SECURITY & DEFENCE QUARTERLY
https://securityandefence.pl/

Critical infrastructure in the shaping of National Security

Ewa Żaboklicka

ewa.zaboklicka@wat.edu.pl

https://orcid.org/0000-0002-4711-6567

Faculty of National Security, Logistic and Management

Military University of Technology, Poland

Abstract

Critical infrastructure plays a key role in ensuring the national security of a state, due to important functions thereof in military, economic, and public administration sectors. The destruction, damage, failure or other deprivation of critical infrastructure of its operational capabilities constitutes a direct threat to the structural and personal security of the state. The research methods and techniques implemented in the research process itself primarily hinge on critical analysis of acts of law and organisational and competence-related documents, subject-matter literature, synthesis and inference in order to reach the formulated objectives based on efficiency criteria. The main findings indicate that critical infrastructure is perceived as a set of systems which exerts a substantial impact on the security of the state and, obviously, its inhabitants. The results advocate for a reflection that critical infrastructure embraces a number of facilities which appear to be remarkably diverse. They are buildings, structures, installations, equipment and services which, integrally, form cohesive systems which allow the proper functioning of a given state. It is the state whose role is just to supervise and coordinate, whereas the operators of critical infrastructure are the ones who are to protect it. The overall findings of this paper present the notion that safeguarding critical infrastructure is a task of crucial importance to the national security of a state and, therefore, it would be worth reconsidering the intensification of rules which apply to the infrastructure of national security and its efficient functioning.

Keywords:

European Union, satellite communication, national security

Article info
Received: 17 February 2020
Revised: 19 February 2020
Accepted: 29 February 2020
Available online: 16 March 2020
DOI: http://doi.org/10.35467/sdq/118585

© 2020 E. Żaboklicka published by War Studies University, Poland.
This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License

Introduction

National critical infrastructure systems play a key role in ensuring national security, whether in the structural or personal dimension. Efficient critical infrastructure is essential both to ensure continuity of the state and to meet the basic needs of citizens. On a national scale, each of the eleven critical infrastructure systems falls within the responsibilities of a relevant Minister or Head of a Central Office. Critical infrastructure operators are directly responsible for the preparation and implementation of security plans. Such operators include both state entities and private owners. Related tasks have been outlined in the National Critical Infrastructure Protection Programme (NPOIK, 2015). This document, however, is of declarative nature, being more guideline based than presenting specific instructions for unconditional execution. The analysis of legal acts and organisational and competence-related documents concerning critical infrastructure indicates the need for the adoption of a single law that governs the problems of broadly perceived state security infrastructure.

The subject of the research conducted for this article were the phenomena and processes taking place within the area of critical infrastructure, its resistance to external threats and disturbances that might occur within individual systems comprising this infrastructure. Particular focus was on matters directly and indirectly related to the problem of safeguarding critical infrastructure within the context of the functioning of all components of the state that are responsible for national security in Poland.

The main research problem is contained in the following question: What challenges to critical infrastructure safety result from the need to ensure security for the state and its citizens? This main problem was further broken down into two more specific questions:

1. What is the significance of critical infrastructure to the security of the state and of its citizens?

2. What are the challenges faced by the entities responsible for safeguarding critical infrastructure in Poland?

Based on hitherto know-how and following preliminary studies of subject-matter literature in response to the research problem included above, the following hypothesis was adopted: Critical infrastructure treated as systems that have a key impact on the security of the state and of its citizens includes a number of extremely diverse facilities. These include equipment, buildings and structures, installations and services that are treated as an entirety and, as such, constitute cohesive systems, necessary for the smooth functioning of the state. Safeguarding critical infrastructure is a task vested in the owner or operator thereof, whereas the role of the state is limited to a coordination and supervisory function. The objective of the research was to identify the key problems associated with the functioning of critical infrastructure and to point out the most important elements of the planning process of the protection thereof. In view of the above, a list of factors that have an impact on the matters analysed are included, along with conceptual works performed in terms of improving the critical infrastructure protection systems in Poland. Research methods and techniques applied in the research process are mainly based on critical analysis of subject-matter literature, acts of law and organisational and competence-related documents, as well as synthesis and inference. Of the research methods applied to achieve the assumed objective, system analysis was of particular importance, as it allowed organisational systems and their modus operandi to be identified. It is of interdisciplinary and synthesising nature, allowing the design of future structures based on efficiency criteria.

Significance of critical infrastructure to national security

The key role of critical infrastructure in national security (Li *et al.*, 2012) is mainly associated with the very nature of such infrastructure. Classification of facilities into the critical infrastructure is one of the most important stages in the process of establishing protection. Missing only one of the facilities that comprises part of the infrastructure may, therefore, bear tragic consequences in the form of material losses and human casualties. On the other hand, taking into consideration the arbitrary classification of facilities and the lack of appeal procedures, it may result in the dissatisfaction of its owner and in unnecessary undertakings. It is a matter of not only social understanding, but also of precise indication of critical infrastructure facilities based on classification criteria (Rogers *et al.*, 2004). The rules governing the identification of facilities that account for some of the critical infrastructure take into consideration the infrastructure of a normative/legal, social, information (info-sphere) and technical (techno-sphere) nature (Wiles, 2008). Because of their attractive nature, all facilities that comprise critical infrastructure are exposed to diverse threats (such as terrorist, natural, and technical threats). One must note here that threats (Polinpapilinho *et al.*, 2012) that have a significant influence on the destruction of infrastructure facilities prove very difficult to anticipate. Pursuant to provisions under the National Critical Infrastructure Protection Plan (NPOIK, 2015), the responsibility for individual critical infrastructure systems in Poland is vested in:

- «ministers of: national economy and treasury (each according to his/her prerogatives) for the supply systems of energy, energy sources and fuel;

- the minister of administration and digitisation for the communication system and the data communication system, as well as for systems that ensure the continuity of operations of public administration;

- the minister of finance for the proper functioning of national financial systems;

- the minister of agriculture and rural development for food supply systems;

- the minister of health for the health protection system;

- the minister of transportation, construction and maritime economy for transport systems;

- the minister of home affairs for rescue systems;

- the minister of environment for production, storage, maintenance and handling of chemical and radioactive substances, including pipelines transferring hazardous substances, and (jointly with the minister of administration and digitisation) for water supply systems (NPOIK, 2015).

The Minister of National Defence was not indicated as one of the Ministers responsible for critical infrastructure systems. It must be noted, however, that the Minister referred to above is responsible for facilities of particular importance to the security and defence of the state that comprise the national security infrastructure (Purpura, 2013).

The Government Security Centre (Rządowe Centrum Bezpieczeństwa) developed detailed criteria for the identification of facilities, installations, equipment and services

that are part of critical infrastructure systems. The criteria referred to above, presented in the form of a confidential document, were approved on 18 December 2009 by the Director of the Government Security Centre. The criteria were divided into the following two groups:

- sectoral (systemic) criteria – defining quantitative or substantive (functions) parameters of a facility, item of equipment, installation or service, the fulfilment of which may result in incorporation into critical infrastructure; the aforementioned criteria have been defined for each of the critical infrastructure systems.

- cross-sectional criteria – referring to the consequences of destruction of cessation of operations of a facility, item of equipment, installation or service, identified by virtue of fulfilment of sectoral (systemic) criteria (Pyznar, 2010).

Some scientific opinions stress cross-section parameters refer to the consequences that occur directly following an event that disrupted the continuity of operations of a given critical infrastructure system (breakdown, disaster, sabotage, external attack). They refer to seeking methods that allow rapid reconstruction. The analysis included financial impact, reconstruction time, assessment of casualties, nature of disaster, its unique nature and international effect (Radziejewski, 2014). The identification process of critical infrastructure is divided into three stages:

1. Stage one – for the purpose of pre-selection of facilities, installations, equipment or services potentially eligible for incorporation into critical infrastructure within a given system, systemic criteria shall be applied to the system infrastructure relevant to the given critical infrastructure system.

2. Stage two – for the purpose of testing whether a given facility, item of equipment, installation or service plays a key role in the security of the state and its citizens and whether it is conducive to ensuring the efficient functioning of public administration bodies, as well as of institutions and entrepreneurs, the infrastructure identified in Stage One must be subjected to the definition given in Article 3 Section 2 *of the Law on Crisis Management*;

3. Stage three – for the purpose of assessment of the potential destruction or cessation of operations of potentially critical infrastructure, the infrastructure identified in Stage One and Stage Two must be subjected to cross-section criteria, whereas potentially critical infrastructure must meet at least two cross-section criteria.

The following parameters are taken into consideration in forecasting the consequences of threats to potentially critical infrastructure facilities:

1) the number of casualties, evacuees, wounded, and those deprived of basic services;

2) costs of a given scenario and its impact on the economy;

3) changes in and disturbances to the environment;

4) disturbances in the performance of constitutional obligations of the state.

Multiplicity of acts of law results in the lack of a clear distribution of competence of the bodies vested with responsibility for identifying critical infrastructure facilities (Dessers, 2014).

Within the scope of classifying facilities into the European critical infrastructure, the procedures and criteria are compatible with the solutions adopted for national infrastructure. The Director of the Government Security Centre, acting together with relevant Ministers, continuously upgrades the confidential document containing the specification of critical infrastructure facilities situated within the territory of the Republic of Poland and the specification of European critical infrastructure situated within the territories of EU Member States that might have a significant impact on our country. When classifying a facility into the European critical infrastructure, the Director of the Government Security Centre shall follow the following criteria:

- sectoral, setting forth the parameters and conditions adopted by the European Union;

- componential, taken into consideration when the consequences of damage to a given facility would prove particularly devastating to national security;

- continuity of actions, taken into consideration when the damage may threaten the security of more than one country;

- cross-sectional, including the assessment of casualties and consequences of a social and economic nature.

If the given facility meets all the requirements referred to above, it will qualify to be part of the European critical structure (Fay and Patterson, 2017).

Critical infrastructure plays a significant role in shaping the security of citizens and of order within the country. Whenever referred to, it is easy to see that it is inextricably associated with security. These two terms constitute an entirety, wherein the level of efficient functioning of critical infrastructure elements depends upon its security level. On the other hand, the level of security of the state and its citizens depends on the efficiency of critical infrastructure (Landucci *et al.*, 2020). Both are embodied in the process, expressing the will to provide continuous security and to adjust to the changes as they occur in relation to the constantly changing environment.

Efficient and proper functioning within the scope of critical infrastructure is based on proper functioning of all facilities that pursuant to the nature of their operations are divided into the following four areas: 1) defence, 2) economy, 3) public security, and 4) protection of other important interests of the state. The responsibility for keeping such registers is vested in the Voivodes (Heads of Provinces). The registers are confidential.

The infrastructure of significance to the areas of state operations listed above, and in particular the facilities incorporated therein, are granted mandatory protection status. Presently, approximately 900 facilities have been incorporated into the critical infrastructure. A considerable part thereof has been classified as economic interests of the state, mostly detached from public administration. However, irrespective of classification into groups, they all contribute to the vitality of the state, the stabilisation of which confirms efficient flow of services of significance to national defence.

Despite awareness of the importance of critical infrastructure and of consequences to disturbances in the operations thereof, political decision makers sometimes fail to take financial matters into considerations, which frequently constitute pre-conditions for the use of defence capability (Stanley *et al.*, 2017). Since it is a factor aimed at improving security essential to the reconstruction process, an adequate reserve of assets must be put aside in the national budget, to be used should a crisis occur. The awareness of the secu-

rity of facilities should be vested both in national authorities and directly in the owners who, on their account, would display stronger incentives in protecting the facilities.

Significance of critical infrastructure as a challenge to state and private entities

Ensuring the continuity of operations of critical infrastructure and its capacity for fast replacement is the essence of critical infrastructure protection. Only when these conditions are met can we talk about effective protection of facilities, as not only the effective functioning of such facilities, but also the national defence capabilities depend upon it (Knapp and Langill, 2011).

Tasks falling within the scope of critical infrastructure are implemented in the following areas: 1) collection of information; 2) analysis of information; 3) development of procedures to counteract the threat to critical infrastructure; 4) reconstruction of critical infrastructure; and 5) public-private cooperation.

Speaking about safeguarding critical infrastructure, one may not be certain of similarities to the notion of national security. Both embody the process aimed at continuously ensuring structural and personal security adjustment to the phenomena as they occur in relation to the constantly changing environment. It is caused by continuous expansion of the notion of protection of critical infrastructure. The number of facilities subject to such protection is also growing (Li *et al.*, 2012).

Critical infrastructure is exposed to threats of any kind, hence the protection system must be well thought-out and prepared for any contingency in order to promptly and effectively restore the functioning of individual facilities. In the era of information society, we may have to deal with ever increasing functioning of people in virtual reality. Under such circumstances, an example of a threat might be "constant cutting-off from IT services offered by the communication technologies of the future" (Szczurek, 2019, p. 90). Such a situation is of particular importance to personal security. The main objectives of protection of critical infrastructure are the actions that will eliminate the impact of any threats, or at least minimise the consequences of their occurrence.

In keeping with the *Law on Crisis Management* and the *Law on Protection of People and Property*, the Government Centre of Security was vested with tasks aimed at ensuring security in the following categories:

- physical, i.e. any actions aimed at reducing the risk of disturbances in the functioning of the state caused by third party actions;

- technical, aimed at reducing risks caused by failures, while meeting the legal regulations and instructions valid for a given critical infrastructure facility;

- personal, aimed at minimising the risk of disturbances in the functioning of critical infrastructure, through actions of persons granted authorised access thereto;

- telecommunications and IT technologies, minimising the risks that might occuras a consequence of an unidentified action against control systems and IT networks;

- legal, reducing risks caused by actions referring to external entities, within the scope of ensuring legal security with the use of any legal measures.

Entities responsible for the security of critical infrastructure develop plans for ensuring continuity of actions and replacement - as nothing other than an attempt to maintain, and then restore, the functions implemented by critical infrastructure. The documentation in this area includes:

- a crisis management plan;

- contingency plans/procedures;

- plans/procedures for reconstruction of lost resources (Pesch-Cronin and Marion, 2016).

The basic tool for the preparation of future protective actions on the part of an entity is the programme for preventing serious industrial failures, presenting a security system that guarantees the protection of people and of the environment. The programme should include:

- determination of the probability of threat with such industrial failure;

- rules for preventing and counteracting the consequences of industrial failure that are expected to be introduced;

- identification of methods for reducing the consequences of industrial failure in relation to people and to the environment should such failure occur;

- identification of frequency of analyses of the failure prevention programme, guaranteeing the upgrades and effectiveness thereof. Following the preparation of actions to be undertaken directly upon the occurrence of such failure, internal and external operational and rescue plans are developed.

Specific protection of facilities is prepared by the bodies, institutions, formations of entrepreneurs or organisational units responsible for such facilities, and is provided by militarised facility protection units, especially established for such purpose based on separate regulations. The following entities participate in the process of the preparation of protection and defence of critical infrastructure facilities:

- the Minister responsible for internal affairs and the Minister of National Defence;

- bodies responsible for special protection of facilities: Head of the Office of the Chairman of the Council of Ministers, Ministers supervising individual critical infrastructure systems, President of the National Bank of Poland, President of the Management Board of Bank Gospodarstwa Krajowego, Voivodes;

- managers of facilities subject to special protection: head of the organisational unit responsible for direct management of such areas, facilities subject to special protection, person or body of an entrepreneur or another organisational unit vested with the authority to manage such unit, liquidator or receiver.

Classification of a facility as an element of critical infrastructure is unanimous with the need to develop a protection concept that must encompass, including but not limited to, formulated goals and guidelines concerning the given facility. The concept must also include the rules governing security management, specification of resources subject to protection, organisational structure, specification of means of protection (organisational and technical), rules of implementation and of controlling the principles adopted, devel-

opment of contingency plans, verification of effectiveness of the solutions adopted and change management. The Ministers responsible for Government administration sectors, Heads of central bodies and the Voivodes should submit the specification to the Director of the Government Security Centre which may be included in the specification of facilities incorporated into the critical infrastructure, and develop crisis management plans, analyse threats and directly implement tasks. The Government Security Centre should develop and update the appendix to the National Crisis Management Plan and cooperate with EU and NATO bodies and their respective Member States. Furthermore, the Director of the Government Security Centre should prepare the specification of facilities incorporated into the critical infrastructure inclusive of breakdown into systems, extracts from the specification of facilities situated within the boundaries of Voivodeships and deliver such specifications to relevant Voivodes. The Director should also notify the owners of the incorporation of their facilities into the critical infrastructure. The responsibility for direct implementation of protection-related tasks is vested in the owners (autonomous or dependent holders) of critical infrastructure facilities, installations or equipment. "Hence, safeguarding critical infrastructure must be the role of its owner or operator, whereas the role of the state is limited to coordination and supervisory function. Intervention is allowed exclusively when a given element of critical infrastructure is devoid of sufficient protection or when the elimination of consequences of a crisis situation (Domalewska, 2019) extends beyond the capabilities of a given owner or operator".

Systems comprising critical infrastructure have common features and require special protection, as they must be prepared rather for the restoration of infrastructure than to fend off attacks. Legal acts governing the matters associated with critical infrastructure mention the protection thereof. However, there are only a few references to the matters associated with the security of critical infrastructure. In accordance with the *Law on Protection of Population and of Property*: "Areas, facilities and equipment of significance to national defence, economic interests of the state, public security and other important interests of the state are subject to mandatory protection by specialist armed security formations or appropriate technical protections (Bielawski *et al.*, 2018), the so-called SUFO – internal security services and the entrepreneurs licensed to run business operations within the scope of protecting people and property" (The law of 22 August 1997 *on the protection of people and of property*).

National Critical Infrastructure Protection Programme

For the purpose of establishing conditions conducive to improvement of critical infrastructure security, the Council of Ministers adopted the National Critical Infrastructure Protection Programme. The Programme includes all four phases of crisis management:

- preventing disturbances in critical infrastructure,

- preparing to handle crisis situations within the area of such infrastructure,
responding to the destruction of or disturbances in the functioning of critical infrastructure, and
- reconstruction of critical infrastructure.

The entity vested by the legislator with the responsibility for the implementation of the National Critical Infrastructure Protection Programme is the Director of the Government Security Centre, and the entities cooperating in the development of that document are the Ministers and Heads of central bodies responsible for the systems comprising

the critical infrastructure and vested with responsibilities in national security matters. The law delegated the task to the Council of Ministers in the form of a Regulation – the implementation method of responsibilities set forth in the law and cooperation within the scope of the National Critical Infrastructure Protection Programme by the public administration and services responsible for national security, jointly with the owners and holders of critical infrastructure facilities, installations, equipment and services. This task was materialised by the issue or Regulation of the Council of Ministers of 30 April 2010 *on the National Critical Infrastructure Protection Programme*.

The Regulation stipulated in detail how public administration bodies are to implement their responsibilities that fall within the scope of protection of critical infrastructure and how they should cooperate in this area with the operators of said infrastructure. The Regulation obligates the Director of the Government Security Centre to develop the criteria for the identification of critical infrastructure and to consult these criteria with the Ministers and Heads of central bodies responsible for such systems. Following consultations, the criteria will provide the grounds for the preparation of draft specification of critical infrastructure. Relevant proposals should be submitted by the Ministers and Heads of central bodies referred to above, responsible for critical infrastructure systems, to be verified by the Director of the Government Security Centre.

The Regulation indicated the important role of Ministers and Heads of central bodies in the process of programme preparation. They are the main coordinators within the scope of creating conditions conducive to improving the security of critical infrastructure within the given system. They should also coordinate cooperation between the operators of critical infrastructure and ensure exchange of information between public administration and such operators (NPOIK, 2015). The Ministers and Heads of central bodies should submit the information concerning the characteristics of the task area that falls within their respective scope of competence to the Director of the Government Security Centre, including the identification of resources of such areas in terms of the need for protection of critical infrastructure. They should also submit proposals concerning the requirements and standards necessary to ensure the continuity of functioning of critical infrastructure. Their responsibilities should also include the presentation of an overall risk assessment in relation to the functioning of a given task area, taking into consideration the susceptibility to threats and possible consequences of disturbances in the functioning of critical infrastructure in such area. Furthermore, they should present the possible methods for preventing disturbances in the functioning of task areas caused by damage to critical infrastructure, and propose the adoption of relevant priorities within the scope of reconstruction thereof. The information and proposals submitted by the Ministers and Heads of central bodies provide the grounds for the development of the National Critical Infrastructure Protection Programme (NPOIK, 2015) to be submitted to the Council of Ministers for approval.

Pursuant to the Law *on crisis management and provisions under the Regulation on the National Critical Infrastructure Protection Programme*, the Director of the Government Security Centre should develop a consolidated specification of facilities, installations, equipment and services comprising critical infrastructure, broken down into systems. Extracts from such specification should be relayed to relevant Ministers and Heads of central bodies, in keeping with their area of authority. Voivodes should receive extracts featuring the facilities, installations, equipment and services comprising critical infrastructure situated within the boundaries of individual Voivodeships. The specification of critical infrastructure and the entire National Critical Infrastructure Protection Programme (NPOIK, 2015) should be upgraded at least bi-annually. It must be noted here that the document produced by the Government Security Centre does not contain accurate wording.

It features no sanctioned orders. The document only contains recommendations addressed to individual entities responsible for critical infrastructure. The Authors of the National Critical Infrastructure Protection Programme (NPOIK, 2015) count on the understanding and good cooperation between public administration and the operators (users) of critical infrastructure.

Conclusions

The basic responsibility of the state before its citizens is to ensure their safe existence and development. The implementation of these tasks depends mostly upon effective functioning of critical infrastructure systems. In the Law *on Crisis Management,* the legislator pointed out eleven critical infrastructure systems, the effective operation of which are of crucial importance to national security. The tasks falling within the scope of protection of such infrastructure are listed in the National Critical Infrastructure Protection Programme (NPOIK, 2015) developed by the Director of the Government Security Centre in cooperation with all interested parties. From the level of Government administration, individual systems are supervised by relevant Ministers or Heads of central bodies. Nevertheless, the main responsibility for efforts within the scope of maintaining and ensuring security are vested in the owners (users) of critical infrastructure. Many such owners and users are private entities, prepared to various degrees to incur high costs of providing security to the critical infrastructure bodies against diverse threats. The National Critical Infrastructure Protection Programme (NPOIK, 2015) document precisely indicates the entities responsible for the implementation of tasks associated with the protection of critical infrastructure, although the tasks indicated therein are not associated with any sanctions for non-compliance.

The analysis of acts of law and organisational and competence-related documents indicated that the problems of critical infrastructure protection are highly dispersed. Classification of facilities into critical infrastructure groups is conducted based on vague criteria, while the legislator developed specific acts of law concerning facilities of importance to national security and facilities subject to special protection as if forgetting that such groups of facilities are strongly equated with critical infrastructure. For this reason, it would be advisable to reconsider the consolidation of regulations broadly governing perceived "national security infrastructure". A single law governing such problems should dissipate any doubts of an interpretative nature, determine the scope of competence of individual entities responsible for efficient functioning of such infrastructure, inclusive of responsibilities, and sanctions for non-compliance.

References

Bielawski, R., Rządkowski, R. and Perz, R. (2018) 'Unmanned Aerial Vehicles in the protection of the elements of a country's critical infrastructure – selected directions of development', *Security and Defence Quarterly*, 22(5), pp. 3–19. doi: 10.5604/01.3001.0012.6422.

Dessers, E. (2014) *Spatial Data Infrastructures at Work: Analysing the Spatial Enablement of Public Sector Processes*. Leuven: Leuven University Press. doi: 10.2307/j.ctt9qf068.

Domalewska, D. (2019) 'The role of social media in emergency management during the 2019 flood in Poland', *Security and Defence Quarterly*, 27(5), pp. 32-43. doi: 10.35467/sdq/110722.

Fay, J. and Patterson, D. (2017) *Contemporary Security Management*. Oxford: Butterworth-Heinemann. doi: 10.1016/C2015-0-04732-3.

Knapp, E. and Langill, J.T. (2011) *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Rockland: Syngress. doi: 10.1016/C2010-0-66555-2.

Landucci, G., Khakzad, N., and Reniers, G. (2020) *Physical Security in the Process Industry: Theory with Applications*. Burlington: Elsevier. doi: 10.1016/C2017-0-00539-6.

Li, W., Kodeswaran P., Jagtap, P., Joshi, A. and Finin, T. (2012) 'Managing and Securing Critical Infrastructure – A Semantic Policy- and Trust-Driven Approach', in Das, S.K., Kant, K. and Zhang, N. (eds.) *Handbook on Securing Cyber-Physical Critical Infrastructure: Foundations and Challenges*. San Francisco: Morgan Kaufmann, pp. 551-573. doi: 10.1016/C2011-0-04434-4.

Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) (2015) Warsaw: Rządowe Centrum Bezpieczeństwa.

Pesch-Cronin, K.A. and Marion, N.E. (2016) *Critical Infrastructure Protection, Risk Management, and Resilience: A Policy Perspective*. Boca Raton: CRC Press. doi: 10.1201/9781315310657.

Polinpapilinho, F.K. and Hester, P.T. (2012) 'Systemic determination of infrastructure criticality', in Thissen, W.A.H., and Herder, P.M. (eds.) *Critical Infrastructures State of the Art in Research and Application (International Series in Operations Research & Management Science Book 65*). Dordrecht: Springer. doi: 10.1007/978-1-4615-0495-5.

Purpura, P. (2013) *Security and Loss Prevention*. Burlington: Butterworth-Heinemann. doi: 10.1016/C2010-0-69612-X.

Pyznar, M. (2010) 'Narodowy Program Ochrony Infrastruktury Krytycznej w systemie ochrony tej infrastruktury – wizja Rządowego Centrum Bezpieczeństwa', in Tyburska, A. (ed.) *Ochrona infrastruktury krytycznej*. Szczytno: Wydawnictwo Wyższej Szkoły Policji.

Rogers, R., Miles, G., Fuller, E. and Dykstra, T. (2004) *Security Assessment: Case Studies for Implementing the NSA IAM*. Rockland: Syngress Publishing.

Radziejewski, R. (2014) *Ochrona Infrastruktury Krytycznej. Teoria a praktyka*. Warsaw: Wydawnictwo Naukowe PWN.

Stanley, J.R., Stanley, J.K. and Hansen, R. (2017) *How Great Cities Happen: Integrating People, Land Use and Transport*. Cheltenham UK & Northampton USA: Edward Elgar Pub. doi: 10.4337/9781784718398.

Szczurek, T. (2019) *Wyzwania dla bezpieczeństwa – niepewna przyszłość – między zagrożeniami a szansami*. Warsaw: Military University of Technology.

The law of 22 August 1997 on the protection of people and of property (Journal of Laws of the Republic of Poland Dz.U. 2016 Item 1432, as amended).

Wiles, J. (2008) *Techno Security's Guide to Securing SCADA: A Comprehensive Handbook On Protecting The Critical Infrastructure*. Rockland: Syngress. doi: 10.1016/B978-1-59749-282-9.X0001-2.