Dr. Krzysztof Kaczmarek
Faculty of Humanities
Koszalin University of Technology
ORCID: 0000-0001-8519-1667
puola@tlen.pl

# CRITICAL INFRASTRUCTURE SECURITY IN FINLAND: STRATEGIES, CHALLENGES AND GOOD PRACTICES

**Abstract**

The article analyses the challenges and strategies to protect critical infrastructure in Finland. It also presents the historical and geopolitical context in which the country's security policy was shaped. Particular attention is paid to the immediate vicinity of Russia and hybrid threats. It also discusses practical actions of Finnish authorities aimed at increasing the resilience of the country. It also analyses the role of society in counteracting acts of sabotage.
Case studies, qualitative analyses, and a polemological approach allowed a positive verification of the research hypothesis, which assumed that Finland's experience in the field of critical infrastructure protection can be used by other countries.

**Keywords:** Finland, Security, Critical Infrastructure, Hybrid Threats, Russia.

## INTRODUCTION

Critical infrastructure security is currently one of the main pillars of state security, and the dynamically changing security environment means that countries whose proper functioning requires effective protection of critical infrastructure are facing constantly emerging challenges in this area[1]. In this respect, Finland's situation is special and the experience of this country can be used by other countries exposed to similar threats. However, it should be emphasised that the factors of threats occurring in a given country depend on many factors, most often political, but also military and economic, and are characteristic of that country. In the case of Finland, as in other countries on the eastern flank of the European Union (EU) and the North Atlantic Treaty Organisation (NATO), the greatest threat is posed by the hybrid actions of the Russian Federation.

[1]M. Czuryk, Cybersecurity and Protection of Critical Infrastructure, "Studia Iuridica Lublinensia" 2023, No. 5, p. 50.

Historically, Finland's foreign and security policy has been largely linked to developments in Russia and the threat it may pose to Finland[2], and throughout the period from the end of World War II to the collapse of the Soviet Union (USSR), the most important issue for Finnish foreign policy was finding its own way in the changing geopolitical situation[3]. Finland's foreign policy at that time was to refrain from involvement in any international disputes or conflicts. It was not until Russia's full-scale invasion of Ukraine, which began on 24 February 2022, that Finland decided to join NATO, becoming a full member of the alliance on 4 April 2023. This led to the intensification of Russia's hostile hybrid activities against that country, some of which are attacks, including cyberattacks, on critical infrastructure[4]. Due to its location and history of relations with Russia, Finland's experience in preventing hybrid threats can be a reference point for other countries.

The aim of this article is to analyse the challenges in the area of critical infrastructure protection that Finland has been facing since joining NATO and its strategy to counteract threats, especially those aimed at critical infrastructure. The adopted research hypothesis assumes that Finland's experience in the field of critical infrastructure protection can be used by other countries. To verify this hypothesis, a polemological approach and a comparative method supplemented by qualitative analyses were used. Case studies were used to illustrate practical aspects of critical infrastructure protection and threat prevention.

## NATURE AND SOURCES OF HYBRID THREATS TOWARDS FINNISH CRITICAL INFRASTRUCTURE

The essence of hybrid threats is their ambiguity and multidimensionality, and the goal of such actions is to destabilise the state and weaken it internally[5]. Hybrid warfare, on the other hand, is a specific operational whole, which consists of all forms of military and nonmilitary actions conducted in all dimensions of social life[6]. One of the vectors of propagation of hybrid actions is cyberspace, which can be used to attack critical infrastructure. Therefore, ensuring cybersecurity is one of the elements of defence against such threats.

---

[2] K. Kaczmarek, Finland in a Geopolitical Perspective - From Finlandization to Integration with NATO, "Przegląd Nauk o Obronności" 2024, No. 19, p. 9.
[3]U. Kekkonen, Nie szukajcie przyjaciół daleko, a wrogów blisko, Warszawa 1983, p. 88.
[4] M. Pesu, Logiczne, ale nieoczekiwane - droga Finlandii do NATO z bliskiej perspektywy, „NATO Review" 2023, https://www.nato.int/docu/review/pl/articles/2023/08/30/logiczne-ale-nieoczekiwane-droga-finlandii-do-nato-z-bliskiej-perspektywy/index.html accessed 15.04.2025.
[5] W. R. Goleński, D. Zimny, Przygotowanie państwa na zagrożenia hybrydowe – konieczność natychmiastowych działań, „Kontrola Państwowa" 2024, No. 5, p. 25.
[6] M. Marciniak, Hybrydowa wojna powietrzna, [in:] A. Radomyski, P. Malinowski, D. Michalski (ed.), Wyzwania i rozwój obrony powietrznej Rzeczypospolitej Polskiej: obronność RP XXI wieku, Dęblin 2018, p. 34.

At the same time, ensuring information security and cybersecurity requires constant adaptation to changing conditions, and security issues must be taken into account in every development process and daily activities. Every country, every industry, every institution, and digital service has its own characteristics. For this reason, ensuring security in the digital domain must be planned based on the specifics of a given entity. It should also be noted that there is no possibility of protection against digital threats only through actions at one level or within one organisation. The same principle applies to countries that are currently connected by a network of international connections, and their residents often use network services whose centres are located beyond their borders. The nature and sources of cyber threats mean that international cooperation and the exchange of experiences within organisations, alliances or bilateral relations are of great importance in combating them. This allows for drawing on the experiences of others, avoiding the repetition of mistakes, and taking preventive measures together. Therefore, the approach to cybersecurity in the context of protecting critical infrastructure should be holistic and take into account all possible factors, both social and technical, while remembering that an effective digital attack can have serious consequences and negatively affect every aspect of the functioning of individuals, societies, and states[7].

However, it should be noted that in the Finnish legal system the concept of critical infrastructure is not defined, and a relevant draft act on protecting critical infrastructure for society and improving resilience was submitted to Parliament by the government on 19 December 2024[8]. However, according to the subject literature, critical infrastructure in Finland includes: power plants and energy grids (e.g., electricity, oil and gas production plants, storage and refining plants, transmission and distribution systems); communications and information technologies (e.g., telecommunications and broadcasting systems, computer software and hardware, and communication networks such as telephone networks or the Internet); financial sector (e.g., banking, securities and investment services); healthcare (e.g., hospitals, healthcare and blood services, laboratories and pharmacies, search and rescue services, emergency services); food (e.g., food safety, production facilities, wholesale distribution, food industry, etc.); water (e.g., dams, water storage facilities, treatment and water supply networks). transport (e.g. airports, ports, railways, public transport

[7] K. Kaczmarek, M. Karpiuk, C. Melchior, A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data, "Prawo I Więź" 2024, No 3, p. 118.

[8]Ministry of Internal Affairs (Finland), Government proposes new act to guide improvement of resilience and protection of infrastructure critical to functioning of society, https://valtioneuvosto.fi/en/-/1410869/government-proposes-new-act-to-guide-improvement-of-resilience-and-protection-of-infrastructure-critical-to-functioning-of-society?utm accessed 15.04.2025.

networks, traffic control systems); production, storage, and transport of dangerous goods (e.g. chemical, biological, radiological, and nuclear materials); public sector (e.g. essential services, institutions, information networks, assets, sites, and monuments of national importance)[9].

However, hybrid activities also include sabotage and diversionary activities. Since such operations require preparation, one way to build the potential for hybrid activities in Finland is for individuals and entities associated with Russia to purchase real estate located in strategic locations that are important for the country's defence and supply security[10]. In connection with this, the Finnish authorities are preparing legislative solutions that will prevent citizens of countries that are waging an aggressive war and may pose a threat to national security from purchasing real estate. This ban will not apply to people with dual citizenship[11]. However, in the future, the purchase of real estate by people with such dual citizenship will have to be approved by the Finnish Ministry of Defense[12]. At the same time, it is planned to tighten the measures on the verification of the advisability of such purchases. Currently, many transactions are blocked if the buyer is associated in any way, directly or indirectly, with entities that may potentially constitute a base of operations for attacks on critical infrastructure and threaten state security[13]. In the context of crisis management and critical infrastructure protection, such actions by the Finnish authorities are part of preventing crisis situations caused by interruptions in the proper functioning of services that are crucial to society.

## SABOTAGE ACTIVITIES, COUNTERACTING THEM, AND THE ROLE OF FINNISH SOCIETY

Preventing damage to critical infrastructure also means cooperation between the services responsible for state security and society, and the awareness of individuals that such cooperation allows for an increase in their level of security. When a series of water supply break-ins occurred throughout Finland in June 2025, the Finnish services appealed to the public to pay attention, for example, to suspicious passersby and drone flights near water

[9] A. Hagelstam, CIP – Kriittisen infrastruktuurin turvaaminen. Käsiteanalyysi ja kansainvälinen vertailu, Huoltovarmuuskeskus, Julkaisuja 1/2005, Helsinki 2005.
[10] A. Gustafsson, Ulkomaalaisten kiinteistön omistamisen rajoitukset Suomessa. Theseus, pp. 23-24.
https://www.theseus.fi/bitstream/handle/10024/858205/Gustafsson_Albert.pdf?sequence=2 dostęp 15.04.2025.
[11]M. Tanner, Venäläisten kiinteistökaupat kielletään, “Iltalehti”, https://www.iltalehti.fi/politiikka/a/7e6a9e86-e7f3-4328-b0b6-05517c31e61d accessed 16/04/2025.
[12]Ministry of Defense (Finland), A permit to non-EU and non-EEA buyers to buy real estate, https://www.defmin.fi/en/licences_and_services/authorization_to_non-eu_and_non-eea_buyers_to_buy_real_estate#e00f2787 accessed 16/04/2025.
[13] E. Kilpinen, I. Ritvanen, Ministeri esti kuusi kiinteistökauppaa Itä-Suomessa – tällaisia ne ovat, https://yle.fi/a/74-20109903 accessed 16.04.2025.

supply networks and critical energy infrastructure, especially at unusual times. According to the Finnish Security and Intelligence Service (Supo), the threat associated with intelligence gathering and influencing Finland's critical infrastructure has increased. According to its response, society has strengthened its readiness to respond to such threats in recent years. The authorities have previously informed key service providers about the importance of reviewing their own security arrangements[14]. Since, according to European intelligence services, Russia is behind most sabotage attacks, threats to critical infrastructure from this country occur throughout Europe. At the same time, Russia uses criminal groups for its own purposes[15].

It should be noted here that acts of sabotage of critical infrastructure can serve not only to damage or destroy them, but also to find weak points and prepare for future actions[16]. At the same time, threats to critical infrastructure can occur in both the physical and digital environment[17]. Therefore, monitoring such events serves not only to prevent crisis situations, but can also provide information about the intentions of hostile state actors. It should also be taken into account that attacks on critical infrastructure can pose serious threats to human health and life. Therefore, in order to increase the effectiveness of critical infrastructure protection, in January 2024, the Ministry of Justice of Finland prepared a draft extension of the Security Clearance Act so that in the future it would be possible to carry out a basic verification of the security clearance also in relation to persons who receive classified information about critical infrastructure[18].

When analysing threats to critical infrastructure and ways to protect it, especially in countries that Russia considers hostile, a polemological approach should be used. This is due to the fact that currently the countries supporting Ukraine in its defensive war with Russia are also in a state of war. Currently, the borders are not crossed by armed forces, but there is

[14] M. Jäntti, J. Ojala, Supo ja Poliisihallitus: Vaikuttamisen uhka kriittiseen infraan kasvanut, https://yle.fi/a/74-20098010 accessed 16.04.2025.
[15] L. O'Carroll, Russia using criminal networks to drive increase in sabotage acts, says Europol, "The Guardian" 18 March 2025, https://www.theguardian.com/technology/2025/mar/18/russia-criminal-networks-drive-increase-sabotage-europol accessed 16.04.2025.
[16] K. Kaczmarek, Znaczenie Laponii w budowaniu potencjału obronnego Finlandii, „Studia Społeczne" 2024, No. 2, p. 30.
[17] J. Terho, T. Wathén, Eurojärjestelmän kyberstrategia Suomeen, "Euro & talous" 2023, No. 5, p. 4, https://publications.bof.fi/bitstream/handle/10024/53136/Kyberstrategia_ET_5_2023.pdf?sequence=1 accessed 17.04.2025.
[18] The Ministry of the Interior (Finland), Government to improve protection of infrastructure critical to functioning of society, https://intermin.fi/-/yhteiskunnan-toimintakyvyn-kannalta-kriittisen-infrastruktuurin-suojaamista-parannetaan?languageId=en_US accessed 17.04.2025,

increased sabotage, diversion, and terrorist activity, which is inspired by Moscow[19].

Another threat to critical infrastructure, which is of great importance not only to the security of Finland but also of the whole of Europe, is the activity of the Russian "shadow fleet", i.e., ships belonging to different owners and sailing under different flags, which are used by the Russian Federation to bypass international sanctions imposed on that country and to destroy critical infrastructure. The shadow fleet is credited with damaging the Balticconnector gas pipeline connecting the gas systems of Estonia and Finland in early October 2023. On 8 November 2024, the C-Lion1 communication cable connecting Finland with Germany was severed, and a few days later the BCS East-West Interlink fibre-optic cable connecting Lithuania with Gotland[20].

As the above examples show, the damage and destruction of critical infrastructure can have a negative effect in many countries. This is because the increasing integration of Europe has led to the development of cross-border cooperation[21]. This leads to the conclusion that no state is able to function economically or confront threats alone, and the concept of state security is associated with both the national and international levels[22].

## TECHNOLOGIES, POLICIES AND SYSTEMIC RESILIENCE

An important vector of attacks on critical infrastructure is cyberspace. Currently, digital services are the basis for the functioning of public administration[23], and digital skills are essential[24]. At the same time, cyber threats have a significant impact on national security[25]. It should also be emphasised that counteracting cyber threats consists of not only the use of appropriate technical measures, but also the conscious and responsible use

[19] F. Bryjka, Rosyjskie działania dywersyjne wobec państw NATO, "The Polish Institute of International Affairs" 2024, Strategic File No. 112, https://www.pism.pl/publikacje/rosyjskie-dzialania-dywersyjne-wobec-panstw-nato accessed 17.04.2025.

[20] D. Szacawa, J. Bornio, „Wartownik Bałtyku" – odpowiedź NATO na działania sabotażowe Rosji na Bałtyku, "The Polish Institute of International Affairs" 2025, Strategic File No. 1267, https://ies.lublin.pl/komentarze/wartownik-baltyku-odpowiedz-nato-na-dzialania-sabotazowe-rosji-na-baltyku/ accessed 17.04.2025.

[21] M. Bielecka, Wsparcie społeczne dla uchodźców z Ukrainy na tle partnerstwa miast i gmin z województwa zachodniopomorskiego, „Ius et Securitas" 2024, No. 1, p. 22.

[22] E. Tkaczyk, Bezpieczeństwo państwa w Konstytucji Rzeczypospolitej Polskiej. Refleksje nad dobrem chronionym, „Ius et Securitas" 2024, No. 1, p. 42.

[23] E. M. Włodyka, Dostępność cyfrowa w Unii Europejskiej – praktyka i założenia teoretyczne, „Rocznik Integracji Europejskiej" 2022, No. 16, p. 356.

[24] E. Włodyka, Dlaczego potrzebujemy e-administracji? Rozwój podstawowych umiejętności cyfrowych pracowników administracji na Pomorzu Zachodnim, „Acta Politica Polonica" 2021, No. 2, p. 95.

[25] A. Bencsik, M. Karpiuk, M. Kelemen, E. Włodyka, Cybersecurity in the Visegrad Group Countries, Maribor, 2023, p. 5.

of digital tools[26]. However, the speed of changes means that individuals are unable to keep up with them, and modern man experiences pressing problems created by the civilisation of the world around him: military, ecological, moral, economic or political threats[27]. It should also be taken into account that new technologies are not the domain of one country, but shape international policy[28] and transform the way individuals and states function[29]. It is also important that advanced technologies such as artificial intelligence can be used for both attack and defense[30].

All this means that each element of critical infrastructure functions properly only in connection with the others. Serious damage or destruction of telecommunications infrastructure means lack of access to financial resources, paralysis of transport control systems and some medical services, lack of control and management of power grids. And this can cause disruptions in electricity supplies and stop the work of all other elements of critical infrastructure[31].

Political conflicts may be a possible problem in protecting key facilities and structures. However, it is important that political antagonisms do not affect the shape of the state's defence in the face of qualified external threats, because in such a case the good of the state must always have priority, and they not only extend the time for making a decision but can also distort it[32].

While the survey results still seem to characterise the Finnish political system as consensus-based cooperation between ideological and interest boundaries, it seems that the belief of Finnish decision-makers in the common public interest has somewhat waned. Although in 2009 two-thirds of the respondents were classified as pro consensus profiles, in 2019 only about half of the respondents were placed in this profile. The results describe a small but clear shift from a consensus-based and network-based decision-making method towards a more ideological decision-making method that relies more on the struggle for power. This may be a cyclical change, but it is also possible that the changes reflect a more permanent trend[33].

[26]E. M. Włodyka, K. Kaczmarek, Cyber Security of Electrical Grids – A Contribution to Research, "Cybersecurity and Law" 2024, No. 2, p. 263.
[27] A. Pieczywok, Złożoność zagrożeń egzystencji człowieka – wybrane zagadnienia, „Ius et Securitas" 2024, No. 1, p. 6.
[28] C. Gaie, M. Karpiuk, A. Spaziani, New Technologies in Public Administration, "Ius et Securitas" 2024, No. 2, p. 50.
[29] K. Kaczmarek, M. Karpiuk, U. Soler, The Potential Use of Artificial Intelligence in Crisis Management, "Sicurezza, Terrorismo e Società" 2024, No. 2, p. 142.
[30]T. Gergelewicz, Bipolarity of Artificial Intelligence – Chances and Threats, "Ius et Securitas" 2024, No. 2, p. 72.
[31] M. Karpiuk, W. Pizło, K. Kaczmarek, Cybersecurity Management – Current State and Directions of Change, "International Journal of Legal Studies" 2023, No. 2, p. 647.
[32] M. Karpiuk, Pozycja prawno-ustrojowa Prezydenta Rzeczypospolitej Polskiej w sferze obronności, „Ius et Securitas" 2024, No. 1, p. 57.
[33] E. Reunanen, R. Kunelius, Suomalaiselle poliittiselle järjestelmälle erityinen konsensuspolitiikka säröilee ja politiikka palaa politiikkaan, kertoo uutuuskirja,

However, the most important thing is that this type of cooperation between political groups increases the state's defence capabilities.

## CONCLUSIONS

The contemporary security environment is uncertain and unpredictable[34], and the imperial policy of the Russian Federation is unpredictable. It can even be assumed that contemporary international relations are based on the assumption that the enemy of my enemy is my friend[35]. At the same time, Finland is in a special position, being treated by Russia as a hostile state, especially since its accession to NATO in 2023. This special position is also due to historical experience and a long direct border with Russia.

Current hybrid threats to which Finland is exposed include disinformation, diversion, sabotage, and cyberattacks. It should also be emphasised that in Finland the concept of critical infrastructure is not defined at the statutory level. However, facilities and systems that are critical to the functioning of society and the state are under special protection. Since Finland is characterised by a high level of trust of citizens in the government, an important means of protecting critical infrastructure is information from the public. The regulations in force in Finland assume that every resident of the country should find shelter in the event of a threat[36].

The historical experience and geographical location of this country have resulted in its security policy and the way it functions in the international arena being shaped in an environment of constant threat from Russia. Therefore, the adopted research hypothesis, which assumes that Finland's experience in the field of critical infrastructure protection can be used by other countries, has been verified positively.

## Bibliography

Bencsik A., Karpiuk M., Kelemen M., The Status of the Armed Forces in Hungary, Poland and Slovakia, „Ius et Securitas" 2024, No. 2.

Bencsik A., Karpiuk M., Kelemen M., Włodyka E., Cybersecurity in the Visegrad Group Countries, Maribor, 2023.

https://www.tuni.fi/fi/ajankohtaista/suomalaiselle-poliittiselle-jarjestelmalle-erityinen-konsensuspolitiikka-saroilee-ja accessed 18.04.2025.

[34] A. Bencsik, M. Karpiuk, M. Kelemen, The Status of the Armed Forces in Hungary, Poland and Slovakia, „Ius et Securitas" 2024, No. 2, p. 6.

[35] C. Partacz, K. Kaczmarek, The War in Ukraine and International Security: Challenges for Central and Eastern Europe, "Ius et Securitas" 2024, No. 2, p. 144.

[36] K. Kaczmarek, Finland's Security System: Lessons for Central and Eastern Europe, „Ius et Securitas" 2024, No. 2, p. 136.

Bielecka M., Wsparcie społeczne dla uchodźców z Ukrainy na tle partnerstwa miast i gmin z województwa zachodniopomorskiego, „Ius et Securitas" 2024, No. 1.

Bryjka F., Rosyjskie działania dywersyjne wobec państw NATO, "The Polish Institute of International Affairs" 2024, Strategic File No. 112, https://www.pism.pl/publikacje/rosyjskie-dzialania-dywersyjne-wobec-panstw-nato accessed 17.04.2025.

Czuryk M., Cybersecurity and Protection of Critical Infrastructure, "Studia Iuridica Lublinensia" 2023, No. 5.

Gaie C., Karpiuk M., Spaziani A., New Technologies in Public Administration, "Ius et Securitas" 2024, No. 2.

Gergelewicz T., Bipolarity of Artificial Intelligence – Chances and Threats, "Ius et Securitas" 2024, No. 2.

Goleński W. R., Zimny D., Przygotowanie państwa na zagrożenia hybrydowe – konieczność natychmiastowych działań, „Kontrola Państwowa" 2024, No. 5.

Gustafsson A., Ulkomaalaisten kiinteistön omistamisen rajoitukset Suomessa. Theseus. https://www.theseus.fi/bitstream/handle/10024/858205/Gustafsson_Albert.pdf?sequence=2 dostęp 15.04.2025.

Hagelstam A., CIP – Kriittisen infrastruktuurin turvaaminen. Käsiteanalyysi ja kansainvälinen vertailu, Huoltovarmuuskeskus, Julkaisuja 1/2005, Helsinki 2005.

Jäntti M., Ojala J., Supo ja Poliisihallitus: Vaikuttamisen uhka kriittiseen infraan kasvanut, https://yle.fi/a/74-20098010 accessed 16.04.2025.

Kaczmarek K., Finland in a Geopolitical Perspective - From Finlandization to Integration with NATO, "Przegląd Nauk o Obronności" 2024, No. 19.

Kaczmarek K., Finland's Security System: Lessons for Central and Eastern Europe, „Ius et Securitas" 2024, No. 2.

Kaczmarek K., Karpiuk M., Melchior C., A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data, "Prawo I Więź" 2024, No 3.

Kaczmarek K., Karpiuk M., Soler U., The Potential Use of Artificial Intelligence in Crisis Management, "Sicurezza, Terrorismo e Società" 2024, No. 2.

Kaczmarek K., Znaczenie Laponii w budowaniu potencjału obronnego Finlandii, „Studia Społeczne" 2024, No. 2.

Karpiuk M., Pizło W., Kaczmarek K., Cybersecurity Management – Current State and Directions of Change, “International Journal of Legal Studies” 2023, No. 2.

Karpiuk M., Pozycja prawno-ustrojowa Prezydenta Rzeczypospolitej Polskiej w sferze obronności, „Ius et Securitas” 2024, No. 1.

Kekkonen U., Nie szukajcie przyjaciół daleko, a wrogów blisko, Warszawa 1983.

Kilpinen E., Ritvanen I., Ministeri esti kuusi kiinteistökauppaa Itä-Suomessa – tällaisia ne ovat, https://yle.fi/a/74-20109903 accessed 16.04.2025.

Marciniak M., Hybrydowa wojna powietrzna, [in:] A. Radomyski, P. Malinowski, D. Michalski (ed.), Wyzwania i rozwój obrony powietrznej Rzeczypospolitej Polskiej: obronność RP XXI wieku, Dęblin 2018.

Ministry of Defense (Finland), A permit to non-EU and non-EEA buyers to buy real estate, https://www.defmin.fi/en/licences_and_services/authorization_to_non-eu_and_non-eea_buyers_to_buy_real_estate#e00f2787 accessed 16/04/2025.

Ministry of Internal Affairs (Finland), Government proposes new act to guide improvement of resilience and protection of infrastructure critical to functioning of society, https://valtioneuvosto.fi/en/-/1410869/government-proposes-new-act-to-guide-improvement-of-resilience-and-protection-of-infrastructure-critical-to-functioning-of-society?utm accessed 15.04.2025.

O'Carroll L., Russia using criminal networks to drive increase in sabotage acts, says Europol, “The Guardian” 18 March 2025, https://www.theguardian.com/technology/2025/mar/18/russia-criminal-networks-drive-increase-sabotage-europol accessed 16.04.2025.

Partacz C., Kaczmarek K., The War in Ukraine and International Security: Challenges for Central and Eastern Europe, “Ius et Securitas” 2024, No. 2.

Pesu M., Logiczne, ale nieoczekiwane - droga Finlandii do NATO z bliskiej perspektywy, „NATO Review” 2023, https://www.nato.int/docu/review/pl/articles/2023/08/30/logiczne-ale-nieoczekiwane-droga-finlandii-do-nato-z-bliskiej-perspektywy/index.html accessed 15.04.2025.

Pieczywok A., Złożoność zagrożeń egzystencji człowieka – wybrane zagadnienia, „Ius et Securitas” 2024, No. 1.

Reunanen E., Kunelius R., Suomalaiselle poliittiselle järjestelmälle erityinen konsensuspolitiikka säröilee ja politiikka palaa politiikkaan, kertoo uutuuskirja, https://www.tuni.fi/fi/ajankohtaista/suomalaiselle-poliittiselle-jarjestelmalle-erityinen-konsensuspolitiikka-saroilee-ja accessed 18.04.2025.

Szacawa D., Bornio J., „Wartownik Bałtyku" – odpowiedź NATO na działania sabotażowe Rosji na Bałtyku, "The Polish Institute of International Affairs" 2025, Strategic File No. 1267, https://ies.lublin.pl/komentarze/wartownik-baltyku-odpowiedz-nato-na-dzialania-sabotazowe-rosji-na-baltyku/ accessed 17.04.2025.

Tanner M., Venäläisten kiinteistökaupat kielletään, "Iltalehti", https://www.iltalehti.fi/politiikka/a/7e6a9e86-e7f3-4328-b0b6-05517c31e61d accessed 16/04/2025.

Terho J., Wathén T., Eurojärjestelmän kyberstrategia Suomeen, "Euro & talous" 2023, No. 5, https://publications.bof.fi/bitstream/handle/10024/53136/Kyberstrategia_ET_5_2023.pdf?sequence=1 accessed 17.04.2025.

The Ministry of the Interior (Finland), Government to improve protection of infrastructure critical to functioning of society, https://intermin.fi/-/yhteiskunnan-toimintakyvyn-kannalta-kriittisen-infrastruktuurin-suojaamista-parannetaan?languageId=en_US accessed 17.04.2025,

Tkaczyk E., Bezpieczeństwo państwa w Konstytucji Rzeczypospolitej Polskiej. Refleksje nad dobrem chronionym, „Ius et Securitas" 2024, No. 1.

Włodyka E. M., Dostępność cyfrowa w Unii Europejskiej – praktyka i założenia teoretyczne, „Rocznik Integracji Europejskiej" 2022, No. 16.

Włodyka E. M., Kaczmarek K., Cyber Security of Electrical Grids – A Contribution to Research, "Cybersecurity and Law" 2024, No. 2.

Włodyka E., Dlaczego potrzebujemy e-administracji? Rozwój podstawowych umiejętności cyfrowych pracowników administracji na Pomorzu Zachodnim, „Acta Politica Polonica" 2021, No. 2.

## BEZPIECZEŃSTWO INFRASTRUKTURY KRYTYCZNEJ W FINLANDII: STRATEGIE, WYZWANIA I DOBRE PRAKTYKI

### Streszczenie

W artykule dokonano analizy wyzwań i strategii ochrony infrastruktury krytycznej w Finlandii. Przedstawiony został również kontekst historyczny i geopolityczny, w którym ukształtowała się polityka bezpieczeństwa tego państwa. Szczególna uwaga została poświęcona bezpośredniemu sąsiedztwu Rosji i zagrożeniom hybrydowym. Omówiono również praktyczne działania władz Finlandii, których celem jest podniesienie odporności tego państwa. Przeanalizowano również rolę społeczeństwa w przeciwdziałaniu aktom sabotażu.

Studia przypadków, analizy jakościowe i podejście polemologiczne pozwoliły na pozytywne zweryfikowanie hipotezy badawczej, która zakładała, że

doświadczenie Finlandii na polu ochrony infrastruktury krytycznej mogą być wykorzystywane przez inne państwa.

**Słowa kluczowe:** Finlandia, bezpieczeństwo, infrastruktura krytyczna, zagrożenia hybrydowe, Rosja.