ISSN: 2450-6869

eISSN: 2719-6763

No. 20, 2024

DEFENCE SCIENCE REVIEW

http://www.journalssystem.com/pno/

DOI: 10.37055/pno/208458

Security and Hybrid Threats

Original article

Received: 2025-07-05

Revised:

Accepted: 2025-07-21

Final review: 2025-07-20

Peer review: 2025-06-05

Double blind

Keywords:

hybrid threats, cognitive warfare, disinformation, critical infrastructure

Krzysztof Kaczmarek [1,2], A-F
ORCID 0000-0001-8519-1667

Dagmara Cholewińska [3,], A-F
ORCID 0009-0006-1570-4854

A - Research concept and design, B - Collection and/orassembly of data, C - Data analysis and interpretation, D - Writing the article, E - Critical revision of the article, F - Final approval of the article

[1] Koszalinski University of Technology, Poland
[2] Department of Humanities, Koszalin University of Technology, Poland
[3] Independent researcher, Poland

Abstract

Objectives: The article aims to explore the evolving nature of hybrid threats, with particular focus on non-kinetic operations conducted during formal peace. It investigates how attacks on critical infrastructure and psychological operations shape contemporary security environments and assesses the vulnerability of democratic societies to disinformation and manipulation

Methods: The study employs a qualitative approach based on literature review, behavioural analysis of societal responses to hybrid operations, and polemological case studies. Empirical references include documented Russian Federation activities, such as the annexation of Crimea, GPS signal disruption in the Baltic region, and coordinated disinformation campaigns in Central Europe.

Results The analysis confirms that hybrid threats are increasingly central to modern conflict strategies. These operations blend informational, cognitive, and infrastructural dimensions, often exploiting internal social divisions and trust deficits. The study highlights the critical role of cognitive warfare in shaping perception and decision-making, thereby limiting state responsiveness.

Conclusions: Hybrid actions are dynamic and tailored to specific vulnerabilities of targeted states. There is no universal model for resilience; effective countermeasures require context-specific diagnosis, public awareness, and intersectoral coordination. Without strategic adaptation, hybrid threats may undermine national cohesion and security without formal declaration of war. Therefore, strengthening cognitive resilience and strategic communication capabilities should be considered a critical element of national security planning.

Corresponding author: Krzysztof Kaczmarek, Politechnika Koszalińska, Poland; email: puola1972@gmail.com

Introduction

Technological progress is changing almost all aspects of the functioning of individuals, societies, and states. It should also be noted that the changes taking place are making humanity increasingly dependent on many previously unknown, neutral, or insignificant factors. These include, among others, disruptions in the proper functioning of critical infrastructure, particularly power grid failures (Włodyka, Kaczmarek, 2024, p. 261).

In the modern world, sustainable and uninterrupted energy supplies are the basis for the existence of stabilised and developing economies, and energy systems currently determine the economic situation and position of the country in the international arena (Kochanek, 2020, p. 118). It should be emphasised that electricity has become a good without which modern man cannot function. Computer systems, communication networks, media are no longer technological novelties that simply make life easier, but have become determinants of human existence. Schools, public administration units, health and public order services, and production plants have been computerized and automated, and the sphere of interpersonal relations has been largely transferred to the virtual reality of social networks (Zakrzewska, Gil-Świderska, 2018, p. 55). It is also important that without electricity, other systems responsible for supplying the population, among others, with drinking water and food or transport systems, supply chains and communications do not function.

In addition, it should be noted that society has transferred many aspects of social life to virtual reality, which has begun to redefine the way people function. In particular, the form of communication and the formation of interpersonal relationships have undergone irreversible changes, including the addictive need to have constant access to information. Globalisation, although it connects people, individual social groups and even countries, is also a source of many threats. It should be remembered that the connection of key infrastructure systems and the sense of social security are becoming global and increasingly complicated. Information, although an intangible resource, has become one of the most important currencies in the world.

Each of the above-mentioned systems is vulnerable to failure or destruction, which may be caused by natural or technical factors, as well as intentional human action. The current tense international situation and the aggressive policy pursued by the Russian Federation towards all countries it considers hostile require a special approach to protection against sabotage, diversion, and disinformation activities. At the same time, it should be emphasised that the functioning of the state, whether in a state of peace, crisis, or war, is determined by maintaining the state's defence readiness based on the efficiency of its structures (Bsoul-Kopowska, Skrabacz, Rodzik, 2022, p. 108). However, the effectiveness of protection against threats also depends to a large extent on public awareness of their existence and the ability to predict, recognise, and neutralise them, with preventive measures also being important.

The traditional way to identify threats was to assess the intentions and potential of potential enemies to cause harm. However, it ignored the complexity introduced by non-state actors and emerging technologies (Rickli, Vllasi, 2025, p. 92). Therefore, both state structures, enterprises, and individuals should always take into account all possible risk assessment factors, technological, social and organisational, and the approach to security should be holistic (Kaczmarek, Karpiuk, Melchior, 2024, p. 105).

In connection with this, the authors of this article decided to put forward a hypothesis that contemporary conflicts increasingly often take the form of hybrid actions, in which the key role is played by attacks on critical infrastructure and psychological and information operations conducted in conditions of formal peace. To verify it, it was decided to analyse the literature on the subject and apply the a behavioral approach aimed at analyzing human behavior in crisis situations caused by hybrid actions. The methodology also includes a polemological approach and case studies of hybrid actions of the Russian Federation conducted against Western countries.

1. Evolution of the concept of hybrid threats

The terms "hybrid threats" and "hybrid warfare" are commonly used today both in public discourse and in academic literature on broadly understood security. Although they are not new concepts, they have only gained importance in recent years, becoming one of the key elements of analyses of contemporary threats.

The literature on the subject defines hybrid warfare as a planned conflict conducted during theoretical peace. Its elements include actions carried out by various entities aimed at weakening the sphere of national security. These actions are referred to as hybrid threats and consist of deliberate and coordinated actions aimed at maintaining crisis situations and achieving political and strategic goals (Goleński, Zimny, 2024, p. 33).

One of the first researchers to describe the concept of hybrid warfare in detail was Frank Gregory Hoffman, author of the 2007 work Conflict in the 21st Century: The Rise of Hybrid Wars . Referring to Hezbollah's actions against Israel, Hoffman proposed a definition of hybrid threats as a set of various forms of hostile activity – from conventional actions, through irregular tactics and formations, to acts of terrorism and organised crime. He described hybrid warfare as a phenomenon combining the lethality of traditional military operations with the fanaticism and duration of irregular conflicts (Hoffman, 2007a, p. 8). The essence of hybridity – as he emphasised – is not only the combination of different means of action, but also their diverse organisational structures (Hoffman, 2007a , p. 28). In another publication, Hoffman also pointed out that future conflicts would be characterised by increasing unpredictability and ruthlessness of actions, which would significantly hinder effective counteraction (Hoffman, 2007b, p. 58).

In turn, Frank J. Cilluffo and Joseph R. Clark emphasise the lack of effective and universal defence mechanisms against hybrid threats, which makes them particularly difficult to neutralise both at the strategic and operational level (Cilluffo, Clark, 2012, p. 47). Erik Reichborn-Kjennerud and Patrick Cullen point out that the very concept of hybrid warfare is constantly evolving, which makes it impossible to define it unequivocally. This problem does not only concern hybrid warfare as a form of conflict, but also the very concept of hybrid threats, which, despite its growing popularity, remains a vague term (Reichborn-Kjennerud, Cullen, 2016, p. 1). Susana Sanz -Caballero points out that perhaps instead of striving for a precise definition, we should rather focus on a deep understanding of the nature of these threats and their specific mechanisms of action (Sanz -Caballero, 2023, p. 2).

The aforementioned Frank Gregory Hoffman deepened his approach to hybrid threats, indicating that their essence is not limited to the combination of means and tactics, but also includes advanced coordination of actions and innovative use of existing systems. In an article published in 2010, Hoffman emphasised that hybrid wars can be conducted by both states and a wide range of non-state actors. He also noted that these actions are often synchronised on both the physical and psychological levels, which allows for achieving synergistic effects that are difficult to counteract with traditional defence mechanisms (Hoffman, 2010, p. 443).

Hoffman also noted that hybrid forces can effectively incorporate modern technologies into the structure of armed forces and their operational strategies, often using them in a way that deviates from the original assumptions of their use. In his view, these forces can gain an operational advantage over Western forces by operating in narrow, strictly defined operational areas. Such an ability to adapt and quickly break the linear model of conflict makes hybrid threats particularly difficult to predict and neutralise (Hoffman, 2010, p. 444). Therefore, such actions allow aggressors to take control of the attacked country without any kinetic actions (Genini, 2025, p. 126). It should also be emphasised that well-planned, prepared and implemented hybrid actions can be extremely effective. The combination of a distorted historical narrative, disinformation, and false flag operations can even lead to a state, region, or social group seemingly voluntarily agreeing to be controlled by a hostile entity. It is also important to note that decisions made on the basis of incomplete or manipulated data are not, in fact, autonomous.

2. Hybrid threat: case analysis

An example of an information and psychological operation, which was an element of hybrid actions, was the preparation by the Russian Federation to take control of the Autonomous Republic of Crimea, which belonged to Ukraine, in 2014. For a long time, Russia conducted actions aimed at building a positive image of its soldiers among the residents of the Republic as defenders of the local population and those who can correct the "historical mistake" of annexing Crimea to Ukraine in 1954. It should also be taken into account that every second resident of the largest city of the Republic, Sevastopol, was associated with the Russian Black Sea Fleet, and 24,000 Russian soldiers lived in the city permanently. For Sevastopol, the army and the Black Sea Fleet meant work and social infrastructure. Therefore, the introduction of Russian armed forces to Crimea and Sevastopol took place met with virtually no opposition from the local population. The annexation of Crimea showed that it was a well- planned and organised operation. It should be noted that pro-Russian organisations in the Republic of Crimea were used as the fifth column (Khoroshko et al, 2022, p. 5).

Furthermore, jamming GPS signals in the Baltic Sea and its surroundings should be treated as an element of hybrid activities. Most of the time, this signal is jammed or faked, and the source is mainly ships located in international waters. Often recipients are deceived by a false GPS signal or retransmission of a previously recorded signal in a different place and time. As a result, the recipient reads an incorrect position or time (Landowski, 2025). Experts clearly point to the actions of the Russian Federation as the primary source of these disruptions (Reuters, 2025).

Although such activities mainly focus on the physical signal infrastructure, an equally important area of hybrid threats remains attacks aimed at users of digital systems, including social engineering techniques such as phishing , which is largely based on social engineering techniques, the most effective countermeasure strategy is to constantly increase user awareness (Birthriya, Ahlawat, Jain, 2025, p. 6). An indispensable element of hybrid activities are also disinformation threats related to influence operations (Dov Bachmann, Putter, Duczynski, 2023, p. 866). Such activities pose serious threats to state security, and Russia, especially in the countries of the former Eastern Bloc, has long been conducting activities aimed at taking control over them. The effectiveness of the Russians is evidenced by the mass anti-government and pro-Russian demonstrations in the Czech Republic in the autumn of 2022 (Cabada, 2023, p. 381).

Hybrid actions aimed at weakening state structures also involve weakening citizens' trust in the state. This involves, among other things, reducing the level of citizens' sense of security. Meanwhile, this is the basic duty of the state and is one of its basic functions (Włodyka, 2024, p. 30). Currently, Russia is intensifying hybrid actions against NATO countries, combining disinformation campaigns, cyberattacks, sabotage and border provocations with the use of migration. It is also increasingly using aggressive methods such as arson, acts of vandalism, and violence against public figures. In recent years, saboteurs inspired by Russian services have attacked civilian and infrastructure targets in Poland, the Baltic states, France, and the United Kingdom.

Arms plants and military installations are also becoming targets; these actions are intended to limit Western support for Ukraine. Russia recruits untrained people for these operations, often from the margins of society or those in personal crisis, offering payment from illegal sources of finance (for example, cryptocurrencies), which makes it difficult to identify clients and other participants in the procedure. In parallel, cyberattacks are carried out against military transport and systems, as well as the previously mentioned GPS signal jamming operations, which affect the safety of air traffic and the functioning of services. Russian services also order terrorist actions against people involved in the production of weapons. These actions serve to intimidate societies and weaken the West's determination to support Ukraine (Bryjka, 2024).

To sum up this part of the analysis, it should be emphasised that the current security environment of Western countries, especially those unequivocally supporting Ukraine in its defensive war with Russia, is so complicated that any event resulting in damage may potentially be the result of hybrid activities. It should be remembered that Russia has been building its structures and influence in other countries for a long time. Due to many years of indoctrination and still vivid nostalgia for the past, this is especially visible in the former Soviet republics (Nistor, Stretea, 2025) and former Eastern Bloc countries (Kekstaite, Vandevoordt, 2025). In this context, the ability of states to quickly and effectively recognise and attribute hybrid threats and adapt countermeasures is of key importance.

3. The role of information during hybrid operations

The international security situation has been in constant change for some time now and unfortunately, at least partly, it is heading in a worse direction. States have rediscovered previously used methods and improved them in order to exert even stronger pressure on the opponent, achieving their political goals faster, more effectively and cheaper. In hybrid operations, conventional and unconventional means are combined and flexibly adapted to the given situation. This activity takes the form of various attempts to influence the political, economic, military, information, and infrastructural structures of society. Attempts to arouse social unrest on a larger scale can also be observed. The aim is to exert effective influence on the physical environment and especially on the mind of the opponent. The behaviour of the opponent is directed in the desired direction – partly even by means that he himself does not notice (Turvallisuuskomitea, 2016, p. 3).

Hybrid threats are complex and difficult to grasp. They challenge established practices for dealing with crisis situations. The activities of security services alone – even at the highest level – are not enough to effectively protect society. An attacker can strike by surprise and simultaneously at all key state functions, adjusting the intensity of actions in individual areas at his own discretion. Sometimes it is almost impossible to distinguish between truly hostile, aggressive actions and seemingly ordinary forms of international relations, in which each state protects its interests as best it can. Are partially camouflaged threats still an element of normal diplomacy or is hybrid influence aimed at hindering decision-making processes in the state? Are additional border controls or customs a deliberate attack on our economy? How should we treat large military exercises organised near our borders? It is also necessary to consider whether alternative media are operators of information operations (Turvallisuuskomitea, 2016, p. 3).

Finding answers to these questions can increase the level of resilience of societies and states to hybrid threats. In this context, international cooperation, exchange of experiences, and use of proven solutions also play a major role. It should always be remembered that hybrid operations are complex and multidimensional. They can cover a wide range of seemingly independent, but in reality coordinated, and often discrete, actions. Influence operations can, for example, begin with seemingly neutral information, the purpose of which is to change the behaviour of individuals and societies, which can ultimately programme electoral preferences and lead to a change in the policy pursued by the state or even hinder the state's actions in the face of crisis situations that are particularly painful for the civilian population.

Modern conflicts take place in the sphere of the human mind, which is becoming a new battlefield. Cognitive warfare, now considered another domain of military operations, uses data, information, and knowledge as non-kinetic weapons to manipulate perception, create uncertainty, and weaken the enemy's ability to make decisions. In the digital era, the information space has become extremely susceptible to such influences, which requires counterintelligence activities and a new approach to protecting societies. Traditional information warfare, focused on disrupting information systems, is transforming into a more advanced knowledge war, in which the advantage is gained by those who can better capture, process and use information. The concepts of data, information, and knowledge are today combined into a broader concept of „content", which becomes a tool in the fight for influence and domination. In this context, the war for narrative is not only a dispute over truth, but also a fight for power over the knowledge and interpretation of reality (Putter, 2025, pp. 173-174). The effectiveness of such actions appears to be indicated by the ideological and cultural divisions in Europe, which became visible after Russia's attack on Ukraine in 2022 (Bliuc, Muntele-Hendreș, 2025, p. 2) Such deep divisions did not appear suddenly or spontaneously. They must have existed much earlier, and it is worth arguing that this was due to Russia's long-established influence in Europe (Kaczmarek, 2024).

In the area of building resilience to the cognitive element of hybrid warfare, all possible factors must be taken into account, including historical, cultural, social, religious, and natural-climatic contexts. Therefore, each community, society, and state must build its resilience in a way that is adapted to all contextual factors. Direct implementation of a solution that is effective in one place may not bring the desired effects in another environment, even if it is exposed to similar threats.

Conclusions

The analysis conducted in this article leads to the conclusion that contemporary conflicts are increasingly taking on the character of hybrid actions, in which the main battlefield is no longer only physical space, but also – and perhaps primarily – the information and cognitive sphere. Hybrid threats are not homogeneous or time-limited. Their specificity lies in combining various, often difficult to clearly identify, means of influence dynamically adapted to the current political and social situation. In this context, the research hypothesis is confirmed, according to which hybrid actions, including attacks on critical infrastructure and psychological and information operations, are currently a fundamental element of confrontational strategies used by states and non-state actors.

In particular, it should be emphasised that hybrid operations are often a prelude to kinetic actions or their supplementation. Examples of sabotage, diversion, or disinformation show that non-kinetic means can prepare the ground for force actions or accompany them, increasing their effectiveness. A well-planned information operation, supported by psychological pressure and social destabilisation, can significantly limit the state's ability to react even before the actual conflict begins. In this sense, hybrid action precedes traditional forms of aggression and reduces the need for their use, which does not exclude their use, on the contrary, it can effectively legitimise them in the eyes of part of the enemy's society.

At the same time, it should be noted that the effectiveness of hybrid operations is largely based on the use of existing social divisions, a deficit of trust in public institutions, and the lack of cognitive resistance of citizens. The enemy does not have to operate using armed forces if they are able to manipulate perception, destabilise public debate and influence political decisions through seemingly legal or neutral actions. In this context, not only the readiness of state structures becomes important, but also social awareness and the resistance of citizens to disinformation and psychological actions.

Hybrid threats are also a phenomenon strongly rooted in local conditions. As the analysis shows, the effectiveness of countering this type of threat depends on specific cultural, historical, and sociopolitical factors. There is no universal resilience model that can be directly adapted from one country to another. Therefore, it is so important to conduct individual diagnoses based on the analysis of risks and contexts specific to a given society.

In an era of high dynamism of threats, hybrid actions are also an ideal tool for attacking the state and society simultaneously on many levels. Such actions can put the state, as the body responsible for the security of the nation, in the face of a sudden and extensive crisis situation, which will require specialists from various fields of science and appropriate technologies. In the face of such threats, it is crucial to build, above all, the resistance of society to disinformation and to shape appropriate habits.

In light of the above findings, it seems justified to formulate several recommendations. First, there is a need for systematic updating of national security mechanisms, taking into account the cognitive and informational dimension. Second, there is a need to expand educational and informational programmes aimed at shaping social resilience, in particular through the development of competences in the field of information analysis, recognition of manipulation, and critical thinking. Third, it seems essential to intensify international cooperation in the field of exchange of experiences, good practices, and early warning mechanisms. Finally, actions to counter hybrid threats should cover not only the security sector, but also education, media, local administration, and the technology sector, creating a coherent, integrated system of response and prevention.

The collected evidence proves that hybrid threats are persistent and evolving, and their effective neutralisation requires flexibility, reflexivity, and the ability to adapt from states. Otherwise, the risk of weakening internal cohesion and losing the ability to act independently will become a real scenario, even without a formal declaration of war.

References

Birthriya, S. K., Ahlawat, P., Jain, A. K. (2025). Detection and Prevention of Spear Phishing Attacks: A Comprehensive Survey. Computers & Security, 151, pp. 1-16. https://doi.org/1 0.1016/j.cose.2025.104317.

Bliuc, A. M., & Muntele-Hendreș, D. (2025). Narratives of moral superiority in the context of war in Ukraine: Justifying pro-Russian support through social creativity and moral disengagement. British Journal of Social Psychology, 64(2), pp. 1-21. https://doi.org/10.1111/bjso.12878.

Bryjka, F. (2024). Rosyjskie działania dywersyjne wobec państw NATO. https://pism.pl/publikacje/rosyjskie-dzialania-dywersyjne-wobec-panstw-nato.

Bsoul-Kopowska, M., Skrabacz, A., Rodzik, J. (2022). The crucial role of crisis management teams in public administration in the context of COVID-19. Polish Journal of Management Studies, 25(1), pp. 107–131.

Cabada, L. (2023). Struggle against Disinformation in the Czech Republic: Treading the Water. Politics in Central Europe, 19(1S), 371-391. https://doi.org/10.2478/pce-2023-0017.

Cilluffo, F. J., Clark, J. R. (2012). Thinking About Strategic Hybrid Threats – In Theory and in Practice, Prism, 4(1), pp. 46-63.

Dov Bachmann, S. D., Putter, D., Duczynski, G. (2023). Hybrid warfare and disinformation: A Ukraine war perspective. Global Policy, 14(5), pp. 858-869. http://dx.doi.org/10.1111/1758-5899.13257.

Genini, D. (2025). Countering hybrid threats: How NATO must adapt (again) after the war in Ukraine.NewPerspectives,33(2),pp.122 149. https://doi.org/10.1177/2336825X251322719.

Goleński, W. R., Zimny, D. (2024). Przygotowanie państwa na zagrożenia hybrydowe.Kontrola Państwowa, 5, pp. 18-37.

Hoffman, F. G. (2007a). Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington: Potomac Institute for Policy Studies.

Hoffman, F. G. (2007b). Preparing for Hybrid Wars. Marine Corps Gazette, 91(3), pp. 57-61.

Hoffman, F. G. (2010). 'Hybrid Threats': Neither Omnipotent Nor Unbeatable. Orbis, 54(3), pp. 441-455. https://doi.org/10.1016/j.orbis.2010.04.009.

Kaczmarek, K. (2024). Rosyjska dezinformacja jako element budowania wpływów w Europie: analiza i perspektywy. Roczniki Nauk Społecznych, 52(1), pp. 109-121.

Kaczmarek, K., Karpiuk, M., Melchior, C. (2024). A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data. Prawo i Więź, 3(50), pp. 103–121. https://doi.org/10.36128/PRIW.VI50.907.

Kekstaite, J., Vandevoordt, R. (2025). Departheid in the Post-Soviet Space? The Shifting Geopolitics and Racialisation of Migration Governance in Lithuania. Antipode, 57(4), pp. 1557-1575. https://doi.org/10.1111/anti.70020.

Khoroshko, V. et al. (2022). Methods of Preparing and Conducting Modern Hybrid Wars. Scientific and Practical Cyber Security Journal, 6(3), pp. 1-12.

Kochanek, E. (2020). Elektroenergetyczna infrastruktura krytyczna w województwie zachodniopomorskim – 10 lat po blackoucie. Przeglad Zachodniopomorski, 3, pp. 117–132. http://dx.doi.org/10.18276/pz.2020.3-06.

Landowski, G. (2025). Większość zakłóceń sygnałów GPS na Bałtyku pochodzi ze statków. Available at: https://www.portalmorski.pl/bezpieczenstwo/57712-wiekszosc-zaklocen-sygnalow-gps-na-baltyku-pochodzi-ze-statkow.

Nistor, R. M., Stretea, A. I. (2025). Dismiss, distort, distract, dismay: the civil society in Moldova in the face of disinformation. Civil Szemle, 22(1), pp. 177-194. https://doi.org/10.62560/csz.2025.01.11.

Putter, D. (2025). Navigating the interplay of cognitive warfare and counterintelligence in African security strategies: insights and case studies. Journal of Policing, Intelligence and Counter Terrorism, 20(2), pp. 173-192. .

Reichborn-Kjennerud, E., Cullen, P. (2016). What is Hybrid Warfare?. Norwegian Institute for International Affairs, 1, pp. 1-4.

Rickli, J. M., Vllasi, G. (2025). The Weaponization of Emerging Technologies and Their Impact on Global Risk: A Perspective from the PfPC Emerging Security Challenges Working Group. Connections: The Quarterly Journal, 24(1), pp. 91-112. https://doi.org/10.11610/Connections.24.1.07.

Sanz-Caballero, S. (2023). The concepts and laws applicable to hybrid threats, with a special focus on Europe. Humanities and Social Sciences Communications, 10(1), pp. 1-8. .

Turvallisuuskomitea. (2016). Katsaus hybridiuhkiin ja niiden vaikutuksiin: Turvallisuuskomitean kevätseminaari 2016 – seminaarijulkaisu (Julkaisusarja 9/2016).

Valtioneuvoston kanslia. Available at: https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/Katsaus_hybridiuhkiin_TK2016.pdf.

Włodyka, E. M. (2024). The Local Government Units Along The Coastal Strip of The Republic of Poland: Implementation Policy Regarding Their Autonomous Tasks in The Field of Healthcare. Selected Seasonal Safety Issues. Online Journal Modelling the New Europe, 46, pp. 30-51. https://doi.org/10.24193/OJMNE.2024.46.02.

Włodyka, E. M., Kaczmarek, K. (2024). Cyber Security of Electrical Grids – A Contribution to Research. Cybersecurity and Law, 12(2), pp. 260-272.

Zakrzewska, S., Gil-Świderska, A. (2018). Energetyczna infrastruktura krytyczna w Polsce – perspektywy i zagrożenia. Rynek Energii, 5(138), pp. 55-64.

Other sources

Reuters (2025). Poland says GPS disruptions over Baltic could be related to Russia. Available at: https://www.reuters.com/business/aerospace-defense/poland-says-gps-disruptions-baltic-could-be-related-russia-2025-06-17.