European Research Studies Journal
Volume XXVI, Issue 3, 2023

pp. 325-332

Spatial Critical Infrastructure and the Role of the National Postal Operator in Improving the Flow of Information

Submitted 15/07/23, 1st revision 10/08/23, 2nd revision 01/09/23, accepted 10/09/23

Anna Drab-Kurowska[1]

Abstract:

Purpose: *The aim of the article is to indicate how national postal operators can secure the flow of information within the critical infrastructure of the state. The article poses the following research hypothesis - the activity of national postal operators will allow securing the flow of information within the critical infrastructure of the state.*
With reference to the stated objective and the adopted hypothesis, the article poses the following research question - what specific actions should be taken by postal operators to ensure the efficient flow of information within the critical infrastructure? In an attempt to answer the question, the article first addresses the essence of critical infrastructure, then focuses on presenting the threats that arise within critical infrastructure. A key element of the article is the presentation of proposals for measures aimed at the efficient flow of information within critical infrastructures using the potential of the national postal operator.
Design/Methodology/Approach: *A critical analysis of the literature and an observational method using argumentation to support generalised theses were used to achieve the aim. In addition, the induction and deduction method, the comparison and generalisation method and the synthesis method were used.*
Findings: *The analysis carried out allowed the identification of key actions to secure the flow of information within the state's critical infrastructure. The analysis has shown that national postal operators have both the experience and the potential to efficiently secure the flow of information within the state's critical infrastructure.*
Practical Implications: *The problems of securing an efficient flow of information within the critical infrastructure presented in the article demonstrate the necessity to develop security solutions. It is important to prepare such protection solutions, which would not allow the destruction of elements forming the state infrastructure. In addition, it is important to provide solutions which, in the event of a disruption in their functioning, organise substitute functions by another link in order to reduce the losses resulting from an incident.*
Originality/Value: *The article presents the results of own desk research. The issue presented has not previously been addressed in discussions published internationally.*

Keywords: *Critical infrastructure, information system, postal operators, state policy.*

JEL codes:*. L87, R28, H12, H41, L97.*
Paper type: *Research article.*

[1]*Assoc. Prof., Institute of Spatial Management and Socio-Economic Geography, University of Szczecin, Poland, ORCID 0000-0003-1396-9390, e-mail: anna.drab-kurowska@usz.edu.pl;*

Research funding: *The project is financed within the framework of the program of the Minister of Science and Higher Education under the name "Regional Excellence Initiative" in the years 2019 – 2022; project number 001/RID/2018/19; the amount of financing PLN 10,684,000.00*

1. Introduction

The continuous development of civilisation leads to society becoming dependent on infrastructure in the broadest sense. This makes citizens no longer self-sufficient in many areas of everyday life. Part of this infrastructure is so-called critical infrastructure.

Critical infrastructure plays a key role in the functioning of the state and the lives of its citizens. As a result of events caused by natural forces or as a consequence of human actions, critical infrastructure may be destroyed, damaged and its operation may be disrupted, so that the lives and property of citizens may be endangered (Journal of Laws 2017, item 1090, item 42 and 2019, item 250).

At the same time, such events negatively affect the economic development of the state. Hence, the protection of critical infrastructure is one of the priorities facing every state. The essence of the tasks related to critical infrastructure boils down not only to ensuring its protection from threats, but also to ensuring that any damage and disruptions to its functioning are as short-lived as possible, easy to remove and do not cause additional losses to citizens and the economy (Szewczyk and Pyznar, 2010)

Detailed obligations in this respect are contained, inter alia, in the Regulation of the Council of Ministers of 24.06.2003 on facilities of particular importance for the security and defence of the state and their special protection.

Critical infrastructure is defined as systems and their functionally related objects, including buildings, equipment, installations, services that are key to the security of the state and its citizens and that serve to ensure the functioning of public administration bodies, as well as institutions and entrepreneurs. However, it should be noted that the term 'critical infrastructure' in Polish legal acts started to function only since 2007, with the entry into force of the Crisis Management Act.

2. Literature Review

Critical infrastructure and its protection are concepts that only emerged worldwide in the last decade of the 20th century. The term 'critical infrastructure' was first used in the early 1990s and was associated with major power grid failures in the United States, which resulted in severe disruption to many

millions of citizens (Gritzalis, Theocharidou, and Stergiopoulos, 2019).

It is important to point out that power grid failures have had a negative impact on other systems and installations that, thanks to the intensive development of civilisation, make life easier and provide a sense of security, however, when their proper functioning is disrupted, it can be observed how dependent society is on them (Wang, Yang, Hu, Stanley, He, and Shi, 2018).

The concept of critical infrastructure was first used in official government documents in the US with then President Bill Clinton's 22 May 1998 directive on critical infrastructure protection. This directive referred to the need for the United States to increase its vulnerability to potential terrorist attacks, especially in the area of securing critical infrastructure (Mao and Li, 2018).

The directive defined infrastructure as real and cyber systems that are necessary for the economy and the state to function at a minimum. These systems are classified as telecommunications, energy, transport, banking and financial systems, among others. It was pointed out that, in order to effectively protect critical infrastructure, there is a need for close cooperation with the private sector (according to the US Department of Homeland Security, about 85% of critical infrastructure is operated or owned by private entities) within the framework of public-private partnerships (Szewczyk and Pyznar, 2010).

It should be noted that since then, critical infrastructure protection issues have been systematically developed and the Americans have become world leaders in this field.

In analysing the term 'infrastructure', the importance of its security should be emphasised. Security should be seen both as a state and as a process in which the state of security and its organisation are subject to dynamic change, which necessitates the continuous activity of individuals, local communities, states and international organisations in creating the desired state of security. The changing nature of threats necessitates the successive expansion of the resources that make up critical infrastructure.

Building the appropriate conditions for improving the security of critical infrastructure is achieved primarily by:

- preventing disruptions to the functioning of critical infrastructure,
- preparing for crisis situations that may adversely affect critical infrastructure,
- responding to situations of destruction or disruption of critical infrastructure,
- restoring critical infrastructure.

The main threats to critical infrastructure can occur through an act of terrorism, sabotage or natural disasters. Through an act of terrorism or sabotage, even a

weaker adversary can launch a strike that significantly disrupts the functioning of selected state structures.

Against natural disasters, critical infrastructure can be protected to a certain extent depending on the type and strength of the elemental impact. Existing and potential threats to critical infrastructure must not restrict the development of the economy and disrupt the functioning of society. The systematic reduction of the threat level and the improvement of the state security system should be a permanent and primary policy objective.

It should be emphasised that critical infrastructure plays a special role in ensuring the continuity of the functioning of the state, its bodies, institutions, services and the exchange of information between them (Rosa, 2022).

The efficiency of critical infrastructure ensures a certain level and continuity of distribution of those services for which the state is responsible. Its proper functioning also allows for the effective use of the possessed resources in the event of extraordinary events, disrupting the normal functioning of the state and its economy (Drab-Kurowska, 2013).

It should be pointed out that technological progress and economic development are responsible for the readiness of a large part of the components of critical infrastructure. An example of this is the system for the supply of liquid fuels to the transport sector and electricity to manufacturing plants.

Long-lasting impediments in this area can have serious economic consequences, with implications for the capacity of the state and society. This may be manifested in a reduction of the defence potential, obstacles to the implementation of socially crucial tasks by the state (e.g. health care), or limited revenues to the state budget. Consequently, this situation will affect the quality of life.

Prolongation of such situations could lead to social unrest, which is why in such situations a rapid response is necessary to restore the functioning of damaged systems.

There is no doubt that critical infrastructure is vital to the existence of the state and, within it, of organised society. In the event of a disruption, the state and its institutions may lose all or part of their ability to perform their basic administrative and service functions, as well as their ability to exercise effective control over their entire territory.

Failure of critical infrastructure impedes economic and social development and, in certain situations, can result in serious social problems. Although an extreme vision, such a situation is one of the main reasons for the emergence of entities

described as 'states in decay' or areas beyond any control of state authorities.

3. Results - Place of the Designated Postal Operator in the Network System of the Critical Infrastructure of the State

An analysis of the possibilities to support entities securing critical infrastructure shows that the role of the national postal operator could undergo a major change. Considering securing the flow of information, the postal operator could realise its competences in the situation of a digital information flow problem.

Its tasks would include:

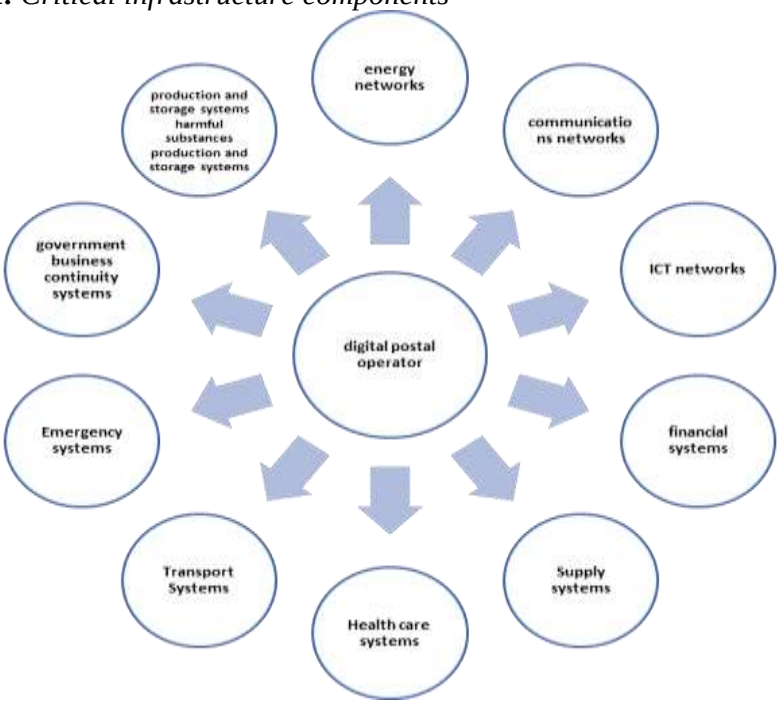
- to provide risk management measures in the space. These would be based on technical and organisational measures to manage the risks to network security for the provision of services;
- analysing the risks and security policies of information flow systems within the components of the state's critical infrastructure;
- the development of procedures, dedicated to critical infrastructure entities in the event of an incident;
- preventing, detecting and responding to incidents;
- ensuring business continuity and crisis management, taking into account the vulnerabilities specific to each critical infrastructure entity;
- applying a specific methodology or certification scheme when implementing the required technical and organisational measures, taking into account the state of the art;
- reporting to the competent authorities or response teams any incident with a significant impact on the provision of services based on critical infrastructure.

The designated postal operator would be one of the institutions coordinating the course of action and the flow of information between the identified critical infrastructure components, as shown in Figure 1. The designated postal operator would be one of the institutions coordinating the course of action and the flow of information between the identified critical infrastructure components.

Moreover, one of the elements of crisis management related to critical infrastructure protection is the cooperation of public administration. This is to consist of joint activities aimed at improving security conditions. Cooperation with business is also an important element in ensuring security (Wolbers, Boersma, and Groenewegen, 2018; Ansell and Boin, 2019; Bundy, Pfarrer, Short, and Coombs, 2019).

Its aim is to develop transparent rules and procedures between the administration and the owners of intrinsic and dependent critical infrastructure facilities, installations or equipment.

Figure 1. *Critical infrastructure components*



Source: *Own study.*

This is due to the fact that much of the infrastructure that is critical to state security is currently in private hands, which may nevertheless pose some risks. Therefore, it seems reasonable to use the potential of the national postal operator, which, on the one hand, is a key element of the communications sector and, on the other hand, is a public trust institution with powerful infrastructural, organisational and social potential (Budziewicz-Guźlecka, Drab-Kurowska, 2020).

4. Discussion

Undoubtedly, critical infrastructure is vital to the existence of the state and, within it, of organised society. When disruptions occur, the state and its institutions may lose all or part of their ability to perform their basic administrative and service functions, as well as their ability to exercise effective control over their entire territory.

Failure of critical infrastructure impedes economic and social development and, in certain situations, can result in serious social problems. Although an extreme vision, such a situation is one of the main reasons for the emergence of entities described as 'states in decay' or areas beyond any control of state bodies.

Currently, it is indicated that a large dynamic of change in the contemporary global security environment is directed towards seeing the main threats in terrorism, the use of weapons of mass destruction, transnational organised crime or threats in cyberspace.

It should be pointed out that probable potential threats may also include such phenomena as the destabilisation of the political system, massive human rights violations, malfunctioning economic and social mechanisms, reduced quality of life for society, reduced water resources, environmental degradation, natural disasters, increasing demand for energy coupled with difficult access to energy resources, or depleting rare metal resources and demographic problems.

Many of these threats can be translated directly into threats to critical infrastructure. It is therefore necessary to develop resilience to national security threats by strengthening critical infrastructure protection and creating a support system. This will allow for a more efficient cooperation and information flow between critical infrastructure actors and public administrations and increase the effectiveness, adequacy and coherence of the strategic reserve system.

A possible solution is the involvement in this activity of the designated postal operator, which currently maintains postal outposts defined by law (their number and distribution is important), creating a network of connections between them. This network, in the event of a threat or destruction of key critical infrastructure, can ensure the functioning of the most important institutions of the state in an emergency (Buko, 2009, Drab-Kurowska, 2019).

5. Conclusions

The specific nature of today's critical infrastructures, their high level of complexity, interconnectedness, as well as reliance on solutions using new technologies, generates massive costs when they need to be rapidly restored (Drab-Kurowska and Drożdż, 2021).

The process of reconstructing a destroyed or severely damaged critical infrastructure component is also extremely difficult and time-consuming. The process of reconstructing a component - which is a key link in the critical infrastructure system - can be further complicated by the occurrence of another crisis situation or military conflict at the same time.

Therefore, it is a very difficult task, for the owners and managers of critical infrastructure and public administration, to prepare such protection solutions, which would not allow the destruction of elements making up the state infrastructure. In addition, it is important to provide solutions that, in a situation of disruption to their functioning, by organising substitute functions by another link, in order to reduce the losses resulting from an incident.

References:

Ansell, C., Boin, A. 2019. Taming deep uncertainty: The potential of pragmatist principles for understanding and improving strategic crisis management. Administration & Society, 51(7), 1079-1112.

Boryczko, K., Rak, J. 2017. Bezpieczeństwo systemów wodociągowych. Dywersyfikacja zasobów wody. Oficyna Wydawnicza Politechniki Rzeszowskiej. Rzeszów: Politechnika Rzeszowska.

Budziewicz-Guźlecka, A. 2019. Oddziaływanie polityki społeczno-gospodarczej na zmiany polskiego rynku usług telekomunikacyjnych. Szczecin: Wydawnictwo Naukowe Uniwersytetu Szczecińskiego.

Budziewicz-Guźlecka, A., Drab-Kurowska, A. 2020. Problems of infrastructure markets with particular emphasis on the postal market in the context of digital exclusion. Sustainability, 12(11), 4719-4737.

Buko, J. 2009. Powszechne usługi pocztowe w Polsce - stan obecny i koncepcja zmian. Szczecin: Wydawnictwo Naukowe Uniwersytetu Szczecińskiego.

Bundy, J., Pfarrer, M.D., Short, C.E., Coombs, W.T. 2017. Crises and crisis management: Integration, interpretation, and research development. Journal of Management, 43(6), 1661-1692.

Drab-Kurowska, A. 2013. The role of social media in economy, w: Europejska przestrzeń komunikacji elektronicznej, t. 2. Zeszyty Naukowe Uniwersytetu Szczecińskiego, (763).

Drab-Kurowska, A. 2019. Polityka konkurencji w obszarze rynku pocztowego Unii Europejskiej. Szczecin: Wydawnictwo Naukowe Uniwersytetu Szczecińskiego.

Drab-Kurowska, A., Drożdż, W. 2021. Digital Postal Operator as an Important Element of the National Energy Security System. Energies, 15(1), 231.

Dz.U. poz. 1090 z 2017 r. poz. 42 oraz z 2019 r. poz. 250.

Gritzalis, D., Theocharidou, M., Stergiopoulos, G. 2019. Critical infrastructure security and resilience. Advanced Sciences and Technologies for Security Applications. Management: Integration, interpretation, and research evelopment. Journal of management, 43(6), 1661-1692.

Mao, Q., Li, N. 2018. Assessment of the impact of interdependencies on the resilience of networked critical infrastructure systems. Natural hazards, 93, 315-337.

Ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U z 2020 r., poz.1856, z 2021r. poz. 159); dalej jako ustawa o zarządzaniu kryzysowym.

Milewski, J. 2016. Identyfikacja infrastruktury krytycznej i jej zagrożeń. Zeszyty Naukowe AON, (4 (105), 99-115.

Mroczko, F. 2014. Infrastruktura krytyczna i jej ochrona. Wydawnictwo Wałbrzyskiej Wyższej Szkoły Zarządzania i Przedsiębiorczości w Wałbrzychu, 13.

Rosa, G. 2022. Use of modern technologies by public transport passengers during the COVID-19 pandemic. Procedia computer science, 207, 3590-3599.

Szewczyk, T., Pyznar, M. 2010. Ochrona infrastruktury krytycznej a zagrożenia asymetryczne. Przegląd Bezpieczeństwa Wewnętrznego, 2(10).

Wang, W., Yang, S., Hu, F., Stanley, H.E., He, S., Shi, M. 2018. An approach for cascading effects within critical infrastructure systems. Physica A: Statistical Mechanics and its Applications, 510, 164-177.

Wolbers, J., Boersma, K., Groenewegen, P. 2018. Introducing a fragmentation perspective on coordination in crisis management. Organization Studies, 39(11), 1521-1546.