information security, cybersecurity and privacy protection. Information security management systems. Requirements).

PN-EN ISO/IEC 27005:2025-01 *Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Wytyczne do zarządzania ryzykami w bezpieczeństwie informacji*. (Eng. Information security, cybersecurity and privacy protection – Guidelines on managing information security risks).

PN-ISO 31000:2012 *Zarządzanie ryzykiem – Zasady i wytyczne*. (Eng. Risk management – Principles and guidelines).

PN-ISO 31000:2018-08 *Zarządzanie ryzykiem – Wytyczne*. (Eng. Risk management – Guidelines).

PN-ISO/IEC 27005:2014-01 *Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji*. (Eng. Information technology – Security techniques – Information security risk management).

Draft act amending the act on crisis management and some other acts, <https://legislacja.rcl.gov.pl/docs//2/12386961/13069020/13069024/dokument711601.pdf> [accessed: 6.04.2025].

Adam Tatarowski

Chairman of the Competence Council for the Protection and Security of Property and Persons at the Polish Agency for Enterprise Development. Expert of the Government Centre for Security in the field of standardisation and conformity assessment

of organisational and technical solutions used in ensuring the security of critical infrastructure. President of the Department of Technical Development for the Protection of Property TECHOM – a specialised certification body and a continuing education institution operating within the educational system. President of the All-Poland Association of Engineers and Technicians of Technical Security and Security Management 'POLALARM'. Member of the Standardisation Council at the Polish Committee for Standardisation.

Contact: tatarowski@techom.com

The value of EU research projects in critical infrastructure protection

Małgorzata Wolbach

Polish Platform for Homeland Security

 <https://orcid.org/0009-0005-1837-0389>

Rashel Talukder

Polish Platform for Homeland Security

 <https://orcid.org/0000-0003-4743-9355>

Critical infrastructure (CI) protection and ensuring its ongoing resilience, particularly against hybrid threats, are fundamental to the stability of modern societies. Reliable access to essential services such as energy, water, food, healthcare, and transportation underpins the secure and stable functioning of daily life.

The institutions of European Union in recent years have placed significant emphasis on strengthening the protection and resilience of CI. This has been influenced by the ongoing war in Ukraine, which has exacerbated concerns about CI security across Europe.

Key areas of EU action include:

- introduction of the CER Directive¹ (The Critical Entities Resilience Directive);
- introduction of the NIS 2 Directive² (Network and Information Systems Directive 2) on network and information security;
- establishment of an EU plan for CI (recommendations adopted by the Council of the EU, inter alia, coordinate responses to CI disruptions of cross-border significance)³;
- cooperation with NATO⁴;
- exchange of information and good practices, inter alia through the involvement of the Critical Entities Resilience Group (CERG), which facilitates cooperation and exchange of information between Member States to ensure the effective implementation of the CER Directive⁵.

Moreover, EU provides substantial financial and strategic support for research and innovation in the field of CI protection through different funding programmes. These help to develop new technologies and introduce solutions to counter emerging threats and improve infrastructure resilience⁶. The EU has established several such programmes. By investing in these initiatives, the EU not only strengthens the protection of its CI but also promotes economic growth and sustainable development. As highlighted in the annual progress report on the implementation of common solutions to counter hybrid threats⁷, EU-funded security research projects

¹ 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.

² 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.

³ Council Recommendation of 25 June 2024 on a Blueprint to Coordinate a Response at Union Level to Disruptions of Critical Infrastructure with Significant Cross-Border Relevance.

⁴ NATO and European Union release final assessment report on resilience of critical infrastructure, NATO, 29.06.2023, https://www.nato.int/cps/en/natohq/news_216631.htm [accessed: 6.01.2025].

⁵ Critical infrastructure resilience at EU-level, European Commission, 23.09.2024, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en [accessed: 6.01.2025].

⁶ Ibid.

⁷ Joint Staff Working Document. Eighth progress report on the implementation of the 2016 Joint framework on countering hybrid threats and the 2018 Joint communication on increasing resilience and bolstering capabilities to address hybrid threats, <https://defence-industry-space>.

play a crucial role in identifying existing gaps and enhancing the security and resilience of CI across the EU.

The article presents selected EU-funded projects under Horizon 2020 and Horizon Europe, such as: EU-HYBNET, EU-CIP, VIGIMARE, TESTUDO, NBSINFRA, ENDURANCE and TRANSCEND. Furthermore, the article analyses challenges associated with the implementation of these projects, including regulatory inconsistencies (different national regulations and inconsistent interpretations of EU directives), financial constraints, and the need for cross-border cooperation. Recommendations for future research directions were made and the importance of cyber security, quantum technology and real-time threat information sharing in enhancing the EU's ability to respond to evolving security threats was highlighted.

Funding for research and innovation in critical infrastructure protection using Horizon Europe as an example

One of the EU funding programmes that stands out for its significant contribution to research and development (aimed at strengthening CI resilience) is Horizon Europe. It is the EU's flagship programme for the period 2021–2027 dedicated to research and innovation (R&I), with a projected budget of EUR 93.5 billion. Supporting advances in science and technology is becoming more urgent, especially in the context of increasing geopolitical instability. Events such as Russia's full-scale invasion of Ukraine have highlighted threats to security, democracy and global supply chains, making the programme's objectives in the second half of its implementation even more relevant. Horizon Europe supports international cooperation and increases the impact of research and innovation on EU policy-making. At the same time, it plays a vital role in addressing pressing global challenges. Horizon Europe provides a diverse set of instruments – from basic research, to disruptive innovation, to the development and implementation of cutting-edge solutions – for research-based solutions⁸.

ec.europa.eu/system/files/2025-01/SWD_Annual-Progress-Report-2024.PDF [accessed: 2.01.2025].

⁸ *Horizon Europe*, https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en [accessed: 7.01.2025].

The Horizon Europe Strategic Plan 2025–2027⁹ details the most important strategic objectives, priority actions, and thematic focus areas for the latter stages of its implementation. It aims to align the final years of this programme with emerging challenges, evolving EU policies, and the changing needs of its Member States. It is the EU's most ambitious research and innovation programme to date due to the fact that it responds to the global context, supports breakthroughs and facilitates access to funding for a diverse research groups and non-EU companies, and has a record budget. The plan combines overarching EU policy goals with the research and innovation activities carried out under the Horizon Europe programme. It offers planning stability that extends beyond the standard two-year work programme cycle. It provides predictability for the research community, while maintaining flexibility to address unexpected changes and challenges¹⁰.

Projects funded under Horizon Europe aim to acquire new knowledge, technologies, and solutions that meet the requirements. These are projects that involve end-users working with researchers and industrial partners. This inclusive model ensures that the outcomes of research and innovation are closely aligned with the practical needs of those who will ultimately implement them, making projects more useful.

These projects play a crucial role in addressing current global challenges, including enhancing the CI resilience¹¹. The war in Ukraine has underscored the importance of R&I in issues, such as providing clean energy, sustainable food, medicines, ensuring defence capabilities, and socioeconomic security. These efforts are essential not only for minimising immediate risks but also for ensuring long-term resilience and stability. Horizon Europe projects already contribute to overcoming rapidly evolving challenges related to CI with cross-border relevance. In the future, this will require even greater innovation and coordinated efforts.

⁹ *Horizon Europe. Strategic Plan 2025–2027*, European Commission, 2024, <https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/6abcc8e7-e685-11ee-8b2b-01aa75ed71a1> [accessed: 7.01.2025].

¹⁰ *Strategic plan*, https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/strategic-plan_en [accessed: 3.01.2025].

¹¹ *Horizon Europe. Strategic Plan 2025–2027. Analysis*, European Commission, 2023, <https://op.europa.eu/en/publication-detail/-/publication/b3baec75-fdd0-11ed-a05c-01aa75ed71a1/language-en> [accessed: 9.01.2025].

The CI resilience, including energy, transport, and telecommunications, is a priority for the EU, particularly in the face of hybrid threats. Actions taken, e.g. the implementation of the CER Directive, aim to ensure both physical and cyber CI resilience. Security research under Horizon Europe supports these efforts by providing innovative methodologies for scenario planning, serving as a test environment for project solutions, stress tests, and threat minimisation. The EU Council has encouraged Member States to make full use of EU-funded research and innovation results, emphasising their importance in enhancing infrastructure resilience. In this context, R&I projects serve as a vital bridge between policy and practice, enabling the EU and its Member States to respond effectively to current and future challenges. Through collaboration, fostering innovation and resilience, these projects are integral to protecting the EU's infrastructure, security and competitiveness in an increasingly complex world¹².

Horizon Europe fosters R&I through its Work Programmes, which outline funding opportunities for various activities. The programme is structured around 3 key Pillars. Pillar II – Global Challenges and European Industrial Competitiveness – is divided into 6 clusters of R&I activities. The clusters were designed to foster integration and complementarities across thematic areas, while ensuring that the EU achieves significant and sustainable impact on the challenges identified in each Horizon Europe cluster in relation to the resources invested.

Cluster 3 – Civil Security for Society is dedicated to enhancing security by supporting efforts to prevent and build resilience to threats to security: internal, individual and society as a whole¹³. It also encompasses tackling the evolving threats, including terrorism, corruption, organised crime, and hybrid attacks on CI. By deepening the understanding of these threats and their societal roots, and by developing advanced tools to prevent, detect, and investigate them, Cluster 3 seeks to enhance the EU's security capabilities. R&I activities within the cluster also focus on ensuring the resilience of CI – such as energy, water, food supply, and healthcare systems – against physical or cyber attacks. A budget of EUR 1.596 billion has been allocated to Cluster 3.

¹² Ibid.

¹³ *Horizon Europe. Strategic Plan 2025-2027*, European Commission, 2024...

Cluster 3 is organised into 6 main destinations, each focusing on specific priorities within the overarching theme of civil security. Destination 3, Resilient infrastructure, is dedicated to enhancing the resilience and autonomy of both physical and digital infrastructures. The expected results are described as follows: *Resilience and autonomy of physical and digital infrastructures are enhanced, and vital societal functions are ensured, thanks to more effective prevention, preparedness, and response, a deeper understanding of the associated human, societal, and technological aspects, and the development of cutting-edge capabilities for infrastructure operators*¹⁴.

This destination is closely linked with Destination 6, Strengthened Security Research and Innovation, which provides the research, technological advancements, and innovative solutions that underpin and support Destination 3. These destinations both create a complementary framework to address EU security priorities, advancing the protection of CI while bolstering societal and economic resilience. They have practical applications in relation to equipping infrastructure operators with advanced tools and capabilities to respond effectively to emerging challenges.

An example of the implementation of Destination 3 was the Resilient Infrastructure (HORIZON-CL3-2024) call for funding in 2024¹⁵ research and innovation to strengthen infrastructure resilience. Themes funded under HORIZON-CL3-2024 are:

- **INFRA01:** *Improved preparedness and response for large-scale disruptions of European infrastructures,*
- **INFRA02:** *Resilient and secure urban areas and smart cities.*

Details about these topics, including their type of action and the expected outcomes, are summarised in the table 1.

¹⁴ Horizon Europe. Work Programme 2023-2025. 6. Civil Security for Society (European Commission Decision C(2024) 2371 of 17 April 2024), https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2023-2024/wp-6-civil-security-for-society_horizon-2023-2024_en.pdf, p. 8 [accessed: 10.01.2025].

¹⁵ Ibid.

Table 1. Sub-topics of the Resilient Infrastructure Programme (HORIZON-CL3-2024).

Sub-topic INFRA01	HORIZON-CL3-2024-INFRA-01-01: Open Topic
Type of action	Innovation Actions
Expected outcomes	<p>Projects’ results are expected to contribute to all of the following outcomes:</p> <ul style="list-style-type: none">• CI operators are more resilient to natural and man-made threats;• improved monitoring, risk assessment, its forecast, limitation and modelling techniques aimed at increasing the CI resilience, validating multi-hazard scenarios, creating interactive hazard maps based on Earth observation and other data sources.
Sub-topic INFRA02	HORIZON-CL3-2024-INFRA-01-02: Resilient and secure urban planning and new tools for EU territorial entities
Type of action	Innovation Actions
Expected outcomes	<p>Projects’ results are expected to contribute to all of the following outcomes:</p> <ul style="list-style-type: none">• evaluation of the resilience of an urban and peri-urban environment, identification of weaknesses and recommendations for changes to organisational processes;• creation of new tools and cost-efficient security upgrades of urban infrastructures with possibilities of pooling and sharing of complex security systems, taking into account limited budgets of local authorities;• improved efficiency of the security forces and emergency services (police, firefighters, paramedics, etc.) for the benefit of the European citizens and residents;• promotion of best practices, creation of EU sovereign trusted decision support tool/solution and spreading of effective tools and capabilities across entities in different EU territories despite their size and location.

Sub-topic INFRA02	HORIZON-CL3-2024-INFRA-01-03: Advanced real-time data analysis used for infrastructure resilience
Type of action	Research and Innovation Actions
Expected outcomes	<p>Projects' results are expected to contribute to some or all of the following outcomes:</p> <ul style="list-style-type: none">• improved capabilities for risk and faulty events identification in infrastructure networks and smart cities through real-time analysis (including big data) by public and private actors via secured and trusted platforms and interconnected systems where the collaboration follows clear legal and political frameworks;• tools and processes for facilitating stakeholders efforts to identify, analyse, assess and continuously monitor risks and boost adaptive capacity to unexpected events risks in advance by allowing for the analysis of various data sources (e.g. audio, video, social media, web-content, spatial information, sensor or machine generated data);• fast and continuous real-time identification, classification and tracking of hazardous agents, contaminants or anomalies in infrastructure networks and supply-chains; interoperable interfaces and improved collaboration between infrastructure operation detection and response systems, national/EU risk management/coordination centres and first responder equipment in order to allow for remote on-scene operations considering citizen knowledge;• increased cyber-resilience of industrial xG networks and cloud data covering specific infrastructure domains;• improved ability to map in real-time the source(s) of risk that could endanger the networked infrastructure supported by Earth Observation and geolocation data. If the analysis includes processing of personal data, it should consider including assessment of associated risk or privacy impact of individuals and society.

Source: *Horizon Europe. Work Programme 2023-2025. 6. Civil Security for Society (European Commission Decision C(2024) 2371 of 17 April 2024)*, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2023-2024/wp-6-civil-security-for-society_horizon-2023-2024_en.pdf, pp. 91–97 [accessed: 10.01.2025].

An indicative budget of EUR 16 million has been allocated for the Resilient Infrastructure Programme in 2024¹⁶. The deadline for applications was 20 November 2024. Of the 79 that were submitted, only three will be successful, with implementation starting in September 2025. This shows not only competitiveness of the contest, but also the reduction in the overall budget for research and innovation in CI protection.

Overview of selected research and innovation initiatives funded under Horizon 2020 and Horizon Europe Programmes

EU-funded initiatives in the field of CI protection are developing both technological and non-technological solutions. At the same time, these initiatives strengthen European cooperation. The aim is to demonstrate the opportunities such projects offer to a wide range of stakeholders, including research institutions driving innovation, businesses developing cutting-edge security solutions, public organisations implementing policies, as well as CI owners and operators responsible for ensuring service continuity.

EU-HYBNET

(Empowering a Pan-European Network to Counter Hybrid Threats)¹⁷

The Project, funded by the European Union's Horizon 2020 Research and Innovation Programme (a predecessor of Horizon Europe). It is the first EU initiative that brings together security practitioners, academics, industry players and business as well as non-government organisations to collaborate, identify and analyse common challenges, and requirements to counter hybrid threats.

The main project objectives of EU-HYBNET are to:

1. Create and develop the network of European organisations countering hybrid threats and ensure long-term sustainability of the network.

¹⁶ *Resilient Infrastructures*, https://rea.ec.europa.eu/funding-and-grants/horizon-europe-cluster-3-civil-security-society/resilient-infrastructures_en [accessed: 10.01.2025].

¹⁷ *Empowering a Pan-European Network to Counter Hybrid Threats*, European Commission, <https://cordis.europa.eu/project/id/883054> [accessed: 13.01.2025].

2. Define common requirements to fill knowledge gaps, address performance needs, and enhance capabilities of research, innovation and training endeavours concerning hybrid threats.
3. Monitor developments in research and innovation activities as applied to hybrid threats.
4. Identify priorities for the implementation of innovation and industrialisation, and to increase the role of European network in effectively countering hybrid threats.
5. Establish conditions for enhanced interaction among security practitioners, industry, and academia to foster meaningful dialogue and increase network membership.
6. Foster capacity building and knowledge exchange on countering hybrid threats.
7. Create a basis for effective cooperation with existing European, national and sub-national networks of practitioners and other actors countering hybrid threats.

The project addresses 4 core themes to ensure coherence in its results, and to facilitate a focus on all hybrid threat domains (including CI). These are:

1. Future trends of hybrid threats.
2. Cyber and future technologies.
3. Resilient civilians, local level and national administration.
4. Information and strategic communication.

These themes emphasise domains, as identified and defined by the European Commission and EU Joint Research Centre (JRC). This provides essential support for research and innovation activities in hybrid threat domains deemed crucial for delivering solutions during the project cycles.

Although the project ended in April 2025, the network is ever-growing (currently consisting of more than 150 organisations from EU countries, Ukraine, and the UK)¹⁸.

¹⁸ EU-HYBNET, <https://euhybnet.eu/> [accessed: 13.01.2025].

EU-CIP

(European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection)¹⁹

This is also a networking initiative, but focused only on CI. It runs from October 2022 to September 2025.

The main goal of EU-CIP is to establish a unique pan-European knowledge network for resilient infrastructures, enabling policymakers to shape and produce data-driven, evidence-based policies, while boosting the innovation capacity and competitiveness of CI operators, authorities, researchers, and innovators. In this direction, the project develops the European Cluster for Securing Critical Infrastructures, ECSCI – established and operated by the project partners – Europe’s most prominent R&I knowledge network for security and resilience of CI. The ECSCI cluster brings together 22 projects that collaborate on CI resilience. EU-CIP leverages the capacity, organisation, community, and achievements of the ECSCI cluster to establish an EU-wide knowledge network.

EU-CIP offers advanced information analysis capabilities for evidence-based policymaking and innovation support to facilitate the exploitation and commercialisation of research outcomes. To maximise the impact of its activities, EU-CIP establishes and expands a vibrant ecosystem of interested and committed stakeholders around the project’s information analysis and innovation support services.

EU-CIP main objectives:

1. **Analysis:** enhancing Europe’s analytical capability regarding research outcomes, technologies, and policies – foster data-driven evidence-based policy and innovation development. EU-CIP establishes a data collection, information monitoring, and analysis methodology and infrastructure, which continually collects, analyses, curates, extracts, and presents information and insights about resilient infrastructures. As part of this objective, EU-CIP presents foresight and insights about gaps in current knowledge and solutions, technologies that address these gaps, as well as research outcomes and practices that can be employed.
2. **Amplification:** maximising the impact of R&I activities in the field of critical infrastructure protection (CIP) and critical infrastructure resilience (CIR) in Europe. The project provides a set of innovation

¹⁹ *European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection*, European Commission, <https://cordis.europa.eu/project/id/101073878> [accessed: 13.01.2025].

support and solution validation services for research outcomes in the areas of resilient infrastructures (CIP/CIR). In this direction, the project leverages the analytical outcomes of the EU-CIP-ANALYSIS pillar to identify gaps in existing solutions and CI areas with significant innovation potential. Accordingly, EU-CIP offers a range of services that will support CIP/CIR innovators (including Small and Medium sized Enterprises, SMEs) in their activities related to the exploitation and commercialisation of research results. Moreover, the project offers a virtualised testbed for the experimentation with standards-based CIP/CIR solutions and certification schemes, along with relevant validation and evaluation processes involving stakeholder engagement.

3. **Creating the ecosystem: establishing a Knowledge-Hub and creation of a vibrant ecosystem of interested and committed stakeholders around the project's results.** EU-CIP establishes and grows an EU-wide ecosystem of CIP/CIR stakeholders, covering EU-27 and other European Economic Area (EEA) countries. The ecosystem facilitates stakeholders' access to the knowledge, results, services, and infrastructures developed in previous objectives, as well as their engagement with innovation development and policymaking outcomes of EU initiatives (e.g. research projects, technology initiatives, policymaking initiatives). At the heart of the ecosystem is a Knowledge-Hub, which provides access (via the relevant digital infrastructure) to the project's knowledge assets, including the infrastructures and results developed in previous objectives. It allows collaboration between different stakeholders.

The expected results of the EU-CIP are as follows:

- enhanced resilience of CI – through comprehensive analysis, the project identifies and addresses gaps;
- evidence-based policy development – by aggregating and analysing a broad spectrum of data, the project supports the creation of more effective policies for CIP/CIR;
- boosting innovation and competitiveness – the project through advanced information analysis capabilities and innovation support services, enhances the capacity of European innovators, particularly in exploitation and commercialisation of research outcomes;
- fostering a collaborative ecosystem – the establishment of a vibrant ecosystem of stakeholders facilitates knowledge

sharing, collaboration, and the co-creation of solutions, enhancing the collective ability to address CIP/CIR challenges²⁰.

VIGIMARE

(Vigilant Maritime Surveillance of Critical Submarine Infrastructure)²¹

This is an innovation action type of project, what means that it is focused on developing solutions with higher Technology Readiness Level (TRL).

The project has developed an innovative solution to improve security and mitigate the risk of physical attacks and cyber threats. The project seeks to identify early warning signals and support analysis by mapping submarine systems, assessing vulnerabilities, and creating real-time awareness of both surface and underwater CI. The project takes a systematic approach to strengthen the European CI sector of submarine telecommunication cables, power cables and gas pipelines. The analysis as well as the VIGIMARE system will support the CI operators of the submarine network by enhancing its resilience against attacks and damages.

VIGIMARE objectives:

- provide information sharing environment to the CI operators against threats to the EU submarine CI;
- increase the resilience of CI operators against physical, cyber and hybrid threats by implementing risk preventing and risk reducing measures;
- strengthen the situational awareness of European maritime areas, both offshore and onshore, to recognise physical (both man-made and natural), cyber and hybrid attacks and incidents for both CI operators and the Member States, enabling better planning of the response and repairs;
- support the EU Member States to fulfil CER and NIS 2 Directives' requirements. The outcomes of this project will also introduce the European Maritime Safety Agency's (EMSA) Common Information Sharing Environment (CISE) to this new area of interest. The solution proposed by VIGIMARE project will be stress-tested using data from real incidents and validated in 3 different European

²⁰ *EU-CIP*, <https://www.eucip.eu/> [accessed: 13.01.2025].

²¹ *Vigilant Maritime Surveillance of Critical Submarine Infrastructure*, European Commission, <https://cordis.europa.eu/project/id/101168016> [accessed: 14.01.2025].

sea areas – the Mediterranean Sea, the Irish Sea and the Baltic Sea – in order to promote its valuable outcome to the European society²².

TESTUDO

(Autonomous Swarm of Heterogeneous resources in infrastructure protection via threat prediction and prevention)²³

This project aims to enhance the surveillance of the European CI and its protection using autonomous systems and advanced technologies to ensure their robust operation.

TESTUDO objectives:

- utilise advanced unmanned vehicles along with existing equipment for continuous monitoring even in harsh environments and remote territories;
- incorporate state-of-the-art technologies for detecting, preventing and anticipating hazardous events to enhance capabilities in this area;
- identify the resources needed for operational activities through optimisation techniques, contributing to the total autonomy of the system;
- bring together a multidisciplinary group comprising specialists in: AI-based models, chemical, biological, radiological, nuclear threats (CBRN), cyber security threats, digital twins (digital replication of physical objects, processes and system) and CI, in order to develop innovative solutions to protect various CI facilities operating in the long term and completely anonymously²⁴.

NBSINFRA

(Citynature-based Solutions Integration to Local Urban Infrastructure Protection for a Climate Resilient Society)²⁵

This is a pioneering European initiative that supports the enhancement of local urban CI protection against natural and manmade hazards.

²² VIGIMARE, <https://vigimare.eu/> [accessed: 15.01.2025].

²³ *Autonomous Swarm of Heterogeneous resources in infrastructure protection via threat prediction and prevention*, European Commission, <https://cordis.europa.eu/project/id/101121258> [accessed: 15.01.2025].

²⁴ TESTUDO, <https://testudo-project.eu/> [accessed: 15.01.2025].

²⁵ *Citynature-based Solutions integration to local urban infrastructure protection for a climate*

It involves co-design and co-creation of Nature-based Solutions (NbS) to build a climate-resilient society. NBSINFRA demonstrates that the NbS are: a) technically viable for the protection of CI against hazards, b) socially acceptable and cost-effective at the local scale, c) efficiently capable to increase the empowerment of communities, through the increase of their ecological, social, and economic resilience.

NBSINFRA establishes 5 representative European regions with an equal number of “City Labs” in: Fingal (Ireland), Cologne (Germany), Ruse (Bulgaria), Aveiro (Portugal), Prague (Czechia). Labs will assess the cost-effectiveness of NbS solutions in the protection of local infrastructure and maximise their impact. These solutions will be owned by citizens and co-created by end-users and managers as well as civil society.

NBSINFRA provides a toolkit that the different stakeholders and society can use to compare and choose the most effective NbS for local CI protection. The main object is to increase its protection against hazards through NbS co-design, co-monitoring, and co-creation, serving the development of sustainable and resilient society²⁶.

ENDURANCE

(Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe)²⁷

The ENDURANCE project aims to strengthen sectors such as energy, health, drinking water in Europe. The project ensures alignment with Europe’s regulatory frameworks, particularly CER and NIS 2 Directives, empowering operators and authorities with the necessary tools, strategies, and knowledge to minimise risks and recover efficiently from disruptions.

ENDURANCE objectives:

- enhance strategic cooperation and collaboration among the CI stakeholders from different sectors and countries at all levels;
- develop datasets, registries, methodologies, technologies, and services (at TRL 6-7) for secure sharing processing of CER-relevant data, joint assessment of relevant risks and resilience, and large-scale stress-testing of preparedness;

resilient society, <https://cordis.europa.eu/project/id/101121210> [accessed: 17.01.2025].

²⁶ NBSINFRA, <https://nbsinfra.eu/> [accessed: 17.01.2025].

²⁷ *Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe*, European Commission, <https://cordis.europa.eu/project/id/101168007> [accessed: 17.01.2025].

- provide harmonised and pragmatic strategy for the continuity of the interconnected essential services²⁸.

TRANSCEND

(Transport resilience against Cyber and Non-Cyber Events to prevent Network Disruption)²⁹

TRANSCEND project aims to:

- provide freight transport operators with an integrated set of advanced tools, guidelines and technological solutions to reduce risks to transport networks and services that may arise from cyber and non-cyber events;
- enhance the protection and resilience of transport systems against physical, cyber and hybrid threats.

To achieve these objectives, the project will provide a digital platform for monitoring threats and risks and will develop 5 real-world pilots. They are divided into 3 main ones: the airport pilot in Luxembourg, the rail-road terminal pilot in Bologna, Italy and the tri-modal port pilot implementation in Spain; and 2 followers: the fluvial port of Budapest and the Egnatia highway in Greece.

The project results will be integrated into a Control Tower, a digital platform with embedded business intelligence giving stakeholders a shared and continuous visibility of threats and risks by breaking down silos within and between organisations. In order to test the effectiveness of the approach, five different transport CI sites will experiment with methodological and technological solutions, 3 in the roles of leaders and 2 followers³⁰.

Challenges and lessons learned with regards projects implementation

Competition for EU funding is intense and securing such funds presents a valuable opportunity for international cooperation. The implementation of successive EU research and innovation projects is highly respected

²⁸ *ENDURANCE*, <https://endurance-horizon.eu/> [accessed: 17.01.2025].

²⁹ *Transport resilience against Cyber and Non-Cyber Events to prevent Network Disruption*, European Commission, <https://cordis.europa.eu/project/id/101168023> [accessed: 17.01.2025].

³⁰ *TRANSCEND*, <https://www.transcend-logistics.eu/> [accessed: 17.01.2025].

within the research community. Compared to national grants, which sometimes include an international component, EU projects assume cooperation between participants from European countries, representing different organisations, including universities, research institutions, private companies, public sector entities, and non-governmental organisations. Although an average project budget of EUR 3–5 million may seem substantial, it must be distributed among consortia of 10–15 or even more partners over a 3-year implementation period. Given the high expectations – according to the authors – for project outcomes, along with the impact of inflation in Europe in recent years, the available budget may not be as significant as it was a few years ago.

After analysing all these factors, conclusions were drawn and several challenges were identified. In the field of coordination across Member States one of the challenges is the different legal regulations and interpretation of EU directives. Albeit the EU provides common directives for CIP, cyber security, and data governance, their implementation and interpretation vary across Member States. Some countries strictly align national laws with EU directives, while others apply looser interpretations or have delays in their transposition into national legislation. For instance, CER and NIS 2 Directives aim for a common security framework, but their practical enforcement differs across countries³¹. These regulatory inconsistencies might lead to delays in project implementation, and complications in joint initiatives between Member States.

Additional challenge might be different perception of risks and national priorities which also have influence on EU projects. It translates into the engagement of these countries in facilitating the exchange of lessons learned and improving knowledge on hybrid threats, as well as in conducting international exercises which involve hybrid scenarios³². This divergence is particularly visible in the case of Russia and China, in relation to which EU Member States have different positions. For example, both governments and societies in Poland and the Baltic States consider China as a threat to cyber security and Russia as an aggressor after the attack on Ukraine,

³¹ *The Commission calls on 23 Member States to fully transpose the NIS2 Directive*, European Commission, 28.11.2024, <https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive> [accessed: 29.01.2025].

³² P. Szymański, *Towards greater resilience: NATO and the EU on hybrid threats*, Ośrodek Studiów Wschodnich, 24.04.2020, <https://www.osw.waw.pl/en/publikacje/osw-commentary/2020-04-24/towards-greater-resilience-nato-and-eu-hybrid-threats> [accessed: 7.02.2025]

while some governments in Member States (e.g. Hungary and Slovakia) are pursuing intensive economic and infrastructure cooperation with China and Russia, particularly in the field of energy. This lack of a unified risk assessment makes it difficult to fully implement joint protective measures and ensure consistent infrastructure security standards across the EU.

Experience from EU projects, confirmed by the observations of the article's authors, shows that Member States have different capacities to successfully implement CI protection projects due to different financial, technological, and human resources. Western and Northern European states are in a better position. Eastern and Southern European countries, on the other hand, face more budgetary constraints, leading to slower implementation of new security technologies and infrastructure upgrades.

A problem in many EU security projects is the complexity of cross-border cooperation including data sharing. However, it should be highlighted that both European Commission and the Member States are implementing specific mechanisms and creating institutions (establishing new structures within existing institutions or new institutions) to support this process in the area of CI protection. These include the CER and NIS 2 Directives, European Programme for Critical Infrastructure Protection (EPCIP), European Cybersecurity Competence Centre (ECCC), and activities provided in cyber security by European Union Agency for Cybersecurity (ENISA). All these mechanisms and institutions should support both the implementation of projects and the use of their results.

Another group of challenges is related to balancing innovation with practicality. EU-funded projects focused on CIP (particularly under Horizon Europe Cluster 3), aim to introduce innovative solutions to enhance security, resilience, and efficiency. However, implementing state-of-the-art solutions is difficult due to technological feasibility, regulatory constraints, safety risks, lack of cost-effectiveness and applicability, among other factors.

Many research projects focus on developing high-tech solutions, such as AI-driven threat detection, advanced cyber security tools, quantum encryption. However, many innovations are in the experimental phase and require months or even years of testing and calibration before they can be safely integrated into existing infrastructure. CI operates for many years (so-called long life cycle), meaning new technology must be compatible with older systems, which is often difficult and expensive. Some emerging technologies (e.g. AI; blockchain; Internet of Things (IoT))

security systems) may not yet be mature enough for real-world application in high-risk environments. Thus, while innovation is essential, it must be practical, scalable, and proven to work in real-life conditions before it can be adopted.

Even when an innovation is technically feasible, it may face legal and regulatory hurdles³³. EU and national regulations on cyber security, data protection, and CI security might slow down or restrict the use of new technologies. Different legal interpretations across Member States create inconsistencies, making it difficult to implement a single innovative solution across multiple countries. Governments and operators must ensure that new technology does not create additional risks, which in practice means long approval processes, testing, and security evaluations. As a result, even the most advanced innovations may take years to gain regulatory approval.

Additional challenge is that innovation often comes with high upfront costs for the development, testing, and implementation of new technologies. Also, CI such as energy grids, transportation networks, water systems, and telecommunications systems is often built on decades-old technologies. Consequently, technological feasibility does not always translate into rapid practical implementation due to incompatibility and operational considerations.

While new technologies can enhance security, they also cause security gaps. Advanced technologies (e.g. IoT, AI, cloud computing) are targeted by cyber criminals and state actors and require constant updates as well as security patches³⁴. Moreover, some innovations can rely on hardware or software from non-EU countries, raising concerns about data security, backdoors, and foreign interference.

Innovation in CI protection requires cooperation between governments, private sector operators, and the public. However, there are often resistance and scepticism regarding new technologies, related to lack of trust in automation and AI, as well as privacy concerns. Technologies like biometric security, and smart monitoring often face public opposition due to fears of mass surveillance and misuse of data. In some countries,

³³ *Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses*, OECD Publishing, Paris 2021. <https://doi.org/10.1787/8fa190b5-en>.

³⁴ *The cybersecurity challenges of legacy OT and how to manage them*, Control Engineering, 21.03.2024, <https://www.controleng.com/the-cybersecurity-challenges-of-legacy-ot-and-how-to-manage-them> [accessed: 7.02.2025].

e.g. Germany, France or Poland, there is a strong public backlash against the involvement of private tech companies or foreign entities in CI projects. If stakeholders do not trust the technology, they will not support its implementation. This inclusion ensures that the voices of the citizenry are considered in shaping policies for technologies that significantly impact society³⁵.

Future directions in EU research on critical infrastructure protection

Definitely future directions on EU research on CI protection must address forthcoming challenges. Based on research and publications, including finding from EU-HYBNET project and reports from European Centre of Excellence for Countering Hybrid Threats, authors point out following areas as most relevant in a short and medium term:

- cyber attacks (including AI driven attacks, and lack of IoT security);
- quantum technology (especially post-quantum cryptography transition and vulnerabilities related to it);
- critical raw materials and supply chain security (batteries, semiconductors, telecommunications);
- physical threats (fires, drones);
- satellites;
- special care on energy resilience;
- secure telecommunications (5G but also 6G).

Due to the rapid development of technologies, geopolitical instability and changing the societies perception around the world, it is difficult to predict and accurately foresee all future risks. Additionally, these areas should be also included in future projects and innovative activities:

- enhance real time joint cyber and physical threat monitoring and real-time threat intelligence sharing;
- joint exercises across EU;
- engaging with global standardisation organisations, to ensuring EU priorities on secure-by-design infrastructure, ethical AI, and privacy-first cyber security are reflected in global standards;
- increasing public-private partnerships with technology providers;

³⁵ K. Kieslich, M. Lünich, *Regulating AI-Based Remote Biometric Identification. Investigating the Public Demand for Bans, Audits, and Public Database Registrations*, preprint, <https://arxiv.org/abs/2401.13605v3> [accessed: 7.02.2025]. <https://doi.org/10.48550/arXiv.2401.13605>.

- cooperation with trusted EU partners including the UK, US, Canada, Japan, South Korea and Australia.

Conclusions

The protection of CI remains a cornerstone of European security policy, particularly in the face of evolving hybrid threats. The European Union is making relevant effort in funding innovation initiatives aimed at strengthening the resilience of CI. Projects such as: EU-HYBNET, EU-CIP, VIGIMARE, TESTUDO, TRANSCEND, NBSINFRA, and ENDURANCE show the extent of efforts to enhance security involving the development of technology, policy coordination, and cross-border collaboration.

One of the conclusions from this analysis is the increasing complexity of threats facing CI operators. The convergence of cyber and physical security risks, difficulties due to differing national regulations and inconsistent interpretations of EU directives across EU Member States, and the challenges of balancing innovative projects with their implementation all emphasise the need for sustained research and development efforts. While Horizon Europe project and other funding mechanisms have provided great support, additional financial and strategic resources are required to maintain the EU's leadership in infrastructure resilience.

Another significant insight is the necessity of fostering stronger cooperation among stakeholders. The projects reviewed in this article demonstrate the importance of integrating perspectives from industry, academia, public authorities, and civil society. Fostering more agile and adaptive partnerships will be essential to keep pace with the rapidly evolving threat landscape. Additionally, ensuring that research findings are translated into practical applications will require closer alignment between policymakers, technology developers, and infrastructure operators.

The next phase of research and policy development should focus on enhancing resilience through strategic foresight, technological innovation, and cross-sector collaboration. In this way, the EU can ensure that its CI remains resilient to future threats, thereby protecting the security and stability of societies on the continent.

The authors believe that it is worth monitoring and analysing whether and how the outcomes of projects described in the article have been implemented in practice.

Bibliography

Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses, OECD Publishing, Paris 2021. <https://doi.org/10.1787/8fa190b5-en>.

Internet sources:

Autonomous Swarm of Heterogeneous resources in infrastructure protection via threat prediction and prevention, European Commission, <https://cordis.europa.eu/project/id/101121258> [accessed: 15.01.2025].

Citynature-based Solutions integration to local urban infrastructure protection for a climate resilient society, <https://cordis.europa.eu/project/id/101121210> [accessed: 17.01.2025].

Critical infrastructure resilience at EU-level, European Commission, 23.09.2024, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en [accessed: 6.01.2025].

Empowering a Pan-European Network to Counter Hybrid Threats, European Commission, <https://cordis.europa.eu/project/id/883054> [accessed: 13.01.2025].

ENDURANCE, <https://endurance-horizon.eu/> [accessed: 17.01.2025].

EU-CIP, <https://www.eucip.eu/> [accessed: 13.01.2025].

EU-HYBNET, <https://euhybnet.eu/> [accessed: 13.01.2025].

European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection, European Commission, <https://cordis.europa.eu/project/id/101073878> [accessed: 13.01.2025].

Horizon Europe, https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en [accessed: 7.01.2025].

Horizon Europe. Strategic Plan 2025–2027, European Commission, 2024, <https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/6abcc8e7-e685-11ee-8b2b-01aa75ed71a1> [accessed: 7.01.2025].

Horizon Europe. Strategic Plan 2025–2027. Analysis, European Commission, 2023, <https://op.europa.eu/en/publication-detail/-/publication/b3baec75-fdd0-11ed-a05c-01aa75ed71a1/language-en> [accessed: 9.01.2025].

Horizon Europe. Work Programme 2023-2025. 6. Civil Security for Society (European Commission Decision C(2024) 2371 of 17 April 2024), https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2023-2024/wp-6-civil-security-for-society_horizon-2023-2024_en.pdf [accessed: 10.01.2025].

Joint Staff Working Document. Eighth progress report on the implementation of the 2016 Joint framework on countering hybrid threats and the 2018 Joint communication on increasing resilience and bolstering capabilities to address hybrid threats, https://defence-industry-space.ec.europa.eu/system/files/2025-01/SWD_Annual-Progress-Report-2024.PDF [accessed: 2.01.2025].

Kieslich K., Lünich M., *Regulating AI-Based Remote Biometric Identification. Investigating the Public Demand for Bans, Audits, and Public Database Registrations*, preprint, <https://arxiv.org/abs/2401.13605v3> [accessed: 7.02.2025]. <https://doi.org/10.48550/arXiv.2401.13605>

NATO and European Union release final assessment report on resilience of critical infrastructure, NATO, 29.06.2023, https://www.nato.int/cps/en/natohq/news_216631.htm [accessed: 6.01.2025].

NBSINFRA, <https://nbsinfra.eu/> [accessed: 17.01.2025].

Resilient Infrastructures, https://rea.ec.europa.eu/funding-and-grants/horizon-europe-cluster-3-civil-security-society/resilient-infrastructures_en [accessed: 10.01.2025].

Strategic plan, https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/strategic-plan_en [accessed: 3.01.2025].

Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe, European Commission, <https://cordis.europa.eu/project/id/101168007> [accessed: 17.01.2025].

Szymański P., *Towards greater resilience: NATO and the EU on hybrid threats*, Ośrodek Studiów Wschodnich, 24.04.2020, <https://www.osw.waw.pl/en/publikacje/osw-commentary/2020-04-24/towards-greater-resilience-nato-and-eu-hybrid-threats> [accessed: 7.02.2025].

TESTUDO, <https://testudo-project.eu/> [accessed: 15.01.2025].

The Commission calls on 23 Member States to fully transpose the NIS2 Directive, European Commission, 28.11.2024, <https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive> [accessed: 29.01.2025].

The cybersecurity challenges of legacy OT and how to manage them, Control Engineering, 21.03.2024, <https://www.controleng.com/the-cybersecurity-challenges-of-legacy-ot-and-how-to-manage-them> [accessed: 7.02.2025].

TRANSCEND, <https://www.transcend-logistics.eu/> [accessed: 17.01.2025].

Transport resilience against Cyber and Non-Cyber Events to prevent Network Disruption, European Commission, <https://cordis.europa.eu/project/id/101168023> [accessed: 17.01.2025].

Vigilant Maritime Surveillance of Critical Submarine Infrastructure, European Commission, <https://cordis.europa.eu/project/id/101168016> [accessed: 14.01.2025].

VIGIMARE, <https://vigimare.eu/> [accessed: 15.01.2025].

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 (NIS 2 Directive) – (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 – (Official Journal of the EU L 333/80 of 27.12.2022).

Council Recommendation of 25 June 2024 on a Blueprint to Coordinate a Response at Union Level to Disruptions of Critical Infrastructure with Significant Cross-Border Relevance (Official Journal of the EU C 2024/4371 of 5.07.2024).

Małgorzata Wolbach

Senior Project Officer in the Polish Platform for Homeland Security (PPBW). Master's degree in Homeland Security and Bachelor's degree in Criminology in the Police Academy in Szczytno. At PPBW she is responsible for the implementation and realisation of projects funded by EU programmes, with a particular focus on projects addressing hybrid threats and the security of public spaces.

Contact: malgorzata.wolbach@ppbw.pl

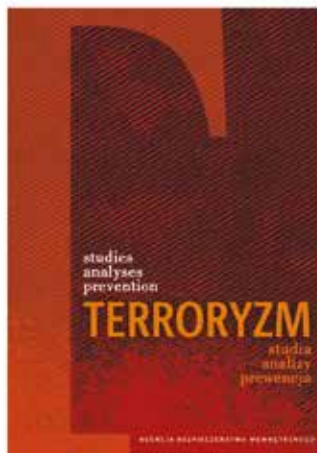
Rashel Talukder

Managing Director of the Polish Platform for Homeland Security (PPBW). Since 2009 he has been actively involved in security research and development in Poland and Europe, including as coordinator of European projects. He was also involved in local community affairs as a municipal councillor of Stęszew (2018–2024).

Contact: rashel.talukder@ppbw.pl



INTERNAL SECURITY AGENCY PUBLISHING HOUSE



The Publishing House of the Internal Security Agency, launched in 2009, issues peer-reviewed scientific monographs devoted to, inter alia, the history of Polish secret services and broadly understood legislative matters as well as publications concerning statutory tasks of the Internal Security Agency. It is also the publisher of two scientific journals: "Internal Security Review" and "Terrorism – Studies, Analyses, Prevention".

The biannual "Internal Security Review" is a scientific journal published since 2009 with a focus on interdisciplinary issues related to the protection of the constitutional order of the state. The topics of the articles cover a wide range of areas related to national security, e.g. legal issues, activities of institutions and organizations responsible for the protection of the constitutional order of the state as well as analyses of current and projected security status in the national and international perspectives.

The biannual "Terrorism – Studies, Analyses, Prevention" is a scientific journal established in 2021, devoted to interdisciplinary issues related to anti-terrorist protection and building resilience to terrorist threats in the national and international perspectives. It is meant to be a platform for the exchange of scientific ideas and experience, connecting the academic world and representatives of institutions and services that cooperate with each other within the Interministerial Team for Terrorist Threats, which is the coordination centre of the anti-terrorist system of the Republic of Poland.

Authors of the articles are officers of the Internal Security Agency and other uniformed services of the Republic of Poland, academics from universities, scientific institutions and research centers as well as specialists in fields related to the history of special services and the protection of national security.

Since July 2021, the Publishing House of the Internal Security Agency has been included in the Polish ministerial list of publishers issuing peer-reviewed scientific monographs. Number of points – 80 (LEVEL I).

For further information concerning the Publishing House of the Internal Security Agency, including terms of cooperation, please visit: www.abw.gov.pl/publ/.

