MODERN MANAGEMENT REVIEW **2020**
MMR, vol. XXV, 27 (3/2020), p. 75-83 **July-September**

Alicja ŻUKOWSKA[1]

LEGAL CONDITIONS FOR CYBERSECURITY OF THE ENERGY SECTOR

The aim of this paper is to review selected legislative acts governing the protection of the energy sector in terms of cybersecurity. The energy supply system is an area increasingly dependent on IT solutions. Rapid technological progress, interconnectedness between sectors, digitization and automation of energy networks, and finally the construction of the so-called smart networks increase the amount of data collected and, consequently, the need for computerization. Computerization of electricity business exposes the energy system to cyberattacks and incidents that can compromise security of energy supply. We are seeing increased sensitivity of energy infrastructure, and this requires a proper assessment of all threats, including cybersecurity threats, and the creation of tools to prevent and minimize the impact of identified threats.

Keywords: cybersecurity, cyber incidents, energy sector, ENISA

1. INTRODUCTION

The energy sector is one of the first industries that began to use various control solutions on a larger scale, and is currently one of the most computerized. OT (Operational Technologies) systems responsible for monitoring and controlling technological processes play a key role in entities in this sector – such as SCADA (Supervisory Control and Data Aquisition), DMS (Distribution Management System) and EMS (Energy) Management System) in the case of energy. Production installations (e.g. power units at power plants or installations at refineries) are controlled in turn by means of DCS (Distributed Control System) solutions which are comprehensive integrated systems responsible for controlling and visualizing the industrial process. Currently, the energy network is an extensive system of cooperating industrial facilities, consisting of a huge number of computers connected to the network. This significantly increases its vulnerability to cyber attacks. The cyber attack on the Ukrainian power system, which took place on December 23, 2015 is considered to be the first known effective cyber attack on electrical networks. Hackers successfully hacked into the computer systems of three Ukrainian distribution companies and temporarily disrupted the supply of electricity to consumers (Gapiński, 2016).

Attacks on IT systems and automation controlling energy infrastructure are one of the key identified threats that affect the level of national security. Energy networks are

[1] Alicja Żukowska, PhD, The Faculty of Command and Naval Operations, Polish Naval Academy, ul. Inż. J. Śmidowicza 69, 80-127 Gdynia; e-mail: a.zukowska@amw.gdynia.pl. ORCID: 0000--0002-1315-8312.

interconnected, violating their security may have a cascading effect on other sectors of the economy (Eurpean Commission, 2013). A cyberattack on energy infrastructure facilities can have catastrophic consequences not only for property, health of employees, but also for the environment, the entire economy, or even the national security. Given the nature of activities in cyberspace and its aterritorial nature, there is a need for cooperation at transnational level in the field of prevention of electricity crises and crisis management, as they cannot be considered as a purely national task. In this regard, a number of important legislative actions are taken in the European Union. Initially, EU activities in the field of cyberspace protection focused on protecting users, combating illegal content, promoting security activities (European Parliament&Council, 2005), protecting personal data, privacy and consumer rights (European Commission, 2009), and securing the interests of end users of electronic services (European Parliament&Council, 2009). Over time, undoubtedly as a result of attacks aimed at power grid operators, large manufacturing companies, oil pipeline operators and equipment suppliers, actions aimed at ensuring cybersecurity in the energy sector were taken at the EU forum (European Parliament, 2016).

2. MAIN ACTS OF EU LAW ON CYBERSECURITY IN THE ENERGY SECTOR

The first element of the Union's horizontal cybersecurity legislation, developing national cybersecurity capabilities, increasing cooperation at EU level and introducing security obligations and reporting incidents on companies called 'key service operators' is Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6, 2016 on measures for a high common level of security of network and information systems within the Union – the so-called NIS Directive. This document provides for the implementation of cyber security preparedness measures by designated entities, taking into account horizontal guidelines issued by the cooperation group on network and information security established pursuant to Art. 11 of the Directive on network and information security. This cooperation group, composed of representatives of the Member States, the European Union Agency for Cybersecurity (ENISA) and the Commission, has adopted guidelines on security measures and incident reporting. The EU NIS-Directive includes critical sectors in the energy industry, transport, banking, financial market infrastructure, the healthcare sector, drinking water supply and distribution centers and digital infrastructure.

In June 2018, the Network and Information Security Cooperation Group created a special energy intervention area. The activities of EU bodies and institutions aim to ensure that all processes, services and devices connected to the network meet the highest cyber security criteria. This postulate is to be served by the EU certification system, created under the supervision of ENISA. The European certificate is to guarantee that smart devices have been designed with attention to cyber security. A review of the implementation of the NIS directive in individual member states is planned for 2021.

Within Commission Recommendation (EU) 2019/553 of 3 April 2019 on cyber security in the energy sector, the Commission identified the main actions to implement appropriate cyber security preparedness measures in the energy sector. The document indicates the need to expand knowledge and skills related to cyber security in the energy sector. Member States should integrate these issues into their national cybersecurity frameworks, in particular in strategies, laws and regulations. Member States' actions

should aim to ensure that energy network operators and technology providers, in particular key service operators, implement appropriate cyber security related preparedness measures related to real-time requirements in the energy sector. Power grid operators should first and foremost apply the latest security standards for new installations and consider complementary physical security measures when the functioning base of old installations is not sufficiently protected by cybersecurity mechanisms. It was also recommended to implement international cybersecurity standards and relevant specific technical standards for secure real-time communication as soon as relevant products become available on the market, and to include real-time limitation in the overall concept. The Commission indicated that private networks should be considered for IT protection systems to ensure the level of quality of service required for real-time restrictions. When using public communications networks, operators should consider ensuring special bandwidth allocation, delay requirements and security measures for communication. The Commission recommends dividing the entire system into logical zones and specifying time and process restrictions for each of the zones in order to enable appropriate cyber security measures or alternative protection methods to be taken into account. The document indicates that Member States should ensure the implementation of appropriate cyber security preparedness measures related to cascading effects in the energy sector. Power grids and gas pipelines are strongly interconnected throughout Europe, and a cyber attack leading to shutdowns or disruptions in part of the energy system can cause far-reaching cascading effects in other parts of the system. In addition, the need to implement appropriate cyber security preparedness measures related to the combination of existing and state-of-the-art technology in the energy sector was emphasized.

Cybersecurity of energy systems is primarily about securing intelligent networks. Their progressing creation is also associated with the implementation of fifth generation (5G) network technologies as one of the most important factors contributing to the development of future digital services and the priority of the digital single market strategy. Due to the dependence of many critical services on the 5G network, the consequences of systemic and widespread interference would be particularly severe. As a result, ensuring 5G cybersecurity is a strategic issue for the Union at a time when cyberattacks are gaining momen-tum and are becoming more sophisticated. In Commission Recommendation (EU) 2019/534 of 26 March 2019 on Cybersecurity of the 5G network, the Commission adopted an action plan for the 5G network so that the EU could have by 2020 the telecommunications infrastructure necessary to carry out its digital transformation. To this end, Member States should assess the 5G network infrastructure for risk, including the most sensitive components whose security breach would have a significant negative impact. Member States should also review the security requirements and risk management methods applicable at national level to identify threats to cybersecurity arising from technical factors (specific technical parameters of the 5G network) and other factors such as the legal framework and policy framework, to which suppliers of information and communication equipment in third countries are subject.

Another important document for cybersecurity in the energy sector is Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and the certification of cybersecurity in the field of information and communication technologies and the repeal of Regulation (EU) No 526/2013 (Cybersecurity Act). The Regulation significantly strengthened the mandate of the European Union Agency for Cybersecurity in supporting Member States in combating cybersecurity threats and

cyberattacks. This act provides the basis for the creation of a European framework for the certification of cybersecurity for products, processes and services in force throughout the Union, which is of particular importance for the energy sector.

Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on preparedness in the electricity sector and repealing Directive 2005/89/EC lays down common rules on how to prevent, prepare and manage electricity crises. It requires Member States to increase transparency during the preparation phase and during the electricity crisis and to ensure the efficiency and coordination of the actions taken. The Regulation points to the need to properly identify the risks arising from cyber incidents and to adequately reflect the remedies taken to address them in emergency preparedness plans.

Provisions on cybersecurity are also contained in Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market in electricity. It provides that the Commission within the Energy Union is empowered to establish network codes covering m.in. sectoral rules on cybersecurity aspects in cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management.

3. LEGAL REGULATIONS ON THE CYBERSECURITY OF THE ENERGY SECTOR IN POLAND

In the Polish legal system, until 2018 the obligation to protect information systems operating in the energy sector stemmed from the provisions on critical infrastructure. The legal definition of critical infrastructure contained in the Crisis Management Act (Art. 3(2) of The Act of 26 April 2007 on crisis management, Journal of Laws of, item 1398.) includes systems and functionally related facilities, including construction facilities, installations, services critical to state security and its citizens and to ensure the proper functioning of public administrations, as well as institutions and entrepreneurs. The entry into force of the Crisis Management Act has created basic mechanisms for organised protection of critical infrastructure and defined the systems that are part of it.

Accordingly to Article 3(4) of the Crisis Management Act is the protection of critical infrastructure that seeks to ensure the functionality, continuity of operations and integrity of critical infrastructure in order to prevent risks, risks or weaknesses and to reduce and neutralise its effects and to rapidly reproduce that infrastructure in the event of failures, attacks and other events interfering with its proper functioning.

Critical infrastructure security programming documents set out a holistic approach to critical infrastructure protection, including: (1) ensuring physical security, a team of organisational and technical activities aimed at minimising the risk of disrupting critical infrastructure following the actions of persons who have attempted to enter or are in critical infrastructure; (2) technical safety assurance – a set of organisational and technical activities aimed at minimising the risk of disruption of critical infrastructure following a disruption of technological processes; (3) ensuring personal security – a set of organisational and technical activities aimed at minimising the risk of disruption of critical infrastructure following the actions of persons who have the right access to critical infrastructure; (4) ensuring ict security, a set of organisational and technical activities aimed at minimising the risk of disruption of critical infrastructure following an unauthorised impact on control equipment and ict systems and networks; (5) ensuring

legal certainty, a set of organisational and technical activities aimed at minimising the risk of disruption of critical infrastructure following the legal actions of external actors; (6) business continuity and playback plans, understood as a team of organisational and technical activities leading to the maintenance and restoration of functions carried out by critical infrastructure (Council of Ministers, 2018).

Critical infrastructure protection tasks are defined in Article 10. 6 and include: collection and processing of information on critical infrastructure threats; developing and implementing procedures in the event of critical infrastructure threats; restoring critical infrastructure; cooperation between public administrations and owners and owners of self-proclaimed and dependent facilities, installations or facilities of critical infrastructure in the field of its protection.

Owners, independent and dependent holders of critical infrastructure facilities, installations or facilities shall be required to protect them, in particular by preparing and implementing, in accordance with the risks envisaged, critical infrastructure security plans and maintaining their own reserve systems ensuring the safety and maintenance of the operation of that infrastructure until it is fully reproduced.

Today, the importance of cybersecurity can be seen as the foundation for the functioning and security of critical infrastructure. This is due to two factors. Firstly, in Poland, ICT networks are one of the systems belonging to critical infrastructure. Secondly, ICT systems are part of different critical infrastructure systems by supporting and often conditioning their proper functioning.

An important step in the construction of cybersecurity was the adoption of the Law of 5 July 2018 on the national cybersecurity system, which implements the so-called "cybersecurity system". Network and Information Systems Directive (NIS), on network and information security, providing the basis for the creation of a national cybersecurity system (NCS). The national cybersecurity system includes: 1) key service operators; 2) digital service providers; 3) CSIRT MON; 4) CSIRT NASK; 5) CSIRT GOV; 6) sectoral cyber security teams; 7) public finance sector entities referred to in art. 9 points 1–6, 8, 9, 11 and 12 of the Act of 27 August 2009 on public finance (Journal of Laws of 2017, item 2077 and of 2018, items 62, 1000 and 1366); 8) research institutes; 9) National Bank of Poland; 10) Domestic Holding Bank; 11) Office of Technical Inspection; 12) Polish Air Navigation Services Agency; 13) Polish Center for Accreditation; 14) National Fund for Environmental Protection and Water Management and voivodship funds for environmental protection and water management; 15) commercial law companies performing public utility tasks within the meaning of art. 1 clause 2 of the Act of 20 December 1996 on municipal economy (Journal of Laws of 2017, item 827 and of 2018, item 1496); 16) entities providing cybersecurity services; 17) competent authori-ties for cyber security; 18) Single Contact Point for cyber security, hereinafter referred to as the "Single Contact Point"; 19) Government Representative for Cyber Security, hereinafter referred to as "Representative"; 20) College for Cybersecurity, hereinafter referred to as "College", whose composition and operating principles are specified in the Regulation of the Council of Ministers of October 2, 2018 regarding the scope of operation and the mode of work of the College for Cybersecurity. The creation of the NCS is intended to m.in. ensuring the unimpeded provision of key services and incident handling by achieving an adequate level of security for information systems for the provision of those services. The NIS Directive is an example of minimum harmonisation. The Polish legislature has taken advantage of the possibility of more detailed regulation.

The Act introduced an obligation for key service providers, digital service providers and public entities to report incidents (Banasiński, Rojszczak, 2020). The legislator has designated three Computer Security and Incident Response Teams (CSIRTs – a team of IT security experts whose task is to respond to incidents and provide services aimed at ensuring IT security and the possibility of resuming operations after removing the threat.) of a national level with a clearly established range of responsibility. The cooperation mechanisms of the three CSIRTs of the national level in case of the critical incidents and the rules for the supervision of operators of essential services in the various sectors of the economy, who are responsible for identifying operators (on the basis of an administrative decision), preparing recommendations for actions that will strengthen the cybersecurity of the sector, supervision of operators in a given sector, participation in exercises and processing of personal data necessary for the performance of tasks. The key service operator is required to ensure that at least every two years, an audit of the security of the information system used to provide the key service is carried out. The audit may be carried out by: a conformity assessment body accredited in accordance with the provisions of the Act of 13 April 2016 on conformity assessment systems and market surveillance (Journal of Laws of 2017, item 1398 and of 2018, item 650 and 1338), to the extent appropriate for undertaken security assessments of information systems; at least two auditors holding: a) certificates specified in the provisions of the Regulation of the Minister of Digitization of October 12, 2018 on the list of certificates authorizing to conduct an audit (including: Certified Internal Auditor; Certified Information System Auditor; Auditor's certificate the leading in-formation security management system according to PN-EN ISO / IEC 27001 issued by a con-formity assessment body accredited in accordance with the provisions of the Act of 13 April 2016 on conformity assessment systems and market surveillance (Journal of Laws of 2017, item 1398 and from 2018, item 650 and 1338), in the scope of certification of persons; Certifi-cate of the auditor of the leading business continuity management system PN-EN ISO 22301 issued by a conformity assessment body accredited in accordance with the provisions of the Act of 13 April 2016 on systems conformity assessment and market surveillance in the field of certification of persons; Certified Information Security Manager (CISM); Certified in Risk and Information Systems Control (CRISC); Certified in the Governance of Enterprise IT (CGEIT); Certified Information Systems Security Professional (CISSP); Systems Security Certified Prac-titioner (SSCP); Certified Reliability Professional; Certificates entitling to hold the title ISA / IEC 62443 Cybersecurity Expert) or b) at least three years of practice in the field of infor-mation systems security audit, or c) at least two years of practice in the field of audit of in-formation systems security and holding a post-graduate diploma in security audit information systems, issued by an organizational unit which, on the day of issuing the diploma, was entitled, in accordance with separate provisions, to confer a doctoral degree in the economic, technical or legal sciences; sectoral cyber security team, established within the sector or subsector, if the auditors meet the above-mentioned conditions.

It is worth noting the introduction of a formula of a sectoral cybersecurity team, set up by competent authorities, which accepts reports of incidents and helps to handle incidents, but also analyses the impact, develops proposals and cooperates with the relevant CSIRT national level. The Regulation of the Council of Ministers of November 15, 2018 on the types of documenta-tion regarding the cybersecurity of the information system used to provide the key service (Journal of Laws 2018, item 2080), obliges to have documentation

covering normative and operational documentation. The sectoral cybersecurity team can also exchange information about major incidents with other European Union countries.

The Act introduces an obligation to prepare a five-year Cybersecurity Strategy of the Republic of Poland, which sets strategic objectives and appropriate policy and regulatory measures to achieve and maintain a high level of cybersecurity. Strategic and political coordination over the cybersecurity system in Poland is carried out by the Representative and the College for Cybersecurity.

The National Cybersecurity System Act provides for the adoption of a number of implementing acts allowing for the full implementation of its provisions. The Regulation of 10 September 2018 on organisational and technical conditions for cybersecurity service providers and the internal organisational structures of key cybersecurity service providers (Journal of Laws of 2018, item 1780) obliges the cybersecurity service provider to create certain organisational conditions, including:

1) to have and maintain a information security management system meeting the requirements of the Polish Standard PN-EN ISO/IEC 27001;
2) ensuring the continuity of the incident response service, consisting in taking action in the recording and handling of events affecting the security of information systems in accordance with the requirements of the Polish Standard PN-EN ISO 22301;
3) holding and making available in Polish and English a declaration of its policy of action in the scope of the document specified by the Internet Engineering Task Force (IETF);
4) provide support to the key service operator 24/7 all days of the year, with response time appropriate to the nature of the key service;
5) the disposal of personnel with skills and experience in identifying risks with regard to information systems, (b) analysing the malware and determining its impact on the information system of the key service operator, (c) securing forensic traces for law enforcement proceedings.

The Regulation in question also sets out the minimum standards to be met by technical safeguards adequate to the carried out risk assessment of premises, which are to be at the exclusive disposal of cybersecurity service providers and the internal organisational structures of key cybersecurity service providers. The requirements are also formulated as regards technical equipment, including:

1) (a) automatic recording of incident reports, (b) analysis of software code deemed harmful, (c) examination of the resilience of information systems to compromise, (d) securing forensic traces for law enforcement investigations;
2) communication measures enabling the exchange of information with the entities for which they provide services and the competent Computer Security Incident Response Team operating at national level.

The Regulation of the Council of Ministers of 11 September 2018 on the list of essential services and materiality thresholds for the disruptive effect of the incident for the provision of essential services (Journal of Laws of 2018, item 1806) sets out a list of the key services and the materiality thresholds of the incident-distorting effect for the provision of key services. Key services in the energy sector have also been grouped by subsectors: mining of mines, (extraction of natural gas, extraction of oil, extraction of lignite, coal mining, copper extraction), electricity (electricity generation, electricity transmission, electricity distribution, electricity marketing, electricity storage, system

services, quality and management of energy infrastructure), heat (heat generation, heat marketing, heat transfer, heat distribution), crude oil (liquid fuel generation, oil transmission, liquid fuel transmission, storage of crude oil, oil transhipment, storage of liquid fuels, transhipment of liquid fuels, marketing of liquid fuels or marketing of liquid fuels from abroad, production of synthetic fuels), gas (production of gaseous fuels, gaseous fuel transmission, marketing of gaseous fuels and marketing of natural gas from abroad, transmission of gaseous fuels, distribution of gaseous fuels, storage of gaseous fuels, liquefaction and regasification of Liquid Natural Gas and importing and loading), supply and services to the energy sector (supply of systems, machinery, equipment, materials, raw materials and provision of services to the energy sector), other services provided by supervised and subordinate entities (production of radiopharmaceuticals, management of radioactive waste, maintenance of strategic reserves and stocks of oil, petroleum and natural gas products, Research & Developments or implementation or technological research for the energy sector).

The Regulation also sets out the materiality thresholds for the disruptive effect of an incident for the provision of a key service, which include the following indicators: the number of users dependent on the key service provided by the entity concerned, the dependence of other sectors on the service provided by that entity, the impact that the incident, in terms of scale and duration, could have on economic and social activities or public security, the share of the principal service provider in the market, the geographical coverage associated with the area to which the incident might be affected, the entity's ability to maintain a sufficient level of provision of a key service taking into account the availability of alternative means of provision, other factors specific to the subsector concerned.

The Regulation of the Council of Ministers of 31 October 2018 regarding the thresholds for recognizing an incident as serious (Journal of Laws of 2018, item 2180) sets out the thresholds for the classification of the incident as serious by type of event in the various sectors and subsectors defined by the National Cybersecurity System Act.

On the basis of the provisions of the Law on the National Cybersecurity System on October 22, 2019 the Council of Ministers adopted a resolution on the Cybersecurity Strategy of the Republic of Poland for the period 2019-2024 (Resolution No. 125 of the Council of Ministers of October 22, 2019 on the Cybersecurity Strategy of the Republic of Poland for 2019–2024, M.P., item 1037). The National Cybersecurity Strategy of the Republic of Poland points to the need to increase the cybersecurity of key and digital services and critical infrastructure, especially with regard to information technology and industrial control systems. Their smooth operation is crucial for the proper functioning of economic sectors, especially the energy sector.

4. CONCLUSION

The legislator recognises at both EU and national level the importance of the energy sector and takes into account the need to protect it, including its cybersecurity. Changes in Polish legislation will significantly improve the protection of the energy sector against cyberattacks, as, unlike the rules on protection of critical infrastructure, cybersecurity regulations are moving away from the concept of sanction-free protection of key sectors for the functioning of the state, citizens and economy. However, it is important to be aware that the EU and Polish legislators must monitor on an ongoing basis the changes

that are taking place in the cyberspace environment and respond to emerging threats on an ongoing basis.

REFERENCES

Gapiński, K. *Blackout w zachodniej Ukrainie – cyber atak o wymiarze międzyn*arodowym, styczeń 2016 [Access: 12.04.2020 r.]. Access on the internet: https://pulaski.pl/komentarz-blackout-w-zachodniej-ukrainie-cyber-atak-o-wymiarze-miedzynarodowym.

Banasiński, C., Rojszczak, M., red. (2020). *Cyberbezpieczeństwo*. Warszawa.

LEGAL ACTS

European Parliament & Council, Decision 854/2005/EC of the Parliament and of the Council of 11 May 2005 establishing a multiannual program for the promotion of safer software with the Internet and new network technologies.

European Commission, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for enforcing consumer protection legislation.

European Parliament & Council, Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22 / EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58 / EC concerning the processing of personal data and protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for enforcing consumer protection legislation.

European Commission (2013), Commission Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union, [online] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013PC0048

European Parliament (2016), Cybersecurity strategy for the energy sector, [online] http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf

Council of Ministers, National Critical Infrastructure Protection Program, consolidated text based on Resolution No. 121/2018 of the Council of Ministers of September 7, 2018 amending the resolution on the adoption of the National Critical Infrastructure Protection Program.

DOI: 10.7862/rz.2020.mmr.23

The text was submitted to the editorial office: May 2020.
The text was accepted for publication: September 2020.