

The Role of Information Security In Protecting the Nation's Critical Infrastructure*

Patrycja LIPOLD¹, Grzegorz WISNIEWSKI², Mateusz CZEKAŁA³ and Robert SADOWSKI⁴

¹ WAR STUDIES UNIVERSITY
AV. ANTONIEGO CHRUŚCIELA 103, 00-910 WARSAW, POLAND

^{2,4} The International University of Logistics and Transport in Wrocław
51-168 WROCLAW STREET SOŁTYSOWICKA 19B, POLAND

³ GENERAL TADEUSZ KOŚCIUSZKO MILITARY UNIVERSITY OF LAND FORCES
WROCLAW, POLAND

Correspondence should be addressed to: Mateusz CZEKAŁA, mateusz.czekala@awl.edu.pl

*Presented at the 47th IBIMA International Conference, 29-30 June 2026, Madrid, Spain

Abstract

This paper addresses the issue of information security as a key determinant of the resilience of a nation's critical infrastructure in the era of digital transformation. The primary goal of the article is to demonstrate that in today's hybrid threat environment, protecting strategic facilities is impossible without ensuring the integrity and availability of data controlling technological processes. Authors argues that information security constitutes the "nervous system" of critical infrastructure, and its breach can lead to the paralysis of key services and the destabilization of state structures. The paper concludes by highlighting the need for a holistic approach to building resilience, combining the legal requirements of the NIS Directive with countering disinformation.

Keywords: critical infrastructure, information security, cybersecurity, facility protection

Introduction

The contemporary national security environment is undergoing dynamic transformations, primarily driven by the unprecedented digital revolution, which is redefining the functioning of modern societies. Increasing computerization and the ubiquitous automation of management systems in key economic sectors have led to the blurring of the previously distinct boundaries between the kinetic sphere and cyberspace. This process, referred to as the convergence of the physical and digital worlds, means that national security can no longer be analyzed in isolation from the processing, transmission, and protection of information. In an era of growing asymmetric and hybrid threats, information has ceased to function solely as a resource supporting administrative and management processes. It has evolved into a key resource, simultaneously becoming one of the main attack vectors, capable of destabilizing state structures without the need to engage conventional military forces. This is particularly evident in relation to the state's critical infrastructure, which forms the existential backbone of society. Energy, transportation, and ICT systems, which underpin the daily functioning of citizens, are now controlled by advanced algorithms and software, exposing them to entirely new categories of risk. The stability of strategic facilities is now inextricably linked to the integrity of the data that controls them. Disruptions in information flow in operational systems can lead to paralysis of the state's ability to provide critical services. Therefore, the aim of this study is to demonstrate that information security is not merely a security framework but is fundamental to the

resilience of critical infrastructure, and that proper information security management is therefore a prerequisite for maintaining the continuity of state operations.

With the above in mind, the aim of this article is to identify the functions of information security in a modern critical infrastructure protection system, from which the following research problem is defined: What impact does information security have on critical infrastructure protection? Its solution is a research hypothesis: it is assumed that information security is an essential and necessary component of a modern critical infrastructure protection system, exerting an increasingly greater influence due to the growing importance of hybrid threats and the digitization of the economy.

The following research methods were used in the following considerations: literature analysis, comparison, abstraction and inference.

Information security in the state security system

Due to the role information plays in the modern world, this concept can be interpreted in many ways, depending on the research context and the area of human activity. In the literature, information is defined as, among other things:

- A strategic commodity – knowledge is a key resource for states, organizations, and individuals alike. Historically, access to the right information at the right time has been crucial to military victories and economic success. Today, information is perceived as a good comparable to other strategic resources, such as energy resources or advanced technologies, which can be traded and require special protection;
- An element of business processes – information is an indispensable component of the functioning of modern organizations, including public administration entities. Disruptions in its flow, loss of integrity, or deliberate manipulation can lead to serious consequences, such as corporate bankruptcy, social unrest, or destabilization of the state;
- a factor controlling production and service processes – information plays a key role in managing automated technological processes, crucial to the functioning of the economy and the security of society. This applies in particular to systems based on sensors, controllers, and digital infrastructure, the improper use or security of which can lead to local, national, and even international crisis situations;
- legally protected value – in order to protect the interests of individuals and the state, a number of legal regulations have been established to protect data against unauthorized access, modification or loss .

The scope of information's application and its functional significance demonstrate the complexity of this issue. Consequently, ensuring an adequate level of information protection is a key element of the efficient functioning of the state and the security of its citizens. Contemporary national security doctrine considers information security to be an integral and overarching component of the state's security system, permeating all other subsystems – from defense, through social, to economic. From a systemic perspective, the state functions as a complex organism processing vast data sets, where information is the fundamental building block of decision-making processes. Ensuring security in this domain is therefore not limited solely to protecting ICT systems against cyberattacks but encompasses a broad spectrum of activities aimed at ensuring the uninterrupted functioning of the public sphere.

According to Kazimierz Malak, information security is one of the key dimensions of international and national security. The essence of this type of security stems from the fact that information is a fundamental resource determining the efficient functioning of most entities in international relations, social life, and the developing information society – both domestically and globally. Information plays a role in determining decision-making processes, resource management, and the achievement of strategic goals in many areas of state and organizational activity.

It should be emphasized, however, that the concept of "information security" is not new. Its origins can be traced back to the 6th century BC, in the thought of the Chinese strategist and philosopher Sun Tzu, who formulated some of the first concepts of information warfare, demonstrating the possibility of gaining an advantage over an opponent without the need for direct military action. However, the contemporary understanding of information security has developed alongside the evolution of communication technologies, the digitization of state processes, and the growing role of information as a strategic resource.

There are many definitions of information security in the literature, mostly focusing on the protection of classified information or the security of IT systems. This tendency is confirmed by K. Liedel , who points out that "information security is very often understood as the protection of information against undesirable (accidental or deliberate) disclosure, modification, destruction, or prevention of its processing." This definition illustrates an

approach that reduces information security to a technical and organizational dimension, focused on ensuring the protection of information resources.

In this context, it's worth noting that some authors present a so-called negative approach to information security, whose primary goal is to eliminate or minimize threats affecting information. This approach is exemplified by, among others, Piotr Potejko, who defines information security as "a set of actions, methods, and procedures undertaken by authorized entities, aimed at ensuring the integrity of collected, stored, and processed information resources by securing them against unwanted, unauthorized disclosure, modification, or destruction." Maciej Marczyk takes a similar approach, pointing out that information security means "protecting information against unwanted access, destruction, or disclosure."

When analyzing the role of information security through the lens of information attributes, three aspects should be considered: confidentiality, integrity, and availability. Confidentiality in the national context refers to the protection of state secrets, official secrets, and diplomatic data, the disclosure of which could jeopardize the interests of the Republic of Poland. However, in the context of modern hybrid threats, the remaining two attributes are gaining increasing importance. Information integrity ensures that the data used by public administration bodies and services to make key decisions is reliable and has not been manipulated. Information availability, in turn, is synonymous with ensuring the continuity of management processes, which is a prerequisite for the implementation of state tasks in crisis situations.

Information security serves as a kind of "nervous system" in the national security architecture, unifying and coordinating the activities of other system components. Without a well-functioning information flow, military components, emergency services, and critical infrastructure operators operate in isolation, losing the ability to respond effectively. In this context, protecting the information space becomes a prerequisite for maintaining sovereignty, understood as the ability to independently define goals and pursue them without the destructive influence of external disinformation campaigns.

One of the key documents addressing information security is the 2020 National Security Strategy of the Republic of Poland. This document addresses both cybersecurity and the broader information sphere. In the area of cybersecurity, the strategy assumes actions aimed at increasing resilience to cyber threats and improving information security in the public, military, and private sectors. Disseminating knowledge and best practices to support citizens in effectively protecting their information is also a key element.

The implementation of the indicated goals is to be achieved through, among others:

- improving the resilience of IT systems used in the military and civilian environment in order to effectively counter cyber threats;
- strengthening the state's defense capabilities through continuous improvement of the national cybersecurity system;
- building national capacity in the field of assessment, research, testing and certification of cybersecurity services and solutions;
- educating public administration and society about cyber threats and challenges;
- developing national research and development capabilities, including through public financing of research into advanced technologies in cooperation with universities, research institutes and the private sector.

Critical infrastructure as an information-sensitive area

Modern critical infrastructure is no longer a collection of isolated physical objects but has evolved into complex, mixed ecosystems in which the material layer is inextricably linked to the digital layer. This architecture makes these systems particularly sensitive to information. This stems from the fact that technological processes such as electricity transmission, rail transport control, or water treatment are now controlled by advanced industrial automation systems and master control and data acquisition systems. In this environment, information ceases to be merely a record of reality and becomes a control impulse, the modification of which translates into direct consequences.

Basically, human life, as shown in Figure 1, may be endangered by six basic causes, referred to in the literature as 6WTD (six WTD. Ways to die), which include: overheating (excessive exposure to high temperatures), hypothermia (excessive exposure to low temperatures), hunger, thirst, illness and injury.

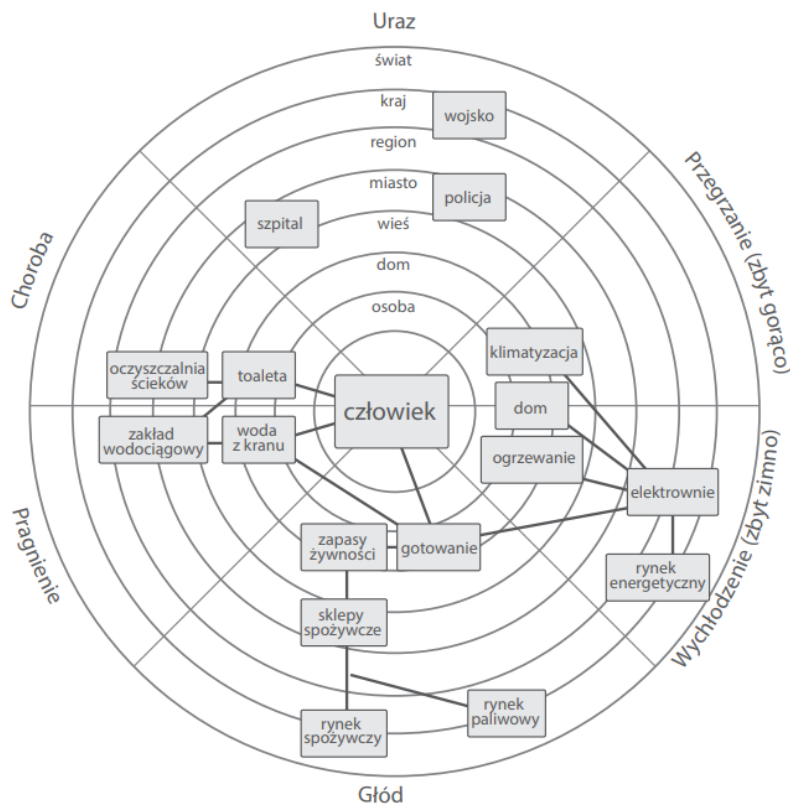


Fig.1. Map of critical infrastructure and its levels

Source: M. Bennett, V. Gupta, *Dealing in Security understanding vital services and how they keep you safe*, 2010.

In this approach, the fundamental role of critical infrastructure is to protect the lives and health of citizens from the effects of the identified threats. According to this concept, critical infrastructure can be divided into the following categories:

- Infrastructure ensuring shelter and its proper functioning, including in particular facilities and systems responsible for maintaining appropriate living conditions, such as combined heat and power plants, power plants and heating systems;
- Infrastructure supporting supply chains, understood as a set of elements necessary to ensure the continuity of supplies of essential goods and services, including transport, water and fuel infrastructure, as well as processing and storage facilities, such as refineries;
- Infrastructure providing access to basic security services, including systems enabling the provision of key public services, including telecommunications networks, energy systems, databases and other elements necessary for the efficient functioning of the state and crisis response.

The specific nature of critical infrastructure information sensitivity is most fully revealed in the interdependence of information technology (IT) and operational technology (OT). While data confidentiality is typically a priority in traditional IT systems, OT systems prioritize data integrity, availability, and real-time operation. Even microsecond delays in the transmission of control data or the introduction of false measurement parameters into the network can lead to device desynchronization, physical damage to equipment, and, in extreme cases, to large-scale failure. In the energy sector, which is the foundation of national security, the introduction of outdated data on grid frequency or transformer load can result in automatic shutdown of power units and blackouts, paralyzing communities at the municipal, and perhaps even county, level.

Another dimension of information sensitivity should also be considered, which concerns data on the structure and security of critical infrastructure facilities. Information regarding the location of key transportation hubs, transmission network diagrams, emergency procedures, and technical specifications of devices constitute an extremely valuable resource for a potential attacker. Obtaining this data through intelligence gathering or information leaks allows for the precise planning of a hybrid attack, striking at the weakest links in the system. In

this approach, critical infrastructure becomes a target not only for physical acts of sabotage but primarily for cyberspace operations, where the weapons are information about the system and the code controlling its operation.

Consequently, the traditional approach and perception of critical infrastructure security through the prism of physical protection must also be supported by a modern cybersecurity system. The virtual realm has become a domain of information warfare, where a key challenge is ensuring the integrity of control systems and verifying the reliability of input data. Every infrastructure element, from a smart energy meter to a rail traffic control center, represents a potential entry point for digital threats. Information sensitivity is therefore becoming an integral feature of modern infrastructure, determining the need to implement advanced mechanisms for anomaly monitoring and building threat awareness among personnel.

Moving on to the analysis of cyberterrorist threats to critical infrastructure systems, it should be noted that the most crucial area from the perspective of national security and operational continuity is the energy, raw materials, and fuel supply system. Potential cyberattacks can impact power system automation protection systems, regional and national power grid management systems, and resource environment monitoring systems. Threats in this sector include, among others, the disabling of generator and high-voltage line protection, disruption of gas and power system connections, and damage to vapor and pressure monitoring devices due to electrostatic discharge. The cascading effects of these incidents lead to the destabilization of services, economic losses, land contamination, and in extreme cases, chaos and human casualties. In the communications and public administration sectors, cyberterrorism threatens public and special teletransmission systems, mobile communications, as well as platforms such as ePUAP and public registers, including the PESEL, KRS, and NIP. Interference with these systems through damage and unauthorized modification of connections, inadequate protection of management sessions, interception of sensitive information, or loss of data integrity leads to disorganization, panic, and a significant decline in public trust, which can ultimately generate a sudden increase in crime. Another critical point is financial and banking systems, where malware can disable or block ATM networks, stock exchange platforms, and market operations systems. This directly results in limited access to online bank and brokerage accounts and the inability to settle transactions, which cuts off the population from means of payment and provokes conflicts, theft, and extortion. Manipulation of food and water supply, healthcare, rescue, and transportation systems poses a significant threat to the life and health of the population. Taking control of automated control systems for dams, water treatment plants, or food quality verification lines, and introducing distortions into them, can lead to uncontrolled water discharges, the risk of epidemics, and the loss of basic services, causing physical suffering. In turn, the disabling of telecommunications nodes in emergency call centers for the 112 number and the disruption of medical services' radio communication channels translates into reduced public confidence and an increased number of sudden deaths. In transportation systems (including rail and road traffic control and intelligent transportation systems), introducing corruption into ICT systems, taking control of track circuits, or manipulating locomotive control computers poses a risk of accidents resulting in casualties or injuries. If the incident involves the transport of hazardous substances, this generates additional ecological consequences. Similar, large-scale environmental effects, such as widespread land contamination, entail the takeover of industrial pipeline control systems, early warning systems, and the supervision of toxic, infectious, and flammable substance installations. In summary, in light of the literature, the presented cyberterrorist threats represent potential destabilizing factors for states, their economies, and the natural environment, while also posing a direct threat to human health and life¹.

The National Critical Infrastructure Protection Program, adopted in 2023, identifies five basic threat categories: physical, technical, personal, ICT, and legal. This document does not specify a separate category. Threats related to the information security of critical infrastructure, understood as impacts on public opinion, the decision-making processes of CI sector entities, or the market environment of business ventures related to the operation of this infrastructure. Phenomena of this type have also not been clearly captured within any of the five identified categories, including in the area of ICT threats.

The need to distinguish these types of impacts is highlighted by solutions adopted in other countries. An example is the work of the U.S. Cybersecurity and Infrastructure Security Agency (CISA) , which clearly distinguishes psychosocial and information threats from classic technical threats occurring in cyberspace. This approach emphasizes that influencing public awareness, citizen attitudes, and decision-making processes can destabilize the functioning of critical infrastructure just as much as physical or digital acts of sabotage.

¹ A. Machnac, Elements of threat to critical national infrastructure, "Computerworld". Website: https://www.computerworld.pl/news/Elementy-zagrozenia-krytycznej-infrastruktury-panstwa,368_103.html , accessed: 30/01/2026.

Unfortunately, the report of the Commission for the Study of Russian and Belarusian Influence published in 2025 concluded that :

- Pro-Russian disinformation in the Polish infosphere is part of a broader cognitive warfare campaign;
- the transition from classical disinformation to actions characteristic of cognitive warfare, understood as a form of non-military aggression, remains largely beyond the general public awareness;
- both Polish society and public administration still largely perceive espionage and sabotage activities primarily through the prism of their traditional forms;
- in the context of the ongoing conflict, greater emphasis in propaganda messages is placed on undermining the credibility and damaging the image of Ukraine than on directly exposing the advantage of the Russian Federation;
- In disinformation narratives, the role of NATO and the European Union is consistently deprecated, Western civilization is presented as fallen and demoralized, while the Russian Federation is shown as an entity impossible to defeat.

The above findings confirm that information activities conducted by the Russian Federation and its allies constitute an important component of contemporary hybrid threats, and their impact goes beyond the classic mechanisms of propaganda, influencing social perception, decision-making processes and the institutional stability of the state.

Threats to the information security of critical infrastructure

The contemporary paradigm for protecting strategic assets is evolving from the concept of the inviolability of system boundaries towards building broadly understood resilience. In this context, information security is no longer perceived merely as a technical protective barrier, but rather becomes a key catalyst for critical infrastructure's ability to survive, adapt, and quickly recover from disruptions. Information resilience refers to the system's ability to maintain critical functions even in the face of a successful cyberattack, data manipulation, or communication system failure. Effective information security allows for real-time anomaly detection, which is crucial for minimizing the impact of incidents. In power and gas systems, information resilience manifests itself in the ability of control algorithms to reject erroneous or manipulated measurement data that could lead to network destabilization. By ensuring the integrity and high availability of information, operators gain the time necessary to take corrective action, which directly translates into limiting the potential scale of paralysis of critical services. A key element in strengthening the resilience of critical infrastructure in the information dimension is the implementation of the European NIS2 Directive and national cybersecurity regulations. These require operators not only to use advanced encryption technologies and multi-factor authentication but, above all, impose the obligation to manage risk throughout the entire supply chain. The information resilience of critical infrastructure is only as strong as its weakest link – often a third-party provider of digital services or automation components. From this perspective, information security becomes a process of continuous monitoring of digital hygiene and emergency preparedness, which is essential for maintaining national stability in times of crisis.

An efficient crisis communication system and the protection of information channels against disinformation prevent panic outbreaks that could lead to secondary threats, such as the sudden overload of fuel or ATM networks. Information security therefore guarantees the credibility of messages from civil protection authorities, which underpins the resilience of the entire state.

In the context of threats targeting critical infrastructure, various forms of cyberattacks are crucial, the most frequently identified of which are:

- DoS (Denial of Service) – an attack that prevents access to a specific service or IT system by overloading it. A specific variant of this type of attack is DDoS (Distributed Denial of Service), in which traffic is generated simultaneously from multiple distributed sources, significantly hindering effective defense;
- hijacking – taking control of the victim's computer system or mobile device in order to gain unauthorized access to data or use system resources;
- sniffing – a technique of monitoring and intercepting network traffic in real time, enabling the acquisition of transmitted information, including authentication data;
- Phishing – a social engineering method that involves obtaining confidential information by impersonating credible entities. These attacks are most often carried out via email, social media, fake websites, or text messages and are based on manipulating user trust;

- Ransomware is malicious software that encrypts the victim's data, after which the perpetrators demand a ransom in exchange for decryption. These types of attacks pose a particular threat to critical infrastructure entities, as they can lead to the paralysis of key services and significant financial losses.

The presented forms of threats clearly indicate that information security is currently one of the key dimensions of critical infrastructure protection, and the effectiveness of the state security system increasingly depends on the ability to prevent, detect and neutralize threats in cyberspace.

For many years, Poland has been the target of information and propaganda operations conducted by the Russian Federation, a finding confirmed by both domestic analyses and reports from international institutions. The increasing intensity of such operations means that the security of critical infrastructure is increasingly becoming an indirect target of hybrid attacks. These operations combine elements of psychological pressure, disinformation, and cyberattacks, and their vector is not traditional technical means, but appropriately manipulated information.

An example of this type of activity, which directly threatens the stability of the energy sector, is an attack involving the deliberate manipulation of end-user behavior. This mechanism relies on the distribution of false messages – most often via text messages, social media platforms, or notifications imitating official grid operator alerts. This message informs about alleged price promotions or preferential tariff rates applicable during specific hours. The primary goal of such an operation is to induce as many consumers as possible to simultaneously shift and increase their energy consumption to periods when the system is already under high demand. A diagram of this type of attack, including a sample disinformation message and household reactions, is presented in Figure 2.

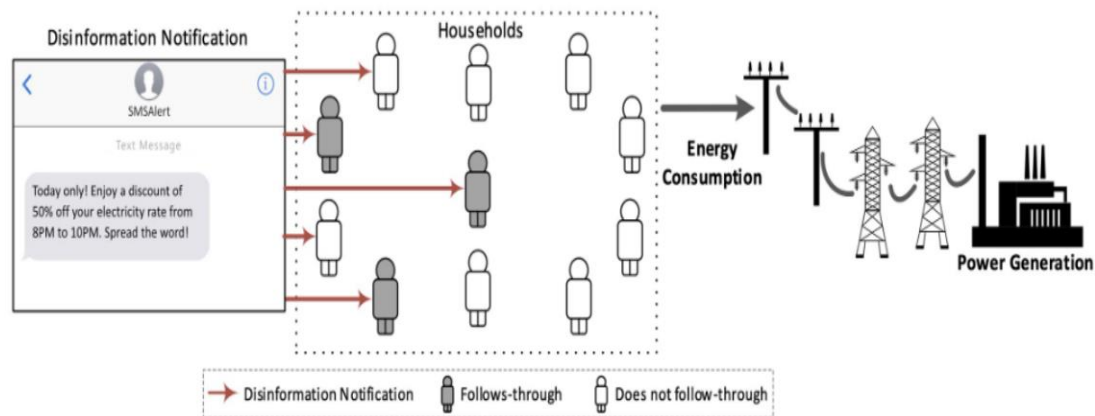


Fig.2. Overview of the disinformation attack on the energy system

Source: G. Raman, B. AlShebli, M. Wanek, i in., *How weaponizing disinformation can bring down a city's power grid*, „PLoS ONE” R. 2020, 15(8)

Successful manipulation can result in an artificial, sudden increase in power consumption within a narrow time window. This leads to the overload of key elements of the power system, particularly transmission lines, transformer stations, and local distribution networks. In extreme cases, this phenomenon results in grid failures, power outages, and cascading disruptions in the functioning of other critical infrastructure sectors that are entirely dependent on a stable power supply.

A key factor determining the effectiveness of this type of attack is the public's susceptibility to manipulation, expressed by the percentage of consumers who modify their behavior in response to the false message. As the diagram illustrates, not all recipients react as intended by the attacker, but even a partial success of the operation may be sufficient to destabilize the grid. This means that the effectiveness of an attack depends not only on the perpetrator's technological advancement, but equally on the level of public awareness and the state's overall information resilience.

The scale of threats stemming from information influence is demonstrated by events that took place in Poland at the end of February 2022, immediately following the launch of the Russian invasion of Ukraine. During this period, disruptions in the fuel distribution system occurred, caused not by technical factors but by a violent social reaction to disinformation disseminated in the media. As indicated by analyses by the Institute for Internet and Social Media Research, numerous posts suggesting an imminent fuel shortage began appearing on social media

as early as February 25, 2022. This content was disseminated primarily via Twitter and Facebook, reaching a potential reach of several million.

As a result of disinformation, a significant number of drivers began mass fuel purchases, leading to temporary shortages at gas stations. IBIMS experts identified the activities of at least several organized groups conducting coordinated disinformation campaigns in Polish-language social media. These entities focused on inciting social unrest, undermining trust in state institutions, and destabilizing the fuel market, which aligned with the Russian Federation's information-based goals. These groups operated accounts with a clearly pro-Russian profile, published content supporting aggression against Ukraine, and took actions aimed at discrediting the authorities of the Republic of Poland, the European Union, and NATO. Simultaneously, they promoted narratives aimed at improving the image of the Russian Federation and undermining trust in Polish businesses, particularly in the energy sector. These activities were particularly intense in the area of disinformation regarding fuel availability and prices.

The actions described here fit within the broader framework of information warfare conducted in accordance with concepts developed in Russian strategic thought. Information warfare is understood as a set of activities encompassing, among others, information-psychological operations, disinformation, propaganda, lobbying, crisis management, blackmail, and image campaigns. Its goal is to achieve long-term political, social, and economic effects without the need for traditional military operations.

Therefore, entities responsible for critical infrastructure protection should consider information threats as a fully fledged element of risk analysis. It is also necessary to systematically raise awareness among staff and end users in recognizing information manipulation and disinformation. It also seems justified to expand the provisions of the National Critical Infrastructure Protection Program to include a component directly addressing information security and societal resilience, as a crucial element in ensuring the continuity of state functioning.

Summary

The analysis demonstrates that, in contemporary geopolitical and technological conditions, information security has ceased to be a purely technical domain and has become a fundamental pillar of state stability. The evolution of threats, particularly in the area of hybrid operations, has forced a redefinition of the approach to critical infrastructure protection. The article's main conclusions indicate that the resilience of strategic facilities – including the particularly sensitive energy system and wireless communications – now depends directly on the integrity of data and the continuity of information processes, which constitute the digital foundation of their operation.

A key conclusion drawn from these considerations is the need to fully integrate information technology (IT) security with operational technology (OT). It has been demonstrated that the most serious risks to the continuity of state operations arise from the possibility of manipulating control information, which can lead to the paralysis of critical services without the use of kinetic means.

All the arguments presented lead authors to conclude that Information security fundamentally influences the functioning of a modern critical infrastructure protection system by ensuring the ability to counter hybrid threats in the era of economic digitization.

A stable and reliable flow of information provides public administration bodies and emergency services with a real ability to protect the public in extreme situations. Future research in this area should focus on implementing artificial intelligence systems to detect digital threats and strengthening society's psychological resilience to disinformation related to infrastructure failures. In summary, only a holistic approach, combining physical, digital, and social security, will effectively address the challenges facing the state security system in the third decade of the 21st century.

All the arguments presented lead authors to conclude that Information security fundamentally influences the functioning of a modern critical infrastructure protection system by ensuring the ability to counter hybrid threats in the era of economic digitization.

References

- Liderman K., Information security. New challenges. (ed.) PWN, Warsaw 2017, 2nd edition, p. 15.
- Mikusek K., Polish approach to information security, Problemy Techniki Uzbrojenia, no. 5/2023 p. 151.
- Liedel K., Information security in the era of terrorism and other threats to national security, Adam Marszałek Publishing House, Toruń 2008, p. 19.
- Potejko P., Information security , [in:] State security, KA . Wojtaszczyk, A. Materska-Sosnowska (ed.), ASPRA-JR Publishing House, Warsaw 2009, p. 193.
- <https://encyklopedia.revite.pl/articles/view/55> [accessed 04/02/2026]
- National Security Bureau, National Security Strategy of the Republic of Poland, 2020, p. 20.
- <https://awpeters.info/six-ways-to-die-6wtd.html> [accessed 04/02/2026]
- Baraniuk K., Information threats to critical infrastructure on the example of 5G technology, PTBN Report Volume III (2022), p. 7.
- <https://ibims.pl/komunikat-ws-prorosyjskich-grup-prowadzcych-dzialania-dezinformacyjne-25-02-22/> [accessed 05/02/2026]
- Witwicka K., The War in Ukraine and the Fuel Shortage. "High Probability of Disinformation Attempts." Website: <https://wiadomosci.radiozet.pl/Biznes/Wojna-w-Ukrainie-a-brak-paliwa.-Wysokie-prawdo-podobienstwo-prob-dezinformacji>, accessed: 01.02.2026.
- Aleksandrowicz T., Basics of Information Warfare, Warsaw 2016, p. 163.
- Darczewska J., Anatomy of Russian Information Warfare. Crimean Operation – A Case Study, Warsaw 2014, pp. 13-15.
- Commission for the Study of Russian and Belarusian Influence on the Internal Security and Interests of the Republic of Poland in the Years 2004–2024 Report of the Disinformation Team Warsaw, 10 January 2025
- Rogalewicz M., Cyberterrorism as a Threat to the State's Internal Security. Website: <https://instytutcyber.pl/publikacje/cyberterroryzm-w-polsce/> [accessed: 25/03/2026]
- Raman G., AlShebli B., Waniek M., et al., How weaponizing disinformation can bring down a city's power grid, " PLoS ONE" R. 2020, 15(8).