UDC 341.362.1 Вестник СПбГУ. Право. 2024. Т. 15. Вып. 3

Genesis of the notion "cybersecurity" in the fuel and energy sector of the European Union: Legal analysis

V. A. Shestak[1], *P. G. Savenkova*[2]

[1] A. Y. Sukharev Moscow Academy of the Investigative Committee of the Russian Federation, 12, ul. Vrubelya, Moscow, 125080, Russian Federation
[2] LLC "FINMARSH", 76, pr. Vernadskogo, Moscow, 119454, Russian Federation

For citation: Shestak, Viktor A., Polina G. Savenkova. 2024. "Genesis of the notion 'cybersecurity' in the fuel and energy sector of the European Union: Legal analysis". *Vestnik of Saint Petersburg University. Law* 3: 866–881. https://doi.org/10.21638/spbu14.2024.320

This paper analyzes cybersecurity as a legal institution, gives its detailed theoretical and legal characteristics. The purpose of this study is to analyze the legal acts, and in particular the criminal law, in order to summarize the existing regulations related to the means of ensuring cybersecurity in the European Union (EU), the study of this institution, both in general and in relation to individual industries, first of all, to the fuel and energy complex. When writing this work, both doctrinal and non-doctrinal methods were used, including: comparative legal and historical-legal methods, as well as macro-comparison and micro-comparison, normative comparison. Based on the results of the study, the authors came to the following conclusions: cybersecurity, like other concepts related to information technology, cannot have a single regulatory fixation due to the nature of such phenomena; at the moment, the priority task of the state authorities of the EU and member states is to create a regulatory framework for the regulation of cybercrime and other threats to cybersecurity and develop legal means and methods to ensure it; among all areas where cybersecurity is necessary, special attention should be paid to the fuel and energy complex, since this sector is inextricably linked not only with national security and welfare, but can also affect other countries, which seems to be especially relevant within the framework of a single internal market European Union. Thus, information technologies have a significant impact on modern society, and ensuring the protection of society from traditional crimes committed using information systems or new types of crimes that are inherently associated with digital devices seems to be one of the most important tasks of each state.

Keywords: cybersecurity, European law, criminal law, legal measures, cybercrime, critical infrastructure, cyber threats, energy sector.

1. Introduction

The importance of cybersecurity cannot be overemphasized taking into consideration the fact that today's society is inherently connected to technology: individuals and organizations, as well as governments, rely on computer systems on a daily basis. The vast majority of the most diverse processes are shifting online, and the networks of digital platforms are constantly expanding. Critical infrastructure facilities, which primarily include the energy sector, are no exception. The safety of such facilities is especially important

for society, because their disabling has a negative impact on the economic situation and public safety. Cybersecurity plays a key role in developing sustainable energy systems and ensuring a reliable supply of energy, as the scale and impact of cyberattacks increase every day. Because such attacks encroach on the most important interests of society and the state, and in case of their implementation, the negative consequences go beyond the borders of one state, it is not surprising that the legislator classifies them as crimes and they are regulated by criminal law. The lack of a uniform legal definition of the term cybersecurity can be distinguished as a peculiarity of the legal regulation of cybersecurity, but it certainly creates difficulties in the process of uniform regulation.

The criminal law of the vast majority of states, including the member states of the European Union (EU), provides for such categories of crimes as crimes against state power and in particular crimes against state security, as well as crimes against public safety and public order. National security is one of the main interests protected by criminal law, and this concept includes both security and cybersecurity of critical infrastructure. Objects of critical infrastructure include various industrial facilities, information and communication technologies, fuel and energy complex facilities, and others. The fact that the stable and uninterrupted functioning of the EU internal market directly depends on the sustainability of national fuel and energy facilities can also explain why it is important to implement state security in the EU member states. The disruption of power grids and information systems in one Member State therefore affects other States and the EU as a whole. It is impossible to solve this problem at the national level; only an integrated approach initiated at the level of the Union and the implementation of a unified security policy can help reduce the risk of such threats (Kelemen, Szabo, Vajdova 2018).

The European Union is conducting a common policy to ensure a high overall level of security for networks and information systems, at the supranational level; competent authorities adopt legal acts, as well as implement other criminal law measures aimed at minimizing the threat of cyber attacks and preventing other adverse actions. Traditional energy technologies also become increasingly more connected to modern digital technologies and networks. Their rising significance makes the process of using fuel and energy facilities more accessible and allows consumers to get more benefits from their use, but at the same time creates considerable risks and makes them more vulnerable to attacks by cybercriminals and jeopardizes power supply security and consumer data privacy. Although the European Commission is adopting legal acts that address cybersecurity issues in the energy sector, the main problem today is the lack of a comprehensive regulatory framework.

To achieve the goal, which is the comprehensive analysis of legal acts of the European Union in the sphere of cybersecurity authors solve a number of tasks. Such as the study of the content of the term cybersecurity and related concepts of cybercrime, cyber threats and cyberspace; the analysis of the main legal acts regulating the provision of cybersecurity both in the EU law and in the national law of the EU Member States.

The methodological basis constitute both general scientific methods (dialectical method, formal logical method, analysis, synthesis, inductive method, deductive method); and special-legal methods, which include comparative-legal and historical-legal, formal-legal. With regard to the comparative legal method, it is possible to single out some methods, which include, among other things, macro-comparison and micro-comparison, normative comparison and doctrinal. Within the framework of this work, authors use macro-comparison when analyzing the influence of European Union law on the national

legal systems of the EU Member States, and micro-comparison when considering legal norms and their separate parts, legal institutions and doctrinal definitions of various law systems. For a more complete study of the elements of national legal systems, it is important to take into account the historical factors that influenced the processes and phenomena that constitute the subject of the study, for which the author uses the historical approach. Another scientific methods used in the paper are doctrinal comparison and normative comparison. The former — is a comparison of scientific definitions; while the latter is a comparison of similar legal norms, articles of legislative acts, legal institutions. Authors use doctrinal comparison within this paper when comparing the positions and approaches of various European legal scholars in respect to their understanding of cybersecurity concept and legal measures suitable for its ensuring.

Finally, the formal legal method, the essence of which is expressed in determining the place of a new phenomenon in the system of legal knowledge and establishing its nature from the point of view of legal instruments. For the purpose of the paper, authors use this method in relation to cybersecurity concept and its place in the legislation of European Union and its member states. Since neither a single spelling of the term, nor a single approach to its understanding was fixed at the legislative level, it is in the doctrinal sources that determine its place in the system of legal knowledge.

2. Basic research

2.1. History of the development of legislation in the sphere of cyber security

The first attempts to legislate Internet security were made at the end of the 20th century, but cybersecurity did not become one of the main security priorities until the mid-2000s. Changes have come with a growing awareness that information systems and technologies are vulnerable to external attacks, especially those of a terrorist nature. It is the confirmation in the believes that organized crime and terrorism pose a clear threat to building a secure information society that has led to the need to address gaps and differences, including between the laws of Member States (Carrapico, Barrinha 2017).

European Union legislation on cybercrime and cybersecurity began to develop even before the adoption of the Treaty of Lisbon in 2007. At the times when the legal framework that determined the basis for the functioning of the European Union was expressed in terms of three pillars: the European Communities, the Common Foreign and Security Policy (CFSP) and police and judicial cooperation in criminal matters. The legal justification for regulating cybersecurity was originally expressed precisely as a measure for the implementation of a common foreign and security policy. Legislation in this area has evolved in parts and was expressed in the form of various legal instruments, which continue to influence its development today. The 2005 Framework Decision on Attacks on Information Systems for the first time criminalized online and off-network activities, along with severe sanctions. More recently, the European Commission issued the Communication "Towards a general policy on the fight against cybercrime"[1]. The purpose

[1] Communication from the Commission to the European parliament, the Council and the Committee of the regions "Towards a general policy on the fight against cyber crime". Accessed August 7, 2024. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF.

of this document was to achieve strong cooperation between law enforcement agencies, public-private partnerships and international cooperation in combating cybercrime.

The three pillars system was abolished with the adoption of the Treaty of Lisbon and today the legal basis for the adoption of laws to regulate cybercrime and security is contained in the EU founding agreements. For example, Art. 82 of the Treaty on the Functioning of the European Union (TFEU) contains provisions allowing the European Parliament and the Council of the European Union to establish minimum rules to the extent necessary to facilitate mutual recognition of judgments and police and judicial cooperation in criminal matters of a cross-border nature. Art. 83 of the same Treaty provides for the powers of the European Union to adopt the rules of substantive criminal law. In particular, Para. 1 of this article, reveals for which types of crimes the Parliament and the Council of the EU may establish minimum standards regarding the definition of criminal offenses and sanctions. Such crimes must be classified particularly serious, cross-border in nature; the combat against them requires the cooperation of several national law enforcement agencies. Crimes in the field of computer information are considered as one of the types of crimes belonging to this category. With the abolition of the system of three pillars and the acquisition by the EU of the status of a single entity, universal documents began to be adopted at the Union level, such as strategies that apply equally to all Member States, as well as to all natural and legal persons.

The highest authorities of the European Union adopt the security strategies and they are considered to be fundamental documents covering priority areas where the EU can contribute to support member states in strengthening security. The adoption of each strategy is due to the emergence of new, more complex cross-border security threats and the need for closer cooperation in the field of its implementation at all levels. Although the responsibility for security lies primarily with States, there has been a growing understanding in recent years that the security of one Member State is the security of all. The growing relationship between internal and external security also takes place. Protecting the Union and its citizens is no longer only about ensuring security within the EU's borders, but also about turning to external security. Cooperation to address common challenges with third countries and globally is crucial for the effective and comprehensive response, while maintaining stability and security with countries located in close proximity and playing an important role in the functioning of the Union is critical to the EU's own security. It is important to note that the measures taken today determine the actions to achieve the set goals in both the physical and digital worlds[2].

2.2. Peculiarities of cybersecurity regulation in the energy sector

Certain objects within the European Union disposes are considered as the most important infrastructure. The violation or destruction of such objects can have significant consequences that go beyond the boundaries of one state.

Due to the need to strengthen the protection of such facilities from external threats in the EU, it has become clear that the implementation of strong criminal penalties as a

[2] Communication COM/2020/605 final. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions "On the EU Security Union Strategy. Accessed August 7, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605.

measure against cyber attacks is crucial; so that such penalties would reflect the seriousness of the harm caused by such attacks. The term "critical infrastructure objects" may refer to facilities or parts thereof located on the territory of a Member State necessary to maintain the vital social functions. The main directions of ensuring the viability are health, safety, economic or social well-being of people; so, the examples of such objects are power plants or transport networks, the violation or destruction of which would have significant consequences in the Member State resulting in the failure to perform these functions. Serious damage within the meaning of one of the main legal acts in this sphere — EU Directive "On attacks against information systems and replacing Council Framework Decision 2005/222/JHA"[3] is determined by the national legislation of each Member State individually. However, violation of system services of great public importance, infliction of large financial costs and loss of personal data or confidential information is provided as an example.

There can be distinguished the following features specific to the energy sector. First, the inevitability of the consequences of cyber attacks: electrical networks and gas pipelines are closely interconnected throughout Europe, as well as far beyond the EU member states. Energy security and security of supply at the European level depends on trans-European connectivity. Unlike other systems, control systems in an energy sector that has been attacked cannot be easily disabled, since a failure can cause negative consequences in various other interdependent energy systems, sectors or other regions that go far beyond the relevant sector or region. Secondly, much of the infrastructure of the energy sector is outdated, many generators and transformers were developed long before cybersecurity was singled out as one of the directions of the state security policy. Therefore, there is a problem that a great number of the energy infrastructure with a relatively long service life has been designed without taking cyber attacks and the growing variety of other threats into consideration. Finally, it can be difficult to implement a number of standard cybersecurity measures due to the fact that disabling some objects can lead to high costs. There is also an evident need to protect legacy systems that are not secure enough due to rapid digitalization and their connection to the Internet, despite the fact that such a connection was not provided in their original design[4].

In relation to the energy sector, there are two opposing positions among individuals and legal entities involved in this area about what is most important: safety or security. Safety is related to the infrastructure and the state of physical security of people, networks, etc., the main goal is not to be harmed. In turn, security includes safety and has a broader meaning, covering both attacks and crimes. Such differences in definitions make it very difficult to raise awareness and further develop cybersecurity. Many companies in the energy sector still place much more emphasis on the safety of their physical infrastructure than the security of their information systems[5].

---

[3] Directive of the European Parliament and of the Council "On attacks against information systems and replacing Council Framework Decision 2005/222/JHA". Date of last revision: 14.08.2013. Accessed August 7, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0040.

[4] NIS Cooperation Group Report "Sectorial implementation of the NIS Directive in the Energy sector" 2019. Accessed August 7, 2024. https://smart-lighting.es/wp-content/uploads/2019/11/SectorialimplementationoftheNISDirectiveintheEnergysectorpdf.pdf.

[5] Report on Cyber Security Information Sharing in the Energy Sector. European Union Agency for Network and Information Security. Accessed August 7, 2024. https://www.enisa.europa.eu/publications/information-sharing-in-the-energy-sector.

The energy sector infrastructure is one of the most complex and most important infrastructures of modern society and serves as the basis of its economic activity and its security. That is the reason why this industry is also at the epicenter of cyberattacks. According to a 2021 report, 17,2 % of all cyberattacks globally target energy organizations, making the industry the biggest target for cybercriminals and attackers[6]. Energy systems today rely more on technology, which in turn affects their openness and vulnerability to cyber attacks, and the success of such attacks depends precisely on the lack of protective measures[7]. Failures resulting from attacks on fuel and energy facilities can lead to further negative consequences with potentially more serious social and economic effects.

The problem seems to be particularly relevant in the region of interest, since, firstly, within the framework of a single market for goods and services established between the member countries of the Union, there is an active exchange, including energy goods, and the development of energy infrastructure is aimed at strengthening the relationship and the creation of a more integrated EU energy market, and secondly, a large share of all energy consumed is imported, which is why third countries are also actively involved in these relations, which creates the need for cybersecurity regulation in the process of interaction with third states.

2.3. Different approaches to the legal definition of cyber security and its characteristics

The legislation of the EU in the field of cybersecurity is characterized by the lack of structuredness. The European Parliament as well as other EU institutions have criticized this fact (Carrapico, Barrinha 2017). The European Union's Cybersecurity Strategy: An Open, Safe and Secure Cyberspace[8] was the first most general-purpose document, in which can also be found the definition of cybersecurity. The strategy entering into force marked the official establishment of cybersecurity as a new area of the EU policy. According to the text of this document, cybersecurity is understood as an umbrella term, which includes a large number of areas of politics, and from the point of view of the EU "implies a combination of cyber resistance, cybercrime, cyber protection and global cyberspace issues" (section 1.1). This term covers such directions as network and information security measures aimed at operators of the main services and suppliers of critical and digital infrastructures; electronic communications, including the issues of confidentiality and data protection; cybercrime.

Although the name of the document implies that the strategy is dedicated specifically to security, it has a complex interaction with cybercrime and other areas, and for the most complete analysis of concepts, they should be considered together. According to the Strategy (section 1.1), cybercrime usually refers to a wide range of different criminal activities in which computers and information systems are used either as the

[6] Lookout. Report "Threat report. At the Epicenter: 2021 Lookout Energy Industry Threat Report". Accessed August 7, 2024. https://www.magonlinelibrary.com/doi/abs/10.1016/S1353-4858%2821%2900126-4.

[7] World Economic Forum 2022 Report "Global Cybersecurity Outlook 2022. Accessed August 7, 2024. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf.

[8] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Accessed August 7, 2024. https://edps.europa.eu/sites/default/files/publication/13-02-07_communication_join_cyber_sec_en.pdf.

main tool or as the main target. Cybercrime includes: traditional crimes (e. g. fraud, identity theft), such crimes as incitement to racial hatred, and crimes specific to computers and information systems (e. g. attacks on information systems, distribution of malware, etc.). Cybersecurity is defined as "the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure"[9]. Cybersecurity seeks to maintain the availability and integrity of networks and infrastructure, as well as the confidentiality of the information they contain (Fuster, Jasmontaite 2020).

The vast majority of legal documents regarding cybersecurity begin with discussion of what cybersecurity exactly means. Often this term is ambiguous and poorly defined, particularly due to the developing nature of cybersecurity. For a long period of time, the term was not mentioned as an independent part of the EU policy, and the EU legislation did not provide any legal basis for it, mainly because of its indissoluble ties with such definition as cybercrime.

Cybersecurity is currently considered as a complex issue that requires the attention of not only technical specialists, but also legislators, since the latter are responsible for creating the relevant legal framework, within which private and state organizations could fulfill their tasks and responsibilities.

This is a significant step forward, since for a long time cybersecurity has been perceived exclusively as a technical issue related to measures that ensure the accessibility, integrity and confidentiality of information and information systems. The regulation of cybersecurity in the EU is also complicated by the fact that its components, such as cybercrime and criminal cooperation are in joint jurisdiction of the EU and Member States. In general, the EU can issue laws in areas where it is believed that European regulation will be more appropriate than national and introduce any regulatory measures, including ones regarding cybersecurity. However such activities require a legal basis. Any legislative proposal must comply with the following criteria: the proposed actions cannot be sufficiently carried out by member states independently or the result from the proposed actions due to scale or significance will be better achieved at the EU level.

European Network and Information Security Agency (ENISA), which was later renamed as European Union Agency for Cybersecurity was established by the Decree of the European Parliament and Council no. 460/2004[10] plays crucial role in determining the definition of cybersecurity, as well as in the implementation of a common policy of its assurance within the European Union. The agency proposed to use the "contextual definition", since cybersecurity is a wide and developing term. While establishing a single definition may provide more clarity, interested parties should choose definitions that suit their particular needs in a particular context.

---

[9] Directive of the European Parliament and of the Council of July 6, 2016 concerning measures for a high common level of security of network and information systems across the Union. Date of last revision: 19.07.2016. Accessed August 7, 2024. https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[10] Regulation 460/2004. Regulation of the European Parliament and of the Council establishing the European Network and Information Security Agency. Date of end of validity: 18.06.2013. Accessed August 7, 2024. https://eur--lex-europa-eu.translate.goog/legal-content/EN/TXT/?uri=celex:32004R0460&_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc.

In 2015, the Agency compiled a document "Definition of Cybersecurity: Gaps and Overlaps in Standardisation"[11]. The document analyzes the way how involved parties use the term and reviews standardization activities in the field of cybersecurity with a review of coincidences and lacunas. According to this document, there is no need and possibility to determine cybersecurity in the usual way. Cybersecurity is an umbrella term, and it is impossible to give a definition covering everything that covers cybersecurity. Thus, the definitions used for the purposes of certain legal acts or used by specific organizations should be considered. The studies show that the definition of cybersecurity is widely used in various fields: military security, information security and others. Each of these spheres provides its own concept of cybersecurity. For example, in the field of information security, the definition is the following: "Protection against the threat of theft, deletion or alteration of stored or transmitted data within a cyber system", and the definition related to the operations security is formulated as "Protection against the intended corruption of procedures or workflows which will have results that were unintended by its owners, designers or users". In view of the above, it does not seem surprising that at this point exist numerous definitions devoted to various aspects of cybersecurity (political, military, economic, technical, legal, etc.).

In 2017, the ENISA agency drafted a review of cybersecurity and the incidental terminology. This document provides a hierarchical classification of protection levels in cyberspace. It is possible to achieve and ensure the state of cybersecurity only by ensuring the security of all listed levels and all components. According to the review, any EU security strategy should cover all aspects in order to ensure an integrated approach in the field of counteracting cyber threats[12].

Definitions of cybersecurity can also be found in other legal acts. The briefing paper of the European Court of Auditors, an organization representing the interests of EU taxpayers, "Challenges to effective EU cybersecurity policy" states that: "cybersecurity involves preventing, detecting, responding to and recovering from cyber incidents"[13]. Incidents may or may not be intentional and range from, for example, accidental disclosures to attacks on businesses and critical infrastructure, identity theft, and even interference with democratic processes. All of this can have widespread harmful effects on individuals, organizations and communities.

According to Para. 1 of Art. 2 of the Cybersecurity Act, "cybersecurity" means "activities necessary to protect network and information systems, the users of such systems and other persons affected by cyber threats"[14]. With regard to the energy sector, the most serious of these activities are associated with disruption of the operation of power grids, gas networks, gas pipelines and oil refining facilities. The Law also contains definitions of

[11] Definition of Cybersecurity — Gaps and overlaps in standardization. Accessed August 7, 2024. https://op.europa.eu/en/publication-detail/-/publication/fece9d1d-f717-11e5-abb1-01aa75ed71a1/language-en.

[12] ENISA Report Overview of cybersecurity and related terminology. Accessed August 7, 2024. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology.

[13] European Court of Auditors 2019 Paper "Challenges to effective EU cybersecurity policy". Accessed August 7, 2024. https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf.

[14] Regulation (EU) 2019/881. Regulation of the European Parliament and of the Council 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). Date of last revision: 07.06.2019. Accessed August 7, 2024. https://eur-lex.europa.eu/eli/reg/2019/881/oj.

a cyber threat, which means "any potential circumstance, event or action that could damage, disrupt operation or otherwise adversely impact network and information systems, the users of such systems and other persons".

The definitions used to refer to cybersecurity by various actors, including EU governmental bodies and institutions, usually represent different points of view, which may, among other things, contradict each other. At the national level, the definitions proposed by states also vary to a large extend. For example, Spain's National Cybersecurity Strategy adopted in 2013 defines cybersecurity as "a necessity of our society and our economic model"[15], the Austrian Cybersecurity Strategy defines it as "security of infrastructure in cyber space, of the data exchanged in cyber space and above all of the people using cyberspace"[16]. Meanwhile the national strategy of the Slovak Republic refers cybersecurity to a component of national security and it is given the following definition: "Cyber security is one of the defining elements of the security environment of the Slovak Republic and a subsystem of national security. At a state level, it is a system of continuous and planned increasing of political, legal, economic, security, defence and educational awareness; also including the efficiency of adopted and applied risk control measures of a technical-organisational nature in cyber space in order to transform it into a trustworthy environment providing for the secure operation of social and economic processes at an acceptable level of risks in cyber space".

2.4. The NIS directive in cybersecurity regulation and its implementation

Different politics of member states regarding cybersecurity measures impede the protection provided to consumers and business and, therefore, reduce the overall level of security of networks and information systems. Directive on security of network and information systems — NIS Directive[17], which entered into force in 2016 and became the first horizontal legal act in the field of cybersecurity, was adopted for these purposes, especially to increase the consistency of the practice of member states in terms of cybersecurity measures. The horizontal direct effect of the act applies to relations arising between persons, both physical and legal, in contrast to the vertical, which extends to relations between the EU's law and national legislation. If any provision of EU legislation has a horizontal direct effect, it means that such provisions can create rights or impose obligations to persons, as well as the possibility to refer to such rules of law in the national court (Rasmussen 2011). The Directive gives the following definition of cybercrime (or computer crime): "the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy".

The definition of cybersecurity or computer security is the following: "the protection of computer systems and information from harm, theft, and unauthorized use". There are four main types of cyber threats: theft of data that constitutes a military secret from gov-

[15] The National Cyber Security Strategy of Spain. Government of Spain. Accessed August 7, 2024. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf.

[16] Austrian Cyber Security Strategy. Accessed August 7, 2024. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS. pdf.

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

ernment computers; vandalism, including data destruction with a computer virus; fraud, the invasion of privacy. One of the main purposes of the NIS directive was to improve the possibilities of ensuring cybersecurity of member states, as well as the cooperation between member states and the supervision of critical sectors of member states. The states independently determine the operators of the main services, which include private enterprises or state organizations that play an important role in society and the economy; however, they should belong to the sectors defined in the Directive, one of most important sector among others is the energy sector (companies that relate to producing or supplying electricity, oil and gas).

The above-mentioned act was adopted in the form of a directive, which means that it is an indirect effect act, so in order to enter into force it has to be implemented into national legislation. In other words, all EU member states were obliged to take measures aimed at achieving the goals defined in the directive. With regard to the NIS directive it was a term of two years. The vast majority of countries drafted and subsequently adopted national laws that complement or amend the current national legislation.

2.5. The experience of implementation of the NIS Directive in different EU member states

In 2018, the national government body of the Slovak Republic adopted the "Cyber Security Law" as a result of the implementation of the NIS directive[18]. Subsequently, amendments were made to the law, the last of which were adopted in 2021 (Vanek 2021). In the analyzed state, an advanced system of legal regulation of cybersecurity has developed today, based on various regulatory legal acts that have the legal nature of a law or a by-law. The law applies to operators of essential services, i. e. organizations in the most vital sectors for life, including the fuel and energy complex.

In 2015, the Cybersecurity Concept of the Slovak Republic (for 2015–2020) came into force — the first comprehensive document that defines the principles, rules and objectives of cybersecurity[19]. This document was also revised and in 2021 the government of the Slovak Republic adopted a new Strategy (for 2021–2025)[20]. The legal basis of the national strategy is the Cyber Security Law[21]; it reflects the mandatory content laid down in the NIS Directive and the state's obligations to transpose its provisions into the national legislation.

Within the framework of the first Concept, the goal was to create an institutional framework for governance, adopt appropriate legislation, develop basic mechanisms for managing cyberspace, and developing international cooperation. Within the time frame set by the Concept, it was possible to create a stable institutional framework for the man-

[18] The Slovak Republic Act on Cybersecurity, no. 69/2018. Date of last revision: 24 of February, 2022. Accessed August 7, 2024. https://www.sk-cert.sk/wp-content/uploads/2018/03/2018_69-Act-on-Cybersecurity.pdf.

[19] Definition of Cybersecurity — Gaps and overlaps in standardization.

[20] National Security Authority of Slovakia: The National Cybersecurity Strategy 2021–2025. Accessed August 7, 2024. https://ccdcoe.org/uploads/2018/10/Slovakia_National_Cybersecurity_Strategy-2021-2025_2021_English.pdf.

[21] Act of January 30, 2018 on Cybersecurity and on Amendments and Supplements to certain Acts. Accessed August 7, 2024. https://www.sk-cert.sk/wp-content/uploads/2018/03/2018_69-Act-on-Cybersecurity.pdf.

agement of cybersecurity, adopt the historically first comprehensive legislation in the field of cybersecurity and create specialized structures for handling cases of cybersecurity breaches.

Within the framework of the second Concept, other goals are set. The main focus is shifting from regulation, since the main goals in this area have already been achieved, to practical activities, such as risk management, detection and elimination of cybersecurity incidents, recovery from cyber attacks, etc. Law enforcement and other bodies are also trained (police officers, prosecutors, judiciary) in the field of cybercrime. Despite the fact that the second Concept was adopted, the provisions laid down by the first one still serve as the basis for legal regulation and the goals outlined in it have yet to be achieved.

Despite the long experience of taking measures within the framework of regulation in this area, there is no agreed formalized terminology in the field of cybersecurity in the Slovak Republic. The term "cybercrime", like "cybersecurity", is not directly defined in the Criminal Code or in a similar legal act. However, the existing Criminal Code defines certain facts of the crimes that constitute cybercrime. Thus, every cybercrime is a cybersecurity incident, while not every cybersecurity breach is a cybercrime. As suggested by ENISA, contextual definitions are used for the purposes of specific laws. However, for the actual activities of public administration in the field of cybersecurity and for understanding the relationship between cybersecurity and the main areas of security of state activity, a legally binding definition of the meaning of these terms is crucial.

2.6. Main legal acts regulating cybersecurity in the energy sector

With regard to cybersecurity and the energy sector in particular, attention should be paid to the following documents: the EU Security Union Strategy and the EU's Cybersecurity Strategy for the Digital Decade as well as some other criminal law acts.

2.7. EU Security Union strategy

The EU Security Union Strategy is a document adopted by the European Union on the proposal of the High Representative of the Union for Foreign Affairs and Security Policy, which identifies the main threats which the European Union is facing, defines the main directions for achieving security, as well as strategic goals and possible consequences for the Union. The EU Security Union Strategy was first drawn up in 2003 and subsequently revised; the current strategy was adopted for the period from 2020 to 2025 and covers a wide range of issues, including those related to cybersecurity in the fuel and energy sector. The EU Security Union Strategy is a document and its main task is to identify the most significant and urgent threats to the security of the EU, as well as to develop ways and methods to counter these threats. The document outlines four priority areas: 1) creating a secure environment that is resilient to future threats; 2) combating emerging threats; 3) protection against terrorism and organized crime; 4) creation of a strong European "ecosystem" of security. Directions 1 and 2 seem to be the most important in the context of cybersecurity in the fuel and energy sector[22].

[22] EU Security Union Strategy: connecting the dots in a new security ecosystem. Accessed August 7, 2024. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379.

Within the framework of the first direction, the following points are distinguished: protection and resilience of critical infrastructures, cybersecurity and protection of public places. All of the above-mentioned components have in common a large number of users, and consequently a large number of potential victims from the attacks. EU citizens rely on key infrastructures, both online and offline, for a variety of purposes and attacks on such infrastructures can cause significant disruption and wide-ranging consequences. Readiness and resilience to attacks are key factors in rapid recovery. The key infrastructure objects, such as transport, healthcare systems, fuel and energy facilities, more often than others become objects of terroristic and other attacks. The current system of protection and resilience of critical infrastructures in the EU does not always keep up with the growing risks. Increasing interdependence means that disruptions in one sector can have a direct impact on operations in others: an attack on power generation can disable hospitals or airports, and an attack on digital infrastructure can disrupt power networks. The process of gradual transition of many areas of public life to the online environment is obvious, which makes such risks more significant. The legal framework must address this increased interconnectedness and interdependence by providing strong protection for critical infrastructure both online and offline.

The measures outlined in the strategy contribute to the expansion of cooperation between the public and private sectors; provide stronger physical protection of public places. Bringing together representatives of the public and private sectors has long been deemed impossible due to the reluctance to disclose information related to security, as this could jeopardize national security or competitiveness. However, the best results can only be achieved through joint efforts, which imply more intensive cooperation between Member States, with the participation of law enforcement, judicial and other public authorities, as well as with EU institutions and agencies, in order to achieve mutual understanding and exchange of data necessary for common decisions. As well as cooperation with the private sector, given that industrial facilities own an important part of the digital and non-digital infrastructure that plays a key role in the effective fight against crime and terrorism. Individual citizens can also provide assistance, such as by raising awareness to combat cybercrime or disinformation[23].

When it comes to cybersecurity, the number and complexity of cyberattacks is increasing every year. The task of the EU today is to anticipate such attacks and respond to them in a timely manner. The need to ensure a high level of cybersecurity in Europe is confirmed by statistics. Studies show that at least 80 % of European companies experienced at least one cybersecurity breach in 2020, and the number of security incidents has increased significantly across all industries[24]. In particular, the energy sector is highly dependent on secure network and information systems. Major gas and electricity companies are suffering from an increase in cyberattacks motivated by vested and criminal intent.

[23] Joint Communication JOIN/2017/0450 final. Joint Communication to the European Parliament and the Council "Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU. Accessed August 7, 2024. https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52017JC0450.

[24] ENISA 2020 Report "Threat Landscape". Accessed August 7, 2024. https://op.europa.eu/en/publication-detail/-/publication/98368007-475a-11ec-91ac-01aa75ed71a1/language-en.

2.8. European Union's cybersecurity strategy for the digital decade

The second fundamental legal act is the European Union Cybersecurity Strategy for the Digital Decade[25]. The strategy outlines the main areas of action for EU bodies to protect citizens and businesses from cyber threats, as well as to develop and protect a global, open, free and secure cyberspace. The goal of the strategy is to achieve the situation in which all persons can fully enjoy digital services and tools without violating their rights and freedoms.

The adoption of a separate act devoted exclusively to cybersecurity issues can be explained with the fact that today the investigation of almost all types of crimes has a digital component. The number of such crimes increases several times every year, and the annual damage from cybercrime to the global economy in 2020 was estimated at € 5,5 trillion.

Critical infrastructure sectors, including energy sector, are increasingly dependent on digital technologies for their core activities. And while digitalization opens up opportunities and provides solutions to many of the challenges Europe faces, it also exposes economies and societies to cyber threats. The effective fight against cybercrime is a key factor in ensuring cybersecurity: its implementation cannot be achieved solely through sustainability, but also requires the identification and prosecution of offenders. Therefore, it is extremely important to develop cooperation and data exchange between cybersecurity actors and law enforcement agencies.

The Strategy defines specific measures that are aimed at achieving this interaction. Thus, it is noted that at the level of the European Union, close cooperation is currently being implemented between the European Union's law enforcement agency (Europol) and ENISA. It is expressed in the exchange of necessary information, the joint development of measures to respond to the most common cybercrimes. Europol also assists national law enforcement agencies in the fight against cybercrime and related crime by helping to define common forensic standards. The Agency also proposed the establishment of a Joint Cyber Unit, a platform for cooperation between various organizations related to cybersecurity in the EU, with a focus on operational and technical coordination in relation to major cross-border cyber incidents and threats. With regard to law enforcement cooperation, the need to increase the capacity of law enforcement and judicial authorities to investigate and prosecute cybercrime is emphasized. This implies facilitated cross-border access to electronic evidence, subject to due process and other safeguards. At the same time, the competent authorities in the field of security and criminal justice should be able to access data primarily through legal means.

2.9. Other criminal law acts

One of the first steps towards improving the criminal law response to cyber attacks was the adoption of Directive 2013/40/EU[26] of August 12, 2013 on attacks on information systems. This document establishes minimum rules regarding the definition of criminal

[25] Joint Communication JOIN/2020/18 final. Joint Communication to the European Parliament and the Council "The EU's Cybersecurity Strategy for the Digital Decade. Accessed August 7, 2024. https://eur-lex.europa.eu/legal-content/ga/TXT/?uri=CELEX:52020JC0018.

[26] Directive of the European Parliament and of the Council "On attacks against information systems and replacing Council Framework Decision 2005/222/JHA". Date of last revision: 14.08.2013. Accessed August 7, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0040.

offenses and sanctions in the field of attacks on information systems, and also provides for measures to optimize operational cooperation between authorized authorities. One of the advantages of the adoption of this directive was the actively developing process of criminalization of cyber attacks, as well as the effective cooperation of law enforcement agencies in the investigation of cross-border crimes of this direction. Despite the fact that this legal act was adopted and entered into force more than five years ago, not all Member States comply with all the stipulated provisions. The European Commission actively promotes the implementation of the provisions of the directive in the EU member states and at the moment does not see the need to revise or amend the document[27].

2.10. Main trends and directions of activities of the EU in ensuring cybersecurity

The European Commission is currently putting forward proposals to revise the Network and Information Systems Security Directive[28]. Despite the progress that has been made with the adoption of the Networks and Information Systems Security Directive, in particular the significant change in the institutional and regulatory approach to cybersecurity in many EU Member States, this document no longer meets all the challenges of modern society.

New threats, and in particular those resulting from the digital transformation of society accelerated by the COVID-19 crisis, appear on a regular basis and therefore require innovative responses. Now, any disruption, even initially limited to one organization or one sector, can have broader implications, potentially leading to far-reaching and long-term negative impacts on service delivery throughout the domestic market. To solve these problems, the European Commission has provided a new legislative proposal.

The Commission's proposals are to overcome the drawbacks of the first NIS Directive in order to adapt it to current needs. To do this, it is put forward to expand the sphere of effect of the Directive and include new sectors important for the economy and society, as well as extend its effect to medium and large businesses. It is proposed to *toughen* the requirements for the security of companies that serve as providers of basic services. Among all the proposed initiatives, the central place is occupied by ensuring the effective work of law enforcement and judicial authorities by developing new tools to combat cybercriminals.

3. Conclusions

The elaboration of information technology simultaneously opens up new opportunities for traditional crimes and creates new types of crimes that are inherently associated with digital devices. While countermeasures are actively being taken to combat cybercrime, the prevalence and high statistics indicate that such measures are insufficient. The main reasons are the essential characteristics of cybercrime, namely transnational nature, decentralization, constant and rapid development, inconsistencies between national laws on cybercrime.

---

[27] Joint Communication JOIN/2017/0450 final. Joint Communication to the European Parliament and the Council "Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU.

[28] NIS Cooperation Group Report "Sectorial implementation of the NIS Directive in the Energy sector" 2019.

Cybersecurity regulation is in constant development, as measures taken within the framework of EU policy lead to changes and adjustments in the legal basis for regulation of this category and vice versa. The EU's cybersecurity policy can be described as flexible, covering a wide range of different sectors and giving Member States the freedom to act in the process of implementing the norms. Today, legal acts regulating the provision of cybersecurity both at the level of the Union and in each state separately are adopted annually, both a legislative and a doctrine dedicated to this problem is being formed. However, due to the unpredictability inherent in new technologies, it seems likely that regulations in this area will need to be changed periodically.

The carried out analysis of legal norms shows that ensuring cybersecurity requires comprehensive and stable legislation. Initially, cybersecurity issues affected a small number of legal acts or their separate parts; over time however both the legislator and specialized organizations began to pay attention to insufficient coverage of this issue. The laws adopted today can be divided depending on the approach taken by a particular state: focusing on computer functions or ensuring the confidentiality and security of data. The European Union legislator takes an approach that focuses on both aspects. Such an approach undoubtedly has advantages: it prevents excessive criminalization and promotes the process of convergence of legal rules of different states or at least the reduction of differences. Within the framework of this approach, the following stages are distinguished: first, the adopted laws on cybercrime and cybersecurity should reflect new crimes against computers and information systems, and traditional crimes moving into the digital environment as well as other threats to cybersecurity. Secondly, in relation to new threats, the legislation should define and distinguish between the reasons why such crimes were committed: violation of data confidentiality or obstruction of the normal functioning of computers and other digital devices. Finally, it seems important to formalize in legislation a unified list of acts that are considered as crimes in order to prevent a situation in which a criminal can escape punishment residing on the territory of a state where such act is not a crime according to the criminal law.

The definition of cybersecurity, as well as related definitions of cyberspace, cybercrime, cyberattacks, do not have a single legal framework and are applied depending on the industry and context. The flexibility, and in some cases the ambiguity, of the term "cybersecurity" entails both advantages and disadvantages. On the one hand, this allows new technologies to be integrated and become subject to EU cyber security policy as they emerge, while at the same time, it can lead to the inclusion of an excessive number of provisions and potentially impede effective regulation in this area. The agencies and services of the European Union specializing in cybersecurity have come to the conclusion that a single legislative consolidation of the term is not possible, and any proposed definition will not fully cover all aspects of this complex phenomenon.

Cybersecurity is a cross-sectoral phenomenon, and it occupies a special place in the field of the fuel and energy complex, since society and various sectors of industry depend on energy supply, and fuel and energy facilities are the most important life support facilities. At the same time, a sector is undergoing constant major changes (e. g. the introduction of renewable energy sources, decentralization of energy generation). As a result, it requires special attention to such specifics as problems that arise in real time, as well as a significant degree of interdependence of objects. In general, the industry can be characterized as vulnerable to various types of attacks, and the digitalization process affects

the openness of industry facilities and reduces their degree of security. While computer security incident response teams, such as ENISA, are slowly emerging throughout the European Union and providing security services to all sectors of the economy, very few focus exclusively on incident management in the energy sector. It is important to promote information exchange initiatives in the energy sector. The European Commission, among other things, sets itself the task of raising awareness on this issue and spreading among all participants the understanding that energy companies are interconnected and that overall security and, therefore, cybersecurity is possible only if each participant is protected. The implementation of the security of such objects, including by legal means, should be given special attention. Since the lack of uniform rules in this area can lead not only to physical restrictions on supplies, but also affect the future development of the sector, in particular, it will affect the slowdown in the implementation of EU energy policy goals, such as integration within the single energy market.

References

Carrapico, Helena, André Barrinha. 2017. "The EU as a coherent (cyber) security actor?" *Journal of Common Market Studies* 55 (6): 1254–1272. https://doi.org/10.1111/jcms.12575

Fuster, Gloria González, Lina Jasmontaite. 2020. "Cybersecurity regulation in the European Union: The digital, the critical and fundamental rights". *The Ethics of Cybersecurity* 21: 97–115. https://doi.org/10.1007/978-3-030-29053-5_5

Kelemen, Miroslav, Stanislav Szabo, Iveta Vajdová. 2018. "Cybersecurity in the context of criminal law protection of the state security and sectors of critical infrastructure". *Challenges to national defence in contemporary geopolitical situation* 1 (2018): 100–104. https://doi.org/10.47459/cndcgs.2018.14

Rasmussen, Scott. 2011. "English legal terminology: Legal concepts in language". *International Journal of Legal Information* 39 (3): 394–395. https://doi.org/10.1017/S0731126500006314

Vanek, Dušan. 2021. *The Slovak National Security Authority may be granted greater powers regarding cyber security*. Accessed August 7, 2023. https://cms-lawnow.com/en/ealerts/2021/03/the-slovak-national-security-authority-may-be-granted-greater-powers-regarding-cyber-security.

Received: September 1, 2023
Accepted: April 29, 2024

Authors' information:

Viktor A. Shestak — Dr. Sci. in Law, Associate Professor; https://orcid.org/0000-0003-0903-8577, viktor_shestak@mail.ru
Polina G. Savenkova — LLB, Lawyer; https://orcid.org/0000-0003-4992-8400, sanverst@yandex.ru