SFT VOL. 54 ISSUE 2, 2019, PP. 132–141

Bogdan Kosowski[a)*]

[a)] *The Jagiellonian University, Institute of Political Science and International Relations / Uniwersytet Jagielloński, Instytut Nauk Politycznych i Stosunków Międzynarodowych*
* *Corresponding author / Autor korespondencyjny: bogdan.kosowski@gmail.com*

Critical Infrastructure in the National Security System

Infrastruktura krytyczna w systemie bezpieczeństwa narodowego

ABSTRACT

Aim: To present relationships resulting from legal regulations impacting the effectiveness of critical infrastructure protection, which is a part of the national security system. An auxiliary objective was a historical analysis illustrating the process of creating critical infrastructure in a modern form in the world and in Poland.
Project and methods: Article is based on the principles of functionalism theory and using literature analysis, expert interviews, participating observation in the organised Critical Infrastructure Forums, inference and deduction. This made it possible to identify the directions for improving the functioning of critical infrastructure protection in terms of institutional cooperation and the impact of infrastructure on the national security system.
Results: Removal of critical infrastructure protection vulnerabilities as a contribution to the elimination of a weak link in the national security system in the context of assessing the effectiveness and efficiency of the national security system.
Conclusions: There is a need to create clear legislation and to integrate security entities in terms of institutional cooperation in the protection of critical infrastructure. This is related to the fact that in an organisation, which is a particular form of team activities, we often encounter chaos intensified by solutions which are the more inaccurate, the less the formation mechanism of disturbing factors is known. Then we experience only the consequences of their impact, responding according to the circumstances.
Keywords: critical infrastructure, national security, infrastructure protection, classified information, security management, efficiency and effectiveness of operations
Type of article: review article

Received: 18.10.2019; Reviewed: 26.11.2019; Accepted: 17.12.2019;
Author's ORCID ID: 0000-0003-3397-4445;
Please cite as: SFT Vol. 54 Issue 2, 2019, pp. 132–141, https://doi.org/10.12845/sft.54.2.2019.10;

ABSTRAKT

Cel: Przedstawienie powiązań wynikających z uregulowań prawnych wpływających na efektywność ochrony infrastruktury krytycznej będącej elementem systemu bezpieczeństwa narodowego. Za cel pomocniczy przyjęto analizę historyczną obrazującą proces tworzenia infrastruktury krytycznej we współczesnej formie na świecie oraz w Polsce.
Projekt i metody: Artkuł został opracowany na podstawie zasad teorii funkcjonalizmu i przy wykorzystaniu analizy literatury, przeprowadzonych rozmów eksperckich i obserwacji uczestniczącej w organizowanych Forach Infrastruktury Krytycznej. Zastosowano także wnioskowanie i dedukcję, co pozwoliło na wskazanie kierunków poprawy funkcjonowania ochrony infrastruktury krytycznej w aspekcie współdziałania instytucjonalnego oraz wpływu infrastruktury na system bezpieczeństwa narodowego.
Wyniki: Eliminacja słabych stron ochrony infrastruktury krytycznej przyczynkiem do likwidacji słabego ogniwa systemu bezpieczeństwa narodowego w kontekście oceny efektywności i sprawności systemu bezpieczeństwa narodowego.
Wnioski: Zachodzi potrzeba tworzenia czytelnego prawa oraz konieczność integracji podmiotów bezpieczeństwa w aspekcie współdziałania instytucjonalnego w ramach ochrony infrastruktury krytycznej. Jest to związane z tym, że w organizacji, będącej szczególną formą działań zespołowych, często spotykamy się z chaosem potęgowanym rozwiązaniami tym bardziej nietrafionymi, im mniej znany jest mechanizm powstawania zakłócających czynników. Doświadczamy wtedy jedynie konsekwencji ich oddziaływania, reagując stosownie do zaistniałych okoliczności.
Słowa kluczowe: infrastruktura krytyczna, bezpieczeństwo narodowe, ochrona infrastruktury, informacje niejawne, zarządzanie bezpieczeństwem, sprawność i efektywność działania
Typ artykułu: artykuł przeglądowy

Przyjęty: 18.10.2019; Zrecenzowany: 26.11.2019; Zatwierdzony: 17.12.2019;
Identyfikator ORCID: – 0000-0003-3397-4445;
Proszę cytować: SFT Vol. 54 Issue 2, 2019, pp. 132–141, https://doi.org/10.12845/sft.54.2.2019.10;

Introduction

The essence of the functioning of each society is to ensure a safe, effective and efficient course of action and elimination of potential threats resulting from the dependence of society on different environmental factors, guaranteeing stability of life at an acceptable level of safety. In addition to the primary existential resources such as water, food production and distribution, shelter and electricity, people are paying more and more attention to the various kinds of stimuli that in a systemic way provide them with the comfort of living. These include telephone communication systems, the Internet and communication and transport systems, which are described as broadly developed consumerism. These systems work in everyday life context and are subject to various types of threats causing disruptions in their functioning. Unfortunately, even small disruptions of one system may increase the level of threat, and the size, extent and scale of such events may affect not only individuals, but also have a significant impact on the functioning of society and the whole country.

The range of emerging disruptions that may turn into threats is very wide, due to the current political situation or the current level of technological and civilisational development. These include, among others, natural disasters, technological failures caused by malfunctions of equipment or unintentional human activity, acts of terrorism, cyber-terrorism, intentional sabotage, mass social unrest or warfare. When they occur, human existence depends on the State, which provides conditions of stability through the use of subsystems for recognising, preventing and combating threats. These subsystems, being connected with each other, form a specific whole, which is considered as a functional unity in the so-called national security system[1] [1]. A change in any of the elements included in the national security system may lead to its disintegration.

In the conducted analytical process, including the paper content, the theoretical concept of J. Alexander, N. Luhmann[2] [2] was used in relation to the conditions for the functioning of critical infrastructure protection[3] [3]. Critical infrastructure is one of the elements of the national security system. In this system, an in-

[1] According to the National Security Strategy of 2014 – the national security system comprises appropriately organised, maintained and prepared forces, means and resources allocated by the State to perform tasks in this area. It consists of the management subsystem and executive subsystems, including operational (defence and protection) and support (social and economic) subsystems.

[2] As cited in Nowa Encyklopedia Powszechna PWN of 1995, the aforementioned theoretical concept in sociology and anthropology refers to the theory of functionalism, which is based on the following assumptions:
- society is a system composed of interconnected parts, each of which has a defined function in that system,
- the social system is in a state of dynamic equilibrium,
- tensions existing within the system can persist even for a long time, but they are solved,
- the system is changing, but gradually and evolutionarily, social macro-structures undergo the greatest changes, while social and cultural micro-structures remain largely unchanged,
- this system is characterised by the existence of diverse social roles and positions, associated with different rights and responsibilities, and by the existence of common standards and values. In order for the system to be sustainable, the following conditions must be met: it must be capable of adapting, achieving objectives, integrating and maintaining the set practice models,
- the social system aims to maintain order, i.e. proper functioning.

[3] According to the Crisis Management Act of 2007, critical infrastructure is systems and their functionally interconnected facilities, including buildings, facilities, systems, services essential for the security of the State and its citizens, and serving to ensure the efficient functioning of public administration bodies, institutions and business entities.

Wprowadzenie

Istotą funkcjonowania każdego społeczeństwa jest zapewnienie bezpiecznego, skutecznego i efektywnego przebiegu procesu działania oraz eliminacja potencjalnych zagrożeń wynikających z uzależnienia społeczeństwa od odmiennych czynników otoczenia, gwarantujących stabilność życia na akceptowanym poziomie bezpieczeństwa. Oprócz podstawowych zasobów koniecznych do egzystencji, takich jak woda, produkcja i dystrybucja żywności, schronienie i energia elektryczna, człowiek przywiązuje coraz większą wagę do różnego rodzaju bodźców, które zapewniają mu komfort życia. Można tutaj wymienić systemy łączności telefonicznej, Internet, czy też system komunikacyjno-transportowy, które zaliczane są do potrzeb z zakresu szeroko rozwiniętego konsumpcjonizmu. Wymienione systemy działają w harmonii życia codziennego i podlegają różnego rodzaju zagrożeniom powodującym zakłócenia w ich funkcjonowaniu. Niestety nawet niewielkie zaburzenia działania jednego systemu mogą doprowadzić do zwiększenia stanu zagrożenia, a rozmiar, zasięg i skala takich zdarzeń mogą dotknąć nie tylko pojedyncze osoby, ale także znacząco wpłynąć na funkcjonowanie społeczeństwa i całego państwa.

Katalog pojawiających się zakłóceń, które mogą przerodzić się w zagrożenia, jest bardzo szeroki – z uwagi na stan aktualnej sytuacji politycznej czy też bieżący poziom rozwoju technologicznego i cywilizacyjnego. Między innymi można tutaj wymienić: klęski żywiołowe, awarie technologiczne spowodowane nieprawidłowym funkcjonowaniem urządzeń lub nieumyślnym działaniem człowieka, akty terrorystyczne, cyberterroryzm, umyślne działania sabotażowe, niepokoje społeczne o charakterze masowym, czy też działania wojenne. W sytuacji ich zaistnienia byt człowieka uzależniony jest od państwa, które zapewnia warunki stabilności poprzez stosowanie podsystemów rozpoznawania, przeciwdziałania oraz zwalczania zagrożeń. Podsystemy te, będąc ze sobą powiązane, tworzą określoną całość, która rozpatrywana jest jako funkcjonalna jedność, w tzw. systemie bezpieczeństwa narodowego[1] [1]. Zmiana któregokolwiek z elementów występujących w systemie bezpieczeństwa narodowego może doprowadzić do jego dezintegracji.

W przeprowadzonym procesie analitycznym wykorzystano teoretyczną koncepcję J. Alexander, N. Luhmann[2] [2] w odniesieniu do

[1] Według Strategii Bezpieczeństwa Narodowego z 2014 r. – system bezpieczeństwa narodowego to siły, środki i zasoby przeznaczone przez państwo do realizacji zadań w tym obszarze, odpowiednio zorganizowane, utrzymywane i przygotowywane. Składa się on z podsystemu kierowania i podsystemów wykonawczych, w tym podsystemów operacyjnych (obronnych i ochronnych) oraz podsystemów wsparcia (społecznych i gospodarczych).

[2] Za Nową Encyklopedią Powszechna PWN z 1995 r., wspomniana koncepcja teoretyczna w socjologii i antropologii odnosi się do teorii funkcjonalizmu, który opiera się na założeniach:
- społeczeństwo jest systemem składającym się z wzajemnie powiązanych części, z których każda pełni określoną funkcję w tym systemie,
- system społeczny jest w stanie dynamicznej równowagi,
- istniejące wewnątrz systemu napięcia mogą się utrzymywać nawet przez dłuższy czas, ale są one rozwiązywane,
- system ten ulega zmianom, ale w sposób stopniowy i ewolucyjny, największym zmianom ulegają społeczne makrostruktury, podczas gdy mikrostruktury społeczne i kulturowe pozostają zasadniczo niezmienione,
- cechą charakterystyczną tego systemu jest występowanie zróżnicowanych ról i pozycji społecznych, związanych ze zróżnicowanymi prawami i obowiązkami, oraz istnienie wspólnych norm i wartości. Aby system ten mógł trwać, muszą być spełnione następujące warunki: musi być zdolny do adaptacji, osiągnięcia celów, integracji i utrzymywania wzorców działania,
- system społeczny dąży do zachowania ładu, czyli prawidłowego funkcjonowania.

ternal balance must be maintained within the activities of many specialised entities performing statutorily assigned functions in order to ensure the stable life of society. Critical infrastructure protection is one of the primary tasks of State authorities responsible for the security of citizens, where the analysis conducted considers the manifestations of collective action resulting from authoritarian rules, principles and practices i.e. derived from a legitimate authority. These rules include, among others, legal regulations and public institutions and entities. The scope of the analysis conducted covered the functioning of critical infrastructure protection. The paper outlines social reality in the form of interconnected and balanced selected elements of the national security system. As already mentioned, the theory of functionalism was used to indicate the impact of critical infrastructure on the national security system in terms of State institutions and entities. It was assumed that the efficiency and effectiveness of the national security system depends on the efficiency and effectiveness of its weakest link.

The concept of critical infrastructure in the international context

The traditional approach to national security was inseparably connected with the balance of political and military forces, while the transformations taking place in the world and in Poland challenge this view. Currently, military threats often give way to threats resulting from the forces of nature, terrorism, dangerous techniques and technologies, generating more and more social and economic threats. Regardless of the type of threats, ensuring generally understood security is the task of each State. Depending on the size and extent of the threat, actions are taken to minimise losses at various levels of public administration and those incurred by individual security entities forming the State. There are many elements influencing the national security system, and in the age of globalisation one of them is the correct, undisturbed functioning of critical infrastructure.

A concept similar to the current concept of critical infrastructure has been used for many centuries. For the Phoenicians, these were ports and port installations used for commercial activities and shipbuilding to control sea trade routes. In ancient Egypt, these were irrigation devices connected to the Nile, and grain warehouses. For colonial Spain, these were gold mines in South America, and for Portugal or Great Britain, overseas estates with transport routes and ports enabling the transportation of various goods to their metropolises. Currently, the term critical infrastructure (CI) is used to refer to resources that are critical to the functioning of the State and its citizens. The term was first used in the US President B. Clinton's Directive of 22 May 1998, which indicated the need to take action to protect facilities, systems that are sensitive to impacts of potential opponents,

warunków funkcjonowania ochrony infrastruktury krytycznej[3] [3]. Infrastruktura krytyczna jest bowiem jednym z elementów systemu bezpieczeństwa narodowego. Aby zapewnić stabilność życia społeczeństwa, w systemie tym musi być zachowana wewnętrzna równowaga w obrębie działań wielu wyspecjalizowanych podmiotów, pełniących przypisane ustawowo funkcję. Ochrona infrastruktury krytycznej jest jednym z nadrzędnych zadań organów państwa odpowiedzialnych za bezpieczeństwo obywateli. W przeprowadzonej analizie rozpatrywane są przejawy zbiorowego działania wynikające z autorytarnych, wywiedzionych reguł, zasad i praktyk prawomocnej władzy. Do reguł tych zalicza się między innymi normy prawne oraz instytucje i podmioty publiczne. Przeprowadzona analiza swoim zakresem objęła funkcjonowanie ochrony infrastruktury krytycznej. Przedstawiono zarys rzeczywistości społecznej w postaci wzajemnie powiązanych i pozostających w równowadze wybranych elementów systemu bezpieczeństwa narodowego. Jak już wspomniano, w celu wskazania wpływu infrastruktury krytycznej na system bezpieczeństwa narodowego w kategoriach instytucji i podmiotów państwa, bazowano na teorii funkcjonalizmu. Przyjęto założenie, iż efektywność i sprawność systemu zależy od sprawności i efektywności najsłabszego ogniwa, wchodzącego w skład systemu bezpieczeństwa narodowego.

Pojęcie infrastruktury krytycznej w ujęciu międzynarodowym

Tradycyjne ujęcie bezpieczeństwa narodowego nieodłącznie związane było z układem sił polityczno-militarnych. Tymczasem przeobrażenia zachodzące w świecie i w Polsce korygują ten pogląd. Obecnie zagrożenia militarne często ustępują miejsca zagrożeniom wynikających z sił przyrody, terroryzmu, niebezpiecznych technik i technologii, generując także zagrożenia społeczno-ekonomiczne. Bez względu na rodzaj zagrożeń zapewnienie ogólnie pojmowanego bezpieczeństwa jest zadaniem każdego państwa. W zależności natomiast od wielkości i rozmiaru zagrożenia podejmowane są działania w zakresie minimalizacji strat na poszczególnych szczeblach administracji publicznej oraz przez poszczególne podmioty bezpieczeństwa tworzące państwo. Istotnym w dobie globalizacji czynnikiem wpływającym na system bezpieczeństwa narodowego jest poprawne, niezakłócone funkcjonowanie infrastruktury krytycznej.

Z zasobami, które współcześnie nazywamy infrastrukturą krytyczną, spotykamy się już od wielu wieków. Dla Fenicjan były nimi porty i instalacje portowe wykorzystywane do działalności handlowej oraz budowy okrętów zapewniających kontrolę morskich szlaków handlowych. W starożytnym Egipcie infrastrukturę tę stanowiły urządzenia irygacyjne związane z Nilem oraz magazyny na zboże. Dla kolonialnej Hiszpanii były to kopalnie złota w Ameryce Południowej, a dla Portugalii i Wielkiej Brytanii – posiadłości zamorskie wraz ze szlakami komunikacyjnymi i portami umożliwia-

[3] Według ustawy o zarządzaniu kryzysowym z 2007 r. infrastruktura krytyczna to 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.

and for the proper functioning of the State [4]. Critical infrastructure protection activities were intensified after the events of 11 September 2001, i.e. the terrorist attack in New York. This event resulted in the intensification and acceleration of work on the development of systems aimed at the protection of critical infrastructure as a resource having a fundamental impact on the functioning of society and the economy of the State. Therefore, the concept of critical infrastructure is associated with means of production, healthcare, telecommunications, transport, security services, etc., and its purely descriptive definition is from the perspective of the functioning of the State. An example is the definition of critical infrastructure in NATO, which indicates, among others, that these are "...facilities, services and information systems that are so vital to the State that their damage or destruction could have a significant impact on State security, national economy, public health and security and the proper functioning of the State..." [5] .

A similar definition can be found in the Directive of the Council of the European Union of 8 December 2008, which states that critical infrastructure "...means assets, systems or parts thereof[4] located in Member States which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions..." [6].

It is interesting to note that in the European Union, the intensification of work on the critical infrastructure protection model followed the attack in Madrid on 11 March 2004, which killed as many as 191 people. In June 2004, the European Council ordered that a strategy be drawn up for the protection of critical infrastructure. The work was aimed at improving systems for preventing terrorist attacks and improving preparedness and response capacity. This work culminates in the aforementioned Council Directive, which does not interfere with the solutions adopted by individual Member States, leaving the designation of critical infrastructure to the discretion of Member States, using the analysis of risk, hazards and vulnerabilities. It also identifies the need to draw up critical infrastructure protection plans, to appoint a liaison officer and to ensure communication, storage and flow of information with a specified classification level. The presented principles are directly related to the need to ensure the protection of the European Critical Infrastructure as infrastructure located in the territory of Member States whose disruption or destruction would have a significant impact on at least two Member States [6]. Thus, Poland, as a country forming the EU community, was obliged to provide a critical infrastructure protection system, which was statutorily implemented in 2007, by adopting in the Polish Parliament the Act on Crisis Management, which also included issues directly related to critical infrastructure.

[4] According to the PWN Encyclopaedia of 1995, infrastructure is the basic facilities and institutions ensuring the proper existence and functioning of communities that provide services in the field of:
- services including transport, communication, energy, irrigation, land reclamation, etc. (economic infrastructure),
- services in the fields of law, security, education and training, health, personal communication, etc. (social infrastructure).

jące transport różnych dóbr do metropolii. Obecnie termin infrastruktura krytyczna (IK) używany jest w odniesieniu do zasobów mających podstawowe znaczenie dla funkcjonowania państwa i jego obywateli. Określenie to pojawiło się po raz pierwszy w dyrektywie prezydenta USA B. Clintona z dnia 22 maja 1998 roku, która wskazywała na konieczność podejmowania działań w sprawie ochrony obiektów, systemów będących wrażliwymi na uderzenia potencjalnych przeciwników, a stanowiących systemy niezbędne dla prawidłowego funkcjonowania państwa [4]. Intensyfikacja działań w zakresie ochrony infrastruktury krytycznej przybrała na sile po zamachu terrorystycznym w Nowym Yorku 11 września 2001 roku. Wydarzenie to spowodowało przyspieszenie prac nad stworzeniem systemów mających na celu ochronę infrastruktury krytycznej jako zasobu wywierającego zasadniczy wpływ na funkcjonowanie społeczeństwa i gospodarki państwa. Stąd też z pojęciem infrastruktury krytycznej kojarzone są środki do produkcji, ochrony zdrowia, telekomunikacji, transportu, służb bezpieczeństwa itp., a jej wyłącznie opisowe definiowanie następuje z perspektywy funkcjonowania państwa. Przykładem jest tutaj definicja infrastruktury krytycznej funkcjonująca w NATO, w której między innymi wskazuje się, że są to „...obiekty, służby i systemy informacyjne, które są żywotne dla państwa, że ich uszkodzenie lub zniszczenie mogłoby mieć niebagatelny wpływ na bezpieczeństwo państwa, krajową gospodarkę, zdrowie i bezpieczeństwo publiczne oraz prawidłowe funkcjonowanie państwa..." [5] .

Podobny opis możemy napotkać w Dyrektywie Rady Unii Europejskiej z 8 grudnia 2008 roku, w której określono, że infrastruktura krytyczna „...oznacza składniki, systemy lub części infrastruktury[4] zlokalizowane na terytorium państw członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz którego zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji..." [6].

Co ciekawe, w Unii Europejskiej intensyfikacja prac nad modelem ochrony infrastruktury krytycznej nastąpiła po zamachu przeprowadzonym w dniu 11 marca 2004 roku w Madrycie, w wyniku którego zginęło aż 191 osób. W czerwcu 2004 roku Rada Europejska nakazała przystąpić do opracowania strategii w zakresie ochrony infrastruktury krytycznej. Działania skupiono na usprawnieniu systemów zapobiegania atakom terrorystycznym oraz podniesieniu gotowości i zdolności do reagowania. Uwieńczeniem tych prac jest wspomniana powyżej Dyrektywa Rady, która nie ingeruje w rozwiązania przyjęte przez poszczególne państwa, pozostawiając wyznaczanie infrastruktury krytycznej w gestii poszczególnych państw członkowskich, przy wykorzystaniu analizy ryzyka, zagrożeń i słabych punktów. Wskazuje jednocześnie na potrzebę opracowania planów ochrony infrastruktury krytycznej, powołania urzędnika łącznikowego oraz zapewnienia komunikowania się oraz magazynowania i przepływu informacji, przy określonej klauzuli tajności. Przedstawione zasady

[4] Według Encyklopedii PWN z 1995 r., infrastruktura to podstawowe urządzenia i instytucje zapewniające należyte istnienie i funkcjonowanie społeczności, które wykonują świadczenia w zakresie:
- usług obejmujących transport, komunikację, energetykę, irygację, melioracje, itp. (infrastruktura ekonomiczna),
- usług w dziedzinie prawa, bezpieczeństwa, kształcenia i oświaty, służby zdrowia, komunikacji osobowej, itp. (infrastruktura społeczna).

związane są bezpośrednio z potrzebą zapewnienia ochrony Europejskiej Infrastruktury Krytycznej, jako infrastruktury zlokalizowanej na terytorium państw członkowskich, której zakłócenie lub zniszczenie miałby istotny wpływ na co najmniej dwa państwa członkowskie [6]. Tym samym Polska jako kraj tworzący wspólnotę UE została zobowiązana do zapewnienia systemu ochrony infrastruktury krytycznej, co ustawowo wykonano w roku 2007, uchwalając w Parlamencie RP ustawę o zarządzaniu kryzysowym, obejmującą także zagadnienia odnoszące się bezpośrednio do infrastruktury krytycznej.

Critical infrastructure protection in Poland

In terms of functionality[5] critical infrastructure protection in Poland has been an issue since the beginning of work on a legal solution for the protection of the most important facilities for the security of the State and its citizens. This work resulted in the Act of 22 August 1997 on the Protection of Persons and Property, in which the legislator specified that facilities subject to mandatory protection are areas, facilities, equipment, transports important for defence and protection of the interests of the State and public security. The obligation to protect systems, equipment and facilities important for State defence, economic protection of the State, public security and protection of other important State interests was indicated [7]. This Act does not specify systems, equipment or facilities. It does, however, specify the necessity of protection due to its importance for defence and economic and social interests that are important for the State. Facilities subject to mandatory protection were detailed in the Regulation of the Council of Ministers of 24 June 2003 [8]. The document divided areas, facilities and equipment subject to compulsory protection as particularly important for the security of state defence into two categories. Category I includes plants involved in the production, repair and storage of military equipment and armaments, as well as research and development plants for security and defence purposes; warehouses of State reserves; facilities of units subordinate to the Ministry of National Defence; facilities of road, railway, water, sea and air transport infrastructure, as well as centres of geodesic and cartographic documentation; water dams and other hydrotechnical equipment; facilities of the Intelligence Agency; facilities of the National Bank of Poland (NBP), BGK, the Polish Security Printing Works and the State Mint; facilities where nuclear materials, radioactive sources and waste are produced, used or stored; telecommunications facilities designed for broadcasting public radio and television programmes. Category II of facilities subject to protection as particularly important for national defence and security includes, among others: facilities of units subordinate to the Minister of Internal Affairs; organisational facilities of the Internal Security Agency; facilities of the Police, the Border Guard, the State Fire Service; facilities within the jurisdiction of the Minister of Justice, prison service; facilities related to the extraction of basic minerals; facilities which

[5] The functional aspect is understood by the author to include, among others, common and similar characteristics of the discussed issue related to critical infrastructure systems.

Ochrona infrastruktury krytycznej w Polsce

O ochronie infrastruktury krytycznej w Polsce w aspekcie funkcjonalnym[5] można mówić od momentu zainicjowanych prac nad prawnym rozwiązaniem ochrony obiektów mających najistotniejsze znaczenie dla bezpieczeństwa państwa i jego obywateli. Efektem tych prac stała się ustawa z dnia 22 sierpnia 1997 roku o ochronie osób i mienia, w której ustawodawca określił, że obiekty podlegające obowiązkowej ochronie to obszary, obiekty, urządzenia, transporty ważne dla obronności i ochrony interesów państwa i bezpieczeństwa publicznego. Wskazana została obowiązkowość ochrony dla systemów, urządzeń, obiektów ważnych dla obronności państwa, ochrony gospodarczej państwa, bezpieczeństwa publicznego i ochrony innych ważnych interesów państwa [7]. Ustawa ta nie precyzuje systemów, urządzeń, czy też obiektów. Określa natomiast konieczność ochrony ze względu na znaczenie dla obronności i interesów ekonomicznych oraz społecznych istotnych dla państwa. Uszczegółowienie wykazu obiektów podlegających obowiązkowej ochronie nastąpiło w rozporządzeniu Rady Ministrów z dnia 24 czerwca 2003 roku [8]. Dokument wprowadził podział obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie jako szczególnie ważne dla bezpieczeństwa obronności państwa na dwie kategorie. Do kategorii I należą: zakłady zajmujące się produkcją, remontem, magazynowaniem sprzętu wojskowego i uzbrojenia oraz zakłady badawczo-rozwojowe na potrzeby bezpieczeństwa i obronności; magazyny rezerw państwowych; obiekty jednostek podległych MON; obiekty infrastruktury transportu samochodowego, kolejowego, wodnego, morskiego, lotniczego oraz ośrodki dokumentacji geodezyjnej i kartograficznej; zapory wodne i inne urządzenia hydrotechniczne; obiekty Agencji Wywiadu; obiekty NBP, BGK, Państwowej Wytwórni Papierów Wartościowych oraz Mennicy Państwowej; obiekty, w których produkuje się, stosuje lub magazynuje materiały jądrowe oraz źródła i odpady promieniotwórcze; obiekty telekomunikacyjne przeznaczone do nadawania programów radia i telewizji publicznej. Do II kategorii zostały zaliczone między innymi: obiekty jednostek podległych ministrowi właściwemu do spraw wewnętrznych; obiekty organizacyjne Agencji Bezpieczeństwa Wewnętrznego; obiekty policji, straży granicznej, straży pożarnej; obiekty znajdujące się we właściwościach ministra sprawiedliwości, służby więziennej; zakłady związane z wydobyciem kopalin podstawowych; obiekty, które produkują, magazynują lub stosują materiały szczególnie zagrożone wybuchem lub pożarem; obiekty, których działalność związana jest z wykorzystaniem toksycznych

[5] Przez aspekt funkcjonalny Autor rozumie między innymi wspólne i zbliżone cechy charakterystyczne dla omawianego zagadnienia związanego z systemami infrastruktury krytycznej.

produce, store or use materials which are particularly prone to explosion or fire; facilities whose activity is related to the use of toxic chemical compounds and biological agents that may cause diseases in humans and animals; power plants and other power facilities; other facilities whose destruction or damage may pose a threat to human life and health, national heritage, the environment, and their destruction or damage may cause disturbances in the functioning of the State [8].

At that time in Poland, a discussion on critical infrastructure issues, including its protection, was also initiated. In 2001, representatives of Poland took part in the NATO SECURE 2001 conference, where the problems related to security in the ICT network were analysed. In 2002, the National Security Bureau and Telekomunikacja Polska SA organised a conference "Secure Infrastructure in Poland", where the leading theme was the coordination of security activities throughout the country. Under the auspices of the Ministry of Interior and Administration, work began on the development of legal solutions for the protection of critical infrastructure [9], which resulted in sanctioning the protection of critical infrastructure in the Act on Crisis Management of 26 April 2007 [3]. The definition of critical infrastructure in the Act refers directly to systems such as: "...energy, raw materials and fuels supply; communications; information and communication networks; financial; food supply; water supply; healthcare; transport; emergency; ensuring the continuous functioning of the public administration; production, storage, keeping and use of chemicals and radioactive substances, including pipelines of dangerous substances..." [3].

Doubts arise at a practical level when analysing the functional understanding of the normative provisions relating to the proposed definition of critical infrastructure. If, for example, transport infrastructure, which is treated as economic infrastructure [2] of the State, is considered to be a transport system in the sense of critical infrastructure, does this mean that the entire transport infrastructure of the State is critical infrastructure for the country? Can it then be critical due to its usability for the safe functioning of the State? In the author's opinion, it cannot, because if we follow this line of reasoning, then we will consider the critical condition of the infrastructure of the entity - the State, and not the critical condition of infrastructure understood as all transport systems. In such a case, systems that include facilities, equipment, installations and services crucial for the security and defence of the State must be subject to special protection, which involves the need to solve the problems contained, among other things, in the following questions[6]:

związków chemicznych, a także środków biologicznych mogących wywoływać choroby u ludzi i zwierząt; elektrownie i inne obiekty elektroenergetyczne; inne obiekty, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia i zdrowia ludzi, dziedzictwa narodowego, środowiska naturalnego a ich zniszczenie lub uszkodzenie może spowodować zakłócenia funkcjonowania państwa [8].

W Polsce w tym czasie rozpoczęto także dyskusję obejmującą bezpośrednio problematykę infrastruktury krytycznej łącznie z jej ochroną. W 2001 roku przedstawiciele Polski uczestniczyli w zorganizowanej przez NATO konferencji SECURE 2001, na której poddano analizie problemy związane z bezpieczeństwem w sieci teleinformatycznej. W 2002 roku Biuro Bezpieczeństwa Narodowego i Telekomunikacja Polska SA zorganizowały konferencję „Bezpieczna Infrastruktura w Polsce", której wiodącym tematem była koordynacja działań w zakresie bezpieczeństwa na terenie całego kraju. Pod patronatem MSWiA rozpoczęto prace nad stworzeniem prawnych rozwiązań ochrony infrastruktury krytycznej [9], co w konsekwencji doprowadziło do usankcjonowania ochrony infrastruktury krytycznej w ustawie z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym [3]. Przedstawiona w ustawie definicja infrastruktury krytycznej odnosi się bezpośrednio do systemów takich jak: „...zaopatrzenia w energię, surowce energetyczne i paliwa; łączności; sieci teleinformatycznych; finansowe; zaopatrzenia w żywność; zaopatrzenia w wodę; ochrony zdrowia; transportowe; ratownicze; zapewniające ciągłość działania administracji publicznej; produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych..." [3].

Przeprowadzając analizę obejmującą funkcjonalne zrozumienie zapisów normatywnych odnoszących się do przedstawionej definicji infrastruktury krytycznej na poziomie praktycznym, pojawiają się wątpliwości. Jeżeli bowiem np. infrastrukturę transportową, którą traktujemy jako infrastrukturę ekonomiczną [2] państwa, przyjmiemy za system transportowy w znaczeniu infrastruktury krytycznej, to czy oznacza to, że cała infrastruktura transportowa państwa jest infrastrukturą krytyczną dla kraju? Czy wówczas może ona być w stanie krytycznym ze względu na jej zdolność użytkową w aspekcie bezpiecznego funkcjonowania państwa? Zdaniem autora odpowiedź na tak postawione pytanie powinna być negatywna – jeśli przyjmiemy powyższy tok rozumowania, wtedy będziemy rozpatrywać stan krytyczny infrastruktury podmiotu – państwa, a nie stan krytyczny infrastruktury jako wszystkich systemów transportowych. W takim przypadku systemy, które obejmują obiekty, urządzenia, instalacje, usługi ważne dla bezpieczeństwa i obronności państwa muszą zostać poddane szczególnej ochronie, co wiąże się z koniecznością rozwiązania problemów zawartych między innymi w pytaniach[6]:

[6] The presented questions are formulated in the light of the adopted course of reasoning and are the result of the conducted participating observation resulting from the author's practice, as well as participation in thematic seminars and the Forum for the Protection of Critical Infrastructure. Active participation in the seminars and the Forum made it possible to hold a discussion and expert interviews on the basis of which the author formulated the questions. These questions are directly related to the effectiveness of the activities of security entities which operate in accordance with and on the basis of the applicable law. The lack of precision of obligations resulting from legal regulations results in dualism or even discontinuation of activities by certain security entities participating in the system. Then it may turn out that when an event occurs, there will be organisational chaos which will contribute to the reduction of the efficiency of the national security system.

[6] Przedstawione pytania są sformułowane wobec przyjętego toku rozumowania i są efektem przeprowadzonej obserwacji uczestniczącej wynikającej z praktyki Autora, a także udziału w seminariach tematycznych oraz Forum Ochrony Infrastruktury Krytycznej. Czynne uczestnictwo w seminariach i Forum pozwoliło przeprowadzić dyskusję oraz rozmowy eksperckie na podstawie, których Autor sformułował pytania. Pytania te są bezpośrednio powiązane z efektywnością działania podmiotów bezpieczeństwa, które funkcjonują na zasadach i w oparciu o obowiązujące prawo. Brak doprecyzowania obowiązków wynikających z unormowań prawnych powoduje dualizm bądź wręcz zaprzestanie działań przez niektóre podmioty bezpieczeństwa uczestniczące w systemie. Wtedy może się okazać, że w przypadku wystąpienia zdarzenia nastąpi chaos organizacyjny, który przyczyni się do obniżenia sprawności systemu bezpieczeństwa narodowego.

1. Will the register of areas, facilities and equipment subject to mandatory protection referred to in Article 5(2) of the Act on the Protection of Persons and Property include obligatorily all facilities also included in the list of critical infrastructure facilities, as indicated, for example, by the amendment to the provisions of the Act on the Protection of Persons and Property contained in Article 33 of the Act on Anti-Terrorist Activities?
2. Do the emergency services of Voivodeship Crisis Management Centres (as well as lower-level centres) have the ability and possibility to access, process and store classified documents with the CONFIDENTIAL clause?
3. Do the emergency services of Voivodeship Crisis Management Centres have 24-hour access to relevant extracts from the critical infrastructure list?
4. Do the plans, procedures and principles of operation used by the emergency services of Voivodeship Crisis Management Centres contain procedures for the notification of events occurring in critical infrastructure facilities?
5. Is it possible that crisis management plans at municipal and district levels, which are public documents, include duplicated information on critical infrastructure facilities?

Answers to such questions are important not only for the protection of information, but also for the protection of critical infrastructure and the integration of the activities of all State security institutions forming the national security system. Unfortunately, the analysis of normative acts and the used participating observation method show many ambiguities and the lack of precise statutory provisions. According to the author, in terms of creating new legal regulations in the discussed scope, there is no integration of security institutions and entities, and the direction of building systems protection in the sectoral system is dominant. An example of this was the work on the Act on the change of specific powers of the Minister of Energy and their exercise in certain corporations or groups of companies operating in the sectors of electricity, oil and gas fuels. At the time of drafting the Act, imprecise provisions appeared, for example, in the scope of wider cooperation between the Internal Security Agency (ABW) and CI operators. This applies, for example, to checking and responding to requests from a CI operator for whom an external economic operator performs modernisation, especially in electronic systems. In the case at hand, it is also important to:

- specify in the legal regulations the level of access to classified information and data to which the entity executing the modernisation order may have access,
- specify how to ensure destroyed or damaged equipment (e.g. destroyed turbines in the electricity sector) necessary for restoration (business continuity),

since these are issues that affect not only the security of critical infrastructure, but also the national security system, its effectiveness and efficiency.

Preserving legal transparency is very important to ensure the continuity of operation of an entity considered to be a critical infrastructure operator. These entities play a key role in citizens' lives and at the same time constitute an economic

1. Czy w ewidencji obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie, o których mowa w art. 5, ust. 2 ustawy o ochronie osób i mienia, znajdą się obligatoryjnie wszystkie obiekty zaklasyfikowane także do wykazu obiektów infrastruktury krytycznej, na co chociażby wskazuje zmiana w przepisach ustawy o ochronie osób i mienia zawarta w art. 33 ustawy o działaniach antyterrorystycznych?
2. Czy służby dyżurne Wojewódzkich Centrów Zarządzania Kryzysowego (a także centrów niższego szczebla) posiadają zdolność i możliwość dostępu, przetwarzania i magazynowania dokumentów niejawnych o klauzuli POUFNE?
3. Czy służby dyżurne Wojewódzkich Centrów Zarządzania Kryzysowego posiadają całodobowy dostęp do właściwych wyciągów z wykazu infrastruktury krytycznej?
4. Czy plany, procedury i zasady działania wykorzystywane przez służby dyżurne Wojewódzkich Centrów Zarządzania Kryzysowego zawierają procedury powiadamiania o zdarzeniach powstałych w obiektach infrastruktury krytycznej?
5. Czy przypadkiem w planach zarządzania kryzysowego szczebla gminnego i powiatowego – które są dokumentami jawnymi – nie dubluje się informacji o obiektach infrastruktury krytycznej?

Odpowiedzi na tak postawione pytania są istotne nie tylko z punktu widzenia ochrony informacji, ale także ochrony infrastruktury krytycznej i integracji działań wszystkich instytucji bezpieczeństwa państwa tworzących system bezpieczeństwa narodowego. Niestety przeprowadzona analiza aktów normatywnych oraz wykorzystana metoda obserwacji uczestniczącej wskazują na wiele niejednoznaczności i brak precyzyjnych zapisów ustawowych. Zdaniem autora w zakresie tworzenia nowych uregulowań prawnych w omawianym obszarze nie następuje integracja instytucji i podmiotów bezpieczeństwa, a coraz bardziej przyjmowany jest kierunek budowania ochrony systemów w układzie sektorowym. Przykładem mogą być prace nad ustawą o zmianie szczególnych uprawnieniach ministra właściwego do spraw energii oraz ich wykonywania w niektórych spółkach kapitałowych lub grupach kapitałowych, prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych. W czasie tworzenia ustawy pojawiły się nieprecyzyjne zapisy chociażby w zakresie szerszej współpracy między ABW a operatorami IK. Odnosi się to między innymi do sprawdzania i odpowiedzi na zapytania operatora IK, dla którego zewnętrzny podmiot gospodarczy wykonuje modernizację, zwłaszcza w systemach elektronicznych. W rozpatrywanym przypadku istotne jest także:

- określenie w unormowaniach prawnych poziomu dostępu do informacji i danych niejawnych, do których dostęp może mieć podmiot wykonujący zlecenie modernizacji;
- uszczegółowienie w jaki sposób należy zapewnić potrzebne do odtworzenia (zapewnienia ciągłości działania) zniszczone lub uszkodzone urządzenia (np. zniszczone turbozespoły w sektorze energii elektrycznej).

Są to bowiem zagadnienia wpływające nie tylko na stan bezpieczeństwa infrastruktury krytycznej, ale także na system bezpieczeństwa narodowego, jego efektywność i sprawność funkcjonowania.

Zachowanie przejrzystości prawa jest bardzo istotne z punktu widzenia zapewnienia ciągłości działania podmiotu uznanego jako

subsystem in the national security system[7]. The destruction, damage or disconnection of a single element of critical infrastructure may compromise or even cause the loss of defence or economic capacity or the functioning of public administration. This is obvious and understandable, which is reflected e.g. in the resolutions of the Council of Ministers [10] adopting the National Programme for Critical Infrastructure Protection. The programme is to contribute to the prevention of disruptions in the efficient operation of systems, preparing them for possible crisis situations, and in the case of failures or damage, develop appropriate response procedures and proceed to restore the damaged elements. The programme [11] primarily defines national priorities for the smooth functioning and restoration of critical infrastructure. It defines the competent ministers and heads of central offices who are responsible for the proper functioning of the systems assigned to them. The criteria for separating facilities, installations, equipment and services that are part of infrastructure systems have also been established. However, it is important to ensure the highest possible level of cooperation between the various institutions operating within the scope of critical infrastructure protection. This problem is partly solved by the Regulation of the Council of Ministers of 30 April 2010 [10], which contains the principles of creation, updating and structure of critical infrastructure protection plans. These plans are drawn up by a critical infrastructure operator taking into account general data, critical infrastructure data, characteristics and essential emergency response options to ensure the smooth restoration of critical infrastructure in the event of failure. The Regulation defines the rules of cooperation with the locally competent crisis management centre and public administration bodies, as well as the agreement of the plan with the Governor, Voivodeship Commander of the State Fire Service, Voivodeship Commander of the Police, Director of the Regional Water Management Authority (Wody Polskie), Voivodeship Building Supervision Inspector, Voivodeship Veterinarian, State Voivodeship Sanitary Inspector, and in the case of coastal areas with the Director of the Maritime Office. Thus, the range of persons having access to classified information in relation to the protection of critical infrastructure is growing significantly, and therefore it is necessary to solve the problems (posed problematic questions) referred to in the paper, especially in the area of cooperation and access, storage and protection of information on critical infrastructure, which significantly affects the national security system in an indirect way.

Conclusions

Critical infrastructure protection has a significant impact on the national security system in Poland, and imprecise legal regulations undoubtedly contribute to lowering the level of national

[7] Based on the provisions of the current National Security Strategy of 2014, the national security system comprises appropriately organised, maintained and prepared forces, means and resources allocated by the State to perform tasks in this area. The system consists of the management subsystem, executive subsystems and support subsystems, which include, among others, an economic subsystem.

operatora infrastruktury krytycznej. Podmioty te spełniają kluczową rolę w funkcjonowaniu życia obywateli, stanowiąc jednocześnie podsystem gospodarczy w systemie bezpieczeństwie narodowego[7]. Zniszczenie, uszkodzenie lub wyłączenie jednego elementu składowego infrastruktury krytycznej spowodować może załamanie lub nawet utratę zdolności obronnych, gospodarczych lub funkcjonowania administracji publicznej. Jest to oczywiste i zrozumiałe, co uwidaczniają np. uchwały Rady Ministrów [10],w których przyjęto Narodowy Program Ochrony Infrastruktury Krytycznej. Program ma przyczynić się do zapobiegania zakłóceniom w sprawnym działaniu systemów, przygotowując je na ewentualne sytuacje kryzysowe, a w przypadku awarii bądź uszkodzeń, wypracować właściwe procedury reagowania i przystąpić do odtworzenia zaistniałych uszkodzeń. Program [11] określa przede wszystkim narodowe priorytety służące sprawnemu funkcjonowaniu, jak i odtwarzaniu infrastruktury krytycznej. Wskazano w nim właściwych ministrów i kierowników urzędów centralnych, którzy są odpowiedzialni za poprawne funkcjonowanie przypisanych im systemów. Ustalono także kryteria, które pozwalają na wyodrębnienie obiektów, instalacji, urządzeń i usług, które wchodzą w skład systemów infrastruktury. Istotne jest jednak, by zapewnić jak najwyższy poziom współdziałania poszczególnych instytucji funkcjonujących w obrębie ochrony infrastruktury krytycznej. Po części problem ten rozwiązuje rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. [10], zawierający zasady tworzenia, aktualizacji oraz strukturę planów ochrony infrastruktury krytycznej. Plany te operator infrastruktury krytycznej opracowuje z uwzględnieniem danych ogólnych, danych o infrastrukturze krytycznej, charakterystyki i zasadniczych wariantów działania w sytuacjach kryzysowych, które mają zapewnić sprawne jej odtworzenie w przypadku jej uszkodzenia. Rozporządzenie określa zasady współpracy z właściwym miejscowo centrum zarządzania kryzysowego i organami administracji publicznej, a także uzgodnienie planu z wojewodą, komendantem wojewódzkim PSP, komendantem wojewódzkim Policji, dyrektorem regionalnego zarządu gospodarki wodnej (Polskimi Wodami), wojewódzkim inspektorem nadzoru budowlanego, wojewódzkim lekarzem weterynarii, państwowym wojewódzkim inspektorem sanitarnym oraz – w przypadku terenów nadmorskich – z dyrektorem urzędu morskiego. Tym samym grupa osób mających dostęp do informacji niejawnych w odniesieniu do ochrony infrastruktury krytycznej znacznie się powiększa. Powoduje to konieczność rozwiązania problemów (postawionych pytań problemowych), o których mowa w artykule, zwłaszcza w zakresie współdziałania oraz dostępu, magazynowania i ochrony informacji o infrastrukturze krytycznej, które w znaczący sposób pośrednio wpływają na system bezpieczeństwa narodowego.

Konkluzje

Ochrona infrastruktury krytycznej znacząco wpływa na system bezpieczeństwa narodowego w Polsce, a nieprecyzyjne za-

[7] W oparciu o zapisy ujęte w obowiązującej Strategii Bezpieczeństwa Narodowego z 2014 r. – system bezpieczeństwa narodowego obejmuje siły, środki i zasoby przeznaczone przez państwo do realizacji zadań w tym obszarze, które są odpowiednio zorganizowane, utrzymywane i przygotowane. System składa się z podsystemu kierowania, podsystemów wykonawczych oraz podsystemów wsparcia, do które zalicza się między innymi podsystem gospodarczy.

security. Critical infrastructure includes equipment, installations, facilities and services which are characterised, among others, by the following features:

- long-term service life,
- they serve as basic and specialised services,
- they are public and serve the public,
- they provide services for the industrial and consumer sectors,
- they are owned by the State, corporations or private individuals,
- they are often international because of the network of connections and interdependencies (energy, telecommunications networks, etc.),

which undoubtedly points to the impact of critical infrastructure on citizens' sense of security. It is therefore necessary for the State to support the activities of critical infrastructure operators, as their activities contribute to the development of the country and ensure acceptable levels of security for people. This is all the more so as the resources of critical infrastructure operators are used in various situations, including emergency situations, disturbing the normal functioning of the State and its economy. This is the case, among others, with liquid fuel supply systems for the transport and electricity sectors. Long-term difficulties in this area always have serious economic consequences, lowering the security and comfort of life of citizens and disturbing their social life. For example, it is difficult to imagine the functioning of an agglomeration without electricity or drinking water supplies for more than a few hours. The prolongation of such a state of affairs may undoubtedly lead to the anarchisation of social behaviours. Critical infrastructure is therefore of key importance for the existence of the State and the national security system, and within its framework - an organised society. If it is disrupted, the State and its institutions may lose all or part of their ability to perform their basic administrative and service functions. Therefore, it is so important to ensure such legal norms that directly affect the proper organisation of activities and the creation of such a structure of security management that will provide a formula of action rather than reaction [12]. Reactions, in relation to an organisation as a particular form of team activities, often give rise to chaos intensified by solutions which are the more inaccurate, the less the formation mechanism of disturbing factors is known. Then we experience only the consequences of their impact, responding according to the circumstances. The effectiveness of the system is manifested by the possibility of functioning and correlation of actions in normal and crisis situations, using the full potential of the State. However, the efficiency of the organisational structures of the State depends on the readiness to face challenges and threats, which is the determinant of the State security.

pisy prawne niewątpliwe wpływają na obniżenie stanu bezpieczeństwa państwa. Infrastruktura krytyczna obejmuje bowiem urządzenia, instalacje, obiekty oraz usługi, które:

- charakteryzują się długotrwałym okresem użytkowania,
- pełnią funkcją usług podstawowych i wyspecjalizowanych,
- posiadają charakter publiczny i pełnią rolę służebną wobec społeczeństwa,
- świadczą usługi dla sfery przemysłowej i konsumpcyjnej,
- stanowią własność państwa, korporacji bądź osób prywatnych,
- często posiadają międzynarodowy charakter z uwagi na sieć powiązań i zależności (sieci energetyczne, telekomunikacyjne itp.).

Powyżej wymienione cechy pokazują wpływ infrastruktury krytycznej na poczucie bezpieczeństwa obywateli. Tym samym konieczne staje się ze strony państwa wsparcie działalności operatorów infrastruktury krytycznej, ponieważ ich działalność służy rozwojowi kraju oraz zapewnieniu akceptowalnego stanu bezpieczeństwa ludzi. Tym bardziej, że zasoby operatorów infrastruktury krytycznej wykorzystywane są również w sytuacji nadzwyczajnych wydarzeń, zakłócających normalne funkcjonowanie państwa i jego gospodarki. Dzieje się tak m.in. w przypadku systemów dostaw paliw płynnych dla sektora transportowego oraz energii elektrycznej. Długotrwałe utrudnienia w tym obszarze zawsze niosą poważne skutki gospodarcze, obniżają stan bezpieczeństwa oraz komfort życia obywateli, zaburzając życie społeczne. Trudno np. wyobrazić sobie funkcjonowanie aglomeracji pozbawionej dostaw energii elektrycznej czy wody pitnej dłużej niż kilka godzin. Przedłużanie się takiego stanu niewątpliwie może doprowadzić do anarchizacji zachowań społecznych. Infrastruktura krytyczna ma zatem kluczowe znaczenie dla istnienia państwa i systemu bezpieczeństwa narodowego, a w jego ramach – zorganizowanego społeczeństwa. Jeśli następuje zakłócenie w jej funkcjonowaniu, państwo i jego instytucje mogą utracić – w całości lub w części – zdolność do wykonywania swoich podstawowych funkcji administracyjnych i usługowych. Stąd też tak istotne jest zapewnienie unormowań prawnych, które bezpośrednio wpływają na poprawne organizowanie działań i tworzenie struktury zarządzania bezpieczeństwem, która zapewni formułę akcji, a nie reakcji [12]. Reakcje bowiem, w odniesieniu do organizacji jako szczególnej formy działań zespołowych, często rodzą chaos potęgowany rozwiązaniami tym bardziej nietrafionymi, im mniej znany jest mechanizm powstawania zakłócających czynników. Doświadczamy wtedy jedynie konsekwencji ich oddziaływania, reagując stosownie do zaistniałych okoliczności. Efektywność systemu przejawia się natomiast możliwością funkcjonowania i korelacji działań w sytuacjach normalnych oraz sytuacjach kryzysowych, przy wykorzystaniu całego potencjału państwa. Sprawność struktur organizacyjnych państwa uzależniona jest natomiast od gotowości do sprostania wyzwaniom i przeciwstawiania się zagrożeniom, co jest determinantem stanu bezpieczeństwa państwa.

Literature / Literatura

[1] Strategia Bezpieczeństwa Narodowego, Warszawa 2014.
[2] *Nowa Encyklopedia Powszechna PWN*, B. Petrozolin-Skowrońska (red.), Wydawnictwo Naukowe PWN, Warszawa 1995.
[3] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2007 nr 89 poz. 590, ze zmianami).
[4] Trejnis Z., *Infrastruktura krytyczna – koncepcje i zarys*, w: *Ochrona infrastruktury krytycznej*, A. Tyburska (red.), Wyższa Szkoła Policji, Szczytno 2010.
[5] Piwowarczyk A., *Europejska infrastruktura krytyczna*, w: *Ochrona infrastruktury krytycznej*, A. Tyburska (red.), Wyższa Szkoła Policji, Szczytno 2010.
[6] Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz. Urz. UE z dnia 23.12.2008, L345/75).
[7] Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. 1997 nr 114 poz. 740, ze zmianami.).
[8] Rozporządzenie Rady Ministrów z dnia z dnia 24 czerwca 2003r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony (Dz. U. 2003 nr 116 poz. 1090, ze zmianami).
[9] Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2018 poz. 452, ze zmianami).
[10] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz. U. 2010 nr 83 poz. 541).
[11] Narodowy Program Ochrony Infrastruktury Krytycznej – Rządowe Centrum Bezpieczeństwa, Warszawa 2013, aktualizowany w 2015 r.
[12] Kosowski B., *Sprawne i elastyczne zarządzanie w kryzysie*, Difin, Warszawa 2008.

BOGDAN KOSOWSKI, D.SC. ENG. – professor at the Jagiellonian University, fire officer. Graduate of the Cracow University of Technology (Eng.), the Main School of Fire Service (fire officer, since 1996 fire safety expert) and the AGH University of Science and Technology in Kraków, the Faculty of Management and Marketing. (MA, Manager in Mining). From 2005 to 2007 he participated in monthly seminars on the Development of the Theory and Practice of Management Sciences, organised by the "Orgmasz" Institute of Organisation and Management in Industry in Warsaw. He received his DSc degree in 2000, at the Faculty of Mining, AGH University of Science and Technology, in the discipline of mining, speciality: management and marketing. In 2013, he received his post-doctoral degree at the Faculty of National Security of the National Defence University of Warsaw in the discipline of safety science. He was, among others: Deputy Voivodeship Commander of the State Fire Service in Katowice, Director of the Crisis Management Department in the Voivodeship Office in Katowice, and Vice-Chancellor and Deputy Commander at the Main School of Fire Service in Warsaw. Currently he holds the position of Professor at the Jagiellonian University and is employed as a researcher of the Institute of Political Science and International Relations at the Department of National Security. Research interests. He specialises in broadly understood issues of the theories of systems related to the organisation of security management in business entities, institutions and public administration bodies. He confronts practical experience gained in the State Fire Service, government and local government administration, public institutions and business entities with theoretical knowledge. He combines and adapts the theory of organisation and management science with safety science, using a systemic approach based on the analysis of risks associated with the variability of threats.

DR HAB. INŻ. BOGDAN KOSOWSKI – profesor UJ, oficer pożarnictwa. Absolwent Politechniki Krakowskiej (inż.), Szkoły Głównej Służby Pożarniczej (oficer pożarnictwa, od 1996 r. rzeczoznawca ds. zabezpieczeń przeciwpożarowych) oraz Akademii Górniczo-Hutniczej w Krakowie na kierunku Zarządzanie i Marketing (mgr, menedżer w górnictwie). W latach 2005–2007 był uczestnikiem comiesięcznych seminariów w zakresie rozwoju teorii i praktyki nauk o zarządzaniu organizowanych przez Instytut Organizacji i Zarządzania w Przemyśle „Orgmasz" w Warszawie. Stopień doktora nauk technicznych uzyskał w roku 2000, na Wydziale Górniczym AGH, w dyscyplinie: górnictwo, specjalność: zarządzanie i marketing. Stopień doktora habilitowanego uzyskał w roku 2013, na Wydziale Bezpieczeństwa Narodowego AON, w dyscyplinie: nauki o bezpieczeństwie. Był między innymi: z-cą Komendanta Wojewódzkiego PSP w Katowicach, Dyrektorem Wydziału Zarządzania Kryzysowego na UW w Katowicach, Prorektorem i z-cą Komendanta SGSP w Warszawie. Obecnie profesor UJ zatrudniony jako pracownik naukowy INPiSM w Zakładzie Bezpieczeństwa Narodowego. Specjalizuje się w szeroko pojętej problematyce teorii systemów związanych z organizacją zarządzania bezpieczeństwem w podmiotach gospodarczych, w instytucjach oraz organach administracji publicznej. Doświadczenia praktyczne nabyte w Państwowej Straży Pożarnej, administracji rządowej i samorządowej, instytucjach publicznych i podmiotach gospodarczych – konfrontuje z wiedzą teoretyczną. Łączy i adaptuje teorię nauki organizacji i zarządzania z nauką o bezpieczeństwie, przy wykorzystaniu podejścia systemowego opartego na analizie ryzyka związanego ze zmiennością zagrożeń.

Ministerstwo Nauki i Szkolnictwa Wyższego

Stworzenie anglojęzycznych wersji oryginalnych artykułów naukowych wydawanych w kwartalniku „BITP. Bezpieczeństwo i Technika Pożarnicza" – zadanie finansowane w ramach umowy 658/P-DUN/2018 ze środków Ministra Nauki i Szkolnictwa Wyższego przeznaczonych na działalność upowszechniającą naukę.