DOI : 10.14746/pp.2024.29.4.17

Marek GÓRKA
Koszalin University of Technology
ORCID: 0000-0002-6964-1581

Małgorzata KAMOLA-CIEŚLIK
The University of Szczecin
ORCID: 0000-0003-2956-3969

The Evolution of the European Union's Cybersecurity Culture in the Context of Selected Political and Economic Changes

Abstract: The purpose of the article is to attempt to characterize the concept of the EU's cybersecurity culture, based on key aspects of modern digitization, such as data protection, prevention of disinformation and responsible use of new technologies, which is relevant to the European and global digital security policy. The research methodology employed includes document analysis and qualitative methods. The article analyzes strategic documents from 2013, 2017, and 2020, which introduced new regulations, such as the NIS2 Directive, aimed at improving resilience to cyber threats and enhancing international cooperation. The study highlights the importance of building a culture of cybersecurity, education and responsible use of new technologies, and analyzes the effectiveness of the EU's response to rapidly changing digital threats. Modern Europe, based on democratic values and innovation, guards the security of its citizens in the online space, but on the other hand seeks to maintain a leadership position in the global digital economy.

Key words: European Union, political culture, security culture, cybersecurity culture, digitization, cybersecurity strategy

Introduction

In the face of increasing reliance on digital technologies, Europe needs to ensure the resilience of its operational systems and infrastructure, especially in the context of global distributions of digital technologies and information systems from different regions. In this new reality, where digital operations can affect the economy and daily life as effectively as traditional military operations, it is crucial to build a coherent cybersecurity policy as an important element in the stable development of the European Union (EU).

Some of the current issues in the public space, such as robotization, artificial intelligence and biotechnology, are the key challenges for the EU's cyber security culture. All these aspects show how important it is to build a solid foundation for a cyber security culture in the EU in order to effectively manage the opportunities brought by digitization and technological development (Ścibiorek, Zamiar, 2016, pp. 20–25).

The purpose of the article is to attempt to characterize the concept of the EU's cybersecurity culture, based on key aspects of modern digitization, such as data protection, prevention of disinformation and responsible use of new technologies, which is relevant to the European and global digital security policy. Challenges faced by the EU and for

which there are no simple solutions are analyzed. The common tasks facing the European community and its individual member states are in the interest of a strong union. This is self-evident, but in order for the union to be strong, it is the decision-makers making political decisions who have to make important and difficult choices. They need the support of citizens and their representatives. Therefore, there is also a need to understand the nature of the cyber security culture, which reflects the ongoing debate on the development of the EU, but also shapes the framework of the security strategies being built and, indirectly, the legal norms (Gryz, 2013, pp. 21–43).

The impact of the COVID-19 pandemic and the war in Ukraine are also of particular relevance to the topic at hand. The study focuses on identifying actions taken by the EU to enhance cybersecurity and assessing the effectiveness of these actions. The authors formulated the following research questions: 1) Is cybersecurity culture a subset of security culture and if so, is it characterized by any “special signs”?; 2) How can the European Union build a coherent cybersecurity policy in the context of new technologies?; 3) What was involved in the EU’s increase of the resilience to cyber threats in the documents it adopted between 2013 and 2023?

In the context of the study conducted, document analysis was used as one of the main research tools. Key EU strategic and operational documents were analyzed, such as the 2013 EU Cybersecurity Strategy and its 2017 update, the 2020 EU Cyber Security Strategy for the Digital Decade, the 2023 NIS2 Directive. The analysis of these documents made it possible to identify the main assumptions of the EU’s cyber security policy, priorities for action and the evolution of the strategy in response to changing threats. In particular, the focus was on analyzing activities related to building a cyber security culture, educating digital users and international cooperation. It enabled an objective evaluation of the effectiveness of cybersecurity measures based on insights drawn from strategic documents. Additionally, it facilitated an understanding of attack mechanisms, institutional responses, and the effectiveness of implemented strategies and countermeasures.

The structure of the article consists of two parts. The first focuses on the theoretical basis of the definition of culture and its relationship to political culture and security, including cyber-security culture. The second offers an analysis of EU policies that have introduced new rules and directives, such as the NIS2 Directive, to improve resilience to cyber threats, increase international cooperation, and educate as well as support citizens and institutions on cyber security.

Selected contexts of political and security culture

Modern culture – both in the political and security sense – must include the management of both physical and cyber space, combining the two realities. The Internet has become an integral part of modern life, encompassing information, banking, communications and other aspects of daily life. The key to success is the proper use of these technologies and an understanding of their potential risks and opportunities.

Culture is the area of human activity, that is viewed as: 1. the aggregate of the material and spiritual achievements of mankind covering the whole of its history or a specific era, or as 2. the level of intellectual development, the degree of excellence, proficiency in

mastering some specialty, skill, etc. (Polański, 2008, p. 387). Thus, culture is “the totality of mankind’s material and spiritual achievements accumulated, perpetuated and enriched in the course of its history, transmitted from one generation to another” (Szymczak, 1995, p. 1015). It also perpetuates social and political experiences. It provides a moral and spiritual foundation (Olechnicki, Załęcki, 1997, p. 106). Communities adopt cultural values and meanings in order to communicate and understand their environment with its institutions, which regulate social practices. This gives rise to another term, political culture, which is related to the adoption of values and patterns by the chosen community, but it is not the set of values themselves that is important, but their hierarchy (Antoszewski, Herbut, 1999, p. 260). However, not all collectivities have the same forms of political culture. Where there are significant socio-political, religious, or historical contrasts, one can note the more frequent presence of conflicts within a single social group. Therefore, more homogeneous political cultures are believed to be characterized by significantly greater stability.

Political culture refers to the ideas, beliefs, values, traditions and practices that form the basis of the political system (Olechnicki, Załęcki, 1997, p. 107). It is also a space of values that are the result of long-standing historical processes, as well as social, political, economic and many other factors. Therefore, each state is distinguished from others by its own individual political culture (Walicka, 2008, p. 279).

The above statements – relating to political culture – allow us to see that there is an interdependence and interaction between the cultural environment and the decision-making process. Thus, it represents the attitudes and orientations of the members of a given society toward politics, which consists of three factors: cognitive, affective and evaluative, i.e. knowledge and interest in politics, a sense of influence and degree of influence on political decisions, as well as ideas about the goals and ways of functioning of the political system (Bankowicz, 1999, p. 121; Antoszewski, Herbut, 1999, p. 260).

A frequent concept in recent years, given military developments, is the term security culture, which is a subset of a broad set identified with political culture. Security culture focuses on aspects related to protecting the state, society and the individual from various threats. Cybersecurity culture plays a specific role within security culture. It is a specific subset of security culture, focused on protecting information resources and digital infrastructure. The culture of cybersecurity within the framework of political culture refers to the technological dimension that shapes the development of institutional and legal frameworks, societies, and the economy in the EU.

The interrelationships between political, security and cyber-security culture outlined above provide some simplification, but also some oversimplification, which ignores the complex nature of the commonly present digitization. Therefore, the remainder of the article attempts to define the very concept of cybersecurity culture. In public discourse, the presence of a position consistent with “technological determinism” is perceived. This term has been an important interpretative key for many researchers used in the context of attempting to describe and understand phenomena at the intersection of society and technology (McLuhan, 1964; Winner, 1986; Mumford, 1967; Postman, 1992; Nye, 2006). These authors assume that social life is a reflection of technology or certain characteristics, preferences and processes within it. They determine the nature of social and political life, as well as the relations between its subjects. Changes in public life are

related to technological changes. This view holds that technology is governed by its own independent rules and is independent of the social environment. It has a dominant role that allows it to create socio-political divisions.

Cybersecurity culture – an attempt to define the concept

The topic of cyber-security culture is an important area of public life that raises serious concerns in the context of today’s challenges. The complexity of the interconnected network of digital systems that manage various aspects of reality, from individual life to national security, imposes increasing demands to ensure the stable functioning of reality based on information systems (Balzaq, Cavelty, 2015). Accordingly, it can be concluded that the culture of cybersecurity has one key feature, which is that participation in this culture is inevitable and independent of the degree of human interaction with technology (Davies, 2017).

In the current scientific discourse, one can observe content that deals with the importance of cybersecurity culture. Issues related to social, political and economic transformations, as well as the role of cyber technology in this context are discussed. Attention is paid to the use of digital tools in shaping social practices and their use as a key element in influencing changes in human behavior. This is in line with an approach that emphasizes understanding the role of technology in creating and perpetuating a culture of cyber security (Seaver, 2018). It also addresses the issue of responsibility for cybersecurity and the need for access to appropriate tools to ensure stable development (Martínez-Caro et al., 2020; Wang et al., 2022).

In the context of cybersecurity culture, it is important to understand how society reacts to new technologies and tools. Overcoming stereotypes and opening up to new technological possibilities has a significant impact on the formation of attitudes toward digital threats, which is a valuable area of research on the evolution in the perception and use of technological solutions. Cybersecurity culture is the subject of ample research, as it has the potential to influence information security behavior. Researchers define security culture differently, but the common denominator in many studies is to understand it as a set of beliefs and values linked to the use of digital technology and its acceptance by an institution, organization or specific social collective.

The very concept of cybersecurity culture can be considered from an institutional perspective, i.e. that of public and private entities, as well as at the organizational level, which concerns operations and countermeasures, and at the individual level, which includes the traits, behaviors, attitudes of individuals (Georgiadou et al., 2020). In addition, in describing cybersecurity culture, it is important to consider the importance of context, both in terms of how the concept itself functions and how it is perceived under specific conditions, such as geographic, political or historical ones (Creese et al., 2021).

The importance of a cybersecurity culture also applies to the exercise of political power. Here, a comprehensive approach is emphasized, involving the realignment of processes and operations at the level of the entire state, not just individual entities and organizations. Of particular relevance here are strategic documents in which policymakers attempt to formulate a clear strategy with action plans at the institutional level, taking

into account a variety of external factors such as the international situation in political, economic and military terms (Scupola, Mergel, 2022). Updating and redefinition of challenges is also a feature of these documents (Hinings et al., 2018).

Cybersecurity culture is conceptualized in various ways, depending on the context and perspective. Thus, an analysis of the concept makes it possible to highlight the relationship between, for example, the use of digital tools and their interpretation as to applications and endemicity in specific countries or regions. This peculiarity of specific entities and collectivities shapes the reception and functionality of cyber technology.

The differences in the absorption of information by people living in different countries is an example demonstrating this process. In authoritarian regimes, such as the current Russia, where social media are severely controlled or even banned, there is less articulation of content through such messengers. By contrast, in democratic countries, where there is free access to multiple sources of information, user activity is higher. However, the existence of a certain paradox about the opportunities and dangers of technological progress should be noted. Although the Internet is opening up space for democratic broadcasting, there is a growing concentration of power in the hands of large technology companies, which can lead to restrictions on freedom in the online space. This is particularly evident in the context of control over data and databases, where technology companies are becoming key players. At the same time, increasing dependence on these platforms can limit the autonomy of individuals.

Analyzing the culture of cybersecurity requires both an awareness of historical contexts and an understanding of contemporary threats. It is important to understand the differences in approaches to cyber security between different countries and regions. For example, the United States and China may have different perspectives on cybersecurity, which can lead to conflicts and tensions. In addition to issues of technology or procedures, international dialogue based on various forms of cooperation plays an important role in this area. Thus, in order to effectively address cyber security issues, cooperation among political actors is also necessary.

Until recently, cyber technology was strongly associated with military aspects and with a form of exercising power and having an advantage over other entities in the political space. The concept of cyber security, as a result of technological advances, naturally began to include the civilian sphere. This, in turn, has forced researchers to move from the traditional model of understanding security to a more complex one that takes into account the integration of different domains. This attitude has also become an important aspect of the evolution of the culture of cyber security, which is evolving with technological advances and changing environments.

A culture of cyber-security is not just for experts, but is an activity that any person can apply in everyday life, both personally and professionally. In this context, it is important to emphasize the need to prepare for possible cyber threats and strengthen personal and organizational resilience.

In colloquial terms, the culture of cyber security is reduced to practical solutions for applying measures to prevent cyber incidents. Hence, there are so many calls in the public space for, among other things, measures to minimize the risk of unauthorized access to user data. This perspective makes it possible to characterize the concept as a comprehensive approach to protecting data and systems from attacks in cyberspace. It

is an ongoing process that requires awareness, innovation and continuous improvement of knowledge to effectively counter the growing threats in the cyber world.

It is also important to note that while technological tools are important in shaping the future of the digital world, a focus on technology development alone may not be sufficient to address the complex issues of cybersecurity culture. The concept has evolved with the development of society, countries and technology, and reflects the changing social groups and their interactions in the online space. As new technologies develop and new threats emerge, it becomes necessary to establish appropriate policies and procedures to ensure security in cyberspace. Therefore, norms and rules of conduct that define expected collective behavior in cyberspace are an important part of building a cyber security culture. It is essential for entities to act in accordance with these norms in order to strengthen security in the global network (Hogan, Coote, 2014).

Given the above, the culture of cybersecurity cannot be clearly and fully defined, as it is too complex and unique to the collective. The value of culture is the result of historical heritage, changes in the organization, and the values and experiences of individuals. A uniform research approach to cybersecurity culture may be inappropriate, as it is necessary to frame the perception to the specific characteristics of the described collectivity or institution in order to fully reflect the picture of cybersecurity culture concerning a particular case (Cenamor, Parida, Wincent, 2019).

The literature highlights the relationship between organizational culture and cyber security culture. Research indicates that improving organizational culture has a positive impact on the state of information security culture and helps minimize cyber threats (Wiley, McCormac, Calic, 2020). Failures in the processes of implementing cyber security measures at the institutional level often result from a lack of alignment with organizational culture. Cybersecurity culture allows organizations to better cope with the challenges of implementing new technologies, making them more flexible and ready for change (Verhoef et al., 2021). Organizational culture, shaped by the shared values and norms of employees, plays an important role in shaping behavior in the organization and is a key factor in shaping the development of the institution (Astakhova, 2020; da Veiga, Astakhova, Botha, Herselman, 2020). Cybersecurity culture, on the other hand, refers to the collective attitudes and values regarding the safe use of digital technologies in business operations (Parsons et al., 2014). So when cybersecurity culture becomes an integral part of an organization, it will be integrated with other elements of organizational culture. It will shape cyber security processes motivated by core organizational values and expectations. However, a prerequisite for implementing an effective cybersecurity culture is to identify and understand the key factors that shape organizational culture and employee behavior (Collett, 2021).

Cyber security culture in European Union documents

After 2010, cyber security threats increased in Poland as well as in other EU countries. An increase in cyberattacks occurred during the COVID-19 pandemic when most services were moved to the Internet. Individuals, companies, corporations and public institutions were the targets of attacks. Since 2022, in the face of the war in Ukraine, cyber threats in

Poland and Europe have intensified, among others, in the media industry, the postal and courier services sector and critical infrastructure (European Union Agency for Cybersecurity). According to the CERT Poland report, in 2022 there were 322 reported incidents, 178% more than the year before (CERT Polska, NASK). Combating cyberattacks has become a goal of the EU, which has taken measures aimed at, among other things, shaping people’s safe behavior online. As a part of the implementation of the EU’s strategies, it sought to broaden the knowledge and attitudes of people using information technology by imparting content and role models in line with a culture of cyber security. Equipping individuals, employers and employees of companies and public institutions with knowledge of procedures and organizational tools and values to protect themselves from cybercrimes was an important part of this effort. At the same time, it should be noted that cybersecurity culture is one of the dynamic phenomena and requires constant attention from the management of state and private companies and public institutions.

Between 2013 and 2023, the EU published documents outlining procedures for responding to cyberattacks that pose a threat to the security, stability and prosperity of member states. The union’s first strategic document on cyber security was the European Commission’s (EC) Cybersecurity Strategy for the European Union: an open, safe and secure cyberspace, adopted in February 2013 (Joint communication to the European Parliament, the Council, the European Economic…). The strategy showed a vision of cybersecurity policy in the context of government and economic activities. The strategy, that is a planned course of action aimed at achieving goals in the long term, envisaged ensuring a cyberspace free of harmful activities and abuses that threaten the security of Internet users.

The 2013 strategy noted that cyberspace was vital to political, economic and social cooperation not only within the union but also around the world. The dependence of business entities on digital technologies has made the public and private sectors victims of cybercrimes. In this situation, it became necessary to build cooperation on cyber security between public authorities, the private sector and society within the EU and with community partners. The goal of the strategy was to enhance the EU’s ability to combat cybercrime especially in the area of information and communication technology. Cooperation among EU countries on cybersecurity was to establish common legal standards and ensure consistency in the political, law enforcement, digital agenda, defense, security and foreign policies (Opinia Komitetu Regionów). The European Network and Information Security Agency (ENISA) was the advisory body to member states and EU institutions on critical infrastructure protection.

The union’s member states have been obliged to take measures to increase citizens’ knowledge of network and information security. The development of the EU’s cybersecurity culture was and is important because of the incompetent use of digital technologies by the majority of its citizens, which affects their security. The EU’s cybersecurity strategy has been focused on promoting knowledge and education, developing computer incident response teams and investing in innovation. Senior management of private and state-owned entities was responsible for implementing a culture of cyber security within work organizations to reduce the risk of cyberattacks.

In September 2017, the EC issued an act called *Resilience, Prevention and Defense: Building a Robust European Union Cybersecurity*, which is an update to the 2013 EU Cyber Security Strategy. The document stated that the rapid development of digital tech-

nology between 2013 and 2017 increased the number of cyber-attacks, both on private and state entities, which had a negative impact on the lives of citizens and the economy globally. Therefore, ensuring an adequate level of cyber security was a challenge for member states. The goal of the 2017 updated strategy was to enhance technological capabilities and skills in the field of cyber security based on three pillars: 1. building the EU’s resilience to cyberattacks; 2. shaping effective EU cyber-prevention; and 3. strengthening international cooperation in the field of cybersecurity (Joint communication to the European Parliament and the Council, *Resilience,* …). Compared to the 2013 strategy, the 2017 strategy placed a stronger emphasis on the EU countries’ common stance against international incidents and cooperation between the military and civilian sectors. A more effective and stronger response to cyberattacks by member states and the structures of EU institutions became necessary. Against this backdrop, the 2017 strategy envisioned expanding the tasks and functions of the European Union Agency for Network and Information Security (ENISA) to more efficiently support the efforts of states and union institutions to guarantee a secure cyberspace in the EU (Proposal for a regulation of the European Parliament…).

The 2017 strategy pointed to the human factor which was 95% responsible for cybersecurity, while being its weakest link. The limited knowledge and skills of employees of companies and public institutions in the field of information and communication technology were a significant reason for the lack of effective cybercrime prevention. Thus, the behavior of these entities had to change in order to understand the risks and skillfully use tools to detect and protect against attacks. Therefore, the development of a cyber-security culture at all levels of the organizational structure of companies and government proved to be so important. The promotion of a cyber-security culture was to be carried out through training and courses for employees. Teachers in elementary and secondary schools, on the other hand, were tasked with sensitizing students to cybercrime issues as part of their acquired digital skills.

In December 2020, the EC and the European External Action Service (EEAS) presented a new EU cyber security strategy called the EU Cyber Security Strategy for the Digital Decade 30. The development of the new strategy was due to the emergence of new cyber threats and the existence of still limited cyber security skills in the workforce. The increase in cyberattacks occurred during the COVID-19 pandemic where most companies operated in remote or hybrid mode. The goal of cybercriminals was usually to gain illegal access to personal data, steal industrial or state secrets, which consequently had the effect of reducing security in cyberspace.

Therefore, the EC developed coherent rules for the functioning of EU institutions and bodies in the area of cyber security, and planned to establish a Joint Cyber Security Unit. The task of the newly established entity was to strengthen cooperation between EU institutions and member state bodies responsible for cyber security (Joint communication to the European Parliament and the Council, *The EU’s Cybersecurity…*).

The goal of the 2020 strategy was to determine how the EU would protect its citizens, businesses and public institutions from cyber threats and develop international cooperation, take action to ensure a global and open Internet. The EU’s work on an open, stable and secure cyberspace was to be based on the rule of law, fundamental freedoms and democratic values, which were an important element in the construction of cyberspace.

According to the EU’s strategy, all citizens and businesses were to have access to reliable services and trustworthy digital tools. To this end, the EC updated the Directive on Network and Information Security (NIS2) to counter current and future online threats. The EC’s updated directive went into effect in 2023 (Directive European Union). Increased levels of cyber resilience were to apply to critical public and private sectors (including, among others, hospitals, power grids, railroads, public administration). The EC’s updated NIS2 directive was to be implemented in 2023.

Legislation introduced as part of the EC NIS2 directive has tightened the security requirements imposed on businesses and public institutions in all member states. The 2020 strategy envisioned the establishment of a Network of Security Operations Centers across the EU, based on artificial intelligence. The center network was to be tasked with early detection of cyberattacks before damage could occur. The implementation of the strategy was to increase the EU’s resilience to cybercrimes, strengthen Europe’s role as a leader in creating international standards and laws in the area of network and information security. The 2020 strategy, alike the 2017 strategy, paid attention to supporting companies and public institutions by creating conditions for upgrading the skills of employees using digitization tools. The implementation of the strategy’s goals was aimed at consolidating a culture of cybersecurity in order to empower employees and increase the security of work organizations.

Recommendations

In the context of the coming global political changes, strengthening cybersecurity is becoming essential. The European Union must act proactively to not only defend its systems from attacks, but also to prevent external influences that could destabilize its democratic and economic structures.

There is a shortage of cyber security experts in the member states, which is reminiscent of the situation regarding the COVID-19 pandemic, where there was a shortage of doctors.

It is therefore necessary to launch new courses and programs at universities and intensify executive cyber training for companies and public administration.

Another important aspect is the issue of the risk of overregulation. A sustainable digital economy needs clear rules. Competition among different markets to set the rules is crucial for the EU. It is important that the best ideas and practical applications, are not hampered by complicated and lengthy legal procedures. On the other hand, the legal system must keep up with the dynamic development of technology.

The notion of strategic autonomy is an important challenge for the union. Currently, many players are seeking to impede competition by increasing protectionism. Many key technologies now come from the United States, but Europe is gradually increasing its autonomy, which in many ways is beneficial to the development of the union. However, the concern for digital autonomy, which is largely based on production capacity, is no substitute for the need to cooperate with such countries as the United States and China, or with global companies in the digital market such as, among others, Google, Apple, Microsoft. Thus, there is a need to develop an effective balance, allowing the EU to hold a leadership position in the digital world.

With the conditions for implementation identified above, it can be assumed that the EU will not only survive the challenges ahead, but will also be able to develop as a dynamic and innovative community.

Conclusions

The culture of cyber security in the European Union requires deep research reflection, as the concept crosses political, social, military or economic boundaries. The very process of building cultural unity and protection against modern cyber threats requires not only political decisions, but also fundamental social and cultural transformations.

The processes and phenomena taking place, or the practices used, that are important for ensuring the coherence and effectiveness of digitization efforts in the EU are crucial, but still not fully explored, especially when it comes to the nature and meaning of the concept of cybersecurity culture.

As the article tries to prove, the term is not only a matter of technology, but also a way of approaching change and adaptation in a dynamic digital world on the part of policy makers as well as society. Modern Europe, based on democratic values and innovation, guards the security of its citizens in the online space, but on the other hand seeks to maintain a leadership position in the global digital economy.

The EU’s cyber security culture is currently in an era of intense change and challenge. Faced with external pressures such as geopolitical crises and climate change, the EU is facing the need to react quickly and adapt digital solutions. This is evident in the transformation of European industry, technological cooperation and changes in international trade.

Author Contributions

Conceptualization (Konceptualizacja): Marek Górka, Małgorzata Kamola-Cieślik

Data curation (Zestawienie danych): Marek Górka, Małgorzata Kamola-Cieślik

Formal analysis (Analiza formalna): Marek Górka, Małgorzata Kamola-Cieślik

Writing – original draft (Piśmiennictwo – oryginalny projekt): Marek Górka, Małgorzata Kamola-Cieślik

Writing – review & editing (Piśmiennictwo – sprawdzenie i edytowanie): Marek Górka, Małgorzata Kamola-Cieślik

Competing interests: The author have declared that no competing interests exist

(Sprzeczne interesy: Autor oświadczył, że nie istnieją żadne sprzeczne interesy)

Bibliography

Antoszewski A., Herbut R. (1999), *Leksykon politologii*, Atla 2, Wrocław.

Astakhova L. (2020), *Issues of the culture of information security under the conditions of the digital economy*, “Scientific and Technical Information Processing”, vol. 47, no. 1, pp. 56–64.

Balzaq T., Dunn Cavelty M. (2015), *A theory of actor-network for cyber-security*, “European Journal of International Security”, vol. 1, no. 2, pp. 176–198.

Bankowicz M. (1999), *Słownik polityki*, Wydawnictwo Wiedza Powszechna, Warszawa.

Cenamor J., Parida V., Wincent J. (2019), *How entrepreneurial SMEs compete through digital platforms: The roles of digital platform capability, network capability, and ambidexterity*, “Journal of Business Research”, vol. 100, pp. 196–206.

CERT Polska, NASK (2022), *Raport roczny CERT Polska 2022, Krajobraz bezpieczeństwa polskiego Internetu*, https://cert.pl/uploads/docs/Raport_CP_2022.pdf, 22.06.2024.

Collett R. (2021), *Understanding cybersecurity capacity building and its relationship to norms and confidence building measures*, “Journal of Cyber Policy”, vol. 6, no. 3, pp. 298–317.

Creese S., Dutton W. H., Esteve-González P., Shillair R. (2021), *Cybersecurity capacity-building: Cross-national benefits and international divides*, “Journal of Cyber Policy”, vol. 6, no. 2, pp. 214–235.

da Veiga A., Astakhova L. V., Botha A., Herselman M. (2020), *Defining organisational information security culture-perspectives from academia and industry*, “Computers & Security”, vol. 92.

Davies W. (2017, July 13), *Who gains from big data?*, Weekly Economics Podcast, 12.11.2023, https://soundcloud.com/weeklyeconomicspodcast/who-gainsfrom-big-data.

Directive European Union (2022), 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), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2022:333:FULL, 30.06.2024.

European Union Agency for Cybersecurity (2022), *Threat Landscape 2022*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022, 22.06.2024.

Georgiadou A., Mouzakitis S., Askounis D. (2022), *Detecting insider threat via a cyber-security culture Framework*, “Journal of Computer Information Systems”, vol. 62, no. 4, pp. 706–716.

Gryz J. (2013), *Strategia bezpieczeństwa narodowego Polski*, PWN, Warszawa.

Hinings B., Gegenhuber T., Greenwood R. (2018), *Digital innovation and transformation: An institutional perspective*, “Information and Organization”, vol. 28, no. 1, pp. 52–61.

Hogan S. J., Coote L. V. (2014), *Organizational culture, innovation, and performance: A test of Schein’s model*, “Journal of Business Research”, vol. 67, no. 8, pp. 1609–1621.

Joint communication to the European Parliament and the Council, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, 13.09.2017, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450, 26.06.2024.

Joint communication to the European Parliament and the Council, *The EU’s Cybersecurity Strategy for the Digital Decade*, 16.12.2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018, 30.06.2024.

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*, 7.02.2013, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001, 22.06.2024.

Martínez-Caro E., Cegarra-Navarro J. G., Alfonso-Ruiz F. J. (2020), *Digital technologies and firm performance: The role of digital organisational culture*, “Technological Forecasting and Social Change”, vol. 154(c).

McLuhan M. (1964), *Understanding Media: The Extensions of Man*, McGraw-Hill, New York.

Mumford L. (1967), *The Myth of the Machine: Technics and Human Development*, Harcourt, Brace and World, New York.

Nye D. E. (2006), *Technology Matters: Questions to Live With*, MIT Press, Cambridge, MA.

Olechnicki K., Załęcki P. (1997), *Słownik socjologiczny*, Graffiti BC, Toruń.

Opinia Komitetu Regionów, *„Strategia bezpieczeństwa cybernetycznego”* (2013/C 280/05). DzUrz UE C280, t. 56, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52013IR1646&from=IT, 26.06.2024.

Parsons K., McCormac A., Butavicius M., Ferguson L. (2010), *Human factors and information security: Individual, culture, and security environment*, “Defense Technical Information Center”, 12.11.2023, https://apps.dtic.mil/sti/pdfs/ADA535944.pdf.

Polański E. (ed.) (2008), *Słownik języka polskiego*, Krakowskie Wydawnictwo Naukowe, Kraków.

Postman N. (1992), *Technopoly: The Surrender of Culture to Technology*, Knopf, New York.

Proposal for a regulation of the European Parliament and of the Council on ENISA, the “EU Cybersecurity Agency”, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (*“Cybersecurity Act”*), 4.10.2017, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0477R(01), 26.06.2024.

Scupola A., Mergel I. (2022), *Co-production in digital transformation of public administration and public value creation: The case of Denmark*, “Government Information Quarterly”, vol. 39, no. 1.

Seaver N. (2018), *Captivating algorithms: Recommender systems as traps*, “Journal of Material Culture”, vol. 24, no. 4, pp. 421–436.

Szymczak M. (red.) (1995), *Słownik języka polskiego*, PWN, Warszawa.

Ścibiorek Z., Zamiar Z. (2016), *Teoretyczne i metodologiczne podstawy problemów z zakresu bezpieczeństwa*, Adam Marszałek, Toruń.

Verhoef P. C., Broekhuizen T., Bart Y., Bhattacharya A., Dong J. Q., Fabian N., Haenlein M. (2021), *Digital transformation: A multidisciplinary reflection and research agenda*, “Journal of Business Research”, vol. 122, pp. 889–901.

Walicka B. (red.) (2008), *Słownik politologii*, PWN, Warszawa.

Wang T., Lin X., Sheng F. (2022), *Digital leadership and exploratory innovation: From the dual perspectives of strategic orientation and organizational culture*, “Frontiers in Psychology”, vol. 13.

Wiley A., McCormac A., Calic D. (2020), *More than the individual: Examining the relationship between culture and information security awareness*, “Computers & Security”, vol. 88.

Winner L. (1986), *The Whale and the Reactor: A Search for Limits in an Age of High Technology*, University of Chicago Press, Chicago.

Ewolucja kultury cyberbezpieczeństwa Unii Europejskiej w obszarze wybranych zmian polityczno-gospodarczych

Streszczenie

Celem artykułu jest próba scharakteryzowania koncepcji kultury cyberbezpieczeństwa UE w oparciu o kluczowe aspekty współczesnej cyfryzacji, takie jak ochrona danych, przeciwdziałanie dezinformacji oraz odpowiedzialne korzystanie z nowych technologii, co ma istotne znaczenie dla europejskiej i globalnej polityki bezpieczeństwa cyfrowego. W ramach zastosowanej metodologii badawczej przeprowadzono analizę dokumentów oraz zastosowano metody jakościowe. Artykuł analizuje dokumenty strategiczne z lat 2013, 2017 i 2020, które wprowadziły nowe regulacje, takie jak dyrektywa NIS2, mające na celu poprawę odporności na zagrożenia cybernetyczne oraz wzmocnienie współpracy międzynarodowej. Badanie podkreśla znaczenie budowania kultury cyberbezpieczeństwa, edukacji oraz odpowiedzialnego korzystania z nowych technologii, a także analizuje skuteczność reakcji UE na szybko zmieniające się zagrożenia cyfrowe. Współczesna Europa, oparta na wartościach demokratycznych

i innowacjach, chroni bezpieczeństwo swoich obywateli w przestrzeni online, jednocześnie dążąc do utrzymania pozycji lidera w globalnej gospodarce cyfrowej.

Słowa kluczowe: Unia Europejska, kultura polityczna, kultura bezpieczeństwa, kultura cyberbezpieczeństwa, cyfryzacja, strategia cyberbezpieczeństwa

Article submitted: 28.07.2024 article accepted: 17.08.2024.
Data przekazania tekstu: 28.07.2024 data zaakceptowania tekstu: 17.08.2024.