Dr hab. Maciej Kaźmierczak, prof. ASzWoj
War Studies University
ORCID: 0000-0001-6985-3157
e-mail: m.kazmierczak@pracownik.akademia.mil.pl

Dr hab. Sławomir Byłeń, prof. WAT
Military University of Technology
ORCID: 0000-0002-4565-4388
e-mail: slawomir.bylen@wat.edu.pl

Security of critical infrastructure in Poland – selected aspects of research

Bezpieczeństwo infrastruktury krytycznej w Polsce – wybrane aspekty badań

Abstract

The subject of research presented in the article are the processes taking place in the national security environment, determining the need to strengthen defence capabilities in terms of protecting critical infrastructure facilities of the state. The purpose of the research is to check, verify and evaluate the functioning of the critical infrastructure protection system of the state and to demonstrate the need for its protection in the light of possible threats. From the opinions of experts in the field of national security, a research hypothesis emerges, which shows that despite taking multi-directional actions, the state administration operating at many organizational levels is not able to foresee all the threats that lie in wait for critical infrastructure facilities. Empirical research methods were used in the study: analysis and criticism of the literature, desk research and a diagnostic survey conducted using the interview technique with experts and military analysts. From the theoretical methods, the following were used: analysis, synthesis, and inference methods. The conducted research shows that there are premises to ensure that critical infrastructure facilities are effectively protected against harmful and destructive intentional or random actions. The problem in ensuring proper protection of critical infrastructure is the fact that they are a relatively accessible and easy target for terrorist attacks, sabotage groups or special groups. Therefore, steps should first be taken to identify which facilities and systems constitute critical infrastructure of strategic, regional and local importance.

Keywords:
state security, critical infrastructure, threats, protection, defensive abilities

Streszczenie

Przedmiot badań przedstawiony w artykule stanowią procesy zachodzące w środowisku bezpieczeństwa narodowego, determinujące konieczność wzmacniania zdolności obronnych pod kątem ochrony obiektów infrastruktury krytycznej państwa. Celem badań jest sprawdzenie, weryfikacja i ocena funkcjonowania systemu ochrony infrastruktury krytycznej państwa oraz wykazanie potrzeby jej ochrony w świetle możliwych zagrożeń. Z opinii ekspertów w dziedzinie bezpieczeństwa narodowego wyłania się hipoteza badawcza z której wynika, że pomimo podejmowania wielokierunkowych działań administracja państwa funkcjonująca na wielu poziomach organizacyjnych nie jest w stanie przewidzieć wszelkich zagrożeń, jakie czyhają na obiekty infrastruktury krytycznej. W opracowaniu zostały zastosowane empiryczne metody badawcze: analiza i krytyka piśmiennictwa, *desk research* oraz sondaż diagnostyczny prowadzony techniką wywiadu z ekspertami i analitykami wojskowości. Z metod teoretycznych wykorzystano: analizę, syntezę i metody wnioskowania. Z przeprowadzonych badań wynika, że istnieją przesłanki ku temu, aby obiektom infrastruktury krytycznej zapewnić skuteczną ochronę przed szkodliwym i destrukcyjnym działaniem celowym lub losowym. Problem w zapewnieniu należytej ochrony infrastruktury krytyczniej stanowi fakt, iż są one względnie dostępnym i łatwym celem ataków terrorystycznych, grup dywersyjnych czy grup specjalnych. W związku z tym należy najpierw podjąć działania zmierzające do identyfikacji, które obiekty i systemy stanowią infrastrukturę krytyczną o znaczeniu strategicznym, regionalnym i lokalnym.

Słowa kluczowe:
bezpieczeństwo państwa, infrastruktura krytyczna, zagrożenia, ochrona, zdolności obronne

JEL: H56, H54

Introduction

Civilization or technological progress, in addition to its positive aspects, also has a negative character. The increased standard of living due to the development of electricity or ICT (*information and communication technologies*) is associated with the dependence of the functioning of societies on their abilities. The electricity subsystem, which is a key component of any economy, can be disrupted, for example, by a terrorist act. Any disruption of the electricity supply can disrupt all areas of socio-economic life and create a local, regional and national emergency. The facilities of this subsystem include nodal transformer stations or power substations, the supervisory system of main transmission lines, power plants and thousands of kilometres of transmission lines. In addition to the electricity subsystem, the ICT network is also important for the smooth operation of the state, its administration and business entities. Unfortunately, it is highly susceptible to paralysis through, among other things, cyber-terrorist attacks.

The subject of research presented in the article are the processes taking place in the national security environment, determining the need to strengthen defence capabilities in terms of protecting critical infrastructure facilities of the state. The cognitive purpose of the study is to check, verify and evaluate the functioning of the critical infrastructure protection system of the state and to demonstrate the need to protect facilities in the light of possible threats. The utilitarian goal was to specify conclusions and indicate recommendations aimed at improving the functioning of the critical infrastructure protection system for state security.

From the opinions of experts in the field of national security, a research hypothesis emerges, which shows that despite taking multi-directional actions in the field of crisis management, public administration operating at many organizational levels is not able to foresee all the threats that threaten the facilities and critical infrastructure.

The general research problem of the article boils down to an attempt to find an answer to the question: What is the impact of threats to critical infrastructure facilities on the forms of their protection, and thus on the security of the state and its citizens? Empirical research methods were used in the study: analysis and criticism of the literature, desk research and a diagnostic survey conducted using the interview technique with military experts and analysts. From the theoretical methods, the following were used: analysis, synthesis and inference methods.

The conducted research (Jakubczak, 2006, p. 355) shows that the problem in providing adequate protection to critical infrastructure facilities and equipment whether point (structures, relay stations, bridges, airports, ports, trains, subways, etc.) or linear (oil and gas pipelines, power and telecommunications lines, roads, railroads, etc.) may be the fact that they are relatively accessible and easy targets for attacks by terrorists, diversionary and special groups, as well as madmen or hackers.

In order to ensure the effective protection of critical infrastructure facilities and systems, steps must be taken to identify, that is, to determine on the basis of clear criteria, which facilities and systems constitute critical infrastructure of national, regional and local importance. In the executive sphere, the organization of critical infrastructure protection at all levels of government and local administration, with the definition of responsibilities, competencies as well as the allocation of forces and resources, will be of fundamental importance. The protection of critical infrastructure facilities and systems is a major challenge for governing entities in view of ensuring the security of the state as well as society as a whole. Therefore, the need to analyse this problem with detailed consideration of threats to critical infrastructure to organise means and ways that will be used to protect critical infrastructure systems and facilities is noticeable.

Background to research (analysis)

After the transformations that took place in Poland after 1989, aspirations related to Polish membership in the European Union (EU) intensified. At that time, it turned out that one of the conditions for future integration was the adjustment of legal solutions and terminology to those already in place in the Member States. Research (Lidwa et al., 2012, p. 9) shows that among the many hitherto unknown concepts appeared e.g. crisis management and critical infrastructure. These formulations are directly related to the security of the state and citizens, becoming the most important in building effective solutions ensuring free and stable existence of modern societies, both at the local, national and international level (Knapp & Lagill, 2011, p. 37).

Prior to the introduction of the term critical infrastructure into the national terminology related to crisis management (Lidwa et. al., 2012, p. 9), there were such formulations as: facilities of particular importance for the security and defence of the state, areas, facilities, equipment, and transports subject to mandatory protection (Presch-Cronin & Marion, 2016, p. 86). However, regardless of the terminology, the protection of the state's critical infrastructure systems is increasingly based not only on the solutions operating in a given country, but primarily on international security standards, designed to ensure

the continuity of their operation in the conditions of interconnected global undertakings, minimizing threats to these systems, and above all through mutual information and warning (Moteff, 2012, p. 73).

In the area of critical infrastructure threats, terminological ambiguity does not prevail, so the consequence is that there is a situation in which a specific object belongs simultaneously to critical infrastructure and is particularly important for the security and defence of the state and is therefore subject to mandatory protection. Thus, there are suggestions that the concept of critical infrastructure should distinguish defence infrastructure (Lidwa et al., 2012, p. 13), which would define facilities that are particularly important for state security and defence.

Defining facilities and installations critical for the functioning of the state is of fundamental importance in shaping the appropriate level of security for citizens. The rules for determining the systems and objects belonging to the critical infrastructure, which are real and cybernetic systems necessary for the minimum functioning of the economy and the state, are contained in a classified annex to the National Program for Critical Infrastructure Protection and only selected persons have the opportunity to check which of the objects belongs to critical infrastructure (Rządowe Centrum Bezpieczeństwa, 2013). The emergency response system, based on the practical aspect that allows systems to be classified into groups to facilitate identification, is divided into system infrastructure elements, which include (Lidwa et al., 2012, p. 14):

- normative-legal infrastructure,
- social infrastructure,
- IT infrastructure (infosphere),
- technical infrastructure (technosphere).

The above elements of the system infrastructure also include critical infrastructure systems defined by law. When talking about critical infrastructure systems, it should be remembered that these are objects, devices and installations constituting a given system, which are interrelated and dependent (Tyburska, 2010, p. 15). Critical infrastructure systems are undoubtedly key facilities and systems from the point of view of the functioning of the state, on the efficiency of which the continuity of operation of specific public utility institutions depends (Ackerman, 2017), including power structures. These facilities and systems can be classified into 4 areas (Lidwa et al., 2012, pp. 17–18):

1. State defence – defence is a key element of the state security system. This area includes plants conducting research in the field of construction work and producing for the needs of national defence. This area also includes state reserve storage facilities and special production facilities. Protection of production facilities and centres for the development of knowledge related to defence matters should include not only physical security, but also relate to the protection of classified information.
2. Protection of the state's economic interest – is related to ensuring the security of facilities such as plants having to do with the extraction of mineral resources of strategic importance to the state, ports, airports, banks, and plants producing, storing or transporting significant amounts of money or securities.
3. Public security – related primarily to the protection of plants, facilities and equipment that significantly affect the functioning of society, the damage or destruction of which would have serious consequences for the life and health of citizens and the environment. These include power plants, heating plants, water intakes, waterworks or sewage treatment plants, plants using or storing fissile, toxic, chemical or explosive materials, pipelines, power and telecommunications lines, hydrological facilities and other facilities located in the open, the damage of which could have negative consequences for people or the environment or bring significant material losses.
4. Protection of other important interests of the state – covering establishments carrying out unique economic production, facilities related to the distribution of information (television, radio, mail, Internet), state archives and facilities related to the protection of national heritage.

Critical infrastructure – the state of knowledge

Pursuant to the Crisis Management Act (April 26, 2007), critical infrastructure includes systems and their functionally related facilities, including buildings, devices, installations, services crucial for the security of the state and its citizens and serving to ensure the efficient functioning of public administration bodies, as well as institutions and entrepreneurs. The records of the above of the legal act indicate that critical infrastructure includes such systems as: energy supply, energy resources and fuels; communications; ICT networks; financial; food supply; water supply; health protection; transport; rescue; ensuring the continuity of public administration and the production, storage, storage and use of chemical and radioactive substances, including pipelines of hazardous substances.

The same act also stipulates that the European critical infrastructure consists of systems and related functional objects that are part of them, including building structures, devices and installations crucial for the security of the state and its citizens and

serving to ensure the efficient functioning of public administration bodies, as well as institutions and entrepreneurs, designated in systems in the field of electricity, crude oil and natural gas, as well as road, rail, air, inland waterway, ocean shipping, sea shipping, short sea shipping and ports, located in the territory of the European Union (EU) Member States, the disruption or destruction of which would have a significant impact on at least two Member States. The basis for qualifying a facility as belonging to the European Critical Infrastructure is checking whether it meets the requirements defined on the basis of the following criteria: sectoral, component, business continuity and cross-sectional (Katina & Hester, 2013), p. 211–225):

- sectoral – referring to the parameters defined by the EU or the functions performed by these facilities as a condition for their acceptance as a component of critical infrastructure;
- constituent – respected when the consequences of the destruction or damage to a specific system or part of the infrastructure could be particularly severe for a country;
- business continuity – occurring when damage or destruction of a system would have an important impact on at least two EU countries;
- cross-cutting – involving three internal criteria: casualties, economic impact and social impact.

Undertakings on the protection and defence of critical infrastructure in the opinion of authors (Piątek & Truchan, 2013, p. 14) include both legislative, educational, physical and technical measures, as well as systemic solutions carried out at all levels of public administration, as well as implemented by the private sector, the public and other entities acting for the benefit of national security.

Preparing effective protection of critical infrastructure requires a comprehensive approach that takes into account the following areas in the organization of protection (Tyburska, 2010, p. 14): physical protection; technical protection; personal protection; ICT protection; legal protection; assistance to the government party in the reconstruction of a damaged or destroyed element. Each of the aforementioned areas constitutes a complex system of activities requiring general and specialized knowledge, a wealth of experience including the use of so-called good practices, the ability to analyse, as well as forecast threats. Critical infrastructure protection is defined as activities aimed at protecting specific sensitive structures of the state. These include (Gopalakrishnan & Peeta, 2010, p. 53): people, fixed assets, communication systems essential for state security, which further condition the country's economic stability and political security.

The methods and measures used in critical infrastructure protection (Tyburska, 2010, p. 23) are aimed at preventing or mitigating the effects of attacks carried out against a specific element of critical infrastructure. These attacks can be caused by people (terrorists, criminals, hackers) or can be the result of natural disasters and technical failures (accidents involving hazardous materials like nuclear, radioactive, biological or chemical substances).

Civilization hazards, also known as technical hazards, are caused by human interference with the natural environment and technical and industrial development. Through improper use of their own achievements and mastery of the natural world, people cause, often irreversible damage to both themselves and nature. Within these risks, we can distinguish four basic groups (Tyburska, 2010, p. 23): fires and landscape disasters, technical contamination, construction disasters and traffic disasters. The most common civilization hazards are fires. They are characterized by a very destructive force. They arise most often as a result of human activity (as many as 80% of fires are a consequence of people's recklessness, lack of knowledge of fire protection rules, malfunction of equipment or sabotage or intentional arson). The cause of area fires is most often ignition of fire, malfunctioning technical equipment or lightning strikes (Tyburska, 2010, p. 91).

Another category of civilization hazards is **chemical contamination**. This is a very broad category that includes chemical accidents, chemical contamination, radioactive activity and biological contamination. With industrial development came the emergence of toxic industrial agents. As they are used in most industries using chemical technologies, they have a very harmful and dangerous effect on the environment and people. Toxic chemicals can also escape into the atmosphere, penetrate the ground or contaminate further areas by wind. Water reservoirs, which constitute the water supply system – as one of the critical infrastructure subsystems – are also often contaminated.

Construction disasters are one of the categories of civilization hazards that can damage critical infrastructure facilities. Within them we distinguish industrial disasters, installation disasters, municipal disasters and mining damage. Their cause is most often the overuse of facilities combined with insufficient repairs and maintenance inspections. Buildings are damaged by, among other things, moisture and poor horizontal insulation, which together cause corrosion and weakening of building structures.

The last group of civilization hazards are **communication hazards**, which include air, rail, sea, vehicle and space disasters. They occur in every region and their intensity is adequate to the degree of development of the communication stream and the security of the region. They result in property

damage and loss of life or health of participants in these incidents. The greatest media publicity is given to air disasters, which is due to their spectacularity and the small possibility of saving passengers or aircraft operators. However, it is worth mentioning that air transportation is currently the safest way to move people. Maritime disasters are also quite rare, with great public concern. Most casualties are caused by road disasters and accidents, the number of which is increasing every year. This is caused, among other things, by the increasing number of cars and the poor quality of roads. However, the main cause of accidents is man himself, who, for example, by breaking traffic regulations, is the perpetrator. Traffic hazards directly affect the disruption of the transportation system, which is a component of critical infrastructure.

Natural hazards are events that arise most often as a result of geological or climatic abrupt changes that can adversely affect the operation of a given critical infrastructure system or cause dangerous changes in its internal or external environment, and are caused by physical factors, forces and natural phenomena. The occurrence of climate hazards is associated with the randomness of natural phenomena. Common categories of these hazards are drought and heat, floods and mudslides, snowdrifts and icy conditions, thunderstorms and lightning, and the intensification of the Earth's greenhouse effect (Tyburska, 2010, p. 85).

Negative human interference with the environment causes irreversible climate changes leading to the **greenhouse effect**. The emission of heat into the earth's atmosphere (created by the burning of raw materials and energy fuels) raises the temperature of the earth's surface and atmosphere which causes glaciers and ice sheets to melt. This automatically raises water levels in the seas and oceans. This means flooding of coastal areas, waterlogging of port cities and disappearance of low-lying islands in the Pacific Ocean. Artificial emissions of chemicals into the atmosphere are destroying the insulating ozone layer, which causes more and more solar heat and harmful thermal radiation to penetrate the Earth's surface.

In summary, almost all critical infrastructure facilities and systems are exposed to natural hazards. Uncontrolled fires or floods pose a serious threat to facilities related to energy, food or water supply. The amount of damage depends on the safeguards and protection a facility or system has in place to protect itself from various dangers.

Terrorist threats. The term terrorism is derived from the Greek word *treo* – 'to fear, to cower, to flee', and the Latin *terror* – 'fear, terror' (PWN, n.d.). The source of terrorist attacks is the transmission by the perpetrators of their social, social, economic, political or religious discontent (Jałoszyński, 2010, p. 275). Its victims are politicians, military officers, police officers, as well as ordinary citizens regardless of gender, age or education. Terrorist groups choose places that are safe for themselves and at the same time accessible to the public as the targets of their attacks. Terrorists planning an attack in another country choose those places where they can remain unnoticed for a long time, such as in big cities or international meetings. The most serious danger among the new threats to both the international system and the security of individual states, including Poland, is posed by organized international terrorism (Polko, 2008, pp. 25–26). This threat extends to individual states, entire regions and even the world in terms of the uncontrolled proliferation of weapons of mass destruction and their means of delivery. This threat continues to grow as the possibility of terrorists coming into possession of such weapons and their means of delivery becomes more and more real.

According to Jaruszewski (2013, p. 142), in addition to the demographic threat and low global economic growth, the greatest terrorist threats are terrorist acts carried out on the seas and oceans, and the most desirable targets for attacks are tankers, ships with dangerous cargoes, passenger and cruise ships, ferries and, interestingly, warships. In addition to floating vessels, threatened facilities also include seaports, transshipment and oil production facilities belonging to another country. The faces of terrorism are changing with changes in the economy, social sphere or technologies (Hoffman, 2001, p. 188).

The phenomenon of terrorism sees elements of guerrilla warfare in the form of the actions of dispersed groups and total warfare, in which there is the possibility of reaching for ABC weapons. The so-called phenomenon of asymmetry is used, which is often seen as a strategic concept of asymmetric warfare. By subjecting the aspect of terrorism to a detailed analysis, it was noticed that the most vulnerable, but also the least prepared, are the communities of developed democratic countries (Polko, 2008, pp. 25–26). It is in such countries that any terrorist act, barring concrete destruction and the fear psychosis created, can cause a restriction of civil liberties, the consequence of which will be the formation of social discontent that harms the foundations of democracy (Wróbel, 2016, pp. 13–14). Therefore, it is believed that terrorist war in the 21st century has become a strategic weapon in the struggle for so-called higher values. Values that, according to the terrorists, are more important than the lives of innocent people and the preservation of human dignity. Therefore, the phenomenon of terrorism is extremely dangerous with regard to the security of citizens and should receive special attention from the relevant services.

Today, one of the threats related to terrorist attacks on the state's critical infrastructure, that has recently emerged, is the threat posed by unmanned

aerial vehicles, commonly known as drones. Today's drone used against critical infrastructure poses a challenge to it. Drones are very quiet, they cannot be heard or seen, and they are capable of spying on technical infrastructure. You need to be aware that the airspace around critical infrastructure is the least secured and you can practically fly with impunity using unmanned aerial vehicles. The elements of critical infrastructure that are most susceptible to attack by drones are: energy supply systems, energy raw materials and fuels, communication systems, ICT network systems, production systems, storage, pipelines. The state's response to disruptions related to drone attacks on critical infrastructure is to build a self-regulation mechanism based on monitoring threats, neutralizing them, and if this fails, restoring the state before the disruption, and until then, providing forms of substitute action (Pietrek & Pietrek, 2022, pp. 169–170).

Analysis of on research results – assessment of critical infrastructure systems and facilities

The research conducted in 2021 was of a pilot and fragmentary nature, showing only the positive or negative feelings of the respondents regarding the assessment of critical infrastructure. The research shows that the economic and social role of critical infrastructure requires a systemic approach to its protection, while ensuring its normal functioning. This is related to organizing such solutions that are adequate to the needs posed by the population. Broad expectations of the reliability of critical infrastructure make it necessary to involve various entities in its protection, which should have sufficient competence, knowledge and tools to counter threats by reducing the possibility of their occurrence and to remove their consequences, including restoring the functionality of this infrastructure.

The extent of preparation of entities protecting critical infrastructure is extremely important. These activities must be subject to control, which can be implemented by preparing, conducting and analysing Multimedia Decision Training. However, due to the declarative and unsanctioned nature of the participation of critical infrastructure protection entities in the infrastructure protection program, its organization may be the subject of exercises, such as in the form of decision-making games, recommended by the Government Security Center (GSC).

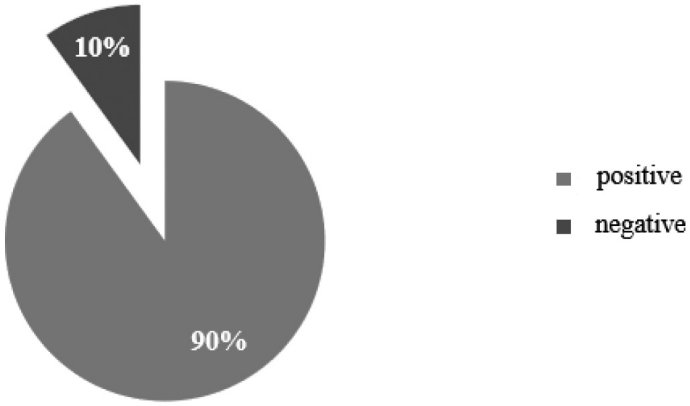
Conducting inspections of the preparation of entities involved in the protection of critical infrastructure in Poland requires:

- defining the essence of critical infrastructure protection, which is a difficult undertaking, carried out in relation to threats of various origins, involving dependencies of critical infrastructures in relation to each other that are not fully recognized;
- clarifying the legal basis for critical infrastructure protection;
- defining the assumptions of critical infrastructure protection in Poland taking into account the assignment of tasks for the protection of critical infrastructure to the tasks and structures of crisis management;
- identifying the entities for critical infrastructure protection in Poland, the tasks they carry out, their capabilities and initiatives aimed at improving critical infrastructure security;
- specifying the principles of cooperation between critical infrastructure protection entities in Poland;
- defining the scope of preparation of critical infrastructure protection entities in Poland.

Given the gradual achievement of the set goals and the acquisition of new experience, the continuous involvement of entities participating in the protection of critical infrastructure in Poland is inevitable. The pursuit of synergistic effects requires the involvement not only of critical infrastructure operators, but also of the public administration responsible for crisis management. Public-private cooperation becomes a guarantee of a more complete involvement of the private sector and public administration in protecting local communities from the effects of critical infrastructure dysfunction. The entities in question should be sufficiently competent for the tasks entrusted to them in preventing threats, risks or vulnerabilities, mitigating and neutralizing the effects of critical infrastructure dysfunctions, and rapidly restoring them when necessary, and their level of preparedness should be subject to regular and evaluation.

In order to be able to assess the security and security methods of critical infrastructure systems and facilities, 50 respondents were asked to express their opinion on this aspect. The metric shows the characteristics of the survey group in terms of gender, age, education, place of residence and affiliation with uniformed formations. The study included 15 women, accounting for 30% of the respondents, and 35 men, accounting for 70%. The respondents participating in the study formed a very diverse group in terms of age. There were no individuals under the age of 20. The largest group, nearly half of all respondents, were middle-aged 31–40 year olds – 48%. Slightly smaller was the percentage of those aged 21–30 – 26% and 41–50 – 22%. The smallest group was made up of people over 50 years old – 4%.

Figure 1
Survey group opinion on the protection of critical infrastructure in Poland



Source: own study.

Taking into account the education of the respondents, the largest group, 68%, were those with higher education. One in five respondents – 20% have so far obtained a secondary education, and only 6% a vocational education. The largest group of those taking part in the survey were those living in the countryside – 40%, 28% live in a city of up to 20,000 residents. One in five respondents lives in a city with a population of 20,000 to 50,000. The remaining 12% of respondents live in a city with a population of 50,000 to 100,000. Most of the survey participants serve in the Polish Army – 64%, 20% in the Police, and only 16% in the Border Guard.

The results of the respondents' opinions on the protection of critical infrastructure presents Figure 1.

Substance-related questions focused on survey participants' opinions on: critical infrastructure protection (including facilities and systems), potential threats to Poland's critical infrastructure, and the hierarchy on the issue of threats related to the protection of critical infrastructure facilities and systems. As many as 90% of respondents believe that the protection of critical infrastructure in Poland is adequate, only 10% believe that it is inadequate, and in justifying their choice, this group recognizes that some elements of this infrastructure are not protected at all, or that protection is reduced to technical or mechanical security only. One person indicates that there are too few IT specialists – programmers who can design security systems, and that it is too expensive to operate security and protection systems. Figure 2 presents the results of respondents' opinions on the protection of critical infrastructure facilities and systems.

In the case of protection of objects and systems of critical infrastructure in Poland, as many as 80% of respondents said that it is sufficient. Unfortunately, one in five respondents felt that this protection was not adequate. Among the reasons cited here was the weakness of safeguards regarding infrastructure related to the provision of water to residents, including insufficient protection of deep wells, transportation systems. Respondents also made comments as to poor security regarding internet access. Table 1 shows potential threats to Poland's critical infrastructure as perceived by respondents.

The largest group of people said that Poland's critical infrastructure is most threatened by disasters and natural hazards. This is the opinion of 82% of respondents; 12% of respondents indicated accidental threats, and 6% indicated deliberate (intentional) threats.

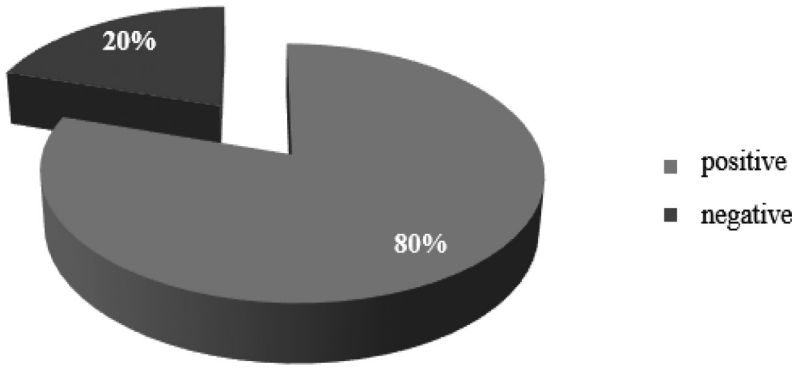
Of the natural threats, respondents see the greatest danger in the depletion of non-renewable resources – 40%, weather problems – 32%, environmental problems – 20%; 4% of respondents each indicated that demographic and social problems are the biggest natural threats.

With regard to accidental threats in the opinion of those surveyed, transportation disasters are the most dangerous, as highlighted by as many as 78% of people; 12% see danger in data loss or damage, 4% in human error, and 2% each in the release of hazardous materials, building disasters and energy disasters.

Considering targeted threats, respondents believe computer crimes are the most dangerous, with 40%, and 30% believe terrorist activity. Among the remaining group, 10% of respondents each express their opinion that the greatest danger is caused by espionage, diversionary or sabotage activities and deliberate disinformation.

The next question asked which system respondents believe is most at risk? Among the most

Figure 2
The opinion of the survey group on the protection of objects and systems of critical infrastructure in Poland



Source: own study.

Table 1
Potential threats to Polish critical infrastructure in the opinion of respondents

Type of threat	*n*	%
Natural hazards	41	82
Accidental threats	6	12
Informed threats	3	6
Total	50	100

Source: own study.

threatened systems, respondents cited the energy, energy resources and fuel supply system at 40%, the financial system at 28%, the water supply system at 10%, the transportation system at 8% and the food supply system; 2% of respondents each cited the communications system, the health care system, the emergency system, the system that ensures the operation of public administration, and the system for the production, storage, storage and use of chemical and radioactive substances as the most endangered system.

Another question asked concerned the most important issues in critical infrastructure protection. The most important issues in critical infrastructure protection were considered by respondents to be cooperation between the public administration and owners or subsidiaries of critical infrastructure facilities, installations or equipment in terms of their protection – 30% as well as restoration of critical infrastructure – 28%. A slightly smaller percentage considers the collection and processing of information on threats to critical infrastructure to be the most important aspect – 22%, and the development and implementation of procedures in case of threats to this infrastructure – 20%.

Analysing the degree of importance of forms of protection in the event of an emergency, the largest number of people considered technical protection – 30%, physical protection – 26%, ICT protection – 20% and personal protection – 14%. The least important, in the opinion of respondents, is legal protection – 2% of respondents believe so, as well as assistance from the government side in the reconstruction of the damaged or destroyed element – as indicated by 8% of respondents.

Considering 10 aspects, such as analysing the degree of threat to the facility, assessing the current state of security, ensuring the safety of the occupants, controlling the movement of people, controlling the movement of materials, controlling the technical security of the facility, complying with regulations and procedures, ensuring the reliable operation of the facility or system, protecting against theft, damage, vandalism and maintaining official secrecy, respondents were asked to prioritize them. Table 2 shows this hierarchy for facilities, and Table 3 – for critical infrastructure protection systems.

Respondents considered ensuring the safety of people on the premises and maintaining official secrecy to be the most important aspect in facility security. The respondents considered control of personnel movement, control of material movement, ensuring reliable operation of the facility or system, protection against theft, destruction and vandalism to be of medium importance. On the other hand, analysing the degree of threat to the facility, assessing the current state of security, controlling the technical security of the facility, and complying with regulations and procedures are considered the least important.

Table 2
Importance of each aspect in protecting facilities

Aspect	Importance of aspect [%]				
	1	2	3	4	5
Analysis of the degree of threat to the facility	72	20	6	2	0
Assessment of the current state of protection	68	18	10	2	2
Ensuring the safety of the occupants of the facility	0	0	0	20	80
Control of personnel movement	24	20	38	10	8
Control of material movement	6	12	60	12	2
Control of technical security of the facility	42	30	12	8	8
Compliance with regulations and procedures	64	20	16	0	0
Ensuring reliable operation of the facility	10	18	50	20	2
Protection against theft, destruction, vandalism	6	22	38	20	14
Maintaining service secrets	2	2	14	20	62

Source: own study.

Table 3
Importance of individual aspects in system protection

Aspect	Importance of aspect [%]				
	1	2	3	4	5
Analysis of the degree of threat to the system	20	64	6	2	8
Assessment of the current state of protection	8	12	72	4	4
Ensuring the security of the system	2	20	56	20	2
Systematic control of the system	2	2	18	10	68
Control of system repairs	18	22	40	18	2
Control of authorizations of people working in the system	0	28	42	26	4
Control of technical security of the system	0	0	0	28	72
Compliance with regulations and procedures	4	22	50	20	4
Ensuring reliable operation of the system	0	20	28	38	14
Protection against theft, destruction, vandalism	0	2	18	28	52
Maintaining service secrets	8	10	20	40	22

Source: own study.

Research conclusions

The most important in the protection of the system according to the opinion of the respondents is the control of technical security of the system, its regularity and protection against theft, destruction, vandalism. A point less important is maintaining official secrecy and ensuring reliable operation of the system. Of medium importance to respondents is the evaluation of the current state of security, ensuring the security of the system, compliance with regulations and procedures, control of the authority of people working in the system, and control of system repairs. Respondents considered the analysis of the degree of threat to the system to be the least important aspect.

The growing importance of critical infrastructure facilities and systems to state security derives from their strategic importance in sustaining the uninterrupted functioning of the state under modern threats. The threat of a terrorist attack, regional instability near national borders, the use of weapons of mass destruction or the potential possibility of a crisis situation requires increased efforts to prevent, limit or minimize the loss and destruction they will bring with them. Critical infrastructure systems and facilities are particularly important for the proper functioning of state security. Their destruction can negatively affect the sense of security in citizens and contribute to the weakening of our country. Particularly dangerous are natural, civilization and terrorist threats hence the need to develop specific systems for the protection of critical infrastructure objects and systems. Their security is provided by physical, technical, ICT and legal protection. To make this protection as effective as possible, the constantly updated and responsive Act on crisis management obliged the Government Security Center to create a National Program for the Protection of Critical Infrastructure.

Summary

This article was an attempt to examine the need to protect critical infrastructure systems and facilities resulting from their strategic importance and their security in light of possible threats.

The objective presented in the paper, the main research problem and the considerations undertaken in the article allowed the author to formulate the following general conclusions:

1. Threats to critical infrastructure systems and objects have a significant impact on the forms of their protection (depending on the projected threat to the object, appropriate measures are applied).
2. The importance of systems and the critical infrastructure objects that form them is particularly important for state security. Critical infrastructure is formed by systems that provide both transportation, health care, food and water supply, the supply of energy resources and many others. Without these basic components, human existence may be impossible, and will certainly be threatened. A reduced sense of security for individual citizens will translate into a reduced sense of security for society as a whole, with even greater losses and dangers behind it.
3. All kinds of threats are dangerous to critical infrastructure. Destructive impact will be brought by natural, civilizational as well as terrorist threats. However, it is impossible to say unequivocally which type of threat will bring the most damage and destruction. It all depends on the area occupied, the damaged system or object as well as the amount of destructive force. Depending on the criterion adopted (material losses, amount of damage, level of danger, etc.), it will be possible to recognize which threat is the most serious and has the greatest destructive power.
4. The elements of critical infrastructure that are most susceptible to attack by drones are: energy supply systems, energy raw materials and fuels, communication systems, ICT network systems, production systems, storage, pipelines.
5. Security of critical infrastructure systems and facilities will be provided by physical, technical, personal, ICT and legal protection. At the same time, respondents considered the most important aspect in protecting facilities to be ensuring the safety of people on the premises and maintaining official secrecy. In turn, the most important aspect of system protection is the control of technical system security, its regularity and protection against theft, destruction, vandalism. Slightly less important is the maintenance of official secrecy and ensuring the reliable operation of the system.

In summary, it should be said that the protection of critical infrastructure systems and facilities should be one of the most important tasks facing our state in the field of national security. Protection plans should be created and updated based also on the experience of institutions as well as member states of the European Union and the North Atlantic Treaty Organization.

References/Bibliografia

Ackerman, P. (2017). *Industrial Cybersecurity: Efficiently Secure Critical Infrastructure Systems*. Packt Publishing.

Act of 26 April 2007 on crisis management (Journal of Laws of 2017 No. 91, item 209, as amended).

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

Dzido, H. (2022). *Europejska infrastruktura krytyczna*, Spatium.

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

Ficoń, K. (2007). *Inżynieria zarządzania kryzysowego – podejście systemowe*, BEL Studio.

Gopalakrishnan, K., & Peeta, S. (2010). *Sustainable and Resilient Critical Infrastructure Systems: Simulation, Modeling, and Intelligent Engineering*. Springer.

Hoffman, B. (2001). *Oblicza terroryzmu*. Grupa Wydawnicza Bertelsmann Media.
Holliday, B. (2017). *Drones: The Complete Collection*. CreateSpace Independent Publishing Platform.
Jakubczak, R. (Ed.). (2006). *Bezpieczeństwo narodowe Polski w XXI w*. Bellona.
Jałoszyński, K. (2010). Obiekty infrastruktury krytycznej a działania defensywne i ofensywne w obszarze zagrożeń terrorystycznych. In: A. Tyburska (Ed.), *Ochrona infrastruktury krytycznej*. Wyższa Szkoła Policji.
Jaruszewski, W. (2013). Terroryzm w dobie współczesnych konfliktów. *Zeszyty Naukowe Wydziału Nauk Ekonomicznych Politechniki Koszalińskiej*, (17).
Katina, P. F. &, Hester, P. T. (2013). Systemic determination of infrastructure criticality. *International Journal of Critical Infrastructures*, *9*(3), 211–225.
Kisilowski, M., Skomra, W., Smagowicz, J., Szwarc, K., & Wiśniewski, M. (2021). *Zarządzanie bezpieczeństwem infrastruktury krytycznej i ciągłością usług kluczowych państwa*. Oficyna Wydawnicza Politechniki Warszawskiej.
Knapp, E. & Langill, J. T. (2011). *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Syngress. https://doi.org/10.1016/C2010-0-66555-2
Lidwa, W., Krzeszowski, W., Więcek, W., & Kamiński, P. (2012). *Ochrona infrastruktury krytycznej*, AON.
Molendowska, M., Ostrowska, M., & Górski, P. (2021). *Infrastruktura krytyczna jako element bezpieczeństwa – wymiar europejski i krajowy*. Wydawnictwo A. Marszałek.
Moteff, J. D. (2015). *Critical Infrastructures: Background, Policy, and Implementation*. Congressional Research Service.
Piątek, Z., & Truchan J. R. (2013). *Technologie w ochronie infrastruktury krytycznej zewnętrznego kraju Unii Europejskiej*. Stowarzyszenie Ruch Wspólnot Obronnych.
Pietrek, G., & Pietrek, M. (2022). Bezzałogowe statki powietrzne jako zagrożenie dla infrastruktury krytycznej państwa. *Zeszyty Naukowe SGSP/Szkoła Główna Służby Pożarniczej*, (83), 163–174. https://doi.org/10.5604/01.3001.0016.0230
Polko, R. (2008). *Grom w działaniach przeciwterrorystycznych*. Biuro Bezpieczeństwa Narodowego.
Presch-Cronin, K., & Marion, N. E. (2016). *Critical Infrastructure Protection, Risk Management, and Resilience: A Policy Perspective*. CRC Press.
PWN. (n.d.). Terroryzm. In: *Słownik języka polskiego PWN*. https://www.sjp.pwn.pl/szukaj/terroryzm.html (accessed 25.04.2023).
Pyznar, M. (2010). The National Critical Infrastructure Protection Program in the protection system of this infrastructure – the vision of the Government Center for Security. In: A Tyburska (Ed.), *Critical Infrastructure Protection*. Police Academy in Szczytno.
Rządowe Centrum Bezpieczeństwa. (2013). *Narodowy Program Ochrony Infrastruktury Krytycznej*. https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej (accessed 25.04.2023).
Tyburska, A. (2010). Infrastruktura krytyczna – kluczowe problemy oraz strategiczne kierunki działań. In: Z. Piątek, & A. Letkiewicz (Ed.), *Terroryzm a infrastruktura krytyczna państwa – zewnętrznego kraju Unii Europejskiej*. Stowarzyszenie Ruch Wspólnot Obronnych.
Wróbel, R. (2016). *Przygotowanie podmiotów ochrony infrastruktury krytycznej w Polsce*. Szkoła Główna Służby Pożarniczej.

Dr hab. Maciej Kaźmierczak, prof. ASzWoj

Associate Professor at the War Studies University at the Institute of Logistics at the Department of Logistics Basis. His has scientific achievements in the field of social sciences in the discipline of security science as well as management and quality, taking into account the issues of logistics, especially related to the processes of supply logistics and warehouse management of economic and military entities, state energy security and military logistics. A significant part of his scientific and didactic interests is supply logistics (supplies, the possibility of obtaining) and warehouse management (inventories, storage, availability, distribution) as an economic and defence practice related to the integration of economic and military logistics theory and practice.

Dr hab. Sławomir Byteń, prof. WAT

Doctor of military sciences in the scientific discipline of defence studies (2009) and habilitated doctor in the scientific discipline of security studies (2022). In the years 2003–2017, senior logistics specialist and head of the Exercise Programming Department at the War Games and Simulation Center at the National Defence University. Currently, he is a research and teaching employee of the Institute of Logistics at the Faculty of Security, Logistics and Management at the Military University of Technology. He specializes in modelling logistics processes in military IT systems. He is the author of five monographs and several dozens of scientific articles on military security.

Dr hab. Maciej Kaźmierczak, prof. ASzWoj

Profesor Akademii Sztuki Wojennej w Instytucie Logistyki w Katedrze Podstaw Logistyki. Jego dorobek naukowy zawiera się w obszarze nauk społecznych w dyscyplinach nauki o bezpieczeństwie oraz nauki o zarządzaniu i jakości, z uwzględnieniem problematyki logistyki, szczególnie związanej z procesami logistyki zaopatrzenia i gospodarki magazynowej podmiotów gospodarczych i wojskowych, bezpieczeństwem energetycznym państwa oraz zabezpieczeniem logistycznym wojsk. Znaczącą część zainteresowań naukowych i dydaktycznych stanowi logistyka zaopatrzenia (dostawy, możliwość pozyskania) i gospodarka magazynowa (zapasy, sposób przechowywania, dostępność, dystrybucja) jako praktyka gospodarczo-obronna związana z integracją teorii i praktyki logistyki gospodarczej i wojskowej.

Dr hab. Sławomir Byteń, prof. WAT

Doktor nauk wojskowych w dyscyplinie naukowej nauki o obronności (2009) oraz doktor habilitowany w dyscyplinie naukowej nauki o bezpieczeństwie (2022). W latach 2003–2017 starszy specjalista ds. logistyki i szef Pracowni Programowania Ćwiczeń w Centrum Symulacji i Komputerowych Gier Wojennych Akademii Obrony Narodowej. Obecnie pracownik badawczo-dydaktyczny Instytutu Logistyki na Wydziale Bezpieczeństwa, Logistyki i Zarządzania Wojskowej Akademii Technicznej. Specjalizuje się modelowaniu procesów logistycznych w wojskowych systemach informatycznych. Jest autorem pięciu monografii i kilkudziesięciu artykułów naukowych z zakresu bezpieczeństwa militarnego.