Article

Digital Postal Operator as an Important Element of the National Energy Security System

Anna Drab-Kurowska ^{1,*} and Wojciech Drożdż ²

¹ Institute of Spatial Management and Socio-Economic Geography, University of Szczecin, Mickiewicza 64, 71-101 Szczecin, Poland

² Institute of Management, University of Szczecin, Cukrowa 8, 71-004 Szczecin, Poland; wojciech.drozd@usz.edu.pl

* Correspondence: anna.drab-kurowska@usz.edu.pl

Abstract: This article presents a solution that strengthens information security in critical infrastructure entities. Critical infrastructure plays a key role in the functioning of the state and the life of its citizens. Therefore, the protection of critical infrastructure is one of priorities in Poland. The aim of this article is to show that designated postal operators may become an important link in the process of information flow and cybersecurity. Based on their multiple-year experience and expended competences, the operators may provide digital services for entities responsible for the energy security infrastructure. Verification of this goal is necessary, since critical infrastructure is exposed to growing threats, both in the area of energy and other sensitive sectors of the economy. Research results presented in the article were obtained by conducting a CATI survey. The study used the purposeful selection method, which allows to influence the structure of a sample in the context of goals set by the authors. The method solicited key information from experts on postal and energy markets. The results constitute a new approach to the role of the designated postal operator. The authors analysed possibilities to support entities that secure critical infrastructure, including those from the energy sector. It shows that the role of the designated postal operator may significantly change. Taking into account the security of information and cybersecurity, the postal operator could expand its competences, secure infrastructure-related information flow, and thus become a key pillar of the state.

Keywords: energy security system; digital ecosystem; postal operator

Citation: Drab-Kurowska, A.; Drożdż, W. Digital Postal Operator as an Important Element of the National Energy Security System. *Energies* **2022**, *15*, 231. <https://doi.org/10.3390/en15010231>

Academic Editor: Ravinesh C. Deo

Received: 14 December 2021

Accepted: 28 December 2021

Published: 30 December 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The continuous development of civilisation leads to growing dependence of society on the widely understood infrastructure. This makes citizens no longer self-sufficient in many areas of their everyday lives. A part of this infrastructure is known as critical infrastructure [1–3]. It is defined as systems and their constituent functional objects, including buildings, equipment, installations, and services that are crucial for the security of the state and its citizens. Moreover, it ensures the functioning of public administration bodies, as well as institutions and entrepreneurs [4]. Critical infrastructure plays a key role in the functioning of the state and lives of its citizens. As a result of events caused by natural or man-made forces, critical infrastructure may be destroyed, damaged or disrupted, putting the lives and property of citizens at risk. At the same time, such events have a negative impact on the country's economic development. Hence, protecting critical infrastructure is one of the priorities facing the state, including Poland. The essence of tasks related to critical infrastructure lies not only in ensuring its protection against threats, but also in ensuring that any damage or disruption to its functioning is as short-lived as possible, easily remedied, and does not cause additional losses to citizens and the economy.

The article refers to critical infrastructure that includes inter alia, energy supply systems, energy resources and fuels, and the communications sector.

One of the elements of crisis management [5,6] related to the protection of critical infrastructure [7–9] is the cooperation between public administration and businesses. Its purpose is to work together to improve safety and ensure security.

The cooperation aims to develop transparent rules and procedures between the administration [10] and the owners of vested and dependent critical infrastructure facilities, installations or equipment [11–15]. This is due to the fact that much of the infrastructure, which is crucial to the security of the state, is currently in private hands, which may, however, pose some risks. Therefore, it seems justified to use the capacity of a designated (The designated operator is a solution introduced by the postal directives of the European Parliament and the Council in order for the state to fulfil its obligation towards citizens regarding the availability of universal postal services. This solution is supposed to reconcile the liberalisation of the postal market with the availability to citizens of basic services of a good standard, provided at an affordable price throughout the country and abroad.) postal operator, which, on the one hand, is a key element of the communications sector and, on the other, is an institution of public trust with powerful infrastructural, organisational, and social potential.

The aim of the article is to demonstrate that designated postal operators may become an important link in the process flow of information and cybersecurity. Based on their multiple-year experience and expanded competences, the operators may provide digital services to entities responsible for energy security of critical infrastructure.

The structure of the article allows for the verification of its purpose. The first part of the article defines key areas of critical infrastructure in relation to the energy sector. This part is a starting point to identify threats in the context of cybersecurity of critical infrastructure. The possibilities of engaging the designated postal operator are then indicated, as confirmed by research. The results of the research presented in the article allow for a discussion, including recommendations for both critical infrastructure operators and the government.

The aim of the article was verified on the basis of a CATI survey conducted among postal market and energy sector experts.

The individual indications obtained made it possible to identify premises demonstrating the involvement of the digital postal operator to ensure the security of energy critical infrastructure. Due to the nature and limited volume of the article, its further part discusses only selected results of the study.

The study aimed at demonstrating the potential of the designated postal operator, which ensures the appropriate level of energy security.

2. Critical Infrastructures and the Energy Sector

It is important to stress that critical infrastructure provides security [16–19] in peacetime, but its reliability is essential in crisis conditions. Therefore, it is worth investing in its stability and ensuring its smooth functioning. Energy generation and distribution [20–22] is a strategic issue for the security of the state. At the same time, geopolitical, environmental, and technological changes [23] have made it necessary to transform existing operating models [24–26] of the energy sector. Figure 1 shows the impact of certain factors on the energy security model.

It is therefore crucial to secure the transmission of information between these factors. Furthermore, while elaborating on energy security, the literature identifies the transition to renewable energy sources and the intensification of energy conservation processes as a key factor [27]. The issue has become the centre of the European Union's political agenda, as presented in the Political Guidelines of the President of the European Commission, the priorities of the European Parliament, and the Strategic Programme of the European Council for 2019–2024. The goal to be achieved is a digital and green transformation that is to encompass all economic and social activities, resulting in increased European competitiveness and prosperity, economic and technological sovereignty, resilience to external shocks, climate neutrality, and digital leadership [28].

Figure 1. Impact of factors on the energy security model. Source: Authors' own elaboration.

The ways to achieve the goal are specified in other documents, among which the European Green Deal [29] and the strategy “Shaping Europe’s digital future” are fundamental [30]. According to them, changes in the energy sector [31] depend substantially on the development of the digital sector, which is expected to be a source of innovation in clean technology [32] and a provider of services that reduce energy consumption. However, in addition to these key areas of energy security, there is a question of how to safeguard the flow of information, and this is where the role of the designated postal operator comes into play.

3. Cybersecurity in the Context of Critical Infrastructure

Progressing digitalisation raises the question of the information security related to internet-connected services and infrastructure. In this view, it is worth recalling the opinion of former FBI Director Robert Mueller who stated that companies could be divided into two types: those that have fallen victim to an attack and those that will become so. Numerous examples support the thesis.

It is important to note that large organisations, including energy sector companies, despite having the knowledge and resources at their disposal, are not free from threats, as exemplified by the attack referred to by researchers as Soliorgate. The attack resulted in a breach of information systems in over 400 of the largest global corporations listed by the Fortune 500. At the same time, SMEs, in addition to being a target in their own right, are exposed to attacks, especially when they are in the supply chain of the actual target. In such a situation, they can be used as an attack vector or to disrupt the functioning of the targeted entity.

The European Union has been trying to provide comprehensive regulation of cybersecurity. Hence, the EU adopted Regulation 2019/88112 (Cybersecurity Act) and Directive 2016/1148, referred to in the literature as the NIS Directive. While analysing provisions of the former from the perspective of the energy sector, it must be noted that its scope includes the setting of objectives and tasks for the European Union Agency for Cybersecurity (ENISA) and the framework for the establishment of European cybersecurity certification schemes [33].

Directive 2016/1148 was introduced to achieve a high common level of security for the network and information systems in the Union, thereby improving the functioning

of the internal market. The way to achieve it is to create a network for the exchange of information and cooperation in this area between EU countries and national cybersecurity systems. This involves the defining of specific groups of entities and imposing on them obligations in the area of cybersecurity. Moreover, it is necessary to appoint bodies within the state to handle incidents, including crisis response and analysis of past attacks and the formulation of recommendations.

The Directive foresees two types of obligated parties. These are key service operators, which include energy sector actors, and digital service providers. The first group includes public or private entities providing services that are vital to the maintenance of critical social or economic activity. Wherever the provision of their services depends on IT networks and systems, an incident may have a significant disruptive effect. The second group includes all legal entities providing digital services.

It should be stressed that in a rapidly changing geopolitical environment, it is essential to maintain good quality of services, such as collective transport, energy [34] and water supply, communications, and postal services. The expansion of critical infrastructure must not be determined by costs or profits. What matters is the security of citizens and the uninterrupted satisfaction of their basic needs.

4. Digitalisation of the Designated Postal Operator

While analysing the situation in the context of secure transmission of information [35] for energy critical infrastructure, the question arises which entity should be responsible for support and security. Such a role could be undertaken by the current designated postal operators who, subject to intensive digitalisation processes, could become an important link in the process. The operators are capable of providing information and cyber security, extending their competence on the basis of their long-term experience in transmission of information, and becoming a supplier of digital services to entities responsible for energy security and critical infrastructure.

The digitalisation [36,37] of the economy and society is one of the most dynamic changes of our times. Although it has created new opportunities for postal operators, at the same time it brings uncertainty and various related risks, inter alia, to the social effects of production automation or security in its broadest sense. The radical nature of the changes brings completely different values to market players and consumers. To cope with these changes, both individual companies, public administrations, and societies and national economies must undergo digital transformation [38,39]. Until recently, the key area of activity of postal operators was the handling of traditional postal items. However, under the influence of digitisation of the economy, the volume of mail has been reduced, especially in highly developed countries. This trend is directly related to the e-substitution of traditional postal services. It should be noted that, although on the one hand it is the most threatened area, on the other hand, it is characterised by powerful opportunities [40]; if a new service provision concept is adopted. This should allow for the replacement of the handling of traditional correspondence with modern information technologies, and the simultaneous extension of the current role of postal operators with digital information security provided for the critical energy infrastructure.

It should be emphasised that modern technologies [41] used by operators allow not only data processing but also provide an added value for clients in the form of e-services [42]. In addition, the use of mobile technologies by postal operators enables more efficient and effective communication, and collection and processing of data on the basis of which further management changes can be implemented. It is also important that, in addition to the development of personalised services in the digital space, postal operators should develop cooperation with their governments. This points to a new role that designated postal operators could perform. Being public trust institutions [43] with an adequate digital infrastructure and with experience in the area of critical infrastructure security, they could expand their activity to include the provision of digital services to entities responsible for the security of critical infrastructure, especially in the energy sector.

It is a result of the strategic character of the postal market that brings together entities that perform similar activities at a micro and macro scale. It is believed that if postal operators combined the physical and digital worlds, they would take a strong position in the market and compete with digital platform providers. Importantly, postal operators are often seen as an institution of public trust. Moreover, the highly accessible network of post offices is also an asset. While operating infrastructure of the largest coverage in the country, designated postal operators may become partners in the provision of digital security for critical energy infrastructure based on modern information technologies. Postal platforms that provide electronic postal services can be used to support communication with critical infrastructure security companies and citizens, because in a critical infrastructure crisis the largest issue is to provide information to the public. The key benefit would be first and foremost a highly secure communication process.

Furthermore, the aim of greater security, in the context of information flow in the area of critical infrastructure, is to strengthen the position of the designated operator by merging it with the structures of government administration. This solution is feasible in states that see the operator as a pillar of their national security. Nowadays, in an environment based on a far-reaching division of labour, the supply of goods and services to citizens is provided using a multifaceted network of production, distribution, and administrative management systems. These systems comprise a network critical for ensuring the security of citizens and the state, and they are collectively referred to as critical infrastructure [44]. From the point of view of the functions of the postal system, the adequate level of information security requires measures to prevent disruptions, as well as increased capacity to coordinate processes within institutions that contain elements of the government postal infrastructure. Through its administration units, the state should counteract attempts to destroy the state's information infrastructure. Provision of a communications system within the country is critical to its security, especially its government administration, armed forces, and the energy sector. A system based on state-of-the-art telecommunications technology and the highest security standards is essential for the development of any country. Therefore, the security of critical infrastructure should be regarded as essential for its functioning [45]. It is also important to highlight threats to critical infrastructure information systems, which may have a variety of causes. There are also risks that adversely affect the performance of tasks and objectives. The risks may depend on external or internal factors. These events can cause difficulty, disruption, or even prevent the transmission of information, and as such they need to be identified in order to plan appropriate actions [46].

The ideal situation for the state, however impossible to achieve, is to undertake all measures to completely eliminate risk in the sphere of information technology. Unfortunately, changes in public sector entities and in their environment, unpredictable external conditions (e.g., statutory, climatic, or technological) make it impossible to reduce the risk to zero permanently and force comprehensive actions to mitigate the risk to an acceptable level. The increasing number of communication systems and their various configurations, as well as databases and data registers, make the IT environment more extensive and sophisticated. Systems are not only interconnected within a given entity, but often communicate with and depend on external systems and people. The number of people with access rights to these systems and data has also been growing. The complexity and range of the infrastructure (often reporting to many different entities) has a significant impact on the management of risk in this area. However, depending on the risk classification, its priority, and importance and state of acceptability, appropriate actions should be taken with regard to the use of the postal infrastructure.

In the context of the information presented, the key role of the state is to secure the communication system. This might be the responsibility of designated postal operators that use facilities and network to fulfil basic tasks of the state when the telecommunications critical infrastructure is not functioning. This primarily results in the fulfilment of national security objectives. In this view, the state would have a wide range of institutional, administrative, and economic tools to achieve its intended goals. It should also be indicated that

heavy state involvement in the operation of postal incumbents would prevent marginalisation of peripheral areas. It can be assumed that as a result of such activity of states, the position of designated operators would strengthen (Significant investment in infrastructure should be highlighted here.), with a smaller share of other postal operators on that market, as presented in Figure 2.

Figure 2. Model strengthening the postal services market. Source: Authors' own elaboration.

The model may be supplemented with a market model that will respond to challenges of the New Economy, e-economy, i.e., a model in which postal operators make extensive use of modern technologies.

It should be pointed out that the digitalisation of postal services in EU countries has seen an intensive increase in the involvement of modern technologies.

To conclude this part of the deliberations, it should be pointed out that research is needed to determine whether a designated postal operator transformed into a digital postal operator would provide secure transmission of information for the critical infrastructure in the energy sector.

5. Materials, Methods and Results

Research referred to in the article has demonstrated that designated postal operators may become an important link in the process of information flow and cybersecurity. Based on their multiple-year experience and expanded competences, the operators may provide digital services for entities responsible for energy security infrastructure.

The aim of the article was verified on the basis of a CATI survey conducted among postal market and energy sector experts (The study involved a team of nationally recognised experts in the postal and energy sectors. These included representatives from universities and a scientific research institute, as well as postal and energy sector operators). The experts were interviewed as part of the study. A total of 28 experts were surveyed (11 related to the postal market, 17 related to the energy market). The survey was conducted in Q4 2021. The study was based on the purposive selection of 26 experts who provided their assessment.

The individual indications obtained enabled the identification of premises demonstrating the involvement of the digital postal operator in the security of energy critical infrastructure. Due to the nature and limited volume of the article, only selected results of the study are discussed further.

The study aimed at demonstrating the potential of the designated postal operator to allow an appropriate level of energy security. The evaluation includes:

- Organisational experience in ensuring a smooth flow of information;
- The property of building an organisational structure—points of contact;
- Expertise of the personnel as regards the operation in the area of critical infrastructure;
- Risk management skills in the context of cybersecurity;
- Ability to ensure business continuity;
- Experience in crisis management;
- Experience in the design and implementation of security procedures for the acquisition, development, and maintenance of information networks and systems.

Experts assessed the potential for the involvement of the designated postal operator in the provision of critical infrastructure security. The scale used by the experts ranged from 1 to 10, where 1 was the lowest score (lowest potential) and 10 the highest (highest potential, which guarantee efficiency). Opinions are presented in Figure 3.

Figure 3. Assessment of the capability of the designated postal operator to provide an adequate level of security for the transmission of information within the energy infrastructure. Source: Authors' own elaboration.

The analysis of responses shows that the major weakness is the organisational structure, which needs to be reformulated. This seems obvious, legitimate, and necessary. When expressing their opinion, the experts were aware of certain shortcomings that limit the positive image of the postal operator on the market. However, considering the potential and experience, in the opinion of the experts, the postal operator is best suited for the new function.

The elements described above enable to meet challenges faced by the energy sector. Taking into account further digitalisation of postal services, it is reasonable to use this public trust institution to perform tasks that secure the critical infrastructure of the energy sector, in terms of transmission of information and cyber threats.

The analysis covered expectations regarding support to secure energy critical infrastructure in terms of information transmission and cyber threats. These include:

- Offering efficient flow of information between the relevant entities responsible for safeguarding national energy security,
- Supporting risk management at all levels of governance in energy sector entities,
- Developing procedures in the event of a cyber incident;
- Helping to prevent, detect and respond to cyber incidents;
- Ensuring business continuity and crisis management, security of the energy supply chain for energy operators, while taking into account vulnerabilities specific to each energy provider; and
- Developing and implementing security procedures in acquisition, development and maintenance of networks and information systems.

After they identified and indicated a set of factors influencing the security of energy critical infrastructure, experts were asked to indicate their expectations regarding the support for the energy critical infrastructure. The scale used by the experts ranged from 1 to 10, where 1 was the least important and 10 the most important (should be implemented immediately). Opinions are presented in Figure 4.

Figure 4. Desirable expectations affecting the energy security of critical infrastructure. Source: Authors' own elaboration.

Energy sector actors articulate their willingness to accept support in a number of areas, with the aim to protect critical infrastructure. However, the assistance to prevent, detect and respond to incidents is seen as the most important. In addition, it is important to have

an efficient flow of information between relevant entities responsible for national energy security. There are clearly problems in this area. Those responsible for critical infrastructure often point to the problem of information chaos, hence the efficiency of information flow is highly important. There are slightly lower expectations in terms of business continuity and crisis management. This is due to the fact that the actors manage this on their own and expect less support.

In conclusion, it is clear that the potential of a designated postal operator allows it to fulfil additional tasks that support critical infrastructure and energy sector players expect such support. Therefore, it seems justified to extend competences of the designated postal operator to secure the transmission of information within the critical energy infrastructure.

6. The Role of the Government in Ensuring the Security of Critical Infrastructure by the Designated Postal Operator

A particularly important area that needs to be discussed is the security of critical infrastructure and cybersecurity provided by the state. The starting point for the implementation of the concept presented in the article is to define regulations and the level of their intensity. This should help to achieve the intended goal, which is to increase competences of the designated postal operator.

The state can apply both institutional and economic regulations. However, due to the key importance of critical infrastructure for strategic sectors of the economy, regulations at the administrative level should be considered crucial, as they allow to expand competences and the scope of activity of the designated postal operator. They will constitute the starting point for further regulations, both institutional and economic. Economic regulations should take into account solutions that support investment in modern technologies and systems that are pivotal for ensuring the security of critical infrastructure and cybersecurity. The regulations are an important link in the process of building the security of critical infrastructure. The state activity in this area should be coordinated and multidirectional using the described tools, especially by integrating the structure of the designated postal operator at local, regional, and national levels, and building awareness and promoting intensive IT education on the security of key elements of critical infrastructure. By means of administrative regulations, the state may oblige to use the potential of the designated postal operator to support information flow between entities in key sectors of the economy, with particular reference to the critical infrastructure.

The proposals for the use of appropriate regulations cannot be considered as a solution to the problem of critical infrastructure security and cybersecurity. However, it should be noted that the regulations may encourage the extension of competences of the designated postal operator. The careful approach to regulations may help to create a platform that strengthens the security of critical infrastructure.

7. Discussion

The analysis of possibilities to support entities that secure critical infrastructure, including those in the energy sector, shows that the role of the designated postal operator may change significantly. Considering the security of information flow and cybersecurity, the postal operator could expand its competences by becoming a digital service provider. Its tasks may include:

- Providing risk management in cyberspace based on technical and organisational measures to manage security risks in networks and information systems used by entities in the energy sector to provide their services;
- Analysing risks and security policies pertaining to information systems;
- Developing procedures dedicated to energy sector actors in the event of an incident;
- Preventing, detecting, and responding to incidents;
- ensuring business continuity and crisis management, security of the energy supply chain for energy operators, taking into account vulnerabilities specific to each energy provider;

- Developing and implementing security procedures in the acquisition, development and maintenance of networks and information systems;
- Developing security policy and procedures to assess the effectiveness of cyber risk management and the use of cryptography and encryption in communications with energy sector entities;
- Applying a specific methodology or certification schemes when implementing required technical and organisational measures, while taking into account the latest knowledge; and
- Reporting incidents that have a significant impact on the provision of energy supply to the competent authorities or response teams.

The digital postal operator can be an institution coordinating the course of actions and the flow of information between parties involved, as presented in Figure 5.

Figure 5. The flow of information between parties. Source: Authors' own elaboration.

The digital postal operator can be responsible for the monitoring and provision of information on cyber risks, cyber threats, and incidents affecting critical parties involved, as well as on measures put in place by competent authorities in response to such risks and incidents. Moreover, similar solutions could be introduced for internationally relevant critical actors.

It would therefore be necessary to introduce a system supporting the provision of standardised information to the designated groups of operators. Since this has not been organised, we are swamped with information and run the risk that important information is overlooked. The digital postal operator may coordinate the information flow while providing the highest possible level of security.

The digital postal operator, which already has an appropriate structure in place, could establish national contact points to ensure cross-border cooperation between authorities in member states, as well as cross-sectoral cooperation with other relevant national authorities. In addition, to strengthen institutions and improve the flow of knowledge and good practices, human resource capacity can be built through a training system.

It should be noted that from the perspective of the energy sector, the security of the infrastructure is pivotal, as inability to supply energy could adversely affect public order, the public and people's health. It may also lead to systemic risk, in particular, where such a disruption could have a cross-border impact. It should be stressed that cyberattacks on large entities often increasingly focus on their suppliers or subcontractors (Kozłowski, 2021).

8. Conclusions

Energy security and cybercrime threats are a real challenge for energy sector players. They can affect all spheres of society and have far-reaching political, economic, or military consequences. The progressing digitalisation of all spheres of life, supported by the European Union, has led to a rapid increase in the number of risks. At the same time, self-regulatory cybersecurity measures by companies have not been successful since these have not been convergent in terms of their level and form and could guarantee only partial security.

Regarding the obligations imposed on the state, the expansion of the information exchange network is crucial. Considering other goals set for the organisations concerned, it is important to define the information sharing structure and avoid the duplication of information leading to information noise. However, this is a purely management issue and hopefully the operation of the structure is free of such noise.

The proposal presented in the article, aimed at increasing the role of the designated postal operator to support energy security, should be taken into account in the context of energy infrastructure security, especially regarding the transmission of information.

The potential and experience of the designated postal operator provides a basis for the creation of a new organisation, which, as a public trust body, would be an institution supporting the important area of critical infrastructure energy security.

It must be stressed that critical infrastructure, especially in the energy sector, plays a key role in the functioning of the state and its citizens, and its security is one of state priorities. In particular, the protection of critical infrastructure is important in terms of the organisational arrangements put in place to ensure the functioning or rapid recovery of critical infrastructure in the event of threats, including failures, attacks, and other disruptions.

It should be emphasised that the essence of tasks related to critical infrastructure lies not only in its protection, but also in ensuring that any damage or disruption to its functioning is as short as possible, easy to remedy, and does not cause additional losses to the society and economy. It is important to involve parties responsible for the management of the infrastructure in the provision of security by enhancing private and public sector cooperation. Indeed, protecting critical infrastructure is in the interest of both private entities and the state administration. The active partnership between private and public operators of critical infrastructure facilities, installations, and equipment will allow a stable functioning of the system.

The research results show that the security of critical infrastructure requires constant monitoring of challenges faced by critical infrastructure operators. It should be pointed out that new challenges arise continuously from the digitalisation of the society and economy. Therefore, it is imperative to observe public entities, such as the designated postal operator, as they have powerful experience and knowledge that can be very convenient in such a volatile environment. The authors of the article consider these challenges to be subject of their further research.

Author Contributions: Conceptualization, A.D.-K. and W.D.; methodology, A.D.-K. and W.D.; formal analysis, A.D.-K. and W.D.; resources, A.D.-K. and W.D.; data curation, A.D.-K. and W.D.; writing—original draft preparation, A.D.-K. and W.D.; writing—review and editing, W.D.; visualization, A.D.-K.; supervision, A.D.-K. and W.D.; project administration, A.D.-K.; funding acquisition, A.D.-K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded from the programme of the Minister of Science and Higher Education “Regional Excellence Initiative” in 2019–2022; project number 001/RID/2018/19; the amount of financing: PLN 10,684,000.00.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Gritzalis, D.; Theocharidou, M.; Stergiopoulos, G. *Critical Infrastructure Security and Resilience*; Springer: Cham, Switzerland, 2019; p. 18. [\[CrossRef\]](#)
2. Wang, W.; Yang, S.; Hu, F.; Stanley, H.E.; He, S.; Shi, M. An approach for cascading effects within critical infrastructure systems. *Phys. A Stat. Mech. Its Appl.* **2018**, *510*, 164–177. [\[CrossRef\]](#)
3. Mao, Q.; Li, N. Assessment of the impact of interdependencies on the resilience of networked critical infrastructure systems. *Nat. Hazards* **2018**, *93*, 315–337. [\[CrossRef\]](#)
4. Kancelaria Sejmu. *Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z Dnia 5 Lipca 2019 r. w Sprawie Ogłoszenia Jednolitego Tekstu Ustawy o Zarządzaniu Kryzysowym*; Kancelaria Sejmu: Warszawa, Poland, 2019.
5. Wolbers, J.; Boersma, K.; Groenewegen, P. Introducing a fragmentation perspective on coordination in crisis management. *Organ. Stud.* **2018**, *39*, 1521–1546. [\[CrossRef\]](#)
6. Ansell, C.; Boin, A. Taming deep uncertainty: The potential of pragmatist principles for understanding and improving strategic crisis management. *Adm. Soc.* **2019**, *51*, 1079–1112. [\[CrossRef\]](#)
7. Pursiainen, C. Critical infrastructure resilience: A Nordic model in the making. *Int. J. Disaster Risk Reduct.* **2018**, *27*, 632–641. [\[CrossRef\]](#)
8. Lanciu, I. The Protection of Critical Infrastructure Management Models of Risk. In *The Fourth Annual Conference of the National Defence College Romania in the New International Security Dynamics*; Carol I National Defence University Publishing House: Bucharest, Romania, 2019; pp. 79–86.
9. Sadowski, J. Ochrona infrastruktury krytycznej: Geneza problemu. *Autobusy Tech. Eksploat. Syst. Transp.* **2018**, *19*, 1237–1241.
10. Budziewicz-Guźlecka, A. *Oddziaływanie Polityki Społeczno-Gospodarczej na Zmiany Polskiego Rynku Usług Telekomunikacyjnych*; Wydawnictwo Naukowe Uniwersytetu Szczecińskiego: Szczecin, Poland, 2019.
11. Trump, B.D.; Poinsatte-Jones, K.; Elran, M.; Allen, C.; Srdjevic, B.; Merad, M.; Palma-Oliveira, J.M. Social resilience and critical infrastructure systems. In *Resilience and Risk*; Springer: Dordrecht, The Netherlands, 2017; pp. 289–299.
12. Sakhnini, J.; Karimipour, H.; Dehghantanha, A.; Parizi, R.M. *AI and Security of Critical Infrastructure*; Springer: Cham, Switzerland, 2020; pp. 7–36.
13. Zimba, A.; Wang, Z.; Chen, H. Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. *Ict. Express* **2018**, *4*, 14–18. [\[CrossRef\]](#)
14. Reingold, L.A.; Reingold, E.A.; Soloviev, A.V.; Grin, O.S. Citizens' Digital Infrastructure as a New Element of Modern Society Critical Infrastructure. 2020. Available online: http://eur-ws.org/Vol-2763/CPT2020_paper_s3-3.pdf (accessed on 1 December 2021).
15. Touhiduzzaman, M.; Gourisetti, S.N.G.; Eppinger, C.; Somani, A. A review of cybersecurity risk and consequences for critical infrastructure. *Resil. Week* **2019**, *1*, 7–13.
16. Drożdż, W.; Głowski, P.; Pawlicki, M.; Midera, A. Capacity Mechanism as a Potential Instrument Increasing Energy Security of the European Union. In *Economic Transformation in Ukraine: Comparative Analysis and European Experience*; Consilium Sp. z o.o.: Warsaw, Poland, 2017; p. 137.
17. Braun, J. Bezpieczeństwo energetyczne jako dobro publiczne—miary i czynniki wpływające na jego poziom. *Studia Ekon.* **2018**, *358*, 23–32.
18. Drożdż, W.; Mróz-Malik, O.J. Challenges for the Polish energy policy in the field of offshore wind energy development. *Polityka Energetyczna* **2020**, *23*, 5–18. [\[CrossRef\]](#)
19. Panasiuk, A.; Sierański, S. Ochrona obiektów infrastruktury krytycznej—bezpieczeństwo państwa i obywateli. *Kontrola Państwowa* **2017**, *62*, 76–86.
20. Cieślak, S. Funkcjonalność stacji elektroenergetycznych w dystrybucji energii elektrycznej w nowym polskim systemie elektroenergetycznym przy braku paliw kopalnych. *Wiadomości Elektrotechniczne* **2020**, *88*, 3–10. [\[CrossRef\]](#)
21. Sarota, A. Ograniczenia swobody prowadzenia działalności gospodarczej—rynek gazu i energii elektrycznej w Polsce. *Kontrola Państwowa* **2018**, *63*, 121–135.
22. Sołtysik, M. Założenia funkcjonowania klastrów energii. XVIII Konferencja Aktualne Problemy w Elektroenergetyce APE'2017 (XVIII); 07.06–09.06.2017. In *Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej*; Politechnika Gdańska: Gdańsk, Poland, 2017.
23. Przybył, M.A.; Śpiewak, R. Oddziaływanie regulatora na czynniki finansowe operatorów systemu dystrybucyjnego energii elektrycznej. *Polityka Energetyczna* **2017**, *20*, 89–104.
24. Czajkowska, A. Prognozowanie prawidłowego funkcjonowania obiektów w sektorze energetycznym. *Rynek Energii* **2019**, *4*, 21–25.
25. Kudełko, M. Metodyka Prognozowania Rozwoju Krajowego Sektora Energetycznego. In *Polityka Gospodarcza w Warunkach Przemian Rozwojowych*; Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu: Wrocław, Poland, 2020; p. 62.
26. Żmigrodzki, M. Innowacyjność w Wytwarzaniu i Przesyłu Energii Jako Współczynnik Bezpieczeństwa Energetycznego Państwa. *Studia humanistyczno-społeczne*, pod red. R. Kubicki i W. Saletra **2016**, *12*, 165–176.
27. Hordeski, M.F. *New Technologies for Energy Efficiency*; CRC Press: Boca Raton, FL, USA, 2021.
28. Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów—w Sprawie Określenia i Usuwania Barier na Jednolitym Rynku. 2020. Available online: <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0093&from=EN> (accessed on 2 December 2021).

29. Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Komitetu Ekonomiczno-Społecznego i Komitetu Regionów—Europejski Zielony Ład. 2019. Available online: https://eur-lex.europa.eu/resource.html?uri=cellar:b828d165-1c22-11ea-8c1f-01aa75ed71a1.0016.02/DOC_1&format=PDF (accessed on 2 December 2021).
30. Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Komitetu Ekonomiczno-Społecznego i Komitetu Regionów—Kształtowanie Cyfrowej Przyszłości Europy. 2020. Available online: <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0067&from=PL> (accessed on 2 December 2021).
31. Rabe, M.; Streimikienė, D.; Drożdż, W.; Bilan, Y.; Kasperowicz, R. Sustainable regional energy planning: The case of hydro. *Sustain. Dev.* **2020**, *28*, 1652–1662. [CrossRef]
32. Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów—Nowa Strategia Przemysłowa Dla Europy. 2020. Available online: <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0102&from=EN> (accessed on 1 December 2021).
33. Greaser, J. Regulacja cyberbezpieczeństwa w sektorze energetycznym w świetle projektu dyrektywy NIS 2. *Internetowy Kwart. Antymonop. I Regul.* **2021**, *10*, 87–101. [CrossRef]
34. Drożdż, W. Operator systemu dystrybucji w dobie wyzwań innowacyjnej energetyki. *Zeszyty Naukowe* **2018**, *102*, 291–300. Available online: <https://journals.pan.pl/dlibra/publication/123743/edition/107950/content> (accessed on 18 November 2021).
35. Budziewicz-Guźlecka, A.; Drab-Kurowska, A. Problems of Infrastructure Markets with Particular Emphasis on the Postal Market in the Context of Digital Exclusion. *Sustainability* **2020**, *12*, 4719. [CrossRef]
36. Greenstein, S.; Goldfarb, A.; Tucker, C. *The Economics of Digitization, International Library of Critical Writings in Economics 280*; Edward Elgar: Cheltenham, UK, 2013.
37. Peitz, M.; Waldfogel, J. *The Oxford Handbook of the Digital Economy*; Oxford University Press: New York, NY, USA, 2012.
38. Pieriegud, J.; Paprocki, W.; Gajewski, J. *Cyfryzacja Gospodarki i Społeczeństwa—Szanse i Wyzwania Dla Sektorów Infrastrukturalnych*; Instytut Badań nad Gospodarką Rynkową—Gdańska Akademia Bankowa: Gdańsk, Poland, 2016.
39. Drożdż, W.; Marszałek-Kawa, J.; Miskiewicz, R.; Szczepanska-Waszczyńska, K. *Digital Economy in the Comporary World*; Wydawnictwo Adam Marszałek: Toruń, Polska, 2020.
40. Budziewicz-Guźlecka, A.; Czaplewski, M.; Drab-Kurowska, A. *Integracja Sektorowa Wybranych Europejskich Rynków Poczтовых i Telekomunikacyjnych w Warunkach Globalizacji*; Wydawnictwo edu-Libri: Kraków, Poland, 2018.
41. Drab-Kurowska, A. Wykorzystanie sieci Internet w przedsiębiorstwie. *Świętokrzyskie Cent. Edukac. Na Odległość. Zesz. Nauk* **2006**, *2*, 197–2010.
42. Budziewicz-Guźlecka, A.; Drab-Kurowska, A. E-administracja w Polsce. In *Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług*; Wydawnictwo Uniwersytetu Szczecińskiego: Szczeci, Poland, 2012; pp. 366–373.
43. Drab-Kurowska, A. Proces liberalizacji rynku usług pocztowych w świetle regulacji Unii Europejskiej. *Informacja Poczta* **2007**, *5*, 1–12.
44. Milewski, J. Identyfikacja infrastruktury krytycznej i jej zagrożeń. *Zeszyty Naukowe AON* **2016**, *4*, 99–115.
45. Buko, J. *Problematyka Zagrożeń dla Systemów Informatycznych Polskiej Infrastruktury Krytycznej. CYWILIZACJA Informacyjna i Jej Oddziaływanie na Transformację Gospodarczą i Społeczną*; Wydawnictwo Naukowe Uniwersytetu Szczecińskiego: Szczecin, Poland, 2018; p. 69.
46. Mazur, Z.; Mazur, H.; Mendyk-Krajewska, T. Ryzyko w sektorze publicznym w kontekście zintegrowanej informatyzacji. *Ekon. Probl. Usług* **2017**, *126*, 371–384. [CrossRef]