A. Kucharska, *Cybersecurity challenges in Poland in the face of energy transition*,
„Rocznik Instytutu Europy Środkowo-Wschodniej" 18(2020), z. 1, s. 141-159,
DOI: https://doi.org/10.36874/RIESW.2020.1.8.

Anna Kucharska*

# Cybersecurity challenges in Poland in the face of energy transition

## Wyzwania cyberbezpieczeństwa w Polsce w obliczu transformacji energetycznej

**Abstract:** The transformation of the energy sector is one of today's global megatrends. The main aim of this process includes shifting energy production to renewable sources, decarbonizing the economy, and improving energy efficiency, especially in the most energy-intensive sectors. These changes lead the energy sectors of different states to ensure security and maintain environmental protection in order to guarantee the civilization's progressive development. One of the tools for the implementation and development of a new model of the energy sector is digitization, which is a direct consequence of the increasing complexity of the energy system. Digitization is an essential element in the management of smart grids and smart meters and for controlling the entire energy system, as well as guaranteeing fair distribution. The digitization process integrates the state energy system; however, it also increases its vulnerability to potential cyber-threats. The aim of this paper is to analyze the cybersecurity challenges facing the Polish power sector in light of the energy transition policy promoted in the EU with a particular focus on the latest legislation presented in the Clean Energy Package. The Polish energy sector is on the verge of structural changes; therefore the main question is: *How to implement them to avoid errors?* The paper provides a glimpse into the most venerable areas, which should be taken into consideration by political decision-makers.

**Keywords:** digitization, energy sector, cybersecurity, energy transition

**Streszczenie:** Jednym z narzędzi służących implementacji celów transformacji energetycznej jest digitalizacja, która bezpośrednio łączy się ze wzrostem stopnia komplikacji systemu energetycznego – pojawia się w nim bowiem coraz więcej podmiotów wytwarzających energię elektryczną na skutek postępującego rozproszenia źródeł energii o nieregularnej częstotliwości wytwórczej. Digitalizacja jest koniecznym elementem zarządzania inteligentnymi sieciami przesyłu energii i inteligentnymi licznikami, służącym kontroli całego systemu energetycznego, a także gwarancji sprawiedliwości

[*] Anna Kucharska, PhD, Jagiellonian University in Kraków, Poland, ORCID ID: https://orcid.org/0000-0002-5184-0902, e-mail: anna.m.w.kucharska@gmail.com.

dystrybucji, co stanowi m.in. element walki z ubóstwem energetycznym. Zaleta procesu digitalizacji, polegająca na scalaniu państwowego systemu energetycznego, podnosi jednocześnie jego wrażliwość na potencjalne zagrożenia związane z działalnością przestępczą i terrorystyczną. Wyzwania z tym związane obejmują takie zagadnienia jak: ochrona przepływu i przechowywania danych, ataki mające na celu zakłócenie działań systemów i wywołanie przerw w dostawach czy też przejęcie kontroli nad mechanizmami dostaw energii, która stanowi konieczny element systemu komunikacyjnego we współczesnym świecie. Z uwagi na rosnące – adekwatnie do stopnia implementacji – znaczenie digitalizacji systemu energetycznego, warto przyjrzeć się bliżej temu zagadnieniu i wyzwaniom, jakie ze sobą niesie. Analiza istniejącego prawodawstwa krajowego i unijnego oraz dotychczasowych działań Polski w obszarze digitalizacji energetyki pozwoli na wyodrębnienie najważniejszych elementów tego procesu, którego jednym z głównych założeń jest gwarancja bezpieczeństwa energetycznego, a w szerszym ujęciu – dyktowanym przez znaczenie energii elektrycznej dla funkcjonowania państwa – także ogólnego bezpieczeństwa narodowego.

**Słowa kluczowe:** digitalizacja, sektor energetyczny, cyberbezpieczeństwo, transformacja energetyczna

## Introduction

This paper aims to analyze the cybersecurity challenges arising with the implementation of the European Union's energy transition concept. These challenges will be soon faced by the Polish power sector together with its development, which is unavoidable considering the worldwide technological changes. The direction of development of this sector in Poland is determined to a large extent by its membership in the European Union and by international trends that aim to improve energy efficiency in the global economy, which is related to the implementation of modern technologies and their digitization. It should be borne in mind that the changes that are taking place in relation to the energy sector serve to ensure the security of energy supplies while preserving the protection of the environment in a way that guarantees constant and sustainable development.

The basic methodological set included a query of strategic documents in the respective field and their critical analysis. The analysis is based on the activities and legislation of the European Union, to which Poland is a member. Other countries' experiences in the area of threats to the cybersecurity of the energy sector are also helpful, mainly through studies from the United States, which have been dealing with this issue in depth for years. The analysis of legislation and experience in the area of energy digitization to date will make it possible to identify the most important elements of this process, one of the main assumptions of which is the guarantee of energy security, and also national security in general – dictated by the importance of electricity for the functioning of the state.

With respect to the energy sector, various subsectors may be distinguished. The Network and Information Systems Directive distinguishes between three energy sub-sectors: electricity, oil, and gas.[1] The Energy Expert Cyber Security Platform (EECSP) report identifies four energy subsectors: electricity, oil, natural gas, and nuclear energy. The European Union Agency for Cybersecurity (ENISA), in its report on information exchange on cybersecurity in the energy sector, has considered four subsectors: electricity, oil and gas, nuclear energy, and alternative fuels.[2] In this paper, the discussion of cybersecurity issues in the energy sector is limited to electricity. The introduction of such a limit serves the reliability and quality of the study while maintaining publication volume requirements.

## 1. Digitization of the energy sector

The energy sector is facing an energy transition concerning a transfer to renewable energy sources (RES). A most basic definition of contemporary energy transition means changing the current energy model, which is based on non-renewable energy sources in the form of fossil fuels, to an energy system based on renewable energy sources.[3] This is linked to the growing complexity of the structure of production, which includes an increasing number of energy sources, which have to be continuously monitored and managed.[4] Therefore, digitization is part of the energy transition process and is essential to its achievement. It offers the possibility of controlling such a complex system by the development of appropriate methods of managing en-

[1] Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[2] *Energy Networks and Smart Grids. Cyber Security for the Energy Sector*, European Cyber Security Organisation (ECSO), November 2018, p. 10.

[3] M. Ruszel, T. Młynarski, A. Szurlej, 'The concept of energy transition', in: *Energy Policy Transition – The Perspective of Different States*, eds. M. Ruszel, T. Młynarski, A. Szurlej, Rzeszów: Ignacy Lukasiewicz Energy Policy Institute, 2017, p. 29.

[4] A. Barichella, *Cybersecurity in the Energy Sector. A Comparative Analysis between Europe and the United States*, Études de l'Ifri, Paris: Ifri, February 2018, p. 32.

ergy sources, i.e. installations for its production and energy storage, on the one hand, and with regard to demand, on the other. Therefore, the solution is seen in efficient and flexible energy system management based on intelligent transmission grids, smart energy meters, and virtual systems that are used to manage and optimize virtual power plants and markets. The development of these technologies and the related virtual infrastructure entails the need for effective flexibility in electricity flow management.[5] Too much electricity leads to an overload of the system, while too little results in a shortage of energy supply.[6] In addition, smart grids allow for a two-way flow of energy, thanks to the real possibility of including individual prosumers in the system.[7] This requires a supply and demand balance, which should be coordinated automatically in the transmission network nodes on the basis of real-time data analysis – this is what smart meters are supposed to do.[8]

However, the growing importance of digitization of the energy system is appropriate to the degree of its implementation and brings with it several security challenges. With the expansion of the smart electricity supply system, it also increases the number of actors. This entails that the number of possible loopholes that may emerge in the system increases, and these are a potential target for hackers and other criminal aggressors.[9] Also, the growing number of operations managed virtually entails that the energy system is increasingly sensitive to cyber incidents or potential attacks.[10] The energy sector is attractive as a potential target for attacks as it is one of the most important pillars of the state's critical infrastructure. For this reason, as well as cross-border interconnections for electricity transmission, there is

[5] E.B. Rice, A. AlMajali, 'Mitigating The Risk Of Cyber Attack On Smart Grid Systems', *Procedia Computer Science*, no. 28, 2014, p. 576.

[6] V. Wittpahl, *Digitalisierung. Bildung – Technik – Innovation*, iit-Themenband, Berlin: Springer, 2017, p. 143.

[7] S.S. Wu, C.C. Liu, A.F. Shosha et al., *Cyber Security and Information Protection in a Smart Grid Environment*, Proceedings of the 18th World Congress The International Federation of Automatic Control Milano (Italy) 28 August–2 September 2011, p. 13696.

[8] 'Sechs Thesen zur Digitalisierung der Energiewende: Chancen, Risiken und Entwicklungen', German Watch, https://germanwatch.org/sites/germanwatch.org/files/publication/15649.pdf, p. 5 [2020-04-28].

[9] V. Wittpahl, *Digitalisierung...*

[10] *CYBERSEC 2019. Recommendations & Key Takeaways*, 5th European Cybersecurity Forum – Cybersec, Katowice 29-30 October 2019, p. 11.

a risk of cascading effects, which may cause power outages in other sectors and countries.[11]

The challenge of digitization and security in the energy sector is its specificity, in that it requires operations between different types of users connected to it in real time.[12] This means that some of the standard cybersecurity solutions cannot be used because they involve some time delay.[13] In addition, a period of transition – equally in terms of increasing digitization in the energy sector as well as in relation to the transition to renewables, and the development of the whole economy towards low-carbonization – means that old solutions and up-to-date ones will be running in parallel for a certain amount of time. Older technologies carry risks for the sector as they were designed at a time when cybersecurity was not a priority. In the case of new technological solutions, however, the greatest security risk is related to the Internet of Things (IoT) devices, which are not made using the "security by design" approach. This is primarily the case with devices that are gaining in popularity as a result of the smart home concept, including devices and equipment such as lighting, thermostats, home security systems, and cameras.[14]

Cybersecurity itself refers to technologies, processes, and controls that aim to protect systems, networks, devices and data against attacks, and unauthorized access.[15] This concept is often equated with information security because the value protected in cyberspace is information.[16] Cyber threats, in turn, are a category in the security sciences of a state, pointing to a new area of vulnerability and sensitivity relating to the stability of functioning and serving to achieve the cyber resilience of the state. An example of a cyberthreat is a cyberattack, which is defined as a cybernetic, offensive or defensive operation that can cause

[11] *CYBERSEC 2019...*

[12] *Energy Networks and Smart Grids…*, p. 3.

[13] *CYBERSEC 2019...*, p. 11.

[14] Ibidem.

[15] *Energy Insight: Cybersecurity in the energy sector*, Energy Institute, https://knowledge.energyinst.org/search/record?id=110329 [2020-04-28].

[16] A. Trubalski, J. Trubalska, Bezpieczeństwo Polski w cyberprzestrzeni', in: *Bezpieczeństwo państwa w cyberprzestrzeni*, eds. J. Trubalska, Ł. Wojciechowski, Lublin: Wydawnictwo WSEI, 2017, pp. 17-20.

injury or death to persons or damage or destruction of objects.[17] It is also defined as an incident that uses software, software code, computer technology or networks to commit a crime. It may be a traditional crime, such as fraud or theft, or it may be an incident that targets computers, connected devices or other information and communication technologies (ICT) to disrupt or damage supply, access or some other aspect of functionality.[18] This is of particular importance in the context of critical infrastructure elements, which should be understood as installations and networks whose security is a strategic priority in view of their crucial importance for the continuity of the functioning of the state.[19] The Polish National Security Strategy identifies ensuring Poland's secure functioning in cyberspace as a strategic objective in the area of cybersecurity. This refers to ensuring an appropriate level of security of national ICT systems with particular emphasis on the critical national infrastructure. This protection should be ensured primarily in such key sectors for the functioning of the economy and society as financial, energy, and healthcare.[20]

In turn, cyberspace is defined as a whole range of connections of a virtual nature, i.e. non-material, created, and existing due to their physical forms in the form of computers, telecommunications infrastructure, etc. In terms of the technical dimension of cyberspace, it is defined as a communicative space created by a system of internet connections.[21] According to the definition given in the "Doctrine of CyberSecurity of the Republic of Poland", cyberspace

*is a space for the processing and exchange of information created by information and communication systems (teams of cooperating IT devices and software ensuring processing, storage, as well as sending and receiving data through telecommunication networks by means of a terminal device appropriate for a given type of telecommunication network and intended to be connected directly or indirectly to the net-*

[17] W. Goździewicz, M. Krupczyński, J. Kulesza et al., *NATO Road to Cybersecurity*, ed. J. Świątkowska, Cracow: The Kosciuszko Institute, 2016, pp. 18-19.

[18] *Cyber security: A growing threat to the energy sector. An Australian perspective*, Hogan Lovells, March 2016, p. 2, https://www.hoganlovells.com/en/knowledge/topic-centers/cybersecurity-solutions/~/media/c14b2cc829b04a6e841237f66882b2df.ashx [2020-04-28].

[19] W. Goździewicz, M. Krupczyński, J. Kulesza et al., *NATO Road to Cybersecurity*…, pp. 18-19.

[20] *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa, 2015, p. 9.

[21] A. Trubalski, J. Trubalska, *Bezpieczeństwo Polski*…, pp. 17-20.

*work terminals) together with the links between them and the relations with users.*[22]

## 2. European Union requirements for the digitization of the energy sector

The Clean Energy Package for all Europeans (also called Clean Energy Package) is a key determinant of the European Union's energy policy development. The package also includes issues relating to the digitization of the energy sector in the Member States, with a distinction between the transmission networks, the energy market, and its participants (energy producers, transmission system operators, consumers). The provisions of the Clean Energy Package are in line with other EU documents regulating cybersecurity issues, including the energy sector. They are listed and described in table 1.

**Table 1. The main cybersecurity regulations regarding the electricity in EU**

| Name of the regulatory document | Year of adoption | Substation of the regulatory document | Date of entry into force |
|---|---|---|---|
| Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA | 2013 | The directive introduced new rules harmonizing criminalization and penalties for a number of offenses directed against information systems. It focuses on ensuring that the same offenses are criminalized in all EU Member States and giving law enforcement authorities the means to act and to cooperate with one another, to establish a national point of contact and use the existing network of 24/7 contact points. | September 2013 |
| Directive on Security of Network and Information Systems [NIS Directive] | 2016 | It is a major component of the European cybersecurity strategy aimed at strengthening Europe's cyber resilience and cooperation across different sectors. One major challenge is to ensure the alignment of NIS Directive implementations among the EU Member States. | May 2018 |

[22] *Doktryna cyberbezpieczeństwa…*, p. 7.

| Name of the regulatory document | Year of adoption | Substation of the regulatory document | Date of entry into force |
|---|---|---|---|
| General Data Protection Regulation [GDPR] | 2016 | The GDPR regulation defines requirements for the protection of personal data. | May 2018 |
| Cybersecurity Network Code | 2016 | The Cybersecurity Network Code proposes cybersecurity technical rules for electricity aiming to go beyond the NIS Directive obligations by addressing energy sector specificities. It emphasizes the importance of ensuring the resilience of the energy supply systems against cyber risks. These risks become increasingly important as the widespread use of information and communications technology and data traffic is becoming the foundation for the functioning of infrastructures underlying the energy systems. | August 2016 |
| Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [the EU Cybersecurity Act] | 2019 | The EU Cybersecurity Act revamps and strengthens the EU Agency for cybersecurity (ENISA) and establishes an EU-wide cybersecurity certification framework for digital products, services, and processes.<br>The EU Cybersecurity Act introduces for the first time an EU-wide cybersecurity certification framework for ICT products, services, and processes. Companies doing business in the EU will benefit from having to certify their ICT products, processes, and services only once and see their certificates recognized across the European Union. | June 2019 |

Source: Own elaboration on the basis of *Energy Networks and Smart Grids. Cyber Security for the Energy Sector*, European Cyber Security Organisation (ECSO), November 2018, pp. 7-8; *Study on Cybersecurity in the energy sector of the Energy Community – Final Report*, Blueprint Energy Solutions GmbH, December 2019, p. 22; *The Directive on security of network and information systems (NIS Directive)*, European Commission, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive [2020-04-28]; *2nd Interim Report. Recommendations for the European Commission on Implementation of a Network Code on Cybersecurity*, Smart Grid Task Force Expert Group 2 on cybersecurity, July 2018, p. 3; *The EU Cybersecurity Act*, European Commission, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act [2020-04-28].

In terms of energy networks, the Clean Energy Package addresses digital challenges such as renewable energy, decentralized power generation, decentralized storage, and prosumerism. The digitization of all these processes and the growing number of smart appliances connected to the grid will be an important element in achieving climate neutrality.[23]

[23] *CYBERSEC 2019...*, p. 11.

In addition to network issues, the Clean Energy Package introduces an obligation for the Member States to implement smart meters. Some European countries, for example Germany, are already advanced in this process. In the case of Poland, this matter has been neglected until the EU regulations forced the implementation of smart meters. These are important elements in the construction of the EU's internal energy market, in line with the concept of active end-users and energy communities. Among other things, measures have been proposed on cybersecurity for smart meters, highlighting the particularly important role of DNOs and TSOs.[24]

The assumptions of the Clean Energy Package include the establishment of a modern project for the EU electricity market, adapted to new market realities, i.e. more flexible, customer-oriented, and better prepared to integrate a greater share of distributed energy sources. Ensuring the cybersecurity of critical infrastructure in the energy sector is intended to guarantee the stability of the European single energy market, which is also intended to enhance EU-wide energy security more broadly.[25] Market developments, in particular, will affect the distribution network operators (DNOs), who will become responsible for integrating local resources in the energy system in the form of RES, energy storage, and demand side response (DSR). Consequently, the obligations of electricity operators to contribute to the development of resilience in the energy sector concerning the risk of malicious cyberattacks or incidents related to information and operational technologies widely used in the electricity sector have been identified.[26]

With regard to energy markets, the Clean Energy Package also pays much heed to flexibility services, although it does not explicitly define flexibility. These services are provided to DSOs, i.e. in relation to networks at medium and low voltage levels. From Poland's perspective, a significant challenge is certainly the issue of financing new investments and the return of expenditures on additional technologies and

[24] Council of European Energy Regulators, CEER Cybersecurity Report on Europe's Electricity and Gas Sectors, 26 October 2018, pp. 12-13.

[25] *Study on Cybersecurity in the energy sector of the Energy Community – Final Report*, Document no. FINR-CS-EC-211019, Blueprint Energy Solutions GmbH, December 2019, p. 3.

[26] Council of European Energy Regulators, *CEER Cybersecurity Report*…, pp. 12-13.

innovative solutions. The initial phase of implementation of elements related to flexibility is associated with high costs, which result from:

- equipping the network with additional devices to monitor its operation status,
- implementing IT systems that process information in order to decide whether or not to use flexibility services,
- ensuring communication with remotely controlled network elements, with a high level of certainty,
- the increasing rate of growth of diverse data, which entails the need to have adequate hardware resources to store it and mechanisms to ensure high security of this data.[27]

The Clean Energy Package contains provisions indicating the need to protect the energy infrastructure against cyberattacks, inter alia, in the form of an obligation for each new low-carbon technology to identify cyber threats, as well as the creation of technical rules such as network code on cybersecurity to protect renewable sources.[28] The proposed grid codex can enable market-based cybersecurity experts to choose the appropriate standards and measures for cybersecurity to ensure coherent and effective action.[29] The implementation of such a code aims to provide elements designed for cybersecurity in the energy sector, including the creation of an early warning system for the energy sector, building cross-border risk management, and developing security requirements for critical infrastructure components.[30]

## 3. Cybersecurity in the Polish energy sector

Over the last decade, electricity infrastructures have undergone profound changes, characterized by a transition from a system where fossil fuel-based production adapts to consumer consumption to a system that has to manage the different types of users connected to it – generators, consumers, and prosumers. This model of increas-

[27] E. Mataczyńska, 'Lokalne rynki usług elastyczności – droga do implementacji', *EPI's Analysis*, no. 1, 2020, https://www.instytutpe.pl/wp-content/uploads/2016/01/Analiza-IPE-nr-1-2020.pdf, p. 4 [2020-04-28].

[28] A. Barichella, *Cybersecurity in the Energy Sector…*, pp. 32-33.

[29] Council of European Energy Regulators, C*EER Cybersecurity Report…*, pp. 12-13.

[30] *Study on Cybersecurity…*, p. 3.

ingly complex infrastructure requires appropriate management, optimization, and monitoring,[31] which is enabled by information and communication technologies allowing more flexible and efficient use of electricity, better control of network use, and more precise control of energy systems.[32] In this way, technologies also lead to more efficient energy consumption. For consumers, demand response services are emerging to optimize their consumption, for example, by reducing or changing their electricity consumption during peak periods. These services rely on interconnected smart devices such as sensors and actuators, widely used in households to measure energy consumption and reduce the consumption of energy devices to prevent overload.[33] Due to cost reductions, these technologies are rapidly spreading, also in Poland – the visualization of the recent changes is presented in table 1. As a result, all these elements are leading to massive digitization of the energy sector. Thus, cybersecurity is becoming increasingly important, and cyberattacks are considered a high risk for the energy sector.[34]

**Table 2. Increase of distributed energy in Poland**

| | 2018 | 2019 | Change |
|---|---|---|---|
| No. of micro-installations | 54,214 | 155,626 | 187% |
| No. of prosumers | 69,246 | 149,308 | 116% |
| Volume of electricity injected by prosumers into the grids [MWh] | 130,370 | 324,333 | 149% |

Source: own elaboration on the basis of *Rekordowy rok dla fotowoltaiki*, URE, 11 March 2020, https://www.ure.gov.pl/pl/urzad/informacje-ogolne/aktualnosci/8771,Rekordowy-rok-dla-fotowoltaiki.html [2020-04-28]; 'URE: Liczba prosumentów wzrosła r/r do 149 308 na koniec 2019 r.', *WysokieNapięcie.pl*, 12 March 2020, https://wysokienapiecie.pl/feeds/ure-liczba-prosumentow-wzrosla-rr-do-149-308-na-koniec-2019-r/ [2020-04-28]; *ME: Liczba mikroinstalacji w Polsce wzrasta*, Ministerstwo Aktywów Państwowych, 21 October 2019, https://www.gov.pl/web/aktywa-panstwowe/liczba-mikroinstalacji-w-polsce-wzrasta [2020-04-28].

At the same time, the increasing digitization is contributing to the vulnerability of the energy sector to cyberthreats. A cyberattack may disrupt the overall functionality or cause specific damage to critical infrastructure. Particularly at risk of cyberattacks are systems associated with operational technology (OT), supervisory control and data

[31] *Energy Networks and Smart Grids…*, p. 3.
[32] C.W. Draffin, *Cybersecurity…*, pp. 2-4.
[33] *Energy Networks and Smart Grids…*, p. 3.
[34] *Energy Insight: Cybersecurity…*

acquisition systems (SCADA), and Programmable Logic Controllers (PLCs), as they are most often connected to the internet. SCADAs control complex industrial processes, including manufacturing, centralized monitoring, and control of distributed meters and sensors. They are responsible for the correct and safe course of the process, controlling complex industrial processes.[35] A cyberattack on such systems may result in business disruption, loss of information, loss of revenue, and destruction of assets and shareholders' property. Cyberattacks can also use remote access to interrupt or disrupt operations and cause physical damage to equipment or even the entire power generation unit. A simple control device that can be used as a portal is sufficient to take over a device without authorization.[36] Therefore, the absolute safety of such control systems is a priority.

The magnitude of a cyberattack's consequences increases in line with the use of ICT and new data interfaces, such as new connection-oriented meters, collectors, and other smart devices that offer new entry points for attackers. Energy systems are potentially high-impact targets, e.g. leading to serious disruptions in supply, allowing the acquisition of confidential information or data on private customers, utilities, and external partners.[37] The combination of distributed energy resources increases the complexity of the digital structure and the size of the attack, and will, therefore, require more intensive protection of the infrastructure.[38] Moreover, a study carried out by the European Union Agency for Cybersecurity (ENISA) shows that energy is one of the three sectors, alongside finance and ICT, where the costs of cybersecurity incidents are highest.[39]

Given the complexity of energy structures, which has been stressed many times, it is necessary to realize that it is not possible to protect this sector fully against cyberattacks. Therefore, in addition to preventive measures, tools should be developed to detect the sources of the attack and recover the system quickly, as well as minimize the con-

[35] A. Kozłowski, 'Cyberbezpieczeństwo w sektorze elektroenergetycznym', *Sektor Elektroenergetyczny*, no. 1, 2019, p. 120.

[36] *Cyber security: A growing threat…*, p. 2.

[37] *Energy Networks and Smart Grids…*, p. 3.

[38] C.W. Draffin, *Cybersecurity…*, pp. 2-4.

[39] *Energy Networks and Smart Grids…*, p. 3.

sequences of such incidents.[40] In addition, the importance of public-private partnerships and sharing responsibility for protecting critical systems from cyberattacks is emphasized in order to strengthen cybersecurity in the energy sector.[41]

Due to the growing importance of cybersecurity, not only in the energy sector but for the entire economy, it is treated as one of the priorities of state security, as defined in the "National Cyber Security Policy Framework of the Republic of Poland for 2017-2022". However, this document stresses that the responsibility for ensuring the cybersecurity of services lies primarily with the providers. The role of the government has been defined mainly in the form of support to build cybersecurity capabilities and competencies and help in responding to serious incidents of cross-sectoral nature.[42] In addition, energy generation has been identified as one of the most important economic sectors due to its centrality in the continuity of the state's functioning, ensuring the security of citizens and the uninterrupted operation of industrial control systems, as expressed in the Resolution on the Polish CyberSecurity Strategy.[43]

However, it should be emphasized that in Poland the issues of cybersecurity in the energy sector have been neglected for a very long time. One possible explanation is the fact that there are not many attempts at attacks in this sector, as presented in Figure 1. Until recently, there was no institution at the strategic or operational level which would be responsible for cybersecurity issues in this sector.[44] Only in 2016 did the Polish Energy Networks establish the Computer Emergency Response Team (CERT), whose main task is to update information on threats to IT security, provide support in the event of an information security incident, and cooperate with companies from the energy sector and government institutions.[45] In view of these facts, it

[40] C.W. Draffin, *Cybersecurity…*, pp. 2-4.

[41] *Multiyear Plan for Energy Sector Cybersecurity*, U.S. Department of Energy, March 2018, p. 4.

[42] Ministerstwo Cyfryzacji, *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*, Warszawa, 2017, pp. 12-13.

[43] Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, p. 12.

[44] *System bezpieczeństwa cyberprzestrzeni RP*, Ekspertyza NASK/CERT Polska na zlecenie Ministerstwa Administracji i Cyfryzacji, Warszawa, 2015, p. 139.

[45] A. Kozłowski, *Cyberbezpieczeństwo…*, p. 123.

has to be emphasized that Poland has made great progress in recent years. According to the National Cyber Security Index (NCSI), which measures the preparedness of countries to prevent cyber threats and manage cyber incidents, Poland is ranked 23rd place out of 160 countries included in the index.[46] Poland is rated lower in the IMD World Digital Competitiveness Ranking, which measures the capacity and the readiness of economies to adopt and explore digital technologies as a key driver for economic transformation in business, government and wider society.[47] In this ranking, Poland is only 33 out of overall 63 analyzed countries.[48]

**Figure 1. Incidents handled by CERT-Poland in 2018 according to the classification by economic sector**

| Economic sector | Number of incidents |
|---|---|
| Digital infrastructure | 29 |
| Healthcare | 13 |
| Banking | 643 |
| Finance | 62 |
| Energy sector | 20 |
| Transport | 51 |
| Public sector | 85 |
| Waterworks | 2 |
| Other | 2834 |
| Total | 3739 |

Source: own elaboration on the basis of *Krajobraz bezpieczeństwa polskiego internetu. Raport Roczny 2018 z działalności CERT Polska*, NASK/CERT Polska, Warszawa, p. 13.

In 2018 the National CyberSecurity System Act[49] was passed, which implements the EU NIS Directive into Polish law. The Act sets out the most important economic sectors for the functioning of the state,

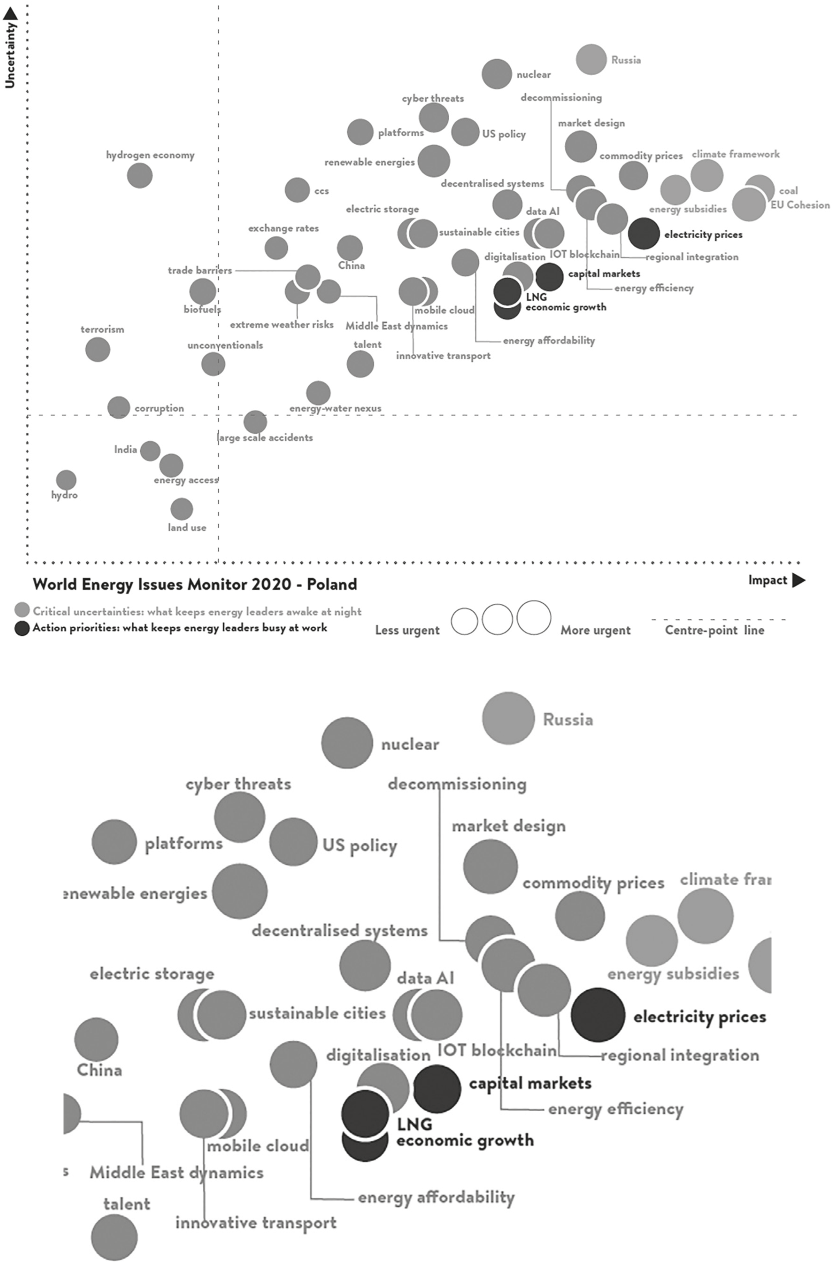
[46] National Cyber Security Index, https://ncsi.ega.ee/country/pl/ [2020-05-04].

[47] IMD World Competitiveness Center, IMD World Digital Competitiveness Ranking 2019, https://www.imd.org/wcc/world-competitiveness-center-rankings/world-digital-competitiveness-rankings-2019/ [2020-05-04].

[48] Ibidem, p. 128.

[49] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. , 2018, item 1560).

**Figure 2. Issues map of the uncertainties and action priorities in implementing the energy transition in Poland**



Source: World Energy Council, *World Energy Issues Monitor 2020*, London, 2020, p. 102.

which also include the energy sector and, following the EU recommendations, indicates the need to designate the so-called key service providers. The document also defines the responsibility for the protection of critical infrastructure, including the energy sector, for the three Computer Security Incident Response Teams, which are run by the Head of the Internal Security Agency (CSIRT GOV), the Minister of National Defence (CSIRT MON) and the National Research Institute (CSIRT NASK). Their tasks include responding and coordinating the handling of incidents reported by critical infrastructure actors (e.g. service providers and infrastructure owners).[50] According to the Act, the competent authority for cybersecurity in the energy sector is the minister in charge of energy (Art. 41).

According to a report by the World Energy Council, in Poland, the greatest threats to the energy sector are seen as macroeconomic and geopolitical issues. They are primarily related to the oil and gas sector and the activities of Russia as demonstrated in Figure 2. The Polish policy towards the domestic energy sector focuses primarily on diversification of both the directions of supply of raw materials, especially natural gas, and energy sources by increasing the use of renewable energy and including nuclear energy in the domestic energy mix. Thus, activities in this area are primarily concentrated on the development of the energy sector, new investments, and modernization.[51]

## Conclusions

The advantage of the digitization process, consisting of the integration of the state energy system, also increases its sensitivity to potential threats from criminal and terrorist activities. Attacks may be motivated by terrorism or may constitute a desire to intercept personal or other sensitive data in order to defraud money or sell on the black market. The sector may also become a field of international provocation, attacks by spying groups, or an element in a hybrid war. There is, therefore, a need to develop elements of protection for systems servicing the

[50] A. Kozłowski, *Cyberbezpieczeństwo…*, p. 123.

[51] World Energy Council, *World Energy Issues Monitor 2020*, London 2020, pp. 102-103.

virtual elements in this sector as it expands. The related challenges include such issues as protection of data flow and storage, attacks aimed at disrupting system operation and causing interruptions in supplies or taking control over the mechanism of energy supply, which constitutes an indispensable element of the communication system in the modern world. It should be borne in mind that an immediate change in the whole system is not possible. The energy transition means that part of the energy infrastructure structures will already be controlled by a high degree of automation, while the remainder will still be using the old system. The energy industry, on the other hand, needs to adopt best practices for cybersecurity and develop a risk management culture. There is also a need for public education and good information policy on the potential risks associated with the use of smart home devices. The necessary human capital should also be remembered – cybersecurity requires qualified teams that understand basic operations, detect and respond to cyber anomalies, reduce the time spent in cyberspace and implement multi-layer cyber defense. The awareness of these issues is crucial for Poland, meaning the political policymakers, energy companies and society, as we are at the very beginning of the long path to the digitization of the energy sector.

## References

Barichella, A., *Cybersecurity in the Energy Sector. A Comparative Analysis between Europe and the United States*, Études de l'Ifri, Paris: Ifri, February 2018.

Council of European Energy Regulators, CEER Cybersecurity Report on Europe's Electricity and Gas Sectors, 26 October 2018.

*Cyber security: A growing threat to the energy sector. An Australian perspective*, Hogan Lovells, March 2016, https://www.hoganlovells.com/en/knowledge/topic-centers/cybersecurity-solutions/~/media/c14b2cc829b04a6e-841237f66882b2df.ashx.

*CYBERSEC 2019. Recommendations & Key Takeaways*, 5th European Cybersecurity Forum – Cybersec, Katowice, 29-30 October 2019.

Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

*Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa: Biuro Bezpieczeństwa Narodowego, 2015.

*Energy Insight: Cybersecurity in the energy sector*, Energy Institute, https://knowledge.energyinst.org/search/record?id=110329.

*Energy Networks and Smart Grids. Cyber Security for the Energy Sector*, European Cyber Security Organisation (ECSO), November 2018.

Goździewicz, W., Krupczyński, M., Kulesza, J. et al., *NATO Road to Cybersecurity*, ed. J. Świątkowska, Kraków: The Kosciuszko Institute, 2016.

IMD World Competitiveness Center, IMD World Digital Competitiveness Ranking 2019, https://www.imd.org/wcc/world-competitiveness-center-rankings/world-digital-competitiveness-rankings-2019/.

Kozłowski, A., 'Cyberbezpieczeństwo w sektorze elektroenergetycznym', *Sektor Elektroenergetyczny*, no. 1, 2019.

Mataczyńska, E., 'Lokalne rynki usług elastyczności – droga do implementacji', *EPI's Analysis*, no. 1, 2020, https://www.instytutpe.pl/wp-content/uploads/2016/01/Analiza-IPE-nr-1-2020.pdf.

Ministerstwo Cyfryzacji, *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*, Warszawa 2017. *Multiyear Plan for Energy Sector Cybersecurity*, U.S. Department of Energy, March 2018.

*National Cyber Security Index*, https://ncsi.ega.ee/country/pl/.

Rice, E.B, AlMajali, A., 'Mitigating The Risk Of Cyber Attack On Smart Grid Systems', *Procedia Computer Science*, no. 28, 2014, https://doi.org/10.1016/j.procs.2014.03.070.

Ruszel, M., Młynarski, T., Szurlej, A., 'The concept of energy transition', in: *Energy Policy Transition – The Perspective of Different States*, eds. M. Ruszel, T. Młynarski, A. Szurlej, Rzeszów: Ignacy Lukasiewicz Energy Policy Institute, 2017.

'Sechs Thesen zur Digitalisierung der Energiewende: Chancen, Risiken und Entwicklungen', German Watch', https://germanwatch.org/sites/germanwatch.org/files/publication/15649.pdf.

Smith, D.C., 'Enhancing cybersecurity in the energy sector: a critical priority', *Journal of Energy & Natural Resources Law*, 36:4, 2018, https://doi.org/10.1080/02646811.2018.1516362.

*Study on Cybersecurity in the energy sector of the Energy Community – Final Report*, Document no. FINR-CS-EC-211019, Blueprint Energy Solutions GmbH, December 2019.

*System bezpieczeństwa cyberprzestrzeni RP*, Ekspertyza NASK/CERT Polska na zlecenie Ministerstwa Administracji i Cyfryzacji, Warszawa, September 2015.

Szulecki, K., Szwed, D., 'Społeczne aspekty OZE: którędy do energetycznej demokracji?', in: *Odnawialne źródła energii w Polsce. Wybrane problemy bezpieczeństwa, polityki i administracji*, eds. K. Księżopolski, K. Pronińska, A. Sulowska, Warszawa: Elipsa, 2013.

Trubalski, A., Trubalska, J., 'Bezpieczeństwo Polski w cyberprzestrzeni', in: *Bezpieczeństwo państwa w cyberprzestrzeni*, eds. J. Trubalska, Ł. Wojciechowski, Lublin: Wydawnictwo WSEI, 2017.

Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U., 2018, item 1560).

Wittpahl, V., *Digitalisierung. Bildung – Technik – Innovation*, iit-Themenband, Berlin: Springer, 2017, https://doi.org/10.1007/978-3-662-52854-9_4.

World Energy Council, *World Energy Issues Monitor 2020*, London, 2020.

Wu, S.S., Liu, C.C., Shosha, A.F. et al., *Cyber Security and Information Protection in a Smart Grid Environment*, Proceedings of the 18th World Congress The International Federation of Automatic Control Milano (Italy) 28 August – 2 September 2011.