SFT VOL. 59 ISSUE 1, 2022, PP. 166–181

Łukasz Roman[a)], Krzysztof Cygańczuk[b)*]

[a)] *The Academy of Justice/ Szkoła Wyższa Wymiaru Sprawiedliwości w Warszawie*
[b)] *Scientific and Research Centre for Fire Protection – National Research Institute / Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej – Państwowy Instytut Badawczy*
[*] *Corresponding author / Autor korespondencyjny: kcyganczuk@cnbop.pl*

Legal Dimension of the Protection of Critical Infrastructure – Selected Aspects

Prawny wymiar ochrony infrastruktury krytycznej – wybrane aspekty

ABSTRACT

Aim: As part of this article, an attempt was made to present the legislative process in Poland regarding critical infrastructure, for which valid is the Act of 26 April 2007 on crisis management, specifying, inter alia, authorities competent in crisis management and their tasks and principles of operation in this area as well as implementing acts issued on its basis. The introduced legal regulations define both the concept of critical infrastructure, its protection and activities related to the prevention of crisis situations, reacting in the event of their occurrence and preparation to take control over them, as well as removing their effects and recreating key resources.

Introduction: Regulations concerning the protection of critical infrastructure are included in legal acts covering various areas of the country's functioning, including telecommunications activities, production and trade in fuels and electricity, performance of defence tasks by entrepreneurs, creation of strategic reserves, powers of the minister competent for the State Treasury in some companies, protection of persons and the property. The protection of critical infrastructure is related to the raison d'état, which indicates the need to make special efforts to protect the country's key infrastructure. Therefore, it is reasonable to present selected legal elements needed to protect critical infrastructure, especially those issues that ensure the continuity of the operation of public administration bodies, which are to ensure the safety of the citizens.

Methodology: The article was prepared based on the analysis of the literature on the subject and the analysis of legal acts in the area of strengthening the concept of critical infrastructure, taking into account the current situation related to the pandemic and, consequently, the loss of some officers and employees. During the analysis of the conducted research, compact publications, acts of Polish law as well as guidelines and recommendations published on the websites of governmental institutions were used.

Conclusions: In the protection of critical infrastructure, there is a need to introduce legal regulations within the framework of cooperation between institutions. The preparation of effective activities in the area of critical infrastructure requires a comprehensive approach, including: physical, technical, personal, ICT, legal protection, as well as assistance from the government in the reconstruction of the damaged element. Each of the areas mentioned above is a complex set of activities requiring general and specialist knowledge, sometimes expert knowledge, extensive practical experience (using the so-called good practices), risk analysis skills, and risk prediction (profiling).

Keywords: act on crisis management, legal acts, crisis management, protection of critical infrastructure, identification
Type of article: review article

Received: 03.01.2022; Reviewed: 18.01.2022; Accepted: 25.01.2022;
Authors` ORCID IDs: Ł. Roman – 0000-0002-4159-3557; K. Cygańczuk – 0000-0003-1550-5880;
The authors contributed the equally to this article;
Please cite as: SFT Vol. 59 Issue 1, 2022, pp. 166–181, https://doi.org/10.12845/sft.59.1.2022.10;

ABSTRAKT

Cel: W ramach niniejszego artykułu podjęto próbę przybliżenia procesu legislacyjnego w Polsce dotyczącego infrastruktury krytycznej, dla której właściwa jest Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym określająca m.in. organy właściwe w sprawach zarządzania kryzysowego oraz ich zadania i zasady działania w tym obszarze oraz akty wykonawcze wydane na jej podstawie. Wprowadzone regulacje prawne określają zarówno pojęcie infrastruktury krytycznej, jej ochrony, jak i działań związanych z zapobieganiem sytuacjom kryzysowym, reagowaniem w przypadku ich wystąpienia i przygotowaniem do przejmowania nad nimi kontroli, a także usuwaniu ich skutków oraz odtwarzaniu kluczowych zasobów.

Wprowadzenie: Regulacje dotyczące ochrony infrastruktury krytycznej znajdują się w aktach prawnych obejmujących różne dziedziny funkcjonowania państwa, m.in. działalność telekomunikacyjną, wytwarzanie i obrót paliwami oraz energią elektryczną, wykonywanie zadań obronnych przez przedsiębiorców, tworzenie rezerw strategicznych, uprawnienia ministra właściwego do spraw Skarbu Państwa w niektórych spółkach, realizację ochrony

osób i mienia. Ochrona infrastruktury krytycznej w swoim przedmiocie związana jest z racją stanu, co wskazuje na konieczność podjęcia szczególnych starań w zakresie ochrony kluczowej infrastruktury państwa. W związku z powyższym zasadne jest przedstawienie wybranych elementów prawnych potrzebnych do ochrony infrastruktury krytycznej, zwłaszcza tych kwestii, które zapewniają ciągłość działania organów administracji publicznej, mających zapewnić bezpieczeństwo obywateli.

Metodologia: Artykuł został opracowany przy wykorzystaniu analizy literatury przedmiotu oraz analizy aktów prawnych w zakresie wzmocnienia pojęcia infrastruktury krytycznej, biorąc pod uwagę obecną sytuację związaną z pandemią i co za tym idzie – utratę części funkcjonariuszy i pracowników. Podczas analizy przeprowadzonych badań wykorzystano publikacje zwarte, akty prawa polskiego oraz wytyczne i zalecenia ogłoszone na stronach instytucji rządowych.

Wnioski: W ochronie infrastruktury krytycznej zachodzi potrzeba wprowadzenia regulacji prawnych w ramach współpracy między instytucjami. Przygotowanie efektywnych działań w zakresie infrastruktury krytycznej wymaga kompleksowego podejścia, obejmującego ochronę: fizyczną, techniczną, osobową, teleinformatyczną, prawną, a także pomoc strony rządowej w odbudowie zniszczonego (uszkodzonego) elementu. Każdy z wymienionych obszarów stanowi złożony kompleks działań wymagający wiedzy ogólnej oraz specjalistycznej, niekiedy eksperckiej, bogatego doświadczenia praktycznego (korzystania z tzw. dobrych praktyk), umiejętności analizy ryzyka, a także przewidywania (profilowania) zagrożeń.

Słowa kluczowe: ustawa o zarządzaniu kryzysowym, akty prawne, zarządzanie kryzysowe, ochrona infrastruktury krytycznej, identyfikacja

Typ artykułu: artykuł przeglądowy

Przyjęty: 03.01.2022; Zrecenzowany: 18.01.2022; Zaakceptowany: 25.01.2022;
Identyfikatory ORCID autorów: Ł. Roman – 0000-0002-4159-3557; K. Cygańczuk – 0000-0003-1550-5880;
Autorzy wnieśli równy wkład merytoryczny w powstanie artykułu;
Proszę cytować: SFT Vol. 59 Issue 1, 2022, pp. 166–181, https://doi.org/10.12845/sft.59.1.2022.10;

Introduction

As part of this article, an attempt was made to present the legislative process in Poland regarding critical infrastructure, for which valid is the Act of 26 April 2007 on crisis management [1] which specifies, inter alia, authorities competent in crisis management and their tasks and principles of operation in this area as well as implementing acts issued on its basis. The introduced legal regulations define both the concept of critical infrastructure, its protection, as well as activities related to the prevention of crisis situations, reacting in the event of their occurrence and preparation to take control over them, as well as removing their effects and recreating key resources [2].

Legal regulations referring to the protection of critical infrastructure have been included in many legal acts [1, 3–5], covering various areas of the functioning of the country. However, some legal acts do not refer directly to the critical infrastructure (CI), and the analysis of the used terms, including those related to the facilities, indicates their similar, and often even the same meaning [6]. In this subject, the following areas of activity are distinguished: telecommunications activities, production and trading of fuels and electricity, performing defence tasks by entrepreneurs, creating strategic reserves, powers of the minister competent for the State Treasury or protection of persons and property [7]. Therefore, it is reasonable to state that the formal and legal conditions for the protection of CI existed before the entry into force of the Act of 26 April 2007 on crisis management [1].

The term critical infrastructure refers primarily to national resources that are essential for the functioning of the state and its citizens. This concept defines physical objects, supply systems, technologies and information networks which, as a result of destruction, disruption or damage, become unavailable for

Wprowadzenie

W ramach niniejszego artykułu podjęto próbę przybliżenia procesu legislacyjnego w Polsce dotyczącego infrastruktury krytycznej, dla której właściwa jest ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym [1] określająca m.in. organy właściwe w sprawach zarządzania kryzysowego oraz ich zadania i zasady działania w tym obszarze oraz akty wykonawcze wydane na jej podstawie. Wprowadzone regulacje prawne określają zarówno pojęcie infrastruktury krytycznej, jej ochrony, jak i działań związanych z zapobieganiem sytuacjom kryzysowym, reagowaniem w przypadku ich wystąpienia i przygotowaniem do przejmowania nad nimi kontroli, a także usuwaniu ich skutków oraz odtwarzaniu kluczowych zasobów [2].

Regulacje prawne dotyczące ochrony infrastruktury krytycznej zostały umiejscowione w wielu aktach prawnych [1, 3–5], obejmujących różne dziedziny funkcjonowania państwa. Niektóre akty prawne nie odnoszą się jednak bezpośrednio do infrastruktury krytycznej (IK), a analiza używanych terminów, w tym dotyczących obiektów, wskazuje na ich zbliżone, a często wręcz tożsame znaczenie [6]. W tym przedmiocie wyodrębnia się takie obszary działalności jak: działalność telekomunikacyjną, wytwarzanie i obrót paliwami oraz energią elektryczną, wykonywanie zadań obronnych przez przedsiębiorców, tworzenie rezerw strategicznych, uprawnienia ministra właściwego do spraw Skarbu Państwa czy ochronę osób i mienia [7]. Zasadne jest zatem stwierdzenie, iż warunki formalno-prawne ochrony IK istniały jeszcze przed wejściem w życie ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym [1].

Termin infrastruktura krytyczna dotyczy przede wszystkim zasobów krajowych mających podstawowe znaczenie dla funkcjonowania państwa i jego obywateli. Pojęcie to określa obiekty fizyczne, systemy zaopatrzenia, technologie i sieci informatyczne,

a certain period of time, and thus may significantly affect the social or economic determinants of the society, as well as affect the ability to provide defence and national security. Critical infrastructure are real and cybernetic systems (and in these systems objects, devices or installations) necessary for the functioning of the economy and the country. It plays a key role in the functioning of the country and the life of its citizens. As a result of events caused by natural forces or resulting from human activities, critical infrastructure may be destroyed, damaged, and its operation may be disrupted, which may endanger the lives and property of the citizens. At the same time, such events negatively affect the economic development of the country.

Legal aspects of critical infrastructure

Pursuant to art. 3 of the Act on Crisis Management [1], the concept of critical infrastructure should be understood as linked systems and their functionally, key objects for the security of the country and its citizens and for ensuring the efficient functioning of public administration bodies, as well as institutions and entrepreneurs. The group of systems that may be part of this infrastructure is extensive and includes, among others: energy supply systems, transport systems, energy resources and fuels, as well as communication systems, IT networks, financial systems, food and water supply systems, systems for production, storage and use of chemical and radioactive substances, health protection and rescue systems as well as systems ensuring the continuity of public administration operations.

które w wyniku zniszczenia, zakłócenia lub uszkodzenia stają się niedostępne przez określony czas, a tym samym mogą znacząco uderzać w społeczne lub ekonomiczne determinanty społeczeństwa, a także wpływać na możliwości zapewnienia obrony i bezpieczeństwa narodowego. Infrastruktura krytyczna to rzeczywiste i cybernetyczne systemy (a w tych systemach obiekty, urządzenia bądź instalacje) niezbędne do funkcjonowania gospodarki i państwa. Pełni ona kluczową rolę w funkcjonowaniu państwa i życiu jego obywateli. W wyniku zdarzeń spowodowanych siłami natury lub będących konsekwencją działań człowieka, infrastruktura krytyczna może być zniszczona, uszkodzona, a jej działanie może ulec zakłóceniu, przez co zagrożone może być życie i mienie obywateli. Równocześnie tego typu wydarzenia negatywnie wpływają na rozwój gospodarczy państwa.

Prawne aspekty infrastruktury krytycznej

Zgodnie z art. 3 ustawy o zarządzaniu kryzysowym [1] przez pojęcie infrastruktury krytycznej należy rozumieć systemy oraz wchodzące w ich skład, powiązane ze sobą funkcjonalnie, obiekty kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Grupa systemów, które mogą wchodzić w skład tej infrastruktury jest rozbudowana i obejmuje, m.in. systemy zaopatrzenia w energię, transportowe, surowce energetyczne i paliwa, a także systemy łączności, sieci IT, systemy finansowe i zaopatrzenia w żywność oraz wodę, systemy produkcji i przechowywania oraz stosowania substancji chemicznych i promieniotwórczych, systemy ochrony zdrowia i ratownicze oraz zapewniające ciągłość działania administracji publicznej.

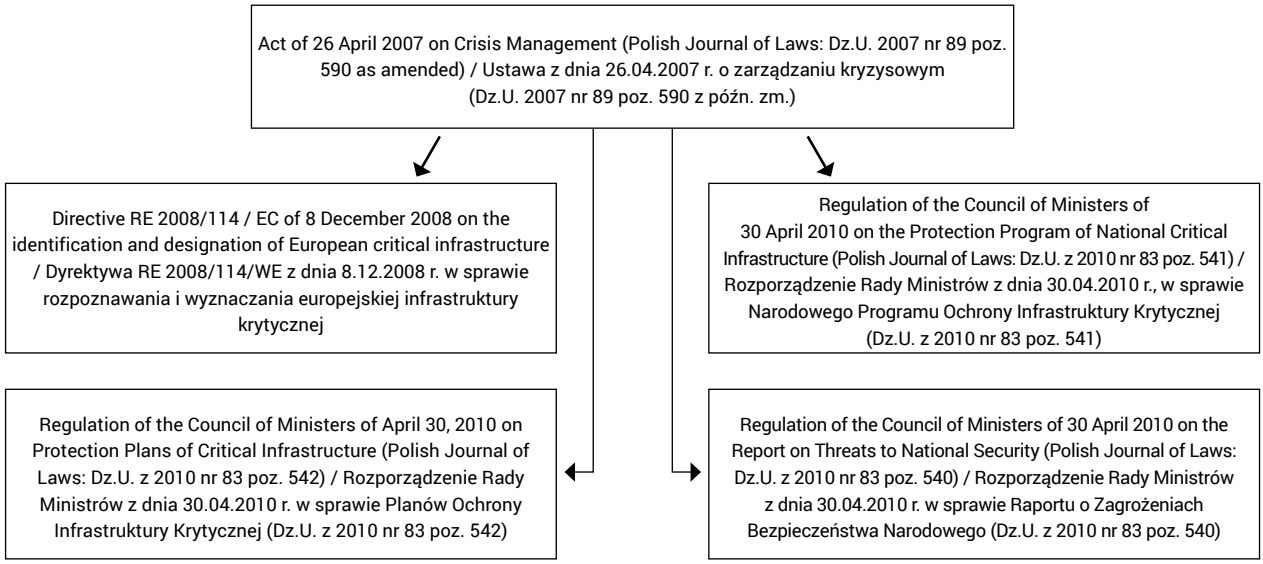

Figure 1. Basic legal acts on critical infrastructure
Rycina 1. Podstawowe akty prawne dotyczące infrastruktury krytycznej
Source: Own elaboration.
Źródło: Opracowanie własne.

The legal act in force in Poland, on the basis of which certain systems are designated to the group of European Critical Infrastructure (ECI), is the EU Council Directive on the identification and designation of ECI [9], establishing the procedure for defining ECI and the rules common to EU approaches to assessing the need to improve the protection of such infrastructure, in order to better protect the population and minimize potential economic and social losses. An important element here is the fact that these are systems whose disruption or destruction would have a significant impact on at least two EU Member States.

Taking into account the applicable legal acts, it can be stated that their scope regulates, among others, the following issues in the area of the functioning and protection of critical infrastructure:

- preparation of solutions in the event of destruction or disruption of the functioning of critical infrastructure, including assistance to the population in ensuring its survival conditions until the infrastructure is restored;
- development and maintenance of protection plans of the critical infrastructure, including resources necessary to perform the tasks included in them;
- ensuring the functioning of public administration in the event of a threat and the possibility of recreating the critical infrastructure;
- ensuring continuous monitoring of threats;
- procedures for implementing tasks related to the protection of critical infrastructure, including response in the event of destruction or disruption of its functioning, and priorities for its protection and recovery;
- risk management by identifying significant threats to critical infrastructure, including prioritization in responding to specific risks and identifying the forces and resources necessary to eliminate them;
- preparation and maintenance of an inventory of objects and systems that make up the critical infrastructure;
- variants of operation in the event of threats or disturbances in the functioning of critical infrastructure and its reconstruction,
- principles of cooperation of public administration with owners and independent and dependent owners of facilities, installations or devices of critical infrastructure in terms of its protection, including the principles of providing information.

In addition to the legal acts mentioned above, special attention has been paid to those elements of critical infrastructure that are important for ensuring the continuity of the country's functioning, regardless of the type of threats. Therefore, other documents have also been issued, which in their records indicate the dimension in question in the area of critical infrastructure. They are, among others:

1. Regulation No. 67 of the Prime Minister of 15 October 2014 on the organization and operation of the Crisis Management Government Team [10], specifying the procedure and form of convening meetings as well as the rules of service and tasks of the team.
2. Regulation of the Prime Minister of 11 April 2011 on the

Aktem prawnym obowiązującym w Polsce, na podstawie którego wyznacza się określone systemy do grona europejskiej infrastruktury krytycznej (EIK), jest Dyrektywa Rady UE w sprawie rozpoznawania i wyznaczania EIK [9], ustanawiająca procedurę definiowania EIK oraz zasady wspólnego dla UE podejścia do oceny potrzeb w zakresie poprawy ochrony takiej infrastruktury, w celu lepszej ochrony ludności i minimalizowania potencjalnych strat ekonomicznych i społecznych. Istotnym elementem jest tutaj fakt, że chodzi o takie systemy, których zakłócenie lub zniszczenie miałoby istotny wpływ na co najmniej dwa państwa członkowskie UE.

Biorąc pod uwagę obowiązujące akty prawne, można stwierdzić, że swoim zakresem regulują one m.in. następujące kwestie w obszarze funkcjonowania i ochrony infrastruktury krytycznej:

- przygotowanie rozwiązań na wypadek zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej, w tym udzielanie pomocy ludności w zapewnieniu jej warunków przetrwania do momentu odtworzenia infrastruktury;
- opracowanie i utrzymywanie planów ochrony infrastruktury krytycznej, w tym zasobów niezbędnych do wykonywania zadań w nich ujętych;
- zapewnienie funkcjonowania administracji publicznej w sytuacji wystąpienia zagrożenia oraz możliwości odtworzenia infrastruktury krytycznej;
- zapewnienie ciągłego monitorowania zagrożeń;
- procedury realizacji zadań związanych z ochroną infrastruktury krytycznej, w tym reagowania w sytuacjach zniszczenia lub zakłócenia jej funkcjonowania oraz priorytety w zakresie jej ochrony oraz odtwarzania;
- zarządzanie ryzykiem poprzez wskazywanie istotnych zagrożeń dla infrastruktury krytycznej, w tym określanie priorytetów w reagowaniu na określone ryzyka i wskazanie sił oraz środków niezbędnych do ich wyeliminowania;
- przygotowywanie i utrzymywanie wykazu obiektów i systemów tworzących infrastrukturę krytyczną;
- warianty działania w sytuacji zagrożeń lub zakłócenia funkcjonowania infrastruktury krytycznej oraz jej odtwarzania,
- zasady współpracy administracji publicznej z właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej w zakresie jej ochrony, w tym zasady przekazywania informacji.

Poza wspomnianymi powyżej aktami prawnymi, szczególną uwagę zwrócono na te elementy infrastruktury krytycznej, które są istotne dla zapewnienia ciągłości funkcjonowania państwa, niezależnie od rodzaju występujących zagrożeń. Wobec tego zostały wydane również inne dokumenty, które w swoich zapisach wskazują na przedmiotowy wymiar w obszarze infrastruktury krytycznej. Są to m.in.:

1. Zarządzenie nr 67 Prezesa Rady Ministrów z dnia 15 października 2014 r. w sprawie organizacji i trybu pracy Rządowego Zespołu Zarządzania Kryzysowego [10], określające tryb i formę zwoływania posiedzeń oraz zasady obsługi i zadania zespołu.

organization and operation of the Government Centre for Security (RCB), specifying the structure and tasks of RCB [11],
3. Regulation of the Council of Ministers of 21 September 2018 amending the regulation on the determination of government administration bodies that will establish crisis management centres and the manner of their operation [12],
4. Act on the organization of tasks for national defence carried out by entrepreneurs [13], which allowed for creating a legal structure of an entrepreneur of special economic and defence importance, implementing tasks for the benefit of state defence (i.e. in the area of economic mobilization, militarization, operational planning, defence training) as well as under HN obligations),
5. Act on the protection of persons and property [14].

In the context of CI, the most important thing is that the Act mentioned above has distinguished the category of areas, facilities, devices and transports subject to mandatory protection, important for the defence, economic interest of the state, public safety and other important interests of the state (art. 5 sec. 2). The Act also indicated entities obliged to prepare lists of these installations (art. 5 sec. 3) and imposed on entities managing the installations the obligation to agree on their protection plans with the locally competent provincial police commander (art. 7 sec. 1). The Act on the protection of persons and property has distinguished in detail the elements of infrastructure of this importance (art. 5).

6. Act on aviation law [15].

The Act covers issues related to air navigation, airport ground infrastructure and aircraft. A separate chapter (art. 84–85) deals with rescue and fire protection of airports. Pursuant to art. 84, the airport operator is obliged, among others, to develop an action plan in an emergency, organize and ensure the functioning of the rescue and firefighting service equipped with specialized equipment, and maintain the necessary rescue and fire-fighting measures.

7. Act on rail transport [16].

The Act applies to railway infrastructure, part of which is part of the critical infrastructure. In this context, the Act also defines the principles of the management of railway infrastructure, by maintaining it in a condition ensuring safe railway traffic management (art. 5 sec. 1 point 3), as well as the manager's obligation to take action to eliminate the risk in a situation where the safety of railway traffic or the safety of passenger and goods transport is at risk (art. 5 sec. 5).

Moreover, for railway lines of national importance, the Act imposes on the Council of the Ministers the obligation to define their list by means of a regulation (art. 6 sec. 2). At the same time, the minister responsible for transport is obliged to define (in agreement with the minister of national defence) a list of railway lines of purely defensive importance (art. 6 sec. 3). The Act also contains provisions on the physical protection of the railway infrastructure. Art. 59 sec. 1 provides for the creation of railway security guards by one or more managers. Art. 60 sec. 1 of the Act specifies the tasks of this formation, indicating that it

2. Rozporządzenie Prezesa Rady Ministrów z dnia 11 kwietnia 2011 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa (RCB), określające strukturę i zadania RCB [11],
3. Rozporządzenie Rady Ministrów z dnia 21 września 2018 r. zmieniające rozporządzenie w sprawie określenia organów administracji rządowej, które utworzą centra zarządzania kryzysowego, oraz sposobu ich funkcjonowania [12],
4. Ustawa o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców [13], która pozwoliła na stworzenie konstrukcji prawnej przedsiębiorcy o szczególnym znaczeniu gospodarczo-obronnym, realizującego zadania na rzecz obronności państwa (tj. w zakresie mobilizacji gospodarki, militaryzacji, planowania operacyjnego, szkolenia obronnego, jak również wynikające z obowiązków państwa-gospodarza),
5. Ustawa o ochronie osób i mienia [14].

W kontekście IK najistotniejsze jest to, że w powyższej ustawie została wyodrębniona kategoria obszarów, obiektów, urządzeń i transportów podlegających obowiązkowej ochronie, ważnych dla obronności, interesu gospodarczego państwa, bezpieczeństwa publicznego i innych ważnych interesów państwa (art. 5 ust. 2). Ustawa wskazała również podmioty zobowiązane do sporządzania wykazów tych instalacji (art. 5 ust. 3) i nałożyła na podmioty zarządzające instalacjami obowiązek uzgadniania planów ich ochrony z właściwym miejscowo komendantem wojewódzkim policji (art. 7 ust. 1). Ustawa o ochronie osób i mienia wyodrębniła szczegółowo elementy infrastruktury o takim znaczeniu (art. 5).

6. Ustawa Prawo lotnicze [15].

Ustawa obejmuje zagadnienia dotyczące żeglugi powietrznej, naziemnej infrastruktury lotniskowej oraz statków powietrznych. Oddzielny rozdział (art. 84–85) dotyczy ratownictwa i ochrony przeciwpożarowej lotnisk. Zgodnie z art. 84, zarządzający lotniskiem zobowiązany jest m.in. do opracowania planu działania w sytuacji zagrożenia, zorganizowania i zapewniania funkcjonowania służby ratowniczo-gaśniczej wyposażonej w specjalistyczny sprzęt oraz utrzymywania niezbędnych środków ratowniczych i przeciwpożarowych.

7. Ustawa o transporcie kolejowym [16].

Ustawa odnosi się do infrastruktury kolejowej, której część wchodzi w skład infrastruktury krytycznej. W tym kontekście ustawa określa także zasady zarządzania infrastrukturą kolejową m.in. poprzez jej utrzymywanie w stanie zapewniającym bezpieczne prowadzenie ruchu kolejowego (art. 5 ust. 1 pkt 3), a także powstający po stronie zarządcy obowiązek podjęcia działań likwidujących zagrożenie w sytuacji, gdy zagrożone jest bezpieczeństwo ruchu kolejowego lub bezpieczeństwo przewozu osób i rzeczy (art. 5 ust. 5). Ponadto dla linii kolejowych o znaczeniu państwowym ustawa nakłada na Radę Ministrów obowiązek określenia ich wykazu w drodze rozporządzenia (art. 6 ust. 2). Jednocześnie minister właściwy w sprawach transportu zobowiązany jest do określenia (w porozumieniu z ministrem obrony narodowej) wykazu linii kolejowych o znaczeniu wyłącznie obronnym (art. 6 ust. 3). Ustawa zawiera także przepisy dotyczące fizycznej ochrony infrastruktury kolejowej. Art. 59 ust. 1 przewiduje tworzenie straży ochrony kolei przez

is, among others, responsible for the protection of human life or health, as well as property in the railway area, in trains and other railway vehicles.

8. Act on telecommunications law [17].

The Act regulates the principles of conducting business by providing telecommunications services. As a critical infrastructure protection tool, it is essential for many reasons. It defines a telecommunications undertaking, which in many cases allows to classify the installations, facilities and devices managed by it as part of the critical infrastructure telecommunications system (art. 2 point 27). In this context, operators are required to submit to the President of the Office of Electronic Communications (UKE) and make available to interested entities the technical specifications of the network termination points, radio interfaces and their changes, before the telecommunications services to be provided via these network termination points or radio interfaces become available to the users (art. 137 sec. 1). From the point of view of the protection of critical infrastructure, art. 178, 179 sec. 1 and 180f of the Act. Art. 178 sec. 1 indicates that "in the event of a particular threat", the President of UKE may, by way of a decision, impose certain obligations on telecommunications undertakings, guided by the size of the threat and the need to limit its effects and the principle of minimizing the negative effects of the imposed obligations. In turn, art. 179 orders such entrepreneurs to perform tasks and obligations in the area of preparation and maintenance of the indicated network elements to ensure telecommunications for the needs of the national security management system, including state defence, implemented in accordance with the principles set out in plans, decisions and agreements concluded between these entrepreneurs and interested entities [7].

9. Act on water law [18].

The Act, comprehensively regulating the issues of water management, includes, among others, regulations concerning strict protection and supervision of specific areas, important for the supply of drinking water, i.e. an element of critical infrastructure. The Act provides for the possibility of establishing protection zones for water intakes and protection areas for inland water reservoirs (art. 51 points 1–2). In the former, there are orders, prohibitions and restrictions on the use of water and land, while the protection zone itself is divided into the area of direct and indirect protection (art. 52). In direct protection areas, it is forbidden to use the land for purposes not related to the operation of water intake (art. 53), while in indirect protection areas, restrictions may or may not apply to activities reducing the usefulness of the abstracted water or the catchment efficiency (art. 54). The above provisions create the possibility of additional protection of the critical infrastructure system related to water supply.

10. Act on strategic reserves [19].

The Act defines critical infrastructure in a similar way as in the Act on crisis management. Art. 3 of the Act indicates the essence of building strategic reserves – in this context, among others, a threat to the state security and defence, public safety and order, support for the implementation of tasks in the area of national security and defence, reconstruction of CI, mitigation of disruptions in the continuity of supplies serving the functioning of the economy and satisfying the basic needs of the citizens.

jednego lub kilku zarządców. Art. 60 ust. 1 ustawy precyzuje zadania tej formacji, wskazując, że jest ona m.in. odpowiedzialna za ochronę życia lub zdrowia ludzkiego, a także mienia na obszarze kolejowym, w pociągach i innych pojazdach kolejowych.

8. Ustawa Prawo telekomunikacyjne [17].

Ustawa reguluje zasady prowadzenia działalności polegającej na świadczeniu usług telekomunikacyjnych. Jako narzędzie ochrony infrastruktury krytycznej jest istotna z wielu względów. Definiuje przedsiębiorcę telekomunikacyjnego, co pozwala w wielu przypadkach kwalifikować zarządzane przez niego instalacje, obiekty i urządzenia jako wchodzące w skład systemu telekomunikacyjnego infrastruktury krytycznej (art. 2 pkt 27). W tym kontekście operatorzy są zobowiązani do przekazywania prezesowi Urzędu Komunikacji Elektronicznej (UKE) oraz udostępniania zainteresowanym podmiotom specyfikacji technicznych stosowanych zakończeń sieci, interfejsów radiowych i ich zmian, zanim usługi telekomunikacyjne, które mają być świadczone przy pomocy tych zakończeń sieci lub interfejsów radiowych, staną się dostępne dla użytkowników (art. 137 ust. 1). Z punktu widzenia ochrony infrastruktury krytycznej bardzo ważne są art. 178, 179 ust. 1 oraz 180f ustawy. Art. 178 ust. 1 wskazuje, że „w sytuacji wystąpienia szczególnego zagrożenia" prezes UKE może, w drodze decyzji, nałożyć na przedsiębiorców telekomunikacyjnych określone obowiązki, kierując się rozmiarem zagrożenia i potrzebą ograniczenia jego skutków oraz zasadą minimalizowania negatywnych skutków nałożonych obowiązków. Z kolei art. 179 nakazuje takim przedsiębiorcom wykonywanie zadań i obowiązków w zakresie przygotowania i utrzymywania wskazanych elementów sieci dla zapewnienia telekomunikacji na potrzeby systemu kierowania bezpieczeństwem narodowym, w tym obroną państwa, realizowanych na zasadach określonych w planach, decyzjach oraz umowach zawartych między tymi przedsiębiorcami a zainteresowanymi podmiotami [7].

9. Ustawa Prawo wodne [18].

Ustawa, regulując kompleksowo zagadnienia gospodarki wodnej, zawiera m.in. unormowania dotyczące ścisłej ochrony i nadzoru określonych obszarów, istotnych z punktu widzenia dostarczania wody pitnej, a więc elementu infrastruktury krytycznej. Przewiduje ona możliwość ustanowienia stref ochronnych ujęć wody oraz obszarów ochronnych zbiorników wód śródlądowych (art. 51 pkt 1–2). W tych pierwszych obowiązują nakazy, zakazy i ograniczenia dotyczące korzystania z wód oraz użytkowania gruntów, sama strefa ochronna dzieli się zaś na teren ochrony bezpośredniej i pośredniej (art. 52). Na terenach ochrony bezpośredniej zabronione jest użytkowanie gruntów w celach niezwiązanych z eksploatacją ujęcia wody (art. 53), natomiast na obszarach ochrony pośredniej ograniczenia mogą, choć nie muszą, dotyczyć działań powodujących zmniejszenie przydatności ujmowanej wody lub wydajności ujęcia (art. 54). Powyższe przepisy stwarzają możliwość dodatkowej ochrony systemu infrastruktury krytycznej dotyczącego zaopatrzenia w wodę.

10. Ustawa o rezerwach strategicznych [19].

Ustawa definiuje infrastrukturę krytyczną w sposób podobny jak w ustawie o zarządzaniu kryzysowym. W art. 3 ustawy wskazano istotę budowy rezerw strategicznych – w tym kontekście

11. Act of 18 March 2010 on the specific powers of the minister responsible for the State Treasury and their exercise in certain capital companies or capital groups operating in the electricity, crude oil and gaseous fuels sectors [20].

The above document replaced the Act of 3 June 2005 on the special rights of the State Treasury and their exercise in capital companies of significant importance for public order or public safety [21]. It refers to the protection of a CI sector – strictly speaking, to the energy and fuel supply system.

12. Regulation of the Council of Ministers of 24 June 2003 on objects of particular importance for national security and defence and on their special protection [22].

The regulation issued on the basis of the Act on the universal defence obligation specifies objects of particular importance for the national security and defence (§ 2). The extensive catalogue, containing nineteen categories, includes, among others facilities of formation and services (including the Police, the Agency of Internal Security and the State Fire Service), facilities related to the extraction of minerals, telecommunications, state reserve warehouses, water dams and hydrotechnical devices, power plants and electricity facilities, as well as facilities subordinate to or supervised by the minister of national defence. According to the Regulation, these facilities are subject to special protection (§ 5). They have also been divided into category I facilities (listed in points 1–9 § 2) and category II facilities (listed in points 10–19 § 2). The minister of national defence is responsible for determining the requirements for the preparation and implementation of special protection for category I facilities, while the minister responsible for internal affairs has the same obligation with regard to category II facilities. In fact, objects of both categories are largely critical infrastructure, which is another example of the fact that its protection was prepared and the decision which was carried out long before was made on its legal and structural separation and additional requirements for its protection, involving the need to prepare, among others, National Protection Program of Critical Infrastructure.

Apart from the aforementioned legal acts, mentioned should also be the Act of 27 March 2003 on spatial planning and development [29] and the Act of 4 September 2008 on the protection of shipping and seaports [30]. They are also related to the issues of critical infrastructure. The first requires that planning and spatial development take into account the needs of state defence and security (art. 1 sec. 2 point 8) [29], while the second regulates the issues of protection seaports and port facilities (art. 2 sec. 1) [30].

wymieniono m.in. zagrożenie dla bezpieczeństwa i obronności państwa, bezpieczeństwa i porządku publicznego, wsparcie realizacji zadań w zakresie bezpieczeństwa i obrony państwa, odtworzenie IK, złagodzenie zakłóceń w ciągłości dostaw służących funkcjonowaniu gospodarki i zaspokojeniu podstawowych potrzeb obywateli.

11. Ustawa z dnia 18 marca 2010 roku o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych [20].

Powyższy dokument zastąpił ustawę z 3 czerwca 2005 r. o szczególnych uprawnieniach Skarbu Państwa oraz ich wykonywaniu w spółkach kapitałowych o istotnym znaczeniu dla porządku publicznego lub bezpieczeństwa publicznego [21]. Odnosi się ona do ochrony wycinka IK – ściśle mówiąc do systemu zaopatrzenia w energię, surowce energetyczne i paliwa.

12. Rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony [22].

Rozporządzenie wydane na podstawie ustawy o powszechnym obowiązku obrony określa obiekty szczególnie ważne dla bezpieczeństwa i obronności państwa (§ 2). Obszerny katalog, zawierający dziewiętnaście kategorii, obejmuje m.in. obiekty formacji i służb (m.in. Policji, Agencji Bezpieczeństwa Wewnętrznego i Państwowej Straży Pożarnej), obiekty związane z wydobywaniem kopalin, telekomunikacyjne, magazyny rezerw państwowych, zapory wodne i urządzenia hydrotechniczne, elektrownie i obiekty elektroenergetyczne, a także obiekty podległe lub nadzorowane przez ministra obrony narodowej. W myśl rozporządzenia obiekty te podlegają szczególnej ochronie (§ 5). Zostały także podzielone na obiekty kategorii I (wymienione w pkt 1–9 § 2) oraz obiekty kategorii II (wymienione w pkt 10–19 § 2). Minister obrony narodowej odpowiada za określenie wymagań przygotowania i prowadzenia szczególnej ochrony obiektów kategorii I, minister właściwy do spraw wewnętrznych ma ten sam obowiązek w odniesieniu do obiektów kategorii II. Faktycznie obiekty obu kategorii stanowią w dużej części infrastrukturę krytyczną, co jest kolejnym przykładem tego, że jej ochrona była przygotowywana i prowadzona na długo, zanim podjęto decyzję o jej prawnym i strukturalnym wyodrębnieniu oraz dodatkowych wymogach jej ochrony, wiążących się z koniecznością przygotowania m.in. Narodowego Programu Ochrony Infrastruktury Krytycznej. Obok wspomnianych aktów prawnych należałoby wskazać również ustawę z 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym [29] oraz ustawę z 4 września 2008 r. o ochronie żeglugi i portów morskich [30]. One również są związane z problematyką infrastruktury krytycznej. Pierwsza wymaga, aby w planowaniu i zagospodarowaniu przestrzennym uwzględniano potrzeby obronności i bezpieczeństwa państwa (art. 1 ust. 2 pkt 8) [29], druga natomiast reguluje zagadnienia ochrony m.in. portów morskich i obiektów portowych (art. 2 ust. 1) [30].

The importance of critical infrastructure for national security

The Act of 26 April 2007 on Crisis Management introduced the concept of critical infrastructure into Polish legislation. According to it, critical infrastructure should be treated as systems and functionally interconnected objects, including construction objects, devices, installations, key services for the security of the country and its citizens, and to ensure the efficient functioning of public administration bodies, as well as institutions and entrepreneurs [1].

In the Republic of Poland, critical infrastructure includes 11 systems (facilities, devices) that are of key importance for the security of the country and its citizens and are used to ensure the efficient functioning of public administration bodies, as well as institutions and entrepreneurs. They are:

1. Energy, energy raw materials and fuel supply systems,:
   - for the production, transmission and distribution of electricity (power industry),
   - for the production, transport and distribution of gaseous fuels,
   - for the production, transport and distribution of crude oil and petroleum products
   - for the production, transport and distribution of heat.
2. Communication systems for the transmission of information, including postal and telecommunications, as well as broadcasting and television.
3. ICT networks – a set of cooperating IT devices and software, ensuring processing and storage, as well as sending and receiving data via telecommunications networks using a terminal device appropriate for a given type of network.
4. Financial systems, i.e. all legal norms and a group of financial institutions whose task is to collect, divide and spend national money resources.
5. Food supply system – a branch of the economy which consists of producing means of production (e.g. fertilizers, feed) and services for agriculture, production and acquisition of food raw materials (in agriculture, fishing, forestry, hunting), purchase of food raw materials, their storage and transport, processing of food raw materials, trade in food products (food warehousing and storage, wholesale and retail trade, export and import) and food safety system covering all components of the food supply chain.
6. Water supply system (drinking water, sewage, surface water) – it consists of interconnected enterprises and devices collecting, upgrading, supplying and treating water for the population and the industry.
7. Health care system (pharmacies, hospitals, clinics) – a team of people and institutions whose task is to provide health care to the population. Its efficient functioning (along with the rescue system) is a guarantee of the citizens' rights enshrined in the Constitution.
8. Transport (roads, railways, airports, ports) – that is the

Znaczenie infrastruktury krytycznej dla bezpieczeństwa państwa

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, wprowadziła do polskiego prawodawstwa pojęcie infrastruktury krytycznej. Według niej infrastrukturę krytyczną należy traktować jako systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców [1].

W Rzeczypospolitej Polskiej w skład infrastruktury krytycznej wchodzi 11 systemów (obiekty, urządzenia), które mają kluczowe znaczenie dla bezpieczeństwa państwa i jego obywateli oraz służą zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Zaliczamy do nich:

1. Systemy zaopatrzenia w energię, surowce energetyczne i paliwa:
   - do produkcji, przesyłania i dystrybucji energii elektrycznej (energetyka),
   - do produkcji, transportu i dystrybucji paliw gazowych,
   - do produkcji, transportu i dystrybucji ropy naftowej i produktów ropopochodnych
   - do produkcji, transportu i dystrybucji ciepła.
2. Systemy łączności, zapewniające przekazywanie informacji, obejmujące pocztę oraz telekomunikację, jak również radiofonię i telewizję.
3. Sieci teleinformatyczne – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego, dla danego rodzaju sieci, urządzenia końcowego.
4. Systemy finansowe, czyli ogół norm prawnych oraz zespół instytucji finansowych, których zadaniem jest gromadzenie, dzielenie i wydatkowanie zasobów pieniężnych państwa.
5. System zaopatrzenia w żywność – dziedzina gospodarki, na którą składa się wytworzenie środków produkcyjnych (np. nawozy, pasze) i usług dla rolnictwa, produkcja i pozyskiwanie surowców żywnościowych (w rolnictwie, rybactwie, leśnictwie, łowiectwie), skup surowców żywnościowych, ich przechowywanie i transport, przetwórstwo surowców żywnościowych, obrót towarowy produktami żywnościowymi (magazynowanie i przechowywanie żywności, handel hurtowy i detaliczny, eksport i import) oraz system bezpieczeństwa żywności obejmujący wszystkie składowe łańcucha zaopatrzenia w żywność.
6. System zaopatrzenia w wodę (woda pitna, ścieki, wody powierzchniowe) – w jego skład wchodzą powiązane ze sobą przedsiębiorstwa i urządzenia pobierające, uszlachetniające, dostarczające i oczyszczające wodę dla ludności i przemysłu.

possibility of movement of people, goods (subject of transport) in space using appropriate means of transport.
9. Rescue systems – all organizational measures and undertakings carried out in order to save health and life, property and the environment which are in danger, as well as to predict, recognize and eliminate the consequences of the events.
10. Systems ensuring the actions of public administraction, i.e. the implementation of the right of authority to perform tasks assigned by the legal order to the state and its organs or other entities performing authority functions.
11. Production systems, storage and use of chemical and radioactive substances (including pipelines of hazardous substances) [23].

The definition of the protection of critical infrastructure contained in the Act on Crisis Management (art. 3 point 3) states that: "Protection of critical infrastructure is all the activities aimed at ensuring the functionality, continuity and integrity of critical infrastructure in order to prevent threats, risks or weaknesses, and the limitation and neutralization of their effects and quick restoration of this infrastructure in the event of failures, attacks and other events that disrupt its proper functioning" [1].

From the cited definition it can be concluded that critical infrastructure plays a special role in ensuring the continuity of the functioning of the country, its organs, institutions, services and the exchange of information between them. The efficiency of critical infrastructure ensures a certain level and continuity of distribution of those services for which the country is responsible for. Its proper functioning also allows for the effective use of resources in the event of extraordinary events that disrupt the normal functioning of the country and its economy. The efficiency of a large part of resources considered as critical infrastructure also determines technological progress and economic development.

Critical infrastructure is crucial for the existence of the country and, within it, of an organized society. If its functioning is disrupted, the country and its institutions may lose all or part of their ability to perform their basic administrative and service functions, as well as to exercise effective control over their entire territory. Improper management of critical infrastructure undoubtedly prevents economic and social development and, in some cases, can even lead to the decay of social life. Therefore, it is worth remembering that critical infrastructure in Poland is not completely free from threats, and the society – from the consequences of its deliberate damage or failure. According to the scale and sources of threats, this infrastructure should be developed and protected using appropriate instruments. As in other countries, also in Poland modern and efficient critical infrastructure – regardless of emerging threats – is a decisive factor in the effectiveness of the functioning of the country. In extraordinary situations it also determines its survival [24]. The elements of critical infrastructure systems constitute a collection of classified information, which means that a specialized group of people with a certificate confirming access to classified information has the right to decide on their composition and functioning.

7. System ochrony zdrowia (apteki, szpitale, przychodnie) – zespół osób i instytucji mający za zadanie zapewnić opiekę zdrowotną ludności. Jego sprawne funkcjonowanie (wraz z systemem ratowniczym) jest gwarantem praw obywatela zapisanych w Konstytucji.
8. Systemy transportowe (drogi, kolej, lotniska, porty) – czyli możliwość przemieszczania się ludzi, ładunków (przedmiot transportu) w przestrzeni przy wykorzystaniu odpowiednich środków transportu.
9. Systemy ratownicze – ogół środków i przedsięwzięć organizacyjnych podejmowanych w celu ratowania zdrowia i życia, mienia i środowiska, znajdującym się w niebezpieczeństwie oraz przewidywania, rozpoznawania i likwidacji skutków zdarzeń.
10. Systemy zapewniające ciągłość działania administracji publicznej, czyli realizację prawa władczego wykonywania zadań przypisywanych przez porządek prawny państwu i jego organom lub innym podmiotom wykonującym funkcje władcze.
11. Systemy produkcji składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych (w tym rurociągi substancji niebezpiecznych) [23].

Ujęcie definicyjne ochrony infrastruktury krytycznej zawarte w ustawie o zarządzaniu kryzysowym (art. 3 pkt. 3) definiuje, że: „ochrona infrastruktury krytycznej to wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie" [1].

Z przywołanej definicji wynika, że infrastruktura krytyczna odgrywa szczególną rolę w zapewnieniu ciągłości funkcjonowania państwa, jego organów, instytucji, służb oraz wymiany informacji między nimi. Sprawność infrastruktury krytycznej zapewnia określony poziom i ciągłość dystrybucji tych usług, za które odpowiada państwo. Jej właściwe funkcjonowanie pozwala także na efektywne wykorzystywanie posiadanych zasobów w razie nadzwyczajnych wydarzeń, zakłócających normalne funkcjonowanie państwa i jego gospodarki. Sprawność dużej części zasobów uznawanych za infrastrukturę krytyczną warunkuje także postęp technologiczny i rozwój gospodarczy.

Infrastruktura krytyczna ma kluczowe znaczenie dla istnienia państwa, a w jego ramach – zorganizowanego społeczeństwa. Jeżeli następuje zakłócenie w jej funkcjonowaniu, państwo i jego instytucje mogą utracić w całości lub części zdolność do wykonywania swoich podstawowych funkcji administracyjnych i usługowych, jak również do sprawowania rzeczywistej kontroli nad całym swoim terytorium. Niewłaściwe zarządzanie infrastrukturą krytyczną bez wątpienia uniemożliwia rozwój gospodarczy i społeczny, a w pewnych przypadkach może nawet doprowadzić do rozkładu życia społecznego. Wobec tego warto pamiętać, że infrastruktura krytyczna w Polsce nie jest w zupełności wolna od zagrożeń, a społeczeństwo – od skutków jej celowego uszkodzenia lub awarii. Stosownie do skali i źródeł zagrożeń, infrastruktura ta powinna być rozwijana i chroniona przy użyciu odpowiednich instrumentów. Podobnie jak

National Protection Program of Critical Infrastructure (NPOIK) – interpretation of regulations

National Protection Program of Critical Infrastructure [25] (NPOIK) was developed pursuant to art. 5b sec. 1 of the Act on Crisis Management [1] – it is a document the purpose of which is to create conditions for the improvement of the security of critical infrastructure. This program defines the rules for the protection of critical infrastructure and the cooperation of owners responsible for critical infrastructure with public administration. Critical infrastructure that is included in it has been included in the uniform list of objects, installations, devices and services included in critical infrastructure with a division into systems referred to in art. 5b sec. 7 point 1 of the Act on Crisis Management. NPOIK is not an operational program or a development program within the meaning of the Act of 6 December 2006 on the principles of development policy (Polish Journal of Laws: Dz. U. z 2014, poz. 1649, as amended) and it is complementary to the Security of the Development of the National Security Strategy System of the Republic of Poland 2022 and the National Security Strategy of the Republic of Poland. Taking into account Poland's membership in the European Union, the North Atlantic Treaty Organization, the Organization for Security and Cooperation in Europe and other international organizations, NCIPP also takes into account international agreements to which Poland is a party [25].

The aim of NPOIK is, above all, to create conditions for the improvement of the security of critical infrastructure. Together with other program documents, it contributes to the overriding goal – to increase the security of Poland.

Its implementation requires the achievement of a number of intermediate (operational) goals, which are [25]:

- gaining a certain level of awareness, knowledge and competence of all participants of the NPOIK in the field of the importance of CI for the efficient functioning of the state and the methods and methods of its protection,
- introducing a risk assessment methodology that takes into account a full range of threats, including a methodology for dealing with threats with a very low probability and catastrophic consequences,
- introducing a coordinated and risk-based approach to the implementation of tasks in the field of critical infrastructure protection,
- building a partnership between the participants of the protection process of critical infrastructure,

w innych państwach, także w Polsce nowoczesna i sprawna infrastruktura krytyczna – niezależnie od pojawiających się zagrożeń – jest czynnikiem decydującym o skuteczności funkcjonowania państwa. W sytuacjach nadzwyczajnych przesądza także de facto o jego przetrwaniu [24]. Elementy systemów infrastruktury krytycznej stanowią zbiór informacji niejawnych i to powoduje, że do decydowania o ich składzie i funkcjonowaniu ma uprawnienia wyspecjalizowana grupa osób, posiadająca certyfikat potwierdzający dostęp do informacji o charakterze niejawnym.

Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) – interpretacja przepisów

Narodowy Program Ochrony Infrastruktury Krytycznej [25] (NPOIK) został opracowany na podstawie art. 5b ust. 1 ustawy o zarządzaniu kryzysowym [1] – to dokument, którego celem jest stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej. Niniejszy program określa zasady ochrony infrastruktury krytycznej oraz współpracy właścicieli odpowiedzialnych za infrastrukturę krytyczną z administracją publiczną. Infrastruktura krytyczna, która jest nim objęta, została umieszczona w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy, o którym mowa w art. 5b ust. 7 pkt 1 ustawy o zarządzaniu kryzysowym. NPOIK nie jest programem operacyjnym ani programem rozwoju w rozumieniu ustawy z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju (Dz. U. z 2014, poz. 1649 z późn. zm.) i jest komplementarny w stosunku do Strategii rozwoju systemu bezpieczeństwa narodowego RP 2022 oraz Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. Mając na uwadze fakt członkostwa Rzeczypospolitej Polskiej w Unii Europejskiej, Organizacji Traktatu Północnoatlantyckiego, Organizacji Bezpieczeństwa i Współpracy w Europie oraz innych organizacjach międzynarodowych, NPOIK uwzględnia również międzynarodowe porozumienia, których Polska jest stroną [25].

Celem NPOIK jest przede wszystkim stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej. Wraz z innymi dokumentami programowymi składa się on na cel nadrzędny – podniesienie bezpieczeństwa Rzeczypospolitej Polskiej.

Jego realizacja wymaga osiągnięcia szeregu celów pośrednich (operacyjnych), którymi są [25]:

- zdobycie określonego poziomu świadomości, wiedzy i kompetencji wszystkich uczestników NPOIK w zakresie znaczenia IK dla sprawnego funkcjonowania państwa oraz sposobów i metod jej ochrony,
- wprowadzenie metodyki oceny ryzyka uwzględniającej pełny wachlarz zagrożeń, w tym metodyki postępowania z zagrożeniami o bardzo małym prawdopodobieństwie i katastrofalnych skutkach,
- wprowadzenie skoordynowanego i opartego na ocenie ryzyka podejścia do realizacji zadań z zakresu ochrony infrastruktury krytycznej,
- budowa partnerstwa między uczestnikami procesu ochrony infrastruktury krytycznej,

– introducing mechanisms for the exchange and protection of information transferred between the participants of the protection process of critical infrastructure.

The Act on crisis management adopts a sanction-free approach to the protection of critical infrastructure. It is based on the assumption that increasing the effectiveness of the protection of critical infrastructure can only take place through the actions of its operators, supported by the possibilities and the potential of public administration. Operators of critical infrastructure have the best knowledge and tools to reduce threats to their operations. They are also able to make the most appropriate strategy to minimize the effects of these threats. Trying to maintain a balance between the imperative influence of the country and the expenses necessary to improve the security of critical infrastructure, the Act on crisis management does not provide sanctions for failure to comply with the obligations set out in it, and budget support for the operators of critical infrastructure.

Therefore, in order to achieve the objectives of the program in question, it is necessary to adopt the principles that should guide its participants [25].

The pillars and the most important principles of NPOIK are primarily [25]:

– shared responsibility – the leading principle adopted in the construction of the protection system of critical infrastructure, understood as a joint (collective) strive to improve the security of critical infrastructure resulting from the awareness of its importance for the functioning of both public administration bodies and operators of critical infrastructure, society, economy and the country. The protection of critical infrastructure is in the interest of both its operators and the administration responsible for the functioning of the country,
– cooperation – the second pillar of the CI protection system. In the context of NPOIK, it means the performance of specific, concurrent and complementary tasks by the participants of CI protection together to achieve a common goal, which results from the principle of shared responsibility. Cooperation is essential in order to avoid duplication of activities and costs, and to use the resources available more efficiently,
– trust – the third pillar of the CI protection system, in NPOIK understood as the belief that the motivation of the participants of CI protection (this applies in particular to the administration and CI operators) is to pursue a common goal – is to improve the security of CI and Poland. Therefore, achieving this goal will be beneficial for all interested parties, including, in particular, the public. Trust is essential to achieving the goals of the program.

NPOIK is guided by the following principles [25]:

– proportionality and risk-based action – actions aimed at increasing the level of CI protection should be adequate to the risk level. This applies to both the adopted CI protection model and the forces and means used. Risk assessment should be the basis for determining CI protection standards and setting priorities for actions.

– wprowadzenie mechanizmów wymiany i ochrony informacji przekazywanych między uczestnikami procesu ochrony infrastruktury krytycznej.

W ustawie o zarządzaniu kryzysowym przyjęto bezsankcyjne podejście do ochrony infrastruktury krytycznej. Jego podstawą jest założenie, że zwiększenie skuteczności ochrony infrastruktury krytycznej może nastąpić jedynie przez działania jej operatorów wspieranych przez możliwości i potencjał administracji publicznej. Operatorzy infrastruktury krytycznej mają najlepszą wiedzę i narzędzia do ograniczenia zagrożeń dla ich działalności. Są również w stanie dokonać najwłaściwszego wyboru strategii minimalizacji skutków tych zagrożeń. Starając się zachować równowagę pomiędzy władczym oddziaływaniem państwa, a wydatkami niezbędnymi do poprawy bezpieczeństwa infrastruktury krytycznej, ustawa o zarządzaniu kryzysowym nie przewiduje zarówno sankcji za niedopełnienie obowiązków w niej określonych, jak i wsparcia budżetowego operatorów infrastruktury krytycznej.

W związku z powyższym, aby osiągnąć cele omawianego programu, niezbędne jest przyjęcie zasad, którymi powinni się kierować jego uczestnicy [25].

Filarami i najważniejszymi zasadami NPOIK są przede wszystkim [25]:

– współodpowiedzialność – wiodąca zasada przyjęta przy budowie systemu ochrony infrastruktury krytycznej, rozumiana jako wspólne (zbiorowe) dążenie do poprawy bezpieczeństwa infrastruktury krytycznej wynikające ze świadomości jej znaczenia dla funkcjonowania zarówno organów administracji publicznej, jak i operatorów infrastruktury krytycznej, społeczeństwa, gospodarki i państwa. Ochrona infrastruktury krytycznej leży bowiem w interesie zarówno jej operatorów, jak i odpowiedzialnej za funkcjonowanie państwa administracji,
– współpraca – drugi filar systemu ochrony IK. W kontekście NPOIK oznacza wykonywanie razem przez uczestników ochrony IK określonych, zbieżnych i wzajemnie uzupełniających się zadań dla osiągnięcia wspólnego celu, który wynika z zasady współodpowiedzialności. Współpraca jest niezbędna w przypadku chęci uniknięcia powielania działań i ponoszonych kosztów oraz efektywniejszego wykorzystania posiadanych sił i środków,
– zaufanie – trzeci filar systemu ochrony IK, w NPOIK rozumiane jako przekonanie, że motywacją działania uczestników ochrony IK (dotyczy to w szczególności administracji i operatorów IK) jest dążenie do wspólnego celu – poprawy bezpieczeństwa IK i RP. Osiągnięcie tego celu będzie zatem korzystne dla wszystkich zainteresowanych stron, w tym przede wszystkim społeczeństwa. Zaufanie jest niezbędne do zrealizowania celów programu.

NPOIK kieruje się następującymi zasadami [25]:

– proporcjonalności i działań opartych na ocenie ryzyka – działania nakierowane na podniesienie poziomu ochrony IK powinny być adekwatne do poziomu ryzyka. Dotyczy to zarówno przyjętego modelu ochrony IK, jak i użytych sił i środków. Ocena ryzyka powinna być

- recognition of differences between CI systems – CI systems have many similarities, but they have some unique features that should be taken into account in the area of CI protection,
- leading role of the minister responsible for the CI system – the initiative to increase the level of protection of infrastructure essential for the functioning of society came from the administration, therefore it should have a significant share in the activities to improve CI security. This role in building trust and effective cooperation is played by the ministers responsible for the CI system, regardless of the CI operator's obligation to protect CI.
- equality of CI operators – CI operators include both private entities, state-owned entities, and the administration itself.
- complementarity – there are many solutions in use that effectively contribute to the safe functioning of CI. The provisions of NPOIK are complementary to the existing legal and institutional solutions. They do not duplicate the accepted practices resulting from the applicable law.

Regardless of the adopted approach [25]:

- in the event of a negative assessment of the effectiveness of the implementation of the Act on crisis management and NPOIK,
- if the identified significant deficiencies in the protection systems of critical infrastructure are not removed by CI operators,
- if, due to the emergence of new risks, the current legal provisions are deemed inappropriate or inapplicable to these risks,
- to optimize the protection of critical infrastructure,
- to reduce certain types of risk,

it is allowed to introduce detailed legal regulations regarding the implementation of NPOIK.

The presented program emphasizes that the operators of a significant part of critical infrastructure are private entrepreneurs not related to the public administration. NPOIK establishes a framework in which the public administration and CI operators cooperate in order to ensure the continuity of CI operations, thus protecting the economic and social foundations of our country. It also outlines the mechanisms of developing partnership relations between the public administration and CI operators in the area of CI protection. Taking into account the above and the obligation imposed on the CI operators by the Act, NPOIK is also addressed to these entities, and in particular to their management boards. Each new CI operator becomes its addressee automatically. CI operators participate in the activities for the benefit of CI protection described in the program [26].

podstawą określenia standardów ochrony IK i ustalenia priorytetów działań,

- uznania różnic między systemami IK – systemy IK cechuje wiele podobieństw, posiadają jednak pewne unikalne cechy, które w obszarze ochrony IK powinny zostać uwzględnione,
- wiodącej roli ministra odpowiedzialnego za system IK – inicjatywa zwiększenia poziomu ochrony infrastruktury kluczowej dla funkcjonowania społeczeństwa wyszła ze strony administracji, dlatego powinna ona mieć znaczący udział w działaniach na rzecz poprawy bezpieczeństwa IK. Tę rolę w budowie zaufania i skutecznej współpracy odgrywają ministrowie odpowiedzialni za system IK, niezależnie od obowiązku ochrony IK ciążącego na operatorze IK,
- równości operatorów IK – operatorami IK są zarówno podmioty prywatne, podmioty stanowiące własność państwa, jak i sama administracja. Program nie dokonuje rozróżnień – w jego rozumieniu wszyscy operatorzy są równi i zobowiązani do realizacji tego samego obowiązku – ochrony IK, którą władają,
- komplementarności – w użyciu pozostaje wiele rozwiązań, które skutecznie przyczyniają się do bezpiecznego funkcjonowania IK. Zapisy NPOIK mają charakter uzupełniający w stosunku do istniejących rozwiązań prawno-instytucjonalnych. Nie powielają przyjętych praktyk wynikających z obowiązującego prawa.

Niezależnie od założonego podejścia [25]:

- w przypadku negatywnej oceny skuteczności realizacji ustawy o zarządzaniu kryzysowym oraz NPOIK,
- jeśli zidentyfikowane istotne braki w systemach ochrony infrastruktury krytycznej nie zostaną usunięte przez operatorów IK,
- jeżeli ze względu na pojawienie się nowych zagrożeń, obecne przepisy prawne uznane zostaną za nieodpowiednie lub niemające zastosowania w odniesieniu do tych zagrożeń,
- w celu zoptymalizowania ochrony infrastruktury krytycznej,
- w celu redukcji niektórych rodzajów ryzyka,

dopuszcza się możliwość wprowadzenia szczegółowych uregulowań prawnych dotyczących realizacji NPOIK.

W prezentowanym programie podkreśla się, że operatorami znacznej części infrastruktury krytycznej są prywatni przedsiębiorcy niepowiązani z administracją publiczną. NPOIK ustanawia ramy, w których administracja publiczna i operatorzy IK współpracują w celu zapewnienia ciągłości działania IK, chroniąc tym samym gospodarcze i społeczne fundamenty naszego kraju. Nakreśla także mechanizmy rozwoju partnerskich relacji między administracją publiczną i operatorami IK w zakresie ochrony IK. Uwzględniając powyższe oraz obowiązek nałożony na operatorów IK przez ustawę, NPOIK adresowany jest także do tych podmiotów, a w szczególności do ich zarządów. Jego adresatem automatycznie staje się każdy nowy operator IK. Operatorzy IK uczestniczą w działaniach na rzecz ochrony IK opisanych w programie [26].

Identification of critical infrastructure – importance for the protection of facilities, installations and devices of critical infrastructure

Identification of objects, devices, installations or services, the destruction or disruption of their functioning which could cause a crisis situation, is a key stage in the protection process of critical infrastructure. In order to achieve maximum objectivity, the Government Centre for Security, in cooperation with the ministers and heads of central offices and with the support of private entrepreneurs, developed criteria for the identification of critical infrastructure [25].

In the individual systems referred to in the Act, critical infrastructure will be selected on the basis of specific criteria. These criteria are divided into two groups [27]:

1. Sector (system) criteria that characterize parameters (functions) of an object, device, installation or service in terms of quantity or subjectivity, the fulfilment of which may result in being classified as elements of critical infrastructure. These criteria are presented for each of the CI systems.
2. Cross-cutting criteria, describing parameters related to the effects of the destruction or non-functioning of a facility, device, installation or service. In order for an object, device, installation or service to qualify as CI, in accordance with the adopted methodology, all three steps presented below must be completed:

– in the first one the first one – in order to make the first selection of objects, installations, devices or services that could potentially be considered CI in a given system, the sector (system) criteria relevant for a given CI system should be applied to the system infrastructure.
– in the second one – in order to check whether the object, device, installation or service plays a key role for the security of the country and its citizens and whether it serves to ensure the efficient functioning of public administration bodies, as well as institutions and entrepreneurs, the infrastructure selected through the fulfilment of the first step should be defined as contained in art. 3 point 2 of the Act.
– in the third one – in order to indicate the effects of the destruction or cessation of the functioning of a potential CI, cross-sectional criteria should be applied to the infrastructure selected through the fulfilment of the first and second steps (the criteria that best reflect the characteristics of the system should be selected), while in order to complete the third step, the potential CI must meet at least two cross-sectional criteria [27].

It is worth mentioning that meeting the cross-sectional criteria is of decisive importance for selecting CI facilities, installations, devices or services. The emphasis on the effects of the destruction or cessation of the functioning of CI, which is directly related to the crisis situation, finds deep justification in the understanding of it as fulfilling a key function for the country as a whole and its citizens. The criteria presented above constitute an important element of the National Protection Program of

Identyfikacja infrastruktury krytycznej – znaczenie dla ochrony obiektów, instalacji i urządzeń infrastruktury krytycznej

Identyfikacja obiektów, urządzeń, instalacji lub usług, których zniszczenie lub zakłócenie funkcjonowania mogłoby spowodować sytuację kryzysową, jest kluczowym etapem procesu ochrony infrastruktury krytycznej. W celu maksymalnej obiektywizacji Rządowe Centrum Bezpieczeństwa, we współpracy z ministrami i kierownikami urzędów centralnych oraz przy wsparciu przedsiębiorców prywatnych, opracowało kryteria identyfikacji infrastruktury krytycznej [25].

W poszczególnych systemach, o których mówi ustawa, infrastruktura krytyczna zostanie wyłoniona na podstawie określonych kryteriów. Kryteria te podzielone są na dwie grupy [27]:

1. Kryteria sektorowe (systemowe), charakteryzujące ilościowo lub podmiotowo parametry (funkcje) obiektu, urządzenia, instalacji lub usługi, których spełnienie może spowodować zaliczenie do elementów infrastruktury krytycznej. Kryteria te przedstawione są dla każdego z systemów IK.
2. Kryteria przekrojowe, opisujące parametry odnoszące się do skutków zniszczenia lub zaprzestania funkcjonowania obiektu, urządzenia, instalacji lub usługi. Aby obiekt, urządzenie, instalacja lub usługa mogły być zakwalifikowane jako IK, zgodnie z przyjętą metodyką muszą być zrealizowane wszystkie trzy niżej przedstawione kroki:

– w pierwszym – w celu dokonania pierwszej selekcji obiektów, instalacji, urządzeń lub usług, które potencjalnie mogłyby zostać uznane za IK w danym systemie, do infrastruktury systemu należy zastosować kryteria sektorowe (systemowe), właściwe dla danego systemu IK.
– w drugim – w celu sprawdzenia czy obiekt, urządzenie, instalacja lub usługa pełni kluczową rolę dla bezpieczeństwa państwa i jego obywateli oraz czy służy zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, do infrastruktury wyłonionej w drodze spełnienia pierwszego kroku należy zastosować definicję zawartą w art. 3 pkt. 2 ustawy.
– w trzecim – w celu wskazania, jakie będą skutki zniszczenia lub zaprzestania funkcjonowania potencjalnej IK, do infrastruktury wyłonionej w drodze spełnienia kroku pierwszego i drugiego należy zastosować kryteria przekrojowe (należy wybrać kryteria najlepiej odzwierciedlające charakterystykę systemu), przy czym, aby wypełnić krok trzeci, potencjalna IK musi spełnić przynajmniej dwa kryteria przekrojowe [27].

Warto nadmienić, że spełnienie kryteriów przekrojowych ma decydujące znaczenie dla wskazania obiektów, instalacji, urządzeń lub usług IK. Położenie akcentu na skutki zniszczenia lub zaprzestania funkcjonowania IK, mające bezpośredni związek z powiązaniem z sytuacją kryzysową, znajduje głębokie uzasadnienie w rozumieniu jej jako pełniącej kluczową funkcję dla państwa jako całości i jego obywateli. Kryteria przedstawione powyżej stanowią istotny element Narodowego Programu Ochrony Infrastruktury Krytycznej i – podobnie jak sam program – wymagają

Critical Infrastructure and – similarly to the program itself – require systematic updating. Thus, it will be possible to use the mechanism to "regulate" the criteria in such a way that they cover a larger or smaller number of CI elements. The assumption is that in the future, after developing tools that would allow for the evaluation of the effects of destruction or cessation of the functioning of CI in a meaningful manner, the sectoral (systemic) criteria should be abandoned at all. As a result, the cross-cutting criteria would be applied to any chosen system infrastructure or to any national infrastructure [27].

Conclusion

Critical infrastructure is characterized by extremely complex, heterogeneous and independent groups (complexes) of objects, systems and functions that are susceptible to any threats. A significant number of each country's critical elements, their ubiquity and interconnectedness attract hostile attention as targets of attack. Even a threat of such an attack can create an extremely difficult situation for any government. Taking into account the usually open location of the element of critical infrastructure, which is a potential target of an attack, there is no possibility of full and complete protection against possible threats to all elements of the critical infrastructure in the country [28].

Referring to the current state of the Polish legal system, there are provisions enabling the implementation of protection of objects classified as critical infrastructure. Trainings of personnel at the managerial and executive level who practically implement its protection are conducted. There are also procedures for dealing with all entities, including owners, security formations, and services in the event of a disruption of work or an attack on critical infrastructure facilities. Nevertheless, there is often neglect in this area. The question is why do these situations take place? There are many answers, pointing to errors in building an appropriate technical and physical protection system, improper cooperation of the owners of critical infrastructure with the services and bodies supporting its protection.

Planning of effective forms of defence of critical infrastructure should take place on the basis of a coherent system for monitoring threats, which may facilitate the diagnosis of the danger. It is the ability to predict a crisis situation, as well as the introduction of preventive mechanisms that use a full range of the offered protection, that is a measure of the country's efficiency in the area of achieving its most important goal, i.e. securing the life and health of the citizens. Therefore, appropriate division of competences and responsibilities, the introduction of effective planning methods, as well as organizational and financial methods, and the appropriate distribution of protective tasks to national and private entities will determine the improvement of the response process related to the emerging crisis situations.

In conclusion, the experience gathered in connection with the protection of critical infrastructure shows that it is not possible to provide complete protection to the elements of the national security infrastructure. For this reason, particular effort should be put into the maximum immunization of the critical infrastructure, and in the event of its destruction or damage – in the quick restoration of the disrupted functions. Man is an important

systematycznej aktualizacji. Można będzie zatem wykorzystać mechanizm do „regulacji" kryteriów w taki sposób, aby objęły one większą lub mniejszą liczbę elementów IK. Założeniem jest, aby w przyszłości, po opracowaniu narzędzi, które w miarodajny sposób pozwalałyby na ocenę skutków zniszczenia lub zaprzestania funkcjonowania IK, w ogóle zrezygnować z kryteriów sektorowych (systemowych). W efekcie kryteria przekrojowe stosowane byłyby do dowolnie wybranej infrastruktury systemu lub do jakiejkolwiek krajowej infrastruktury [27].

Podsumowanie

Infrastruktura krytyczna charakteryzuje się niezwykle złożonymi, heterogenicznymi oraz niezależnymi zespołami (kompleksami) obiektów, systemów i funkcji, które są podatne na wszelkie zagrożenia. Znacząca liczba elementów krytycznych każdego państwa, ich wszechobecność i wzajemne powiązania skupiają na nich wrogie zainteresowanie jako celów ataku. Nawet groźba takiego ataku może spowodować wyjątkowo trudną sytuację dla każdego rządu. Biorąc pod uwagę zazwyczaj jawne położenie elementu infrastruktury krytycznej, będącego potencjalnym celem ataku, nie ma możliwości pełnej i całkowitej ochrony przed możliwymi zagrożeniami wszystkich elementów infrastruktury krytycznej w państwie [28].

Odnosząc się do stanu obecnego w polskim systemie prawnym, istnieją przepisy umożliwiające wdrożenie ochrony obiektów zaliczanych do infrastruktury krytycznej. Prowadzone są szkolenia personelu szczebla kierowniczego oraz wykonawczego praktycznie realizującego jej ochronę. Istnieją również procedury postępowania wszystkich podmiotów, w tym właścicieli, formacji ochrony, służb na wypadek wystąpienia zakłócenia pracy lub ataku na obiekty infrastruktury krytycznej. Mimo to, często dochodzi do zaniedbań w tym obszarze. Nasuwa się pytanie, dlaczego takie sytuacje mają miejsce? Odpowiedzi jest wiele, wskazując chociażby błędy w budowaniu właściwego systemu ochrony technicznej i fizycznej, niewłaściwego współdziałania właścicieli infrastruktury krytycznej ze służbami i organami wspomagającymi jej ochronę.

Zaplanowanie skutecznych form obrony infrastruktury krytycznej powinno odbywać się na podstawie spójnego systemu monitoringu zagrożeń, co może ułatwić diagnozę niebezpieczeństwa. To właśnie umiejętność przewidzenia sytuacji kryzysowej, a także wprowadzenie prewencyjnych mechanizmów, wykorzystujących pełen zakres posiadanego asortymentu ochrony, stanowi miarę sprawności państwa w obszarze realizacji najważniejszego jej celu, czyli zabezpieczenia życia i zdrowia obywateli. Zatem właściwy podział kompetencji i odpowiedzialności, wprowadzenie skutecznych w zakresie zarówno metod planistycznych, jak i organizacyjno-finansowych, a także odpowiednie rozdzielenie zadań ochronnych podmiotom państwowym i prywatnym decydować będzie o usprawnieniu procesu reagowania, dotyczącego powstałych sytuacji kryzysowych.

Podsumowując, doświadczenia zgromadzone w związku z ochroną infrastruktury krytycznej wskazują, że nie jest możliwe zapewnienie całkowitej ochrony elementom infrastruktury bezpieczeństwa państwa. Z tego też względu szczególny wysiłek powinien zostać włożony w maksymalne uodpornienie infrastruktury

element of the country's protection system of critical infrastructure. His activity may increase or decrease the resilience of critical infrastructure, and in drastic cases – lead to its disruption, deprivation of functions or complete destruction. Human activity – both positive (creating) and destructive – can be the result of deliberate or accidental actions. In order to limit the destructive activities of people as much as possible, a significant challenge in the protection of critical infrastructure has become not only the development of appropriate procedures, but also the raising of public awareness of that infrastructure.

Critical infrastructure plays a key role in the functioning of the country and its citizens. As a result of the events caused by forces of nature or resulting from human activities, i.e. in crisis situations (situations that negatively affect the level of safety of people, property to a large extent or the environment, causing significant restrictions in the operation of competent public administration bodies due to the inadequacy of the resources available to them according to the above-mentioned Act, art.3 point 1) [1], critical infrastructure may be destroyed, damaged, and its operation may be disrupted. Such events negatively affect the economy of the country and the lives of its citizens. The essence of the tasks related to critical infrastructure boils down not only to ensuring its protection against threats, but also to ensuring that any disruptions in its functioning are as short-lived as possible, easy to remove and do not cause additional losses. Hence, the protection of critical infrastructure is one of the priorities facing Poland and has a significant impact on the national security system. Therefore, it is so important that the legal provisions are precise and do not affect security, and that the efficiency of organizational structures is ready to face new challenges and to counter threats, which may be decisive for the state of security of the country.

krytycznej, a w przypadku jej zniszczenia bądź uszkodzenia – w szybkie przywrócenie zakłóconych funkcji. Istotnym elementem systemu ochrony infrastruktury krytycznej państwa jest człowiek. Jego aktywność może wpłynąć na zwiększenie lub obniżenie odporności infrastruktury krytycznej, a w drastycznych przypadkach – doprowadzić do jego zakłócenia, pozbawienia funkcji bądź całkowitego zniszczenia. Aktywność ludzka – zarówno ta pozytywna (kreująca), jak i destruktywna (niszcząca) – może być efektem celowego lub przypadkowego działania. Aby w jak największym stopniu ograniczyć destruktywne działania ludzi, istotnym wyzwaniem w ochronie infrastruktury krytycznej stało się nie tylko opracowanie odpowiednich procedur, ale również podniesienie świadomości społeczeństwa co do infrastruktury krytycznej.

Infrastruktura krytyczna pełni kluczową rolę w funkcjonowaniu państwa i jego obywateli. W wyniku zdarzeń spowodowanych siłami natury lub będących konsekwencją działań człowieka, tzn. w sytuacjach kryzysowych (sytuacjach wpływających negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołujących znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków zgodnie z ww. ustawą art. 3. pkt 1) [1], infrastruktura krytyczna może być zniszczona, uszkodzona, a jej działanie może ulec zakłóceniu. Wydarzenia takie negatywnie wpływają na gospodarkę kraju i życie jego obywateli. Istota zadań związanych z infrastrukturą krytyczną sprowadza się więc nie tylko do zapewnienia jej ochrony przed zagrożeniami, ale również do tego, aby ewentualne zakłócenia w jej funkcjonowaniu były możliwie krótkotrwałe, łatwe do usunięcia i nie wywoływały dodatkowych strat. Stąd też ochrona infrastruktury krytycznej jest jednym z priorytetów stojących przed państwem polskim i znacząco wpływa na system bezpieczeństwa narodowego. Dlatego też tak ważnym jest, aby zapisy prawne były precyzyjne i nie wpływały na obniżenie bezpieczeństwa, a sprawność struktur organizacyjnych była gotowa do sprostania nowym wyzwaniom i przeciwstawienia się zagrożeniom, co może decydować o stanie bezpieczeństwa państwa.

Literature / Literatura

[1] Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym (Dz. U. 2007 r. Nr 89, poz. 590 z późn. zm.).

[2] Stawnicka J., Wiśniewski B., Socha R. (red.), *Zasadnicze problemy zarządzania kryzysowego w organizacjach zhierarchizowanych*, Katowice 2011, 77–101.

[3] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (Dz. U. 2010 r. Nr 83, poz. 540).

[4] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz. U. 2010 r. Nr 83, poz. 541).

[5] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz. U. 2010 r. Nr 83, poz. 542).

[6] Lidwa W., Krzeszowski W., Więcek W., Kamiński P., *Ochrona infrastruktury krytycznej*, Akademia Obrony Narodowej, Warszawa 2012, 37.

[7] Stec K., *Wybrane prawne narzędzia ochrony infrastruktury krytycznej w Polsce*, „Bezpieczeństwo Narodowe" 2011, nr 3, 181–197.

[8] Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 7 sierpnia 2013 r. w sprawie ogłoszenia jednolitego tekstu ustawy o zarządzaniu kryzysowym (Dz. U. 2013 r., poz. 1166).

[9] Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz. U. L 345 z 23.12.2008 r.), 75–82.

[10] Zarządzenie nr 67 Prezesa Rady Ministrów z dnia 15 października 2014 r. w sprawie organizacji i trybu pracy Rządowego Zespołu Zarządzania Kryzysowego (M.P. 2014 r., poz. 926).

[11] https://www.gov.pl/web/rcb/o-rcb2 [dostęp: 10.05.2021].

[12] Rozporządzenie Rady Ministrów z dnia 21 września 2018 r. zmieniające rozporządzenie w sprawie określenia organów

administracji rządowej, które utworzą centra zarządzania kryzysowego, oraz sposobu ich funkcjonowania (Dz. U. 2018 r., poz. 1974).
[13] Ustawa z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców (Dz. U. 2001 r. Nr 122, poz. 1320).
[14] Ustawa o ochronie osób i mienia (Dz. U. 2005 r. Nr 145, poz. 121).
[15] Ustawa Prawo lotnicze (Dz. U. 2006 r. Nr 100, poz. 696).
[16] Ustawa o transporcie kolejowym (Dz. U. 2007 r. Nr 16, poz. 94).
[17] Ustawa Prawo telekomunikacyjne (Dz. U. 2004 r. Nr 171, poz. 1800).
[18] Ustawa Prawo wodne (Dz. U. 2005 r. Nr 239, poz. 2019).
[19] Ustawa o rezerwach strategicznych (Dz.U. 2010 r. Nr 229, poz. 1496).
[20] Ustawa z dnia 18 marca 2010 roku o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych (Dz. U. 2010 r. Nr 65, poz. 404).
[21] Ustawa z 3 czerwca 2005 r. o szczególnych uprawnieniach Skarbu Państwa oraz ich wykonywaniu w spółkach kapitałowych o istotnym znaczeniu dla porządku publicznego lub bezpieczeństwa publicznego (Dz. U. z 2005 r. Nr 132, poz. 1108).
[22] Rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony (Dz. U. 2003 r. Nr 116, poz. 1090).
[23] Sadowski J., *Ochrona infrastruktury krytycznej. Uregulowania prawne*, „Autobusy: technika, eksploatacja, systemy transportowe" 2018, nr 6, 1242–1248.
[24] Sadowski J., *Podstawy prawne ochrony infrastruktury krytycznej a zarządzanie kryzysowe*, [w:] B. Kosowski (red), *Elementy ochrony infrastruktury krytycznej w zarządzaniu kryzysowym*, Katowice 2014, 30.
[25] *Narodowy Program Ochrony Infrastruktury Krytycznej – tekst jednolity*, Rządowe Centrum Bezpieczeństwa 2020, https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej [dostęp: 3.05.2021], 8–10, 13–14.
[26] Świątkowska J. (red.), *Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny*, Kraków 2014, s. 32.
[27] Szewczyk T., Pyznar M., *Ochrona infrastruktury krytycznej a zagrożenia asymetryczne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 2, 55–56.
[28] Kopczewski M., Sienkiewicz D. (red.), *Edukacja warunkiem bezpieczeństwa w XXI wieku – Sektory infrastruktury krytycznej i ich zagrożenia*, Koszalin 2018, 15.
[29] Ustawa z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym (Dz. U. 2003 Nr 80, poz. 717).
[30] Ustawa z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. 2008 Nr 171, poz. 1055).

COL. RET. KRZYSZTOF CYGAŃCZUK, PH.D. ENG. – he completed his master's studies at the University of Szczecin and doctoral studies at the War Art Academy in Warsaw, as well as postgraduate studies in foreign service at the National Defense Academy, data protection and information security at the Cardinal Stefan Wyszyński University in Warsaw and crisis management at NATO Defense College (Rome) and NATO School (Oberammergau). In 2004–2008 he was a liaison officer of the NATO Office (NLO) in Kyiv, in 2008–2010 he was a consul at the Consulate General of the Republic of Poland in Lviv. He is an assistant professor at the Department of Studies and Scientific Projects at CNBOP-PIB in Józefów. Specialty – environmental engineering, safety science. Representative of the Technical Committee No. 176 for Military Technology and Supply in the Polish Committee for Standardization.

ŁUKASZ ROMAN, PH.D. – has a PhD in social sciences in the area of defence sciences, specializing in polemology. He obtained his academic degree at the Faculty of Management and Command at the National Defence University in Warsaw. He completed post-graduate studies in history and knowledge about society. In 2015–2019, a research and didactic employee at Alcide De Gasperi University of Euroregional Economy in Józefów. In 2017–2019, the Dean of the Faculty of Social Sciences in Mińsk Mazowiecki. From January 2020, a research and didactic employee as an assistant professor at the Institute of Safety Sciences at the University of Justice. Organizer and co-organizer of many conferences and scientific seminars, as well as many trainings, courses and projects in the area of security. Reviewer of many scientific articles and monographs. Author of scientific and research works and numerous scientific publications in the area of national security.

PŁK REZ. DR INŻ. KRZYSZTOF CYGAŃCZUK – ukończył studia magisterskie na Uniwersytecie Szczecińskim oraz studia doktoranckie w Akademii Sztuki Wojennej w Warszawie, a także studia podyplomowe z zakresu służby zagranicznej w Akademii Obrony Narodowej, ochrony danych i bezpieczeństwa informacji na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie oraz zarządzania kryzysowego w NATO Defence College (Rzym) i NATO School (Oberammergau). W latach 2004–2008 był oficerem łącznikowym Biura NATO (NLO) w Kijowie, z kolei w latach 2008–2010 był konsulem w Konsulacie Generalnym RP we Lwowie. Jest adiunktem w Dziale Prac Studialnych i Projektów Naukowych w CNBOP-PIB w Józefowie. Specjalność – inżynieria środowiska, nauki o bezpieczeństwie. Przedstawiciel Komitetu Technicznego nr 176 ds. Techniki Wojskowej i Zaopatrzenia w Polskim Komitecie Normalizacyjnym.

DR ŁUKASZ ROMAN – jest doktorem nauk społecznych w zakresie nauk o obronności– specjalność polemologia. Stopień naukowy uzyskał na Wydziale Zarządzania i Dowodzenia w Akademii Obrony Narodowej w Warszawie. Ukończył studia podyplomowe z zakresu historii i wiedzy o społeczeństwie. W latach 2015–2019 pracownik naukowo-dydaktyczny w Wyższej Szkole Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie. W latach 2017–2019 Dziekan Zamiejscowego Wydziału Nauk Społecznych w Mińsku Mazowieckim. Od stycznia 2020 pracownik badawczo-dydaktyczny na stanowisku adiunkta w Instytucie Nauk o Bezpieczeństwie Szkoły Wyższej Wymiaru Sprawiedliwości. Organizator i współorganizator wielu konferencji i seminariów naukowych, a także wielu szkoleń, kursów i projektów dotyczących obszaru bezpieczeństwa. Recenzent wielu artykułów naukowych i monografii. Autor prac naukowo-badawczych i licznych publikacji naukowych z zakresu bezpieczeństwa narodowego.