Articles

Studia Iuridica Lublinensia vol. XXX, 4, 2021
DOI: 10.17951/sil.2021.30.4.333-351

Wojciech Konaszczuk
Maria Curie-Skłodowska University in Lublin, Poland
ORCID: 0000-0003-0364-0727
wojciech.konaszczuk@ umcs.pl

Cybersecurity Threats in the Sectors of Oil, Natural Gas and Electric Power in the Context of Technological Evolution

Zagrożenia cyberbezpieczeństwa sektora ropy naftowej, gazu ziemnego i energii elektrycznej w kontekście ewolucji technologicznej

ABSTRACT

The announcement of the state of global COVID-19 pandemic, in addition to the negative health, economic and social phenomena, has triggered a massive phenomenon of transferring most aspects of human life to cyberspace. The last decade has shown a geometric progression of the growth of cybersecurity incidents worldwide, including the energy sector. This paper is a conceptual work, while the basic research problem refers to the determination of the level and area of cybersecurity regulation of the energy sector in the supranational, EU and national systems. The fundamental thesis is to confirm the initial assumption of insufficient degree of legal protection of the network, both in the systems of international and internal law. The main purpose is to demonstrate critical legal solutions that will result in the future in critical and serious incidents in the energy supply chain, as well as energy logistics. The originality of the study is associated with the attempt to compile separate legal systems, the subject of regulation of which is cybersecurity of the energy sector. The cognitive value for practice is associated with the indication of a unified conceptual grid and the indication of the main regulations of the issue.

Keywords: cyberspace; cybersecurity of the energy sector; legal systems; technological evolution

CORRESPONDENCE ADDRESS: Wojciech Konaszczuk, PhD, Dr. habil., Professor Associate, Maria Curie-Skłodowska University (Lublin), Faculty of Law and Administration, Institute of Law, Plac Marii Curie-Skłodowskiej 5, 20-031 Lublin, Poland.

INTRODUCTION

On 11 March 2020, the World Health Organization (WHO) declared the start of the state of global COVID-19 pandemic, which has resulted in historic, multi-faceted changes in all sectors of the legal, social, cultural and economic life of countries, members of the international community. One of the consequences of the global pandemic is undoubtedly the reduction in people-to-people contacts resulting from the need to reduce the spread of the virus. As a result, it has become natural to move life in an uncontrolled way to ICT networks, starting with the need to perform work remotely around the world, through learning or even medical consultations. Fears of loss of life and health have forced unregulated access to a variety of IT tools. They have thus contributed to the significant infiltration of the network by the computer crime world, thus endangering strategic sectors of the economy in this energy sector.

The aim of this study is (a) discussion of selected international-law solutions in the field of cybersecurity of the energy sector, (b) presentation of normative solutions for cybersecurity in the European Union, and (c) brief outline of the Polish aspects of the issue.

The basic hypothesis that will be proven in the study is to conclude that legal normativism in the context of regulating energy sector cybersecurity issues in the world is detached from reality and we should be inclined towards solutions operating within the common law system. The summary will show the flaws and shortcomings of transnational solutions, which will then result in internal regulations that duplicate these shortcomings.[1] The study used legal-dogmatic, comparative and statistical methods.

OUTLINE OF THE CONCEPTUAL GRID OF THE SUBJECT

To facilitate the understanding of the discussed issue, it seems appropriate, at least to the extent necessary, to clarify concepts that may cause difficulties of interpretation in the sense that they belong to the IT terminology that has been implemented into the language of social sciences. Reference should first be made to the definition of "cybersecurity". The very concept of "cybersecurity" has evolved in the past and is a consequence of the emergence of "cybercrime". Thus, in order to understand the effects of the phenomenon of cybercrime, it is necessary to discuss it, even incidentally. The emergence of cybercrime requires the existence of a tool

[1] For more on cybersecurity in the context of the latest Polish national regulations, see M. Karpiuk, *Organisation of the National System of Cybersecurity: Selected Issues*, "Studia Iuridica Lublinensia" 2021, vol. 30(2), pp. 233–244; K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The Legal Status of Public Entities in the Field of Cybersecurity in Poland*, Maribor 2021, p. 98.

that can be used to commit a crime: a computer, software, a network and a human factor. The very concept of a computer is rather difficult to define. The professional literature on the subject considers a computer to be a machine capable of processing any data through a specific algorithm. This operation is characterised by processing data by means of a set of instructions, i.e. a programme. In turn, according to Georges Ifrah, a historian and mathematician, a computer is an automaton composed of an input and output device, a memory, a central unit performing all kinds of transformations of data expressed in the form of character strings (which are material representations of coded information), which allows, within the physical limits of the machine, to perform any symbolic type of calculation (and therefore to solve any task whose solution can be expressed as an algorithm) under the direction of a control unit which operates in accordance with a program stored in memory (and therefore treats instructions in the same way as the data to be processed).[2]

One of the first machines that may be considered a computer was an IBM product called the IBM ASCC (Automatic Sequence Controlled Calculator), which was a computing machine known as the Mark 1, which was designed by Howard Hathaway Aiken.[3] Subsequent versions of this product over the following decades revolutionised the development of computing globally. The turning point in the development of the world wide web was the idea that desktop computers should be linked together to increase their computing power. This gave rise to a computer network that allowed information to be transmitted between devices. In September 1969, the first nodes of a network known as ARPANET (Advanced Research Project Agency Network) used for research for the US Army were launched at this university. The ARPANET was intended to create a network that would allow communication between computers without a central unit (server). This was to guarantee the effectiveness and security of information exchange in the event of war, even if some part of it was damaged. During its development, the ARPANET network originally used many versions of protocols related to the identification of computers. The unification took place only at the beginning of the 1980s, thanks to Jonathan Bruce Postel,[4] who in 1982–1983 laid the foundations for linking the IP (addressing) protocol with hierarchically built Internet domain names – DNS (Domain Name Servers). The DNS allows the assignment of numerical addresses to names. This process was crowned by the adoption of TCP/IP and DNS as standards of the world wide web in the US Army.

[2] See J. Dauben, *Book Review: The Universal History of Numbers and The Universal History of Computing (part 1)*, "Notices of the AMS" 2002, vol. 49(1).

[3] In more detail, see I. Bernard Cohen, *Howard Aiken: Portrait of a Computer Pioneer*, Cambridge 1999, pp. 73–114.

[4] Jonathan Bruce Postel (1943–1988) – lecturer at the University of California, Los Angeles (UCLA), creator of many innovative solutions, including the first electronic mail protocol SMTP (Simple Mail Transfer Protocol).

One of the first described cases of cybercrime occurred in the early 1980s. In 1983, Kevin Mitnick, an American national, obtained unauthorized access to the ARPANET network, for which he was sentenced to a 6 months imprisonment.[5] It is one of the first instances of a cybercrime offence using a computer for which a custodial sentence was imposed. Thus, the prohibited act committed by Mitnick started the era of cybercrime. The importance of the problem is evidenced by the fact that between 11 and 17 April 2000, the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders was held in Vienna, during which a definition of cybercrime was formulated. According to the adopted definition in the broad sense, these are all activities of an illegal nature committed with the use of computers and affecting computer systems or networks. On the other hand, the concept of cybercrime in the strict sense covers activities against the security of computer systems or database software.[6]

Cybercrime, which emerged as a spontaneous phenomenon, resulted in an effect of an opposite pole in the form of cybersecurity as a natural necessity to prevent, counteract and eliminate the consequences of computer offences.[7]

According to the currently developed practice, there are many uniform definitions of the concepts of cybersecurity. However, it is worth pointing to the definition developed in the longest functioning cybersecurity institution, namely the American CISA (Cybersecurity & Infrastructure Security Agency), according to which "Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information".[8] This quite broad definition has some vague elements that allow the definition to be interpreted quite freely. On the other hand, the definition that has been developed in Polish law, which was included in the Act of 5 July 2018 on the national cybersecurity system,[9] has a closed character. Pursuant to Article 2 (4) of this Act, cybersecurity is "the resistance of information systems to activities that violate the confidentiality, integrity, availability and authenticity of the data processed or related

[5] B. Gengler, *Super-hacker Kevin Mitnick takes a plea*, "Computer Fraud & Security" 1999, no. 5.

[6] United Nations, *Report of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, Vienna, 10–17.04.2000, https://digitallibrary.un.org/record/432663/files/A_CONF.187_15-EN.pdf [access: 17.07.2021]. On cybercrime in more detail, see W. Konaszczuk, *Legislacyjne rozwiązania w zakresie przeciwdziałania cyberprzestępczości w prawie podatkowym*, Warszawa 2018.

[7] A particular role is currently played in this field by special services. In the Polish practice, these powers are generally exercised by counter-intelligence services. In more detail, see M. Karpiuk, *Zakres działania służb specjalnych*, [in:] M. Bożek, M. Czuryk, M. Karpiuk, J. Kostrubiec, *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe*, Warszawa 2014, pp. 62–104.

[8] *Security Tip Report (ST04-001)*, 6.05.2009, https://us-cert.cisa.gov/ncas/tips/ST04-001 [access: 14.07.2021].

[9] Journal of Laws 2020, item 1369, hereinafter: ANCS.

services offered by these systems".[10] The term "information system"[11] raises doubts for the simple reason that, for example, the theft of data in the form of a banking system client's login and password does not relate to an "information system" but undoubtedly, also in the light of the CISA definition, constitutes a breach of cybersecurity. Hence, it is appropriate to use the concept of incident and critical incident introduced by the Polish legislature. An incident should be understood as "an event that has or may have an adverse impact on cybersecurity" (Article 2 (5) ANCS), while a critical incident is "an incident resulting in significant damage to public security or order, international interests, economic interests, activities of public institutions, civil rights and freedoms, or human life and health, classified by the competent CSIRT MON, CSIRT NASK or CSIRT GOV" (Article 3 (6) ANCS).

The basic threats to ICT systems in the world include information leakage, malware, phishing, or the use of social engineering methods to the victim. Malware is the use of an intrusive or harmful type of software that accesses a device without the user's knowledge in order to infect or obtain data on disks or server arrays. These include, among others: viruses, Trojan horses, worms, ransomware. Phishing, on the other hand, is a fraud method that involves impersonating the identity of another person or institution in order to obtain specific information in the form of login details or credit card information. Social engineering, in turn, serves to achieve specific goals through manipulation and is currently one of the most dangerous cybercrime tools.[12] In the group of ICT threats mentioned, one can also indicate subgroups occurring in them: (D)Dos attacks,[13] malware infection via LAN or WAN,[14] malware infection via

[10] It should be pointed out that, apart from special services within the national security system, a specific role is played by uniformed services, such as the Police, Military Police, etc., as well as local government. In more detail, see M. Czuryk, *Właściwość Ministra Spraw Wewnętrznych oraz Ministra Obrony Narodowej w dziedzinie bezpieczeństwa publicznego*, [in:] *Prawo bezpieczeństwa publicznego*, eds. M. Karpiuk, K. Walczuk, Warszawa 2013, p. 62 ff.; J. Kostrubiec, *The Role of Public Order Regulations as Acts of Local Law in the Performance of Tasks in the Field of Public Security by Local Self-government in Poland*, "Lex localis – Journal of Local Self-Government" 2021, vol. 19(1), pp. 111–129.

[11] The definition of information system for the purposes of the Polish regulation has been contained in Article 2 (14) ANCS, and pursuant to it an information system is an "ITC system referred to in Article 3 (3) of the Act of 17 February 2005 on the computerization of operation of entities which perform public tasks (Journal of Laws 2020, items 346, 568 and 695), together with the data electronically processed therein". The above-mentioned incidental doubts relate to non-public entities.

[12] Access data, i.e. logins and passwords, are often obtained by engineering methods. Most often, it involves "impersonating" individuals or institutions or creating a chain of trusted, interconnected people. Such persons induce the employee to provide certain information. As a result, this most often leads to loss of confidentiality of important data and is an important element in the chain of the cyber-attack. Attacks can be conducted electronically, by telephone or in person.

[13] Distributed denial of service.

[14] This includes malware distribution within the Local Area Network or the Wide Area Network.

storage media,[15] hacking by remote access devices, attack against software supply chains, APT-Advanced persistent threat. A particular threat to cybersecurity, due to the underestimation of its potential, is the platform of attacks related to the use of portable storage media as a device. Researchers from Ben Gurion University in Israel made a list of 31 types of threats related to USB storage devices and divided them into four subgroups: a) exploiting flaws in the normal communication of operating systems with USB protocols; b) placing a malware download code in USB boot files; c) attack with use of USB microcontroller; d) programmable electrical attack when connected device triggers the charge/discharge cycle.[16]

The development of the skills and techniques described above is clearly expansive. The expansiveness is directly proportional to the number of network participants and the amount of capital flowing through the network, including virtual currencies.

ENERGY SECTOR CYBERSECURITY IN THE INTERNATIONAL SYSTEM

It is first necessary to systematise and establish the place of cybersecurity in the international hierarchy. In the sphere of international relations, an area much broader than international law, energy security appears alongside the three traditional pillars of sustainable development expressed in economic prosperity, development of societies and biodiversity. It should be clearly emphasized what is forgotten in today's theory and practice of international energy security, that originally the concept of energy security was associated with the embargo on oil supplies to the Western Hemisphere in 1973.[17] The definition of energy security appears in the literature and in international documents in various contexts.[18] As regards inter-

[15] Portable memory devices are becoming a growing source of potential threat. Removable devices include: USB memory, SD card, MMC, SIM, CD, DVD. Mobile removable devices include: smartphones, PDAs, tablets. Removable devices can easily introduce malware when used uncontrollably. One example is the lack of restrictions on the use of USB ports in computer stations.

[16] *Malboard: New Computer Attack Mimics User's Keystroke Characteristics and Evades Detection*, 5.06.2019, https://in.bgu.ac.il/en/Pages/news/Malboard.aspx [access: 14.07.2021].

[17] A kind of obsession with energy security in the context of the supply of energy carriers is described quite broadly in American literature. It takes a form that goes far beyond issues of domestic law, international law or economic relations, and enters the sphere of philosophy. A striking example is the introduction of concepts relating to "gas weapon" or "fuel weapon" into the world politics of countries. See more in J. Taylor, P. Van Doren, *Energy Security Obsession*, "Georgetown Journal of Law & Public Policy" 2008, vol. 6(2), pp. 475–486.

[18] An example of an unconventional approach to energy security is the thesis presented by Matthew F. Smith and Naing Htoo (*Energy Security: Security for Whom*, "Yale Human Rights and Development Law Journal" 2008, vol. 11, pp. 217–235). These researchers formulated the concept of the impact of energy security on human rights using the example of Burma. They pointed out that achieving a stable level

national cooperation, issues related to energy security in the broad sense are well regulated. Among the systems of energy security protection, the universal system, such as the UN system, and regional systems can be distinguished. The leading organization of the universal system is the International Energy Agency (IEA). The establishment of the IEA in 1974 was a deliberate response to the first fuel crisis, formulated on 11–13 February 1974 at the Washington Conference convened to address energy problems.[19] The organization was established by a decision of the OECD Council adopted on 15 November 1974. The organization currently brings together 29 countries, including Poland.[20] It is natural that digitalization of life caused a natural transfer of the energy security sphere to the network as well.

Undoubtedly, cybersecurity of the energy sector will belong to the field of international energy security. The universal character of cybersecurity requires that regulations in this field of a supranational nature be treated as universal solutions.

First of all, in the global aspect, the recommendations of the IEA in the field of cybersecurity should be taken into account.[21] One of the newest solutions in the field of cybersecurity in the electric power sector was developed during the congress on cyber threats held on 28–31 January 2020 in Paris. This was the basis for a report prepared in 2021 which has set the assumptions and goals of network security for the years to come.[22] The preamble to the report indicates that the governments of

---

of energy security would clearly and directly impact the erosion of human rights in developing and least developed countries. In contrast, the International Energy Agency defines energy security as "ensuring the uninterrupted availability of energy sources at an affordable price". One could argue with such a statement for the simple reason that acceptability of price is determined by many factors, including the state and degree of security, the state of legal obligations and the situation of the global energy price market. It has often been the case, particularly during the fuel crisis, that countries have been forced to accept the price in the absence of other solutions. See more in International Energy Agency, *Energy security Reliable, affordable access to all fuels and energy sources*, www.iea.org/topics/energysecurity [access: 14.07.2021].

[19] The main initiative for taking action in response to the crisis of 1973–1974 was undertaken by the US side, represented by Secretary of State Kissinger, who in his address delivered at the Pilgrims Society on 12 December 1973 in London pointed to the need for cooperation between European states and the United States in the global oil trade. He explicitly stressed that the crisis was not only the result and product of the Arab–Israeli war, but also an inseparable consequence of the rapid growth of global demand for oil supplies. In more detail, see USA Documents, Public Affairs Office, *United States Mission to the European Communities*, 1973, no. 61, p. 8 ff.

[20] Poland has been a full member of the organization since 25 September 2008. Other members of the organization are: Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, South Korea, Luxembourg, the Netherlands, New Zealand, Norway, Portugal, Slovakia, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States. See more in International Energy Agency, *Member countries*, www.iea.org/countries/membercountries [access: 12.07.2021].

[21] More on energy security in W. Konaszczuk, *Prawnomiędzynarodowe aspekty obrotu ropą na świecie,* Lublin 2017, pp. 185–229.

[22] *Cyber Security in Energy Sector: Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector*, EECSP

the Member States should increase their resilience to cyber threats through political and regulatory solutions, ranging from normative to programme solutions. The latter should be adapted to internal regulations, but taking into account the global aspect consistent with IEA standards. Effective government policies should go beyond utility companies and take into account the energy supply chain. Cybersecurity in the supply chain is an international issue. The internationalization of energy cybersecurity should be institutionalised and operational at the global level. At the same time, the IEA, meeting the expectations of the member states, proposed its own definitions within the cybersecurity conceptual grid. This term "broadly refers to the ability to prevent or defend against cyberattacks and cyber incidents, preserving the availability and integrity of networks and infrastructure and the confidentiality of the information these contain. Commonly also refers to the safeguards and actions available to do this". Undoubtedly, this definition is similar to that of CISA, thus referring to the common-law system. It is all the more important since, as a formal definition within an international organization, it is binding on the member states as to the scope of its validity. The same applies to the definition of incident, which according to IEA is "the ability to anticipate, withstand, adapt to and recover from adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyber resources". Unlike in internal solutions, including the Polish National Cybersecurity System Act, the definition of cyber attack has been introduced. It is "an event that could jeopardise the confidentiality, integrity or availability of digital information or information systems. Such incidents could also result in the physical disruption of operations". The organization attaches great importance to the issues of cybersecurity, pointing out that cyber attacks on energy systems can have very serious consequences for the environment, consumers and economies.[23]

Understanding past incidents and their causes can help prevent them from happening again, but it does little to address new types of attacks. Preventing and addressing the effects of new types of attacks, including with multiple attack mechanisms, requires research and understanding of likely scenarios that could have a severe impact on power grids. One of the new tools suggested by the IEA is Artificial Intelligence (AI), thanks to which there is a good chance to improve threat detection and prevent attacks. Unfortunately, it can also increase the capabilities of attackers, who can also rely on decisions made on the basis of predefined algorithms with limited knowledge and information. Another issue remaining in the sphere of cybersecurity of the energy sector is supply chain security. The supply chain supports electric power

Report, February 2017, https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf [access:12.07.2021].

[23] *Analysis of Selected Electric Sector High Risk Failure Scenarios*, December 2015, https://smartgrid.epri.com/doc/NESCOR%20Detailed%20Failure%20Scenarios%20v2.pdf [access: 14.07.2021].

system operations with critical hardware and software. An example is the inclusion of malware at an early stage of development. Back doors can be built into hardware to allow remote access once installed. Then the attacker has easier access to steal data or disable the system.[24] It is also possible to compromise the functionality of a large number of IoT devices.[25] An attacker through the network may lead to a rapid increase in power consumption by these devices, thus causing a rapid increase in the demand for electricity and leading to disturbances in the balance of supply and demand, which may translate into stock exchange listings.[26]

Electric power system cyber threats constantly develop and evolve. All participants in the system, within the IEA member states, must continuously monitor and assess their main vulnerabilities and risk profile. The risk profile assessment is essential for implementing defence programmes against attacks.

The mechanisms developed at the Vienna Congress on the Prevention of Crime and the Treatment of Offenders are also important in the international forum. Based on the guidelines developed by the Vienna Congress, the United Nations Convention against Transnational Organized Crime was adopted.[27] The Convention has not explicitly adopted a definition of cybersecurity or cybercrime, which must be assessed negatively. Article 29 UNTOC sets out the obligation to provide training and technical assistance, which refers, among other things, to cybercrime (and *a contrario* to cybersecurity). According to the wording of this Article, each State (including Poland) Party shall, to the extent necessary, initiate, develop or improve specific training programmes for its law enforcement personnel, including prosecutors, investigating magistrates and customs personnel, and other personnel charged with the prevention, detection and control of the offences covered by this Convention.[28]

Such programmes may include secondments and exchanges of staff. The training should cover "Methods used in combating transnational organized crime committed through the use of computers, telecommunications networks or other forms of modern technology" (Article 29 (h) UNTOC). The practice of application of

[24] *Best Practices in Supply Chain*, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Utility_093015.pdf [access: 14.07.2021].

[25] Internet of Things (IoT) are devices equipped with software which allow connecting to the network and data transmission. They may be remotely controlled by users. The most often used IoT devices currently include: TV, household appliances, monitoring systems, air conditioning, heat exchangers, freezers, etc.

[26] More on this topic in *Critical Infrastructure Protection: Actions needed to address significant cybersecurity risks facing the electric grid*, August 2019, www.gao.gov/assets/gao-19-332.pdf [access: 14.07.2021].

[27] United Nations Convention against Transnational Organized Crime (UNTOC) adopted by General Assembly on 15 November 2000, United Nations Treaty Series, vol. 2225, p. 209.

[28] J. Kostrubiec, *Formy działania służb specjalnych*, [in:] M. Bożek, M. Czuryk, M. Karpiuk, J. Kostrubiec, *op. cit.*, pp. 105–139.

the Convention for more than a decade confirms the significant increase in crimes committed with the use of new technologies, including on an international scale.[29] In addition to the conventions that are binding for the member states, it is also necessary to point to the UN resolutions, the subject of which are issues in the field of cybersecurity. One of the first is the UN General Assembly Resolution on combating the criminal use of information technology, adopted on 22 January 2001.[30] It specifically calls for increased cooperation and coordination between states in the fight against cybercrime. Subsequent resolutions, i.e. Resolution no. 56/121[31] and Resolution no. 60/177,[32] urged member states to engage in intensive cooperation to ensure cybersecurity. More specific and precise is Resolution no. 64/211,[33] which addresses the global culture of cybersecurity and protection of critical information structures, pointing to the necessity of implementing solutions to protect information structures in the member states, including networks responsible for the energy security cycle. This character has also had Resolution no. 65/230,[34] which provided constructive framework for the so-called Salvador Declaration, addressing the problem of rapid development of cybercrime.

Unfortunately, it should be noted that the UN, both in its preventive and normative activities, is at present far behind the practice of threats to cybersecurity. The main criticisms faced by the organization include: the lack of a unified conceptual framework (terminology); the inability to adopt a convention imposing specific obligations on member states in this area, with sanctions in the event of failure to implement them; the avoidance of confrontation with the real problems of cybersecurity in the least developed countries; the lack of support for the poorest Asian and African countries in the sector of new technologies.

ALGORITHM OF THREATS IN INTERNATIONAL PRACTICE

1. Georgia–Turkey

The problem of cybercrime threats to energy security is not purely theoretical, as it has already become practical. One of the first attacks with the use of software and computer tools occurred on 5 August 2008 in the area of the Baku–Tbilisi–Ceyhan (BTC) pipeline in Erzincan, Turkey. The attack on the pipeline was initially claimed

[29] S. Massoud Amin, *Power and Energy Infrastructure: Cyber Security, Defense, and Resilience*, "Georgetown Journal of International Affairs" 2015, no. 16, pp. 70–82.

[30] Resolution of the UN General Assembly no. 55/63 of 22 January 2001, A/RES/55/63.

[31] Resolution of the UN General Assembly no. 56/121 of 22 January 2001, A/RES/56/121.

[32] Resolution of the UN General Assembly no. 60/177 of 16 December 2005, A/RES/60/177.

[33] Resolution of the UN General Assembly no. 64/211 of 17 March 2010, A/RES/64/211.

[34] Resolution of the UN General Assembly no. 65/230 of 21 December 2010, A/RES/65/230.

by Kurdish separatists from the Kurdistan Workers' Party, but circumstances do not indicate that the explosion occurred as a result of traditional measures. Indeed, immediately before the explosion, all the cameras monitoring the pipeline were switched off and there was a failure in the management of the pump system used for maintaining adequate pressure inside the pipeline.[35]

According to confirmed information from the secret services of two states of the western hemisphere, the direct cause of the explosion was a sudden increase in pressure in the pipeline over a short distance and the shutdown of the alarm system,[36] which was confirmed by the lack of symptoms indicating the use of conventional explosives. It should also be emphasized that the pipeline ran through Georgian territory and the attack took place exactly 2 days before the outbreak of the Russian–Georgian conflict in August 2008. A few days later, Russian media quoted claims made by Alexander Dugin, a leading Russian ideologist of traditionalism, that the BTC pipeline had ceased to exist.[37] This was probably the first time that the Stuxnet[38] software was used, which was formally confirmed only in 2010. It was thanks to Stuxnet that the monitoring systems in Turkey did not record the explosion, and the BTC security centre learned about the incident not from the system records but from a witness who noticed the explosion of the pipeline.

2. Saudi Arabia

Another situation involved a cyber attack on a state-owned legal entity, Saudi Aramco. The system operation was suspended on 15 August 2012, when a computer virus blocked the operation of Aramco servers. An extremist group operating in Syria and Bahrain, seeking to seize power in Saudi Arabia, has admitted to introducing the virus called Shamoon into the system. The attack resulted in the removal of non-structural data at three Aramco offices, which caused disruptions in oil supplies and huge financial losses.[39]

[35] The journalists of "Bloomberg" refer to the fact that 60 hours of camera recordings along the entire length of the pipeline were deleted from the system. The only camera that operated independently of the cameras connected to the system network recorded two people near the pump station, one of whom used a laptop computer.

[36] In the light of the knowledge and circumstances of the incident, the cyber attack was carried out by entering the system through a "back door", by modifying the programme of working pumps so as to lead to an increase in their work cycles and thus pressure in the pipeline.

[37] J. Robertson, M. Riley, *Pipeline Blast Opened New Cyberwar*, "Bloomberg", 10.12.2014. For more on the topic, see W.Konaszczuk, *Prawnomiędzynarodowe aspekty…*, pp. 219–230.

[38] Stuxnet was only used to attack the Siemens software that operated nuclear power plants, power units, traditional power plants, gas and oil transmission systems, and power grids.

[39] U.S. Energy Information Administration, Saudi Arabia Analysis, 2013, www.eia.gov/countries/cab.cfm?fips=SA [access: 14.07.2021].

3. Ukraine

On 23 December 2015, almost half of residential buildings in the Ivano-Frankivsk region in Ukraine were cut off from electricity supplies, most likely as a result of a cyber attack. The blackout lasted for 4 to 6 hours. Shortly after the information was released by the Ukrainian news agency TNS, the authorities in Kiev identified the Russian Federation as the source of the hostile attack.[40]

4. Qatar

An equally spectacular action took place in August 2012, when the Qatari company Qatar's Ras Gas was attacked, almost leading to the explosion of the gas installation and suspended operation of the computer network and selected equipment of the company.[41]

5. United States

The United States has traditionally been the place where cybersecurity incidents in the energy sector are the most frequent in the world. This view is supported by a statement made to the House Committee on Energy and Commerce by the president of North American Electric Reliability Corporation in July 2019, in which he stated that "the threat from cyber attacks by nation states, terrorist groups, and criminals is at an all-time high".[42] The number of cybersecurity incidents in the US energy sector began to rise sharply in 2003. This year, the US Nuclear Regulatory Commission (NRC) confirmed that the US Office of Technology Assessment (OTA) faced the issue of attacks on energy networks. Based on the information obtained, NRC confirmed that a computer virus named Slammer, infecting Microsoft SQL servers, caused a serious disruption to the Davis–Besse nuclear power plant located in Oak Harbor, Ohio. The incident caused a shutdown of the safety monitoring system for more than 5 hours. Fortunately, the power station blocks remained shut down also. Seven months later, the failure to restore the plant's safety systems back

[40] K. Gapiński, *Blackout w zachodniej Ukrainie – cyber atak o wymiarze międzynarodowym*, 20.01.2016, https://pulaski.pl/komentarz-blackout-w-zachodniej-ukrainie-cyber-atak-o-wymiarze-miedzynarodowym [access: 14.07.2020].

[41] P. Paganini, *RasGas, new cyber attack against an energy company*, "Malta Independent", 31.08.2012.

[42] Testimony of James B. Robb, President and Chief Executive Officer, North American Electric Reliability Corporation, Before the House Committee on Energy and Commerce, Subcommittee on Energy "Keeping the Lights On: Addressing Cyber Threats to the Grid", 12 July 2019, www.nerc.com/news/testimony/Testimony%20and%20Speeches/House%20Energy%20and%20Commerce%20Cyber%20Hearing%20Testimony%207-12-19.pdf [access: 14.07.2021].

to normal conditions caused a massive blackout in power supplies in the west and northeast states of the US.[43] In January 2008, the CIA reported that it was aware of four attacks from US territory in other countries that could have significantly disrupted electricity supplies in four cities outside the US.[44]

According to recent reports from the Edison Electric Institute, major energy companies may face thousands to millions of potentially malicious attempted network attacks every day.[45]

6. Iran

Referring to cyber attacks on power grid systems, the above considerations addressed only those activities that were criminal in the sense of their origins. Above, there is no reference to a very important type of incident in the network committed for government agencies, states or international organizations. Their authorship is out of control and remains in the realm of conjecture. Undoubtedly, such actions occurred in relation to Iran's ICT systems. In 2011, the attackers used the Stuxnet virus, which was implemented in programmable Logic Controllers (PLC). The activation of the infected drivers led to physical damage to the Iranian energy infrastructure Natanz, without the knowledge of the operators.[46]

EUROPEAN UNION

To start with, it should be emphasised that from an international point of view the European Union is an international governmental organization, which entails certain inclinations, including in the area of cybersecurity in the energy sector.

The starting point is undoubtedly the Commission Recommendation (EU) 2019/553 of 3 April 2019 on cybersecurity in the energy sector.[47] In this document, the Commission addressed many important components of the sphere of cybersecurity, especially cybersecurity in the energy sector. It pointed out that technological progress, sector coupling and digitalisation are transforming the European energy grid into a "smart grid", which brings new risks as digitalisation increasingly

[43] S. Massoud Amin, *op. cit.*, p. 73.

[44] S. McLaughlin, S. Zonouz, D. Pohly, P. McDaniel, *A Trusted Safety Verifier for Process Controller Code*, 22.02.2014, www.ndss-symposium.org/wp-content/uploads/2017/09/02_2_1.pdf [access:29.08.2021], pp. 1–3.

[45] Edison Electric Institute, *Report 2019*, www.eenews.net/energywire/stories/1060089829?t=https%3A%2F%2Fwww.eenews.net%2Fstories%2F1060089829 [access: 14.07.2021].

[46] N. Hopkins, *Stuxnet attack forced Britain to rethink the cyber war*, 30.05.2011, www.theguardian.com/politics/2011/may/30/stuxnet-attack-cyber-war-iran [access: 14.07.2021].

[47] OJ L 96/50, 5.04.2019.

exposes the energy system to cyber attacks and incidents that could threaten the security of energy supply. The Recommendation identifies the EU-relevant issues related to energy cybersecurity, i.e. real-time requirements, cascading effects and the combination of legacy and state-of-the-art technology. Member States are required to implement appropriate cybersecurity preparedness measures related to real-time in the energy sector. Real-time operation should be understood as response to instructions within a few milliseconds. With regard to cascading effects, it has been indicated that States should implement appropriate cybersecurity preparedness measures that address cascading effects in the energy sector. Power grids and gas pipelines are highly interconnected across Europe, and a cyber attack leading to outages or disruptions in part of the energy system may result in far-reaching cascading effects on other parts of the system. At the same time, emphasis was put on "state-of-the-art technology". According to the Recommendation, countries should urge power grid operators and technology providers, in particular essential service operators as defined under the Directive (EU) 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,[48] to implement adequate cybersecurity preparedness measures relating to the combination of legacy and state-of-the-art technology in the energy sector.

As a rule, the Recommendation duplicates and complements the provisions of the NIS Directive. An important achievement of the Directive was the establishment of a Cooperation Group, composed of representatives of the Member States, the Commission, and the European Union Agency for Network and Information Security (ENISA). The group adopted guidelines on security measures and incident reporting. In June 2018, this group created a special area of intervention related to energy.

In addition to normative solutions at the EU level, an important technical support can also be mentioned. International standards organizations have published various standards on cybersecurity (ISO/IEC 27000: Information technology) and risk management (ISO/IEC31000: Risk management implementation). The detailed standard for the energy sector (ISO/IEC 27019: Information security controls for the energy utility industry) was issued under the ISO/IEC 27000 series in October 2017.

POLAND

The starting point for cybersecurity of the energy sector in Poland is undoubtedly the aforementioned National Cybersecurity System Act and also EU and international regulations. The specific situation of Poland stems from the fact that

[48] OJ EU L 194/1, 19.07.2016, hereinafter: the NIS Directive.

Poland has borders with Ukraine, the Republic of Belarus, the Russian Federation, through whose territory both gas pipelines and oil pipelines run.[49]

The Polish Energy Policy until 2040 (hereinafter: PEP2040), attached to Resolution no. 22/2021 of the Council of Ministers of 2 February 2021, does not contain specific provisions relating to cybersecurity in the energy sector. Only in the specific purpose concerning the expansion of electricity generation and grid infrastructure, it was indicated that "In order to ensure the security of electricity supply, it is necessary to modernize, maintain and expand the production infrastructure and network infrastructure (transmission and distribution), as well as to safeguard the systems in terms of cybersecurity". To this end, it has been established that for the security of supply, the transmission system operator (TSO) – Polish Power Grids Company (Pol. *Polskie Sieci Elektroenergetyczne S.A.*, PSE S.A.) will remain a sole shareholder company owned by the State Treasury. To ensure the security of energy supply to consumers, the TSO is obliged to prepare 10-year development plans on how to meet energy demand, while the DSO (distribution system operator) is required to prepare such plans for a period of not less than 5 years. In addition, the companies indicated as operators of essential services are required to protect key systems in terms of cybersecurity.[50] The postulates contained in PEP2040 in the field of cybersecurity refer to nuclear energy, currently non-existent in Poland, or the need to improve qualifications by employees of the energy sector.

At present, there are no comprehensive solutions in the field of cybersecurity of the energy sector in Poland.

CONCLUSIONS

As noted above, the issues of cybersecurity of energy at the transnational level have not yet been regulated in a uniform and concrete manner. There is no international convention, adopted under the auspices of the UN, that would regulate these issues. At the international level, cybersecurity is characterized by fragmentation, lack of a coherent conceptual grid and hierarchical approach. Particularly negative is the UN's lack of attention to the development of cybersecurity in the poorest countries, especially in Asia and Africa.

[49] For more on the topography and threats to the natural gas and oil supply chains, see W. Konaszczuk, *Zarządzanie kryzysowe jako element bezpieczeństwa państwa w sytuacji ograniczenia lub braku dostaw gazu ziemnego tranzytem przez Ukrainę do Polski z Federacji Rosyjskiej w świetle regulacji unijnych i krajowych*, [in:] *Współpraca międzynarodowa w zakresie zarządzania kryzysowego. Teoria i praktyka*, eds. A. Furgała, P. Niemczuk, Rzeszów 2013.

[50] Ministerstwo Klimatu i Środowiska, *Polityka Energetyczna Polski do 2040 roku*, www.gov.pl/web/klimat/polityka-energetyczna-polski [access: 14.07.2021].

In this context, EU solutions look much better, especially if we take into account the fact that EU countries are not unanimous about the field of energy.

The Polish national level of cybersecurity in the energy sector is regulated by the National Cybersecurity System Act, which does not take into account the specificities of the sectors of oil, natural gas and electricity. This is not conducive to creating comprehensive, holistic and coherent solutions. Individual Polish operators of essential services have been burdened with the implementation of cybersecurity solutions in their networks.

The practical examples presented indicate new trends in the area of actions aimed at energy security in the broad sense. There are also crucial questions, namely about the international legal assessment of cyber attacks inspired by national governments. While defining the criminal activities of non-state groups is relatively simple, the issue of using computer devices and cyber infrastructure for purposes justified by the interests of individual countries is a considerable problem,[51] especially since the question of sincerity in the process of creating a common energy policy of western hemisphere countries also raises doubts.

REFERENCES

Literature

Bernard Cohen I., *Howard Aiken: Portrait of a Computer Pioneer*, Cambridge 1999, **DOI: https://doi.org/10.7551/mitpress/3594.001.0001**.

Chałubińska-Jentkiewicz K., Karpiuk M., Kostrubiec J., *The Legal Status of Public Entities in the Field of Cybersecurity in Poland*, Maribor 2021, **DOI: https://doi.org/10.4335/2021.5**.

Czuryk M., *Właściwość Ministra Spraw Wewnętrznych oraz Ministra Obrony Narodowej w dziedzinie bezpieczeństwa publicznego*, [in:] *Prawo bezpieczeństwa publicznego*, eds. M. Karpiuk, K. Walczuk, Warszawa 2013.

Dauben J., *Book Review: The Universal History of Numbers and The Universal History of Computing (part 1)*, "Notices of the AMS" 2002, vol. 49(1).

Gengler B., *Super-hacker Kevin Mitnick takes a plea*, "Computer Fraud & Security" 1999, no. 5, **DOI: https://doi.org/10.1016/S1361-3723(99)90141-0**.

Karpiuk M., *Organisation of the National System of Cybersecurity: Selected Issues*, "Studia Iuridica Lublinensia" 2021, vol. 30(2), **DOI: http://dx.doi.org/10.17951/sil.2021.30.2.233-244**.

[51] An example of this was the use of a virus called Gauss (the name of this German mathematician was discovered in its source code), proof of a kind of genius of the creators of cryptography, which attacked sites exclusively on the territory of Lebanon, Palestine and Qatar between 2011 and 2013. The activity discovered so far consisted in decrypting the information of clients of banks in the aforementioned countries and sending it to an unidentified server. The mutation of the virus operated only on 30 computers, after which the virus was self-liquidated in the unit. Now Kaspersky Lab, a world's leading anti-malware company, has confirmed that Gauss has an affinity for US and Israeli government agencies. To date, cryptographers around the world have been unable to determine the full source code.

Karpiuk M., *Zakres działania służb specjalnych*, [in:] M. Bożek, M. Czuryk, M. Karpiuk, J. Kostrubiec, *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe*, Warszawa 2014.

Konaszczuk W., *Legislacyjne rozwiązania w zakresie przeciwdziałania cyberprzestępczości w prawie podatkowym*, Warszawa 2018.

Konaszczuk W., *Prawnomiędzynarodowe aspekty obrotu ropą na świecie,* Lublin 2017.

Konaszczuk W., *Zarządzanie kryzysowe jako element bezpieczeństwa państwa w sytuacji ograniczenia lub braku dostaw gazu ziemnego tranzytem przez Ukrainę do Polski z Federacji Rosyjskiej w świetle regulacji unijnych i krajowych*, [in:] *Współpraca międzynarodowa w zakresie zarządzania kryzysowego. Teoria i praktyka*, eds. A. Furgała, P. Niemczuk, Rzeszów 2013.

Kostrubiec J., *Formy działania służb specjalnych*, [in:] M. Bożek, M. Czuryk, M. Karpiuk, J. Kostrubiec, *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe*, Warszawa 2014.

Kostrubiec J., *The Role of Public Order Regulations as Acts of Local Law in the Performance of Tasks in the Field of Public Security by Local Self-government in Poland*, "Lex localis – Journal of Local Self-Government" 2021, vol. 19(1), **DOI: https://doi.org/10.4335/19.1.111-129(2021)**.

Massoud Amin S., *Power and Energy Infrastructure: Cyber Security, Defense, and Resilience*, "Georgetown Journal of International Affairs" 2015, no. 16.

Paganini P., *RasGas, new cyber attack against an energy company*, "Malta Independent", 31.08.2012.

Robertson J., Riley M., *Pipeline Blast Opened New Cyberwar*, "Bloomberg", 10.12.2014.

Smith M.F., Htoo N., *Energy Security: Security for Whom*, "Yale Human Rights and Development Law Journal" 2008, vol. 11.

Taylor J., Van Doren P., *Energy Security Obsession*, "Georgetown Journal of Law & Public Policy" 2008, vol. 6(2).

USA Documents, Public Affairs Office, *United States Mission to the European Communities*, 1973, no. 61.

Online sources

Analysis of Selected Electric Sector High Risk Failure Scenarios, December 2015, https://smartgrid.epri.com/doc/NESCOR%20Detailed%20Failure%20Scenarios%20v2.pdf [access: 14.07.2021].

Best Practices in Supply Chain, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Utility_093015.pdf [access: 14.07.2021].

Critical Infrastructure Protection: Actions needed to address significant cybersecurity risks facing the electric grid, August 2019, www.gao.gov/assets/gao-19-332.pdf [access: 14.07.2021].

Cyber Security in Energy Sector: Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector, EECSP Report, February 2017, https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf [access:12.07.2021].

Edison Electric Institute, *Report 2019*, www.eenews.net/energywire/stories/1060089829?t=https%3A%2F%2Fwww.eenews.net%2Fstories%2F1060089829 [access: 14.07.2021].

Gapiński K., *Blackout w zachodniej Ukrainie – cyber atak o wymiarze międzynarodowym*, 20.01.2016, https://pulaski.pl/komentarz-blackout-w-zachodniej-ukrainie-cyber-atak-o-wymiarze-miedzynarodowym [access: 14.07.2020].

Hopkins N., *Stuxnet attack forced Britain to rethink the cyber war*, 30.05.2011, www.theguardian.com/politics/2011/may/30/stuxnet-attack-cyber-war-iran [access: 14.07.2021].

International Energy Agency, *Energy security Reliable, affordable access to all fuels and energy sources*, www.iea.org/topics/energysecurity [access: 14.07.2021].

International Energy Agency, *Member countries*, www.iea.org/countries/membercountries [access: 12.07.2021].

Malboard: New Computer Attack Mimics User's Keystroke Characteristics and Evades Detection, 5.06.2019, https://in.bgu.ac.il/en/Pages/news/Malboard.aspx [access: 14.07.2021].

McLaughlin S., Zonouz S., Pohly D., McDaniel P., *A Trusted Safety Verifier for Process Controller Code*, 22.02.2014, www.ndss-symposium.org/wp-content/uploads/2017/09/02_2_1.pdf [access:29.08.2021].

Ministerstwo Klimatu i Środowiska, *Polityka Energetyczna Polski do 2040 roku*, www.gov.pl/web/klimat/polityka-energetyczna-polski [access: 14.07.2021].

Security Tip Report (ST04-001), 6.05.2009, https://us-cert.cisa.gov/ncas/tips/ST04-001 [access: 14.07.2021].

Testimony of James B. Robb, President and Chief Executive Officer, North American Electric Reliability Corporation, Before the House Committee on Energy and Commerce, Subcommittee on Energy "Keeping the Lights On: Addressing Cyber Threats to the Grid", 12 July 2019, www.nerc.com/news/testimony/Testimony%20and%20Speeches/House%20Energy%20and%20Commerce%20Cyber%20Hearing%20Testimony%207-12-19.pdf [access: 14.07.2021].

United Nations, *Report of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, Vienna, 10–17.04.2000, https://digitallibrary.un.org/record/432663/files/A_CONF.187_15-EN.pdf [access: 17.07.2021].

U.S. Energy Information Administration, Saudi Arabia Analysis, 2013, www.eia.gov/countries/cab.cfm?fips=SA [access: 14.07.2021].

Legal acts

Act of 17 February 2005 on the computerization of operation of entities which perform public tasks (Journal of Laws 2020, items 346, 568 and 695).

Act of 5 July 2018 on the national cybersecurity system (Journal of Laws 2020, item 1369).

Commission Recommendation (EU) 2019/553 of 3 April 2019 on cybersecurity in the energy sector (notified under document C(2019) 2400) (OJ L 96/50, 5.04.2019).

Directive (EU) 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 (OJ EU L 194/1, 19.07.2016).

Resolution of the UN General Assembly no. 55/63 of 22 January 2001, A/RES/55/63.

Resolution of the UN General Assembly no. 56/121 of 22 January 2001, A/RES/56/121.

Resolution of the UN General Assembly no. 60/177 of 16 December 2005, A/RES/60/177.

Resolution of the UN General Assembly no. 64/211 of 17 March 2010, A/RES/64/211.

Resolution of the UN General Assembly no. 65/230 of 21 December 2010, A/RES/65/230.

United Nations Convention against Transnational Organized Crime (UNTOC) adopted by General Assembly on 15 November 2000, United Nations Treaty Series, vol. 2225.

ABSTRAKT

Ogłoszenie światowej pandemii COVID-19 – obok negatywnych zjawisk zdrowotnych, gospodarczych i społecznych – wywołało masowe zjawisko przenoszenia większości aspektów życia osób do cyberprzestrzeni. W ostatniej dekadzie miał miejsce geometryczny postęp wzrostu incydentów cyberbezpieczeństwa na świecie, w tym również w sektorze energetyki. Niniejszy artykuł jest pracą o charakterze koncepcyjnym, a podstawowy problem badawczy odnosi się do określenia poziomu i obszaru regulacji prawnych w zakresie cyberbezpieczeństwa sektora energetyki w systemie ponadnarodowym, unijnym i wewnętrznym. Zasadnicza teza ma potwierdzić wstępne założenie o niewystarczającym poziomie ochrony normatywnej sieci, zarówno w systemie prawa międzynarodowego,

jak i w systemie prawa wewnętrznego. Celem jest wykazanie newralgicznych rozwiązań prawnych, które w przyszłości będą skutkować krytycznymi i poważnymi incydentami w łańcuchu dostaw energii, jak również w logistyce energii. Oryginalność opracowania wiąże się z próbą zestawienia odrębnych systemów prawnych, których przedmiotem regulacji jest cyberbezpieczeństwo sektora energii. Wartość poznawcza dla praktyki wiąże się ze wskazaniem ujednoliconej siatki pojęciowej oraz zasadniczych regulacji problematyki.

Słowa kluczowe: cyberprzestrzeń; cyberbezpieczeństwo sektora energii; systemy prawne; ewolucja technologiczna