Humanities and Social Sciences **2023**
Research Journal 30, No. 4 (2023) – part I, pp 183-197 **October-December**

Received: May 2023
Accepted: December 2023
DOI: 10.7862/rz.2023.hss.50

Izabela OLEKSIEWICZ[1]
Mustafa Emre CIVELEK[2]

WHERE ARE THE CHANGES IN EU CYBERSECURITY LEGISLATION LEADING?

Cybersecurity policy is a response to the growing instability of the virtual world and the threats emanating from this area. This article tries to show how changes in legislative and strategic provisions can affect the EU's cybersecurity policy. The analysis of the field of cybersecurity in the European Union, the subject of which is the union itself, allows the authors to demonstrate the existence of such a policy in the EU. The subject of the analysis is the phenomenon of cyberterrorism as a threat and its specificity as a form of violence. The article shows how policy and strategy are interrelated, paying particular attention to the security concept of the European Union. The starting point of the research is the analysis of issues related to the specific nature of EU cyberterrorism policy and the most important legal bases in this field, on which EU cybersecurity policy is built. The preliminary study defines the concepts of cyberterrorism, cybercrime, and cyberwar, showing their impacts on the national security policy of the information society and, thus, also on the cybersecurity policy of the EU.

Keywords: cybersecurity strategy, European Union, security, threat.

1. THE CONCEPT OF CYBERSECURITY POLICY

After the end of the Cold War and the collapse of the bipolar system, the scale, scope, and intensity of traditional military threats decreased significantly (primarily in the transatlantic area) (Zięba, 2010). On the other hand, reducing the risk of a global war did not translate into mitigation of regional or local conflicts – they even intensified. Even today, asymmetric threats have developed or acquired new forms, the best example of which is the terrorist attacks that are taking place on the eastern border between Ukraine and Russia. Further evidence of such an asymmetric threat in recent years has been the so-called COVID-19 crisis, the effects of which we are still experiencing today and the more recent migration crisis of the EU (Ryan [ed.], 2022).

The subject matter of security policy depends primarily on many actors and conditions that fall within security theory. As a rule, it is divided into internal and external, and

[1] Izabela Oleksiewicz, Rzeszow University of Technology, Poland; e-mail: oleiza@prz.edu.pl (corresponding author). ORCID: 0000-0002-1622-7467.
[2] Mustafa Emre Civelek, Antalya Bilim Üniversitesi, Turcja; e-mail: mustafa.civelek@antalya.edu.tr. ORCID: 0000-0002-2847-5126.

objective and subjective (Majer, 2012; Jałoszyński, 2008). The structure of security policy is also important, especially when we consider all three areas – national, regional, and global. It should be stated that global and local security depends upon many factors, including political ones. The internal and external policies pursued by a given entity affect the sense of security of citizens and condition its place in international reality. An immediate threat is related to the possibility of war, to the state of being at war or to the official conduct of a military conflict (Tomaszyk [ed.], 2017). A political, economic, social, or cultural crisis can also affect a country's international situation. Potential threats and challenges to shaping the security of a given country have its relations with its neighbors.

The cybersecurity policy defines how user accounts and data stored in the system are used, ensuring that the institution's information is properly protected (Andersson, Biscop, Giegerich, Mölling, 2017). In every organization, there is protected information, e.g., personal data, financial information, and non-confidential information, e.g., marketing information (Wawrzyniak, 2019). The policy of protecting the cyberspace of the state is addressed to all users of cyberspace within a given state and outside its territory, in places where representatives operate. Its task is to oblige government administration bodies to create a system of protection of the cyberspace of the state, which will both react quickly and prevent the occurrence of a cyber attack and, in the event of this, will be able to efficiently defeat the cyber attack.

Defining cyberterrorism as a combination of cyberspace and terrorism means that such activity involves not only hostile use of Internet Technology (IT) and virtual activities, but also has all the elements constituting terrorist activity. The term refers to unlawful attacks and threats against computers, networks, and information stored in them with the purpose of intimidating or coercing the government or its people in order to obtain certain political or social benefits. In addition, to qualify as cyberterrorism, an attack should be perpetrated as a result of violence against persons or property, or at least cause significant damage to create fear. Examples of such attacks could be those that lead to death or injury, cause explosions, or economic damage. According to D. Denning, attacks that disrupt non-essential services or are primarily costly are not among them (Denning, 2023).

Thus, it must be concluded that the term "cyberterrorism" is used in the context of a politically motivated attack on computers, networks, or information systems to destroy infrastructure and intimidate or coerce far-reaching political and social objectives in the broad sense of the word (Manzano, 2018). These definitions prove that cyberterrorism (Daniluk, 2019) can be understood in two ways around the world. According to one concept, it differs from classical terrorism only by the use of information technology to carry out an attack, while the other emphasizes computer systems as a target for attacks, not a tool to carry them out. It seems that a true definition arises only after the combination of these two approaches.

In the literature, in addition to the concept of cybercrime, one can use such terms as: "computer crime", "computer-related crime", and "Internet crime". These terms often used interchangeably, have not been precisely defined due to the lack of general agreement on their scope of meaning. As A. Adamski emphasizes, computer crimes are discussed both in substantive and procedural aspects. In the light of substantive criminal law, two types of computer crimes can be distinguished. The first group includes all attacks directed at systems, data processed and maintained in them, and computer programs. Computer systems and networks are, in this case, the object or environment of attack. The second group includes crimes committed with the use of a computer to infringe on goods traditionally protected by criminal law.

The term ‘cybercrime’ refers to forms of use of telecommunications networks, computer networks, and the Internet, the purpose of which is to infringe any interest protected by law (Suchorzewska, 2010). What distinguishes cybercrime from classic crime is primarily its operation in a computer technology environment and the use of computer networks for committing a crime (*Cyberbezpieczeństwo*, 2018). Its distinguishing feature, on the other hand, is not the protection of a single common good. Today, almost every illegal activity is reflected on the Internet. The global nature of the Internet has enabled extremely fast communication and the transfer of most forms of human activity to the network, including those negatively perceived. There is more and more talk about cyberspace as a new social space in which the same problems are reflected as in the real world. Cybercrime is, therefore, a modern form of crime, exploiting the possibilities of digital technologies and the environment of computer networks (Carrapico, Barrinha, 2017).

The concept of cybercrime appears more and more often in the literature on the subject, although it should be noted that it has not yet had its normative determination. Cybercrime is defined as a sub-category of computer crime, covering all types of crimes that have been committed using the Internet or other computer networks. At the same time, computers and computer networks can be used to commit crimes in several ways: as a tool of crime, as a target of a crime, or for other additional tasks (e.g., storing data obtained as a result of a crime) (Krztoń, 2017). It, therefore, includes all attacks directed against interconnected computer systems and aimed at preventing them from working properly, either data stored in electronic form on a single computer, or several connected by a common network. The most characteristic feature of cybercrime is that individual acts can be carried out using a computer connected to the Internet or internal intranets (Davis, Fisher, Merry [ed.], 2012).

The purpose is to infringe any interest protected by law (Wojciechowski 2017 [za:] Sroka, Castro-Rial Garrone, Torres Kumbrian [ed.], 2017). Cybercrime is distinguished from classic crime primarily by operating in a computer technology environment and using computer networks to commit a crime (Bossong, 2018). Its distinguishing feature, on the other hand, is not the protection of a single common good (Oleksiewicz, 2020). Today, almost every illegal activity is reflected on the Internet. The global nature of the Internet has enabled extremely fast communication and the transfer of most forms of human activity to the network, including those negatively perceived. There is more and more talk about cyberspace as a new social space in which the same problems are reflected as in the real world. Cybercrime is, therefore, a modern form of crime, exploiting the possibilities of digital technologies and the environment of computer networks.

Cybercrime is a relatively new phenomenon, spreading at a dizzying pace in well--computerized and highly networked societies. It poses a very serious threat and is difficult to combat. This is determined by the special properties that characterize this phenomenon. The first feature – obligations – means that the activities of cybercriminals easily penetrate the barriers that are national borders. Very often, cybercriminals conduct their activities in one place, and their effects are revealed completely elsewhere, in a place hundreds of kilometers away, often in another country, on another continent. This makes it impossible to define the legal system according to which such offenses are to be prosecuted, while at the same time making it much more difficult to designate the entities responsible for taking protective and preventive measures. Another feature – anonymity – certainly does not make it easier to quickly identify the perpetrators of crimes and detect the ways in which they operate. However, this is not entirely impossible but requires a tedious search and the implementation of well-thought-out planned activities. Convenience and the speed

provided by the use of modern computer techniques and networking foster a huge increase in this form of crime in most developed countries (Banasiński, Rojszczak, 2020).

Cyberterrorism and its threats are asymmetric and transnational (Dela 2020: Oleksiewicz, 2020). Counteracting the phenomenon is not a simple issue, because it is necessary to carry out systemic activities on many levels. There are many reasons that countering cyberterrorism faces many obstacles, including non-state character, indirectness of the attack, conducting an attack at a distance, the possibility of spreading it over time, the ease of carrying out an attack, and the need to constantly refine formal and legal solutions to counteract cyberterrorism. Acts of cyberterrorism can be carried out at a relatively low cost, all you need is a laptop and Internet access (Weimann, 2014).

All this makes the policy of protection against threats related to cybercrime extremely difficult and requires numerous undertakings, including those requiring multifaceted and wide-ranging international cooperation (Gross, Canetti, Vashdi, 2017). For this protection to be effective, individual countries must work together to establish a common cybercrime policy, and then concretize it by defining the necessary priorities and uniform rules for joint action. The general principles thus identified require implementation into the domestic law of States, becoming the basis for an institutional and functional system of instruments for combating the obligations of animity (Hoffman, 2018, za Dębski, 2018). Creating an effective system for counteracting cybercrime is not easy, it requires an in-depth analysis of the phenomenon in the long term, and when creating such a system, there may be numerous problems with the adaptation of general guidelines of international or EU law to internal law.

2. CYBERSECURITY STRATEGY OF THE EU

Policy and strategy determine the state's existence and development. The reason for this lies mainly in the strategy, i.e., in the methods, ways and tools of execution. Simplifying the answer, we can say that strategy is a "tool" of policy, and if so, in my opinion, the definition of strategy can be expressed as: "Security strategy is the means of creating and applying effective systems to respond to all threats to achieve long-term goals". Answering the question of what place strategy occupies in politics, we can say that it occupies a significant, or essential place. At the same time, policy and strategy tend to be volatile, dynamic, and constantly updated (most often as part of the so-called strategic review, which periodically revises the assumptions of the strategy). The relationship between policy and strategy, that is, the long-term concept of political action and the practical methods of their implementation in time and space with the use of available, potential, and created forces and means, is at the same time a fundamental factor in shaping the existence and development of the state (Oleksiewicz, 2022).

In the model functioning of the national or international security system, policy determines long-term goals in a given area, while strategy determines specific ways and methods and means of their implementation. These relations are particularly close at the design stage, that is, at the layer of goals. This is based on the fact that the objectives of the polystrategy, which should be a tool for the implementation of the general policy of the state in matters of national security, to a large extent, should be an expression of those objectives of state policy that relate to the external activity of the state. Precisely because of this, there is a need to ensure that the most important bodies of the state have a coordinated influence on the operation of strategies that are responsible for security, in response to contemporary threats. All of this supports the need for increasingly deep

research analysis that will take into account the phenomenon of linking politics with strategy and strategy with politics in the areas of national, regional, and global security (Biscop, 2019).

Peace-building strategy aims to prevent the emergence of disputes, armed conflicts, and other serious security crises, and peacekeeping strategy to resolve or reduce individual disputes and certain potential threats to prevent armed conflict for political or other reasons. The essence of a peacemaking strategy is to respond to conflicts or other serious security crises when there is no agreement. The peacemaking strategy, on the other hand, is used after an armed conflict if the parties to the conflict agree to peace cooperation.

The role of the strategic review as a tool for analyzing strategy internally and externally, identifying strengths and weaknesses, verifying potential (actual capabilities), and formulating the basis for future strategic actions (political, economic, socio-cultural, military) is crucial in this regard. This is because it allows policy and strategy to be adjusted, making them two complementary elements. In this way, the chosen direction of policy and strategy, expressed in the form of goals derived from the interests, needs, and values of society, is constantly maintained, although the forms and methods of its implementation may change. In addition, the use of a strategic review as a tool for verifying assumptions, and ways of implementing policies and strategies makes it possible to carry out: constant analysis of the strategy in the external and internal dimensions of the entity, recognition of its strengths and weaknesses, verification of potential (real opportunities) and verification of the basis for future strategic actions.

Referring to the state policy and strategy implemented in the external dimension will essentially be the result of the interaction between the entity and the environment in the context of existing or potential opportunities, challenges, and threats (Hua, Chen, Xin Luo, 2018). Speaking of the importance of policy and strategy for the state in the context of its formulation, it is necessary to point to the categories of scientific cognition that define the mutual relationship. These are the previously mentioned challenges, threats, and opportunities, fulfilling the functions of criteria for assessing the essence, scope, and nature of state policy and strategy, both externally and internally. At the same time, these criteria in the context of state policy and strategy do not occur on their own but are usually related to the vision, mission, and purpose of the entity's activities. In this regard, it should be noted that the entity's vision expresses the conceptual readiness to meet challenges, threats, and opportunities, usually defining its actions to ensure existence and development in the medium and long term. The entity's mission determines the way of its current activities to ensure the existence and development of existing (identified) challenges, threats, and opportunities. The entity's objectives, on the other hand, determine the direction of activities (implemented or undertaken) with existing (recognized) and projected challenges, threats, and opportunities. As already mentioned, strategy is a policy tool that can exist without a strategy or polystrategy, the goals set may be far-reaching, only they will not be realized. The reason for this lies mainly in the strategy, i.e., in the methods, ways and tools of execution. Security strategy is the way to create and apply effective systems to respond to any threat to achieve long-term goals.

In its communication i2010 on 1st June 2005 – A European Information Society for Growth and Employment (Communication from the Commission, 2005), the Commission identified three policy priorities in this area: completing the Single European Information Space, strengthening innovation and investment in ICT research, and creating an inclusive European information society. According to the Commission, one of the goals of European policy should be the creation of a Single European Information Space that provides secure

and affordable broadband connectivity, rich and diverse content, and digital services. Actions taken to achieve this should address four key elements: speed (spreading high-speed broadband services), multimedia content (improving economic and legal completeness to foster the emergence of new online services and content), interoperability (ensuring communication between different platforms and devices) and security (increasing consumer confidence in new technologies by protecting the Internet from fraud, harmful content, and technological failures). The Commission stressed the need to review the regulatory framework for electronic communications and develop and implement a strategy for the security of the European information society. Attention was also drawn to the need to create a coherent framework for the internal market in audiovisual services, including modernizing the legal framework and supporting the implementation of the existing acquis on services in this area.

Another priority identified by the Commission is innovation and investment in research. The Commission's goal in this area is to achieve a world-class level of research and innovation in the field of information and communications technology by putting it on par with Europe's main competitors. Measures taken by the Commission in this area include supporting strategic research on ICT, encouraging private investment in this area, and removing technological, organizational, and legal barriers to ICT implementation, thus negatively impacting better research results for economic gain. The measures applied in this area are intended to encourage the translation of technological advances into innovative applications in the public and private sectors. Strategic research focuses on technologies for knowledge, content, and creativity, open communications networks, secure and reliable software, embedded systems, and nanoelectronics.

The next priority area, as described in the i2010 strategy, is social inclusion, better services and higher quality. Particular attention has been paid here to the need to spread ICT products and services, including in less developed regions. The Commission pledged to provide policy guidance on e-accessibility and broadband coverage, adopt an e-government action plan, and establish model ICT initiatives in the field of quality of life.

The summary of the i2010 strategy emphasized that its implementation would make Europe a more attractive place for investment and innovation in knowledge-based goods and services. The important role of each of the entities responsible for its implementation was emphasized: The European Commission – carrying out the tasks presented, the Member States – introducing the new regulatory framework and taking their own initiatives in this area, and the other actors responsible for conducting an open and constructive dialogue.

The Communication from the Commission to the European Parliament, the Council, and the Committee of the Regions Towards a General Strategy to Combat Cybercrime, adopted on the 22nd of May 2007 ({SEC(2007) 641},{SEC(2007) 642}), is very important from the point of view of singling out from a series of activities broadly defined as 'preventing threats to common security' issues directly related to the fight against cybercrime and cyberterrorism. It emphasizes the fundamental importance of the ICT critical infrastructure for the security of EU states - the first time in strategic documents that this system is so clearly identified as one of the most important. The communiqué also indicates the need for EU institutions to develop a unified strategy to combat cybercrime. It defines the main operational tasks of combating cybercrime at the EU level, but also signals the need to harmonize definitions of crimes and state criminal laws in this area, although at the same time, "due to the wide variety of types of crimes covered by the concept of cybercrime [it stated that] it is not yet appropriate to harmonize definitions

across the board. In the years that followed, the European Union developed a series of strategic documents that were also a development of the findings of the 22nd of May 2007 Communication. On the one hand, these actions appear as a reaction to the 2008 financial crisis, fostering the destabilization of the global banking system, and on the other hand, they are the result of work undertaken by EU agencies to unify provisions for preventing threats to critical infrastructure in cyberspace. On the 31st of March 2011, the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions was adopted on Critical Infrastructure Protection "Achievements and next steps: towards global cyber-security" (COM(2011) 163 final).

3. CHANGES IN THE EU CYBERSECURITY STRATEGY

Given the dynamically evolving threats and in connection with the fact that cyberterrorism had been recognized as another important challenge for the European Union in 2013, the EU cybersecurity strategy (*Joint Communication*…, 2013) was adopted, the main objectives of which were to promote both the improvement of cybersecurity throughout the EU and beyond, as well as international cybersecurity cooperation.

The first key area described in the 2013 strategy is the prosperity of the digital single market and highlighting the importance of the EU's latest information and communication technology (ICT) and the ICT security sector in relation to strengthening cybersecurity. It stresses that legislation should support innovation and economic growth, research and should focus on infrastructure protection, as the digital economy is a major driver of growth, innovation and employment, and cybersecurity is key to protecting the digital economy.

The second identified area is the achievement of cyber resilience through measures improving network and information security across the EU at the Member State level, and cooperation between Member States and across the EU. It emphasizes the role of the Computer Emergency Response Team (CERT)[3] and the European Network and Information Security Agency (ENISA) (Rozporządzenie (UE) 2019/881 w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych (akt o cyberbezpieczeństwie) and encourages ENISA to cooperate with state institutions.

It was noted that the EU's resilience of critical infrastructures should be increased and strengthened through close cooperation and coordination between the relevant actors, including between civilian and European military actors. There is also a need to strengthen close cooperation and coordination in responding to cyber incidents by defense actors, law enforcement agencies, the private sector, and cybersecurity authorities to successfully tackle cyber challenges (Oleksiewicz, 2021).

The third priority was combating cybercrime, although it was also emphasized that it is of the greatest importance in the area of Internet security protection policy. Therefore, upon request, Member States should be assisted in identifying gaps and strengthening their capacity to pursue a preventive policy and combat cybercrime, use the Internal Security Fund (ISF) within its budget limit to support relevant anti-cybercrime authorities, take

[3] The organization was created in November 1988 by DARPA, after the Morris Worm Incident. The main CERT's task is to supervise Internet traffic 24/7 and takes immediate action in the event of threats. CERT-EU was created in 2011 and it is a part of European Commission. Its legal basis is Interinstitutional Agreement (Dz. Urz. UE C 12, 13.01.2018).

advantage of Instrument for Stability (IfS) to develop the fight against cybercrime, develop capacity-building initiatives, including police and judicial cooperation in third countries from where cybercrime organizations operate.

The fourth area is the Common Security and Defence Policy (CSDP). In this case, the main task is to develop a cyber defense framework and identify specific measures on security and defense by enhancing Member States' cybersecurity capabilities, leveraging existing pooling and sharing mechanisms, and exploiting synergies with wider EU policies to build the necessary cyber defense capabilities in a Member State. In this situation, it was necessary to adopt a new EU external security strategy[4].

From today`s additional perspective, it could be assessed that it was adopted too late concerning the actual needs and threats, but this does not change the fact that it remains relevant, as well as a basis for further legislative and programmatic work. The provisions of the adopted strategy have also led to the establishment of the European Center for Combating Cybercrime. This centralizing and coordinating institution, which began operations on the 11th of January 2013, mainly provides information exchange between police authorities of member states, supports operations against organized crime, and organizes training and exercises on cybersecurity and critical infrastructure for both government agencies and the private sector.

The Directive of the European Parliament and of the Council of 12th August 2013 on attacks against information systems (Dz.Urz.UE L 218/8 z 14.08.2013) and replacing Council Framework Decision was aimed at correlating the laws of member states in preventing, combating, and criminalizing crimes related to information and communication systems. The directive first pointed to the need to develop common definitions and correlations of typologies of these crimes. Another demand was to bring about effective, close, and proper cooperation between law enforcement agencies in individual countries, as well as between them and European institutions (Eurojust, Europol, ENISA, and the European Cybercrime Center). According to the Directive, cybercrimes include:

- illegal access to a system,
- illegal integration into a system,
- illegal integration into data,
- illegal interception of data, and illegal tools for committing cybercrimes.

Not only individuals, but also legal entities can be held liable.

In September 2017, the European Commission launched a review of the 2013 European Cybersecurity Strategy with a working document presenting its assessment (European Commission, 2017a). According to it, the strategy had been only partially successful due to insufficient resources and limited involvement of key actors. In addition, the opportunities and threats in cyberspace have expanded significantly since then. Therefore, these factors justified taking an important step, i.e., renewing the cyber security strategy. This situation changed with the introduction of the Directive on the security of network and information systems (the NIS Directive) (Dyrektywa…, 2016). This act formally

[4] Soldiers, like most people, use smartphones and social networks. Thus, they can become a potential target of an attack aimed at weakening their will to fight. It is only necessary to recognize the first and last names of crew members, determine the place of service and residence, link them with accounts on social networks, identify family ties, beliefs, values, prepare an attack and execute it. It is even more possible because we are too reckless about the use of smartphones by soldiers and their activity on social networks. Often even the personal data of soldiers and their images are publicly available on official websites.

created a network of Member States' Computer Security Incident Response Teams (CSIRTs), and the secretariat of this network is provided by ENISA.

On the 13th of September 2017, Jean-Claude Juncker said: "We have made progress in keeping Europeans safe online in the last three years. However, Europe is still not well equipped when it comes to cyber-attacks, which is why the Commission has adopted the cybersecurity package" (COM (2017) 477). It builds on existing instruments and presents new initiatives to further improve the EU's cyber resilience and response. This document identifies, for the first time, the need for the EU to maintain and develop essential capabilities to ensure the security of the digital economy, society, and democracy (European Commission, 2017b). The aim of EU policy has been to reduce market fragmentation, as well as develop economic capacity, and improve the response to cyber incidents. Specific political actions took place in 2017. In this context, EU action on public-private partnerships for research and innovation should be mentioned. As part of this policy, the need for a new European certification system was identified to ensure that products and services in the digital world are safe to use.

To equip the EU with the right tools to fight cyber attacks, the European Commission and the High Representative have proposed a wide range of measures to strengthen cybersecurity. To this end, an updated strategy has been introduced to improve the common approach of Member States to the phenomenon of cyber threats. So far, the role of the Network and Information Security Agency has been mainly to provide knowledge and advice, without operational activities in the area of cyber security. The new regulations in 2017 relate primarily to the strengthening of this agency, transforming it into an entity with a strong advisory role in the development and implementation of cybersecurity activities. Guidelines have been defined for its next mandate, which will start in 2020 and will be aligned with the new European digital security framework.

The reform was based on the actions envisaged in the cybersecurity strategy and the main pillar of the strategy – the Network and Information Security Directive (NIS Directive). In addition, the reform stipulates the following:

- establishment of the European Cybersecurity Competence Centre (ECCC) (pilot project launched in 2018). Working with Member States, it will help develop and implement the tools and technologies needed to meet the ever-changing threats and ensure that defense is as modern as the weapons used by cybercriminals. ECCC will complement capacity-building activities in this field at EU and national levels (Ilves, Evans, Cilluffo, Nadeau, 2016).
- development of a Member States' rapid response plan for an immediate, effective, and coordinated response in the event of large-scale cyber attacks. In addition, Member States and EU institutions are called upon to establish a cyber crisis response framework so that this plan can be implemented. It will be tested on a regular basis as part of cyber and other crisis management exercises.
- greater solidarity – in the future, the possibility of establishing a new emergency response fund for cybersecurity could be considered for those Member States that will responsibly implement all cybersecurity measures required under EU law. The fund could be used to provide emergency support to Member States, just as the EU Civil Protection Mechanism is used to improve response to fires or natural disasters.
- strengthening cyber defense capabilities – Member States are encouraged to integrate cyber defense into the Permanent Structured Cooperation (PESCO) framework and the European Defense Fund to support cyber defense projects. Cyber

defense could also be extended to the scope of the European Cybersecurity Competence Centre. To address the shortage of qualified staff in this area, in 2018 the EU created a cyber defense training and education platform. The EU and NATO support cooperation in cyber defense research and innovation. Cooperation with NATO will be strengthened through participation in parallel and coordinated exercises

- deepening international cooperation – the EU will strengthen its capacity to respond to cyber attacks by introducing a framework for a joint EU diplomatic response to malicious cyber activities in support of a strategic framework for conflict prevention and stabilization in cyberspace. This will be combined with efforts to build new capabilities to support third countries in the fight against cyber threats (European Commission, n.d.).

An important legal act is the General Data Protection Regulation (GDPR) (Regulation…, 2013), which introduced a set of consistent and uniform regulations for all companies operating in the EU that process the personal data of EU citizens. The purpose of this regulation was to protect the rights of individuals with regard to the processing of personal data. The regulation defines the right of access to information, regulates the collection of information, the processing and transfer of data between public entities, and gives citizens the right to 'be forgotten', requiring companies to delete certain personal data at the request of the citizen. It is worth noting that the NIS Directive only applies to critical operators and the GDPR – to anyone dealing with personal data. Another difference is that the GDPR potentially imposes high fines for breaches of personal data protection, however, so far, the fines related to network and information security appear to be smaller (Garrison, Hamilton, 2019).

On 9th April 2019, the Council adopted a regulation known as the Cybersecurity Act (Rozporządzenie Parlamentu Europejskiego…, 2019), which established a certification system at the EU level and a modernized EU cybersecurity agency replacing ENISA. It has also enacted rules that allow for the imposition of EU-targeted restrictive measures and sanctions to prevent and respond to cyber attacks that pose an external threat to the EU or its Member States. As part of the same reform, the EU also introduced legislation to establish a European Cybersecurity Competence Centre, supported by a network of National Coordination Centers. These structures will help to secure the digital single market and increase the EU's autonomy in the field of cybersecurity. In addition, the EU may impose sanctions against EU persons or entities, as well as against non-EU countries or international organizations, if it deems it necessary to achieve the objectives of the common foreign and security policy (Parlament Europejski i Rada Unii Europejskiej, 2019).

An important move in cybersecurity policy was the publication of the White Paper of 2020 on artificial intelligence (AI) and digitization, which is to be the key to combating cyberterrorism and achieving climate order by improving AI (Komisja Europejska, 2020). This is a necessary element to maintain the EU's single market through research, innovation, and the implementation by December 2020 of a coordinated action plan under the Digital Europe and Horizon Europe 2021-2027 programs. The latest move as part of the above-mentioned program is the establishment of the Joint Cyber Unit (European Commission, 2021) on 4th August 2021 (*Cybersecurity*…, 2023). Its role is to develop, by 31st December 2021, an EU cybersecurity incident and crisis response plan based on national cybersecurity incident and crisis response plans. The assumption is that the EU cybersecurity incident and crisis response plan is to set out the procedure and information

exchange, as well as the criteria for activating the mutual assistance mechanism based on the agreed incident classification and the list of available EU capabilities (Konkluzje Rady…, 2021).

In December 2020, the EU released its second Cybersecurity Strategy (EUCSS)[5]. This new strategy aims to guarantee a global and open Internet with strong safeguards in the event of risks to the security and fundamental rights of citizens in Europe. It is a major update to the first one, and its main goal is to implement and promote the main areas of EU action:

- resilience, technological sovereignty and leadership,
- building operational capacity to prevent, deter and respond,
- advancing a global and open cyberspace through increased cooperation.

The most commonly known change mentioned in the 2020 EUCSS was the announcement of the upgrade and update of the NIS Directive. The EU Cybersecurity Strategy answers the challenges of geopolitical competition in cyberspace, and the increased cyber threat landscape, especially following the COVID-19 pandemic. It allows the EU to increase its resilience and show leadership in cyberspace; build capacities to prevent, deter, and respond to cyber-attacks; and strengthen its partnerships in favor of a global and open cyberspace.

The Commission proposal expands the scope of the current NIS Directive by adding new sectors based on their criticality for the economy and society, and by introducing a clear size cap – meaning that all medium and large companies in selected sectors will be included in the scope. At the same time, it leaves some flexibility for Member States to identify smaller entities with a high-security risk profile.

On the 21st of April 2021, the European Commission published a draft Regulation of the European Parliament and the EU Council concerning the creation and adoption of harmonized legal standards for artificial intelligence systems in the European Union (Proposal…, 2021) (hereinafter the Regulation). The horizontal nature of this proposal is intended to ensure consistency with existing Union regulations applicable to sectors where artificial intelligence systems are already being used or are likely to be used in the near future. From the content of the draft, we can learn that AI, as a rapidly developing technology that can bring a number of economic and social benefits, can also give rise to risks for humans or society. In this situation, the EU simultaneously wants new technologies to be created and used in accordance with the supreme values of human rights and the fundamental principles of the organization. It was these elements that guided the Commission's work in drafting the Regulation. This project was intended to implement a political commitment made by President Ursula von der Leyen - in the policy guidelines for the Commission for 2019–2024.

Cyber Resilience Act (Proposal…, 2019), adopted on 15th September 2022, contains two main objectives aims to ensure the proper functioning of the internal market the first one is creating conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product's life cycle and creating conditions allowing users to take cybersecurity into account when selecting and using products with digital elements. Four specific objectives were set out:

[5] https://www.headmind.com/en/cybersecurity-in-the-eu-european-commissions-strategy-and-legislation [access: 20.04.2023].

- ensuring that manufacturers improve the security of products with digital elements from the design and development phase and throughout the whole life cycle.
- ensuring a coherent cybersecurity framework, facilitating compliance for hardware and software producers.
- enhancing the transparency of security properties of products with digital elements, and enabling businesses and consumers to use products securely.

The NIS 2 Directive (Directive…, 2022) eliminates the distinction between operators of essential services and digital service providers. Entities are classified based on their importance and divided respectively into essential categories with the consequence of being subjected to different supervisory regimes. In that regard, due account should be taken of any relevant sectoral risk assessments or guidance by the competent authorities, where applicable. The supervisory and enforcement regimes for those two categories of entities should be differentiated to ensure a fair balance between risk-based requirements and obligations on the one hand, and the administrative burden stemming from the supervision of compliance on the other. Given the intensification and increased sophistication of cyber threats, Member States should strive to ensure that entities that are excluded from the scope of this Directive achieve a high level of cybersecurity and support the implementation of equivalent cybersecurity risk-management measures that reflect the sensitive nature of those entities. It introduced more precise provisions on the process for incident reporting, content of the reports and timelines, more stringent supervisory measures for national authorities, stricter enforcement requirements, and aims at harmonizing sanctions regimes across Member States. It also enhanced operational cooperation, including cyber crisis management.

4. CONCLUSION

The scope of changes in EU law in the area of protecting cyberspace policy and combating cybercrime is closely related to the European Commission's program "Safer Internet". The program was run from 1999–2014 and aimed at promoting the safer use of the Internet and new online technologies, particularly for children. Starting in 2005, the program also covered all new online technologies, including mobile and broadband content, online games, peer-to-peer file transfer, and all forms of real-time communication (chat rooms and instant messaging). The scope of the program for 2009–2013 was to include emerging online technologies and cover harmful conduct, like grooming and cyberbullying. In 2015–2021, a "Safer Internet" project was amended to "Connecting Europe Facility" (CEF), and since 2022, it has been funded under the "Digital Europe" Program". Cyberattacks and cybercrime are becoming more frequent and more sophisticated across Europe, according to recent research. This trend will intensify in the future, as it is predicted that in 2025, as many as 41 billion devices will be connected to the Internet of things worldwide. An important role in this process, in the conditions of widespread digitization of Europe and the growing use of modern technologies, is to ensure security in cyberspace and prevent financial losses as a result of cybercrime.

The EU is trying to identify the reasons resulting from the development of the integration process, institutional, legal, and economic factors. Cybersecurity provisions under the policy of the area of freedom, security, and justice mainly concern the prevention and mitigation of cybercrime and the way the EU decides. Thanks to the so-called Under the qualified majority system, Member States try to regulate in a very detailed way the provisions on the protection of cyberspace. The EU is fighting cybercrime and stepping up

cyber defense while promoting cyber resilience. One can still ask the question of whether the actions taken are sufficient to meet the existing needs. This is evidenced by the results – an increase in the number of attacks in cyberspace. As you can see, the EU goes further in its activities, entering the sphere of defense, despite the fact that these competences are generally reserved for the member states. The EU cybersecurity policy is beginning to go beyond its "typical" nature, by creating more and more advanced forms of cooperation between EU Member States. It should be emphasized that the EU makes every effort to achieve the assumed economic, climate and political goals thanks to the cyberspace protection policy, and thus reduce the number of successfully carried out attacks in cyberspace, as, for example, the Belgians did. It is worth emphasizing that in the current institutional and legal conditions, it is difficult to talk about the creation of a fully independent cybersecurity system that would cover aspects of cybercrime and cyber defense.

REFERENCES

Andersson, J., Biscop, S., Giegerich, B., Mölling, Ch., Tardy, T. (2017), *Envisioning European Defence: Five Futures*. *„Chaillot Paper"*, No. 137.

Banasiński, C., Rojszczak, M. [ed.] (2020). *Cyberbezpieczeństwo.* Warszawa: Wolters Kluwer.

Biscop, S. (2019). *The EU Global Strategy 2020* ("Security Policy Brief" No. 108). Brussels: EGMONT – Royal Institute for International Relations. [Access: 31.03.2023]. Access on the internet: http://www.egmontinstitute.be/content/uploads/2019/03/ SPB108.pdf?type=pdf.

Bossong, R. (2018). *A Typology of Cybersecurity and Public – Private Partnerships in the Context of the European Union* [In:] Bures, O., Carrapico, H., ed., *Security Privatization. How Non-security-related Private Businesses Shape Security Governance*. Warszawa.

Carrapico, H., Barrinha, A. (2017). *The EU as coherent (cyber) security actor? "Journal of Common Market Studies"*, Vol. 55, No. 6.

Cyberbezpieczeństwo A.D. 2018: strategia, Policy, rekomendacje – cyberbezpieczeństwa w perspektywie Policy. Warszawa: NASK 2018.

Daniluk, P. (2019). *Wojna informacyjna – złożona przeszłość i niepewna przyszłość*, *„Rocznik Bezpieczeństwa Międzynarodowego"*, Vol. 13, nr 2.

Davis, K., Fisher, A., Merry, S.E. [ed.] (2012). *Introduction: Global Governance by Indicators*. Oxford.

Dela, P. (2020). *Teoria walki w cyberprzestrzeni.* Warszawa.

Denning, D. (2023). *Cyberterrorism, Prepared for Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives.* Access: 15.03.2023]. Access on the internet: http://www.cs.georgetown.edu/~denning/infosec/ cvberterror.html.

Gross, M.L., Canetti, D., Vashdi D.R. (2017). *Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. "Journal of Cybersecurity"*, Vol. 3, issue 1.

Garrison, Ch., Hamilton, C. (2019). *A comparative analysis of the EU GDPR to the US's breach notifications. „Information & Communications Technology Law"*, Vol. 28/1.

Hua, J., Chen, Y., Luo Xin (2018). *Are we ready for cyberterrorist attacks? – Examining the role of individual resilience. "Information & Management"*, Vol. 55.

Hoffman, T. (2018). *Główni aktorzy cyberprzestrzeni i ich działalność* [w:] Dębski T., red., *Cyberbezpieczeństwo wyzwaniem XXI wieku.* Łódź–Wrocław.

Ilves, L.K., Evans, T.J., Cilluffo, F.J., Nadeau, A.A. (2016). *European Union and NATO Global Cybersecurity Challenges: A Way Forward. „PRISM"*, Vol. 6/2.

Jałoszyński, K. (2008). *Współczesny wymiar antyterroryzmu*. Warszawa.

Krztoń, W. (2017). *Walka o informację w cyberprzestrzeni w XXI wieku*. Warszawa.

Majer, P. (2012). *W poszukiwaniu uniwersalnej definicji bezpieczeństwa wewnętrznego*. *„Przegląd Bezpieczeństwa Wewnętrznego"*, t. 4, nr 7.

Manzano, M. (2018). *Cyberwarfare, Greenhaven Publishing*. New York.

Oleksiewicz, I. (2020). *Znaczenie zagrożeń asymetrycznych w polityce bezpieczeństwa Unii Europejskie* [w:] Oleksiewicz, I., Delong M., ed., *Bezpieczeństwo państwa a bezpieczeństwo człowieka.* Rzeszów.

—— (2021). *Polityka – strategia – prawo*. Warszawa.

—— (2021). *Transformacja polityki cyberbezpieczeństwa RP w XXI wieku*. Warszawa.

—— (2022). *Artificial intelligence versus human – a threat or a necessity of evolution? "Przegląd Europejski"*, Vol. 3.

Ryan, J.M. [ed.] (2022). *Covid-19*. London.

Suchorzewska, A. (2010). *Ochrona prawna systemów informatycznych*. Warszawa.

Tomaszyk, M. [ed.] (2017), *Polityczno-społeczne i ekonomiczne zmiany w świetle Globalnej strategii na rzecz polityki zagranicznej i bezpieczeństwa Unii Europejskiej*. Poznań.

Wawrzyniak, A. (2019). *Społeczeństwo informacyjne: szanse i zagrożenia. „Poradnik Bibliograficzno-Metodyczny"*, t. 52, nr 2.

Weimann, G. (2014). *Cyberterrorism. How Real Is the Threat? „Special Report"*, Vol. 119.

Wojciechowski, S. (2017). *Reasons of Contemporary Terrorism. An Analysis of Main Determinants* [In:] Sroka, A., Castro-Rial Garrone, F., Torres Kumbrian, R., ed., *Radicalism and Terrorism in the 21st Century*. Frankfurt am Main–Bern–Bruxelles–New York–Oxford–Warszawa–Wien.

Zięba, R. (2010). *Główne kierunki polityki zagranicznej Polski po zimnej wojnie*. Warszawa.

LEGAL ACTS

Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions {SEC(2005) 717}.

Communication from the Commission to the European Parliament, the Council, and the Committee of the Regions Towards a General Strategy to Combat Cybercrime, adopted on the 22nd of May 2007 ({SEC(2007) 641},{SEC(2007) 642}).

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (O.J.L. 333, 27.12.2022).

Dyrektywa Parlamentu Europejskiego i Rady nr 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194/1 z 19.07.2016).

European Commission, *Cybersecurity Policies*. Shaping Europe's digital future. https://ec.europa.eu/digital-single-market/en/cyber-security (20.04.2023).

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 (Join/2013/01 final).

Komisja Europejska. (2020). Biała Księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania [Access: 20.04.2023]. Access on the internet:

https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_pl.pdf.

Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM/2022/454 final).

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts, COM (2021), 206 final.

Rada Unii Europejskiej (2021). Konkluzje Rady w sprawie zbadania potencjału inicjatywy dotyczącej wspólnej jednostki ds. cyberprzestrzeni – uzupełnienie skoordynowanego reagowania na szczeblu UE na cyberincydenty i cyberkryzysy na dużą skalę – Zatwierdzenie [Access: 20.04.2023]. Access on the internet: https://data.consilium.europa.eu/doc/document/ST-12534-2021-INIT/pl/pdf.

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), Dok. PE-CONS 86/1/18 REV 1(2017/0225 (COD) LEX 1899).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (Dz. Urz. UE L 151, 7.6.2019).