Aleksandra Pleśniarska
http://orcid.org/0000-0003-3257-8416
Krakow University of Economics
plesniaa@uek.krakow.pl
DOI: 10.35765/HP.2833

Horyzonty Polityki
2025, Vol. 16, N° 56

OPEN ACCESS

The EU Cybersecurity Strategy: Implications and Lessons for Other Regions[1]

Abstract

RESEARCH OBJECTIVE: This article aims at a description of the structure of cybersecurity in the EU, taking into account its most important objectives and characteristics, as well as its geopolitical and international context.

THE RESEARCH PROBLEM AND METHODS: The cybersecurity-focused discourse usually refers to the national dimension of security. However, the multidimensionality of cybersecurity determines the need to build cyber capacity also on the basis of cooperation in international relations, including the economic dimension. The article attempts to fill the gap in the discussion of the perception and implementation of cybersecurity at the transnational level, with reference to European Union activities. In carrying out this task, the paper relies on institutional and legal analysis, combined with a review of the literature and documents and normative acts.

THE PROCESS OF ARGUMENTATION: The article is composed of three parts. Part one sets out considerations on the conceptualisation of cybersecurity; part two describes the framework of cybersecurity in the EU; finally, taking into account the perspective of international organisations, part three presents implications resulting from the EU's experience.

1 The article presents the result of the Project no 085/EES/2024/POT financed from the subsidy granted to the Krakow University of Economics.

Suggested cittation: Pleśniarska, A. (2025). The EU Cybersecurity Strategy: Implications and Lessons for Other Regions. *Horizons of Politics*, *16*(56), 75–91. DOI: 10.35765/HP.2833.

RESEARCH RESULTS: The economic dimension (link to the functioning of the European single market) is of particular importance in the practical application of the EU's integrated approach to cybersecurity, alongside technical issues, building digital resilience and citizen awareness. What distinguishes the implementation of cybersecurity in the EU is the activity in the field of implementing regulations concerning, among other things: the resilience and responsiveness of selected public and private entities throughout the EU, the security of ICT products, services and processes, or the protection of consumers and businesses.

CONCLUSIONS, INNOVATIONS, AND RECOMMENDATION: EU action can serve as a global example of an active approach in the field of cybersecurity by an international organisation which is not concerned with military or defence issues, while seeking to promote cybersecurity principles and standards internationally.

Keywords:
cybersecurity, European Union, European Single Market

INTRODUCTION

Progressive digitisation covering all spheres of life, including the economy, provides an important stimulus to change in the perception and implementation of the paradigm of state security. Despite the ongoing fundamental and revolutionary socio-economic changes, connected with dynamic technology development, the comprehensive use of the Internet, quantum computers, 5G mobile technology and artificial intelligence, internal as well as external security is still largely identified with the ability of countries to take adequate reactive and proactive measures. The biggest challenges involve the difficulty in identifying potential new areas exposed to cyberthreats and the predictability of the nature of threats and effective methods of their prevention (Jacuch, 2021). Cyberspace, thus cybersecurity, although related to the intensified use of new technologies, is hardly a separate sphere of human activity, being strongly connected with the traditional domain of international politics (Valeriano & Maness, 2015). Problems and challenges relating to cybersecurity are becoming increasingly important in the context of international relations (Bockett, 2017). As noted by Senol and Karacuha (2020, p. 17) based on analyses of cyberattacks and cyber incidents in many countries,

the causes of their serious implications are as follows: insufficient or ineffective implementation of cybersecurity regulations and policies, inadequate technology and infrastructure, lack of knowledge or lack of coordination and cooperation between institutions and organisations, etc. Cybersecurity is therefore inextricably linked to cyber capacity (Senol & Karacuha, 2020). The cybersecurity-focused discourse usually refers to the national dimension of security (e.g. Adamiec et al., 2021; Senol & Karacuha, 2020; Chałubińska-Jentkiewicz et al., 2022). However, the multidimensionality of cybersecurity determines the need to also build cyber capacity on the basis of cooperation in international relations. Therefore, attempts to implement strategies, regulations or to develop policies related to cybersecurity should be seen as a natural element of creating security in the international dimension as well. The relevant activities of international organisations are therefore necessary and desirable. The specificity of organisations, of socio-economic, political and cultural conditions of countries that are members of a given international organisation determines a varying approach to the implementation of cybersecurity-related tasks. This article aims at a description of the structure of cybersecurity in the EU, taking into account its most important objectives and characteristics, followed by a critical and reflective analysis of geopolitical conditions and activities in international relations. Another added value of the article is a special focus on the implementation of cybersecurity in the EU in the economic dimension. The article relies on institutional and legal analysis, combined with a review of the literature and source materials (including documents and normative acts).

CYBERSECURITY: CONCEPTUALISATION

The term *cyber* tends to be used to describe a concept that is associated with data networks, computers, information and communication technologies (Jacuch, 2021). The dynamics of the digitisation-related sphere implies the need to adapt terminology as well as introducing a kind of difficulty in constructing unambiguous and universal definitions. One example is the lack of consensus on the term *cyberspace*. Lan and Inster (2020) emphasise the uniqueness of cyberspace, combining the virtual aspect offering exceptional technical capabilities with the

traditional real world, with the boundary between them, importantly, becoming increasingly blurred, or even negligible. As defined by the European Union Agency for Network and Information Security (2017, p. 6), cyberspace is 'the time-dependent set of tangible and intangible assets, which store and/or transfer electronic information'.

Table 1. Selected definitions of cybersecurity

Author/source	Year	Definition of cybersecurity
Weiss et al.	2013	'Cybersecurity encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology security. Cybersecurity is distinctive in its inclusion of the offensive use of information technology to attack adversaries.'
Galinec et al.	2017	'Cybersecurity is not simply synonymous with information security, OT security, or IT security, nor is it merely the use of information security to protect enterprises from crime.'
Solms & Solms	2018	Cybersecurity is 'that part of information security which specifically focuses on protecting the confidentiality, integrity and availability (CIA) of digital information assets against any threats, which may arise from such assets being compromised via (using) the internet.'
ENISA	2019	Cybersecurity 'covers all aspects of prevention, forecasting; tolerance; detection; mitigation, removal, analysis and investigation of cyber incidents. Considering the different types of components of the cyber space, cybersecurity should cover the following attributes: Availability, Reliability, Safety, Confidentiality, Integrity, Maintainability (for tangible systems, information and networks) Robustness, Survivability, Resilience (to support the dynamicity of the cyber space), Accountability, Authenticity and Non-repudiation (to support information security).'
INTERPOL	2021	'Cybersecurity is typically defined as the protection of confidentiality, integrity and availability of computer data and systems in order to enhance security, resilience, reliability and trust in ICT. The concept usually covers political (national interests and security), technical and administrative dimensions.'

Source: prepared by the author based on: Weiss et al., (2013), Galinec et al. (2017), von Solms & von Solms (2018), ENISA (2017), Interpol (2021).

Similarly, many researchers and institutions or international organisations have attempted to conceptualise cybersecurity (Table 1). Based on a review of the definitions of the term, a couple of conclusions come to mind:

- cybersecurity is a complex, multidimensional concept that evolves over time: from terms emphasising more technical aspects (e.g. Weiss et al., 2013) to those of a more comprehensive

nature – referring additionally to more organisational or strategic issues (e.g. ENISA, 2017);
- changes taking place in the digital space determine further additions as more and more attention is paid to aspects related to risk management (Schatz et al., 2017) or resilience (Tzavara & Vassiliadis, 2024).

The multidimensional nature of cybersecurity implies the need for an increasingly holistic approach to actions undertaken by governments or organisations that aim not only to manage security risks, but also to care for data protection or data availability in cyberspace (Schatz et al., 2017). Therefore, those activities also have a political or administrative dimension rather than only a technical one (Interpol, 2021).

In summary, cybersecurity is a concept that is not easy to define unambiguously. In the ongoing discourse, it is difficult to refer to one coherent and universal definition. The evolution of this concept and the observable variability towards an ever-wider treatment of cybersecurity confirms the multi-context nature of the phenomenon.

THE STRUCTURE AND FRAMEWORK OF CYBERSECURITY IN THE EU

In 2001, the European Union obtained the status of Observer Organisation to the Cybercrime Convention Committee (Budapest Convention on Cybercrime) (European Court of Auditors, 2019). Since then, the EU has been actively involved in cybersecurity. Some of the first policy initiatives directly or indirectly related to the area concerned were as follows: the 2013 Cybersecurity Strategy (European Commission, 2013); the 2015 European Agenda on Security (European Commission, 2015a); the 2015 Digital Single Market Strategy (European Commission, 2015b); the 2016 EU Global Strategy (European External Action Service, 2016); the Cyber Defence Policy Framework adopted in 2014 and updated in 2018 (Council of the European Union, 2018); and the 2016 Joint Framework on countering hybrid threats (JOIN(2016) 18 final). The first legal regulations in the field of cybersecurity included the 2016 Network and Information Security (NIS) Directive (Directive (EU) 2016/1148)

and the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). Although the process of implementing cybersecurity measures has been going on for several decades, the authorities and institutions of the EU have been more active in the area concerned in recent years. This applies to both EU initiatives and legislation.

In order to understand the essence of the approach to cybersecurity in the European Union, it is important to note several important issues:

- the European Union's actions are multi-contextual in nature: the EU is committed to building a secure cyberspace within and beyond the organisation – in the forum of global cooperation on cybersecurity;
- relevant measures concern both activities undertaken by EU institutions and the creation of EU secondary legislation or non-binding legal acts;
- actions taken at the EU level result from the competences conferred on the EU by the Member States, especially in the field of security in general (Treaty provisions – Treaty on European Union, Treaty on the Functioning of the European Union).

Cybersecurity is one of the key elements of the EU Security Union Strategy (European Commission, 2020a). The document setting the contemporary direction of cybersecurity development in the EU is *The EU's Cybersecurity Strategy for the Digital Decade* of 2020 (European Commission, 2020b). What underlies the strategy is the assumption of the essential importance of cybersecurity for 'building a resilient, green and digital Europe' (European Commission, 2020b). Cybersecurity is usually treated in terms of cyber defence or military actions; therefore, it is worth pointing out that the rationale for adopting the EU strategy was the belief that due to ever-more frequent attacks on critical infrastructure and related disruptive geopolitical or technical events, the reliance of sectors such as energy, transport, health on networks and information systems, various types of crime have a digital component, digital services and the financial sector, along with the public sector, are increasingly vulnerable to cyberattacks. At the same time, there is a lack of sufficient collective situational awareness of cyberthreats as well as inadequate safeguards for fundamental rights and freedoms, including the rights to privacy and to data protection (European Commission, 2020b). To address those problems, the EU strategy proposes deploying regulatory, investment

and policy instruments in three areas of EU action: (1) resilience, technological sovereignty and leadership; (2) building operational capacity to prevent, deter and respond; and (3) advancing a global and open cyberspace (European Commission, 2020b). The strategy envisages a number of measures, e.g. (European Commission, 2020b):

- security of Network and Information Systems (NIS);
- building a network of AI-enabled Security Operations Centres (SOCs);
- implementing the 5G Toolbox;
- promoting synergies between the civil, defence and space industries;
- dedicated support to SMEs under the Digital Innovation Hubs;
- defining a set of objectives for international standardisation in the field of cybersecurity;
- expanding cyber dialogue with non-EU countries.

In the field of legislation and certification, particular attention should be paid to the implementation of normative acts introduced into the EU legal order in recent years and important to the execution of the strategy. Table 2 breaks down those acts into the four principles (*prevent*, *detect*, *respond*, *deter*) which determine the main directions of action taken at EU level. It is worth noting that the regulations mentioned are those relating to the functioning of the internal market, e.g. the NIS2 Directive (in the field of resilience and responsiveness of selected public and private entities throughout the EU), the Cybersecurity Act (concerning the security of ICT products, services and processes), the Cyber Resilience Act (the protection of consumers and businesses buying software or hardware with a digital component).

Table 2. The EU cybersecurity principles and selected actions

Principle	Key actions	Selected legislation and initiatives
PREVENT	Strengthening cybersecurity across public and private sectors by enhancing preparedness and resilience	The NIS2 Directive (Directive (EU) 2022/2555), or the revised Directive on the security of network and information systems, sets out a common regulatory framework for cybersecurity aimed at enhancing the level of cybersecurity within the European Union. It requires the EU Member States to strengthen their cybersecurity capabilities and introduces cybersecurity risk-management measures. The Directive includes provisions related to cooperation, information sharing, supervision and enforcement. It covers key sectors such as energy, transport, banking, financial market infrastructure, healthcare, digital infrastructure, ICT service management (between enterprises) and public administration entities.
	Establishing a European cybersecurity certification framework to create uniform security standards	The Cybersecurity Act (Regulation (EU) 2019/881) strengthens the role of the European Union Agency for Cybersecurity (ENISA) and establishes the European Cybersecurity Certification Framework (ECCF). The framework defines common cybersecurity requirements and evaluation criteria for the certification of ICT products, ICT services and ICT processes.
	Enforcing mandatory cybersecurity requirements for digital products throughout their life cycle	The Cyber Resilience Act (Regulation (EU) 2024/2847) establishes common standards for products with digital elements, including hardware and software. The Act requires that products meet cybersecurity requirements throughout their life cycle, including automatic security updates and incident reporting. Those provisions aim to protect consumers and businesses from cyber threats, ensuring a safer digital environment. Manufacturers will be required to place products on the EU market that comply with those requirements by 2027.
DETECT	Enhancing cross-border detection of cybersecurity threats and incidents through robust monitoring systems	The Cyber Solidarity Act (Regulation (EU) 2025/38) establishes a European Cybersecurity Alert System, i.e. a pan-European network of infrastructure consisting of National Cyber Hubs and Cross-Border Cyber Hubs, to enhance the coordinated detection of cyber threats and common situational awareness.
RESPOND	Improving incident response and crisis management through collaboration and information sharing	Cyber crisis management: relying on EU-CyCLONe and the CSIRTs Network to facilitate effective coordination during cyber incidents. The Cyber Solidarity Act (Regulation (EU) 2025/38) also includes the Cybersecurity Emergency Mechanism to test critical sectors, set up an EU Cybersecurity Reserve and provide financial support for mutual assistance.

DETER	Implementing proactive measures to prevent cyberattacks and applying sanctions to deter malicious activities	EU Policy on Cyber Defence (JOIN(2022) 49 final) aims to strengthen EU-wide cyber defence capabilities, secure the defence ecosystem and foster partnerships. The Cyber Diplomacy Toolbox (2017, updated 2023, Document No. 13007/17) offers diplomatic measures within the EU's Common Foreign and Security Policy to respond to malicious cyber operations targeting Member States.

Source: prepared by the author based on: Directive (EU) 2022/2555, Regulation (EU) 2019/881, Regulation (EU) 2025/38, (JOIN/2022/49 final), Document No. 13007/17, Cybersecurity, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity (accessed on 24th February 2025).

Table 3 describes the EU's centres and agencies whose activities are focused on the implementation of cybersecurity-related tasks.

Table 3. The EU's cybersecurity entities

Full name	Abbreviation	Description
European Union Agency for Cybersecurity	ENISA	ENISA provides support to the Member States, EU institutions and businesses in cybersecurity, including the implementation of the NIS Directive.
Information Sharing and Analysis Centres	ISACs	ISACs facilitate collaboration between cybersecurity communities across different economic sectors. The Commission, with ENISA, supports the establishment of new ISACs, offering legal, technical and organisational assistance.
Joint Research Centre	JRC	The JRC contributes to EU cybersecurity through initiatives such as developing a Cybersecurity Taxonomy and publishing reports, e.g. *Cybersecurity – our digital anchor*.
Computer Security Incident Response Teams / Computer Emergency Response Teams	CSIRTs/CERTs	CSIRTs handle cybersecurity incidents, provide warnings and cooperate at EU level. Under the NIS2 Directive, all essential service operators and digital providers must be covered by designated CSIRTs.
European Cyber Security Organisation	ECSO	The ECSO, established in 2016, acts as a strategic partner to the European Commission in public-private partnerships, focusing on advancing research, innovation and industrial development in the cybersecurity sector across Europe. The ECSO also plays a key role in building a strong European cybersecurity ecosystem through collaboration with industry, academia and public sector stakeholders.

Source: prepared by the author based on: ENISA, https://www.enisa.europa.eu/ (accessed on 24th February 2025), Cybersecurity, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity (accessed on 24th February 2025),

ECSO, https://ecs-org.eu/ (accessed on 24th February 2025), JRC. https://commission.europa.eu/about/departments-and-executive-agencies/joint-research-centre_en (accessed on 24th February 2025).

In addition, programmes such as Horizon Europe and the Digital Europe Programme provide funding for research on digital security. Similarly, the area of cybersecurity is one of the Commission's priorities in the framework of investments envisaged in the Recovery and Resilience Facility. Support for cybersecurity is also aimed at implementing measures such as the European Cybersecurity Competence Centre (ECCC), helping to create an EU-wide cybersecurity industrial and research ecosystem, and the Cybersecurity Skills Academy, addressing the critical shortage of cybersecurity professionals within the European Union by consolidating existing cyber skills initiatives.

It is also worth mentioning the most recent initiatives, such as the Commission's proposal for a Council recommendation for an EU Blueprint on cybersecurity crisis management, or the Cyber Blueprint (COM(2025) 66 final), the secure implementation of the 5G network in the EU (the Member States, through the NIS Cooperation Group, together with the Commission and with the support of ENISA, developed the EU 5G Toolbox), securing electoral processes (e.g. C/2024/3014) and the European action plan on the cybersecurity of hospitals and healthcare providers (COM(2025) 10 final).

CYBERSECURITY IN THE EU – IMPLICATIONS

What distinguishes the approach to cybersecurity in the EU is its link with the internal market, especially in the area of the digital single market, IT products or consumer protection. According to Cybersecurity Ventures, the need to protect increasingly digitised businesses, the Internet of Things (IoT) devices and consumers from cybercrime will result in global expenditure on cybersecurity products and services reaching a total of USD 1.75 trillion over the five-year period from 2021 to 2025, with the cybersecurity market growing at a rate of 15 per cent year-on-year. For comparison, the world's cybersecurity market was worth USD 3.5 billion in 2004 (Cybersecurity Ventures, 2024). Every IT position is now also a cybersecurity post. Every IT worker, every technology worker must be involved in protecting

and defending applications, data, devices, infrastructure and people. The data volume is also of interest; as predicted by Cybersecurity Ventures, total global storage will exceed 200 zettabytes by the end of 2025. This figure includes the storage of private and public data centres in the cloud, utilities infrastructure, computer hardware and IoT (Internet of Things) devices (Cybersecurity Ventures, 2024). The European Union, acting within its powers, has been taking measures for the implementation of regulations aimed to protect the internal market on the one hand and to support its development in a manner adequate to the changes taking place on the other hand (e.g. the NIS2 Directive, the Cybersecurity Act, the Cyber Resilience Act). As pointed out by Farrand et al. (2024), commercial and economic security affects cybersecurity and vice versa. In this context, 'there is something of a return to a mercantilist understanding that international relations are not about trade-offs between economic goals and distinct security goals, but represent a system in which economic goals *are* security goals, and vice versa' (Farrand et al., 2024, p. 2397). At the same time, there are numerous problems and challenges that reveal weaknesses and gaps in the implementation of the cybersecurity concept. These include issues of strategic dependence (e.g., reliance on foreign technologies and digital service providers), matters related to human capital, such as the shortage of cybersecurity specialists and insufficient digital skills across society, as well as legal challenges, for example, delays in the transposition and implementation of key directives such as the NIS2 Directive (COM(2025) 290 final). As demonstrated by an interesting study by Wang (2023), the UN's norm-making processes on cybersecurity create only minimum standards, which reflects a broad understanding that international law is not keeping up with the challenges posed by cyberspace, institutional linkages would be a way to recouple trade and cybersecurity, whereas the *soft legalisation* of cybersecurity could be seen as a first step towards more formal regulations. In this respect, the EU's actions represent an area of good practice and real experience (mainly in the field of binding legal regulations as well as initiatives with a more political dimension of cooperation, supported by *soft law*), could be an inspiration for other economic communities, such as ASEAN (the ASEAN Cybersecurity Cooperation Strategy 2021–2025 mainly focuses on the establishment of non-binding standards of responsible

state behaviour, based on cooperation in the field of cybersecurity). Similarly, activities of organisations such as the OECD aim to point out challenges, threats or recommendations to the member countries rather than to implement and enforce binding legal regulations.

Ensuring internal and external security is an essential function of the state. Accelerated technological development is one of the reasons for the verification of the current security paradigm, especially in the digital dimension. Scholars (e.g. Adamiec et al., 2021, Senol and Karacuha, 2020) draw attention to the national dimension of cybersecurity assurance systems. However, EU action has shown the growing importance of and the need for cooperation in this respect at the transnational level. It concerns intensified active and reactive measures, including political initiatives or cyber diplomacy (e.g. Document No. 13007/17), undertaken within the European Union itself as well as in relations with non-Community partners. EU security is an area of intergovernmental policy; therefore, the assumption of the Member States being the key players in this policy has been somewhat revised lately by the growing role of the European Commission in the area (Brandão & Camisão, 2022). Undoubtedly, the events of recent years, such as the COVID-19 pandemic, showing the reliance of societies and economies on information and communication networks, Russia's war against Ukraine, leading to more frequent cyberattacks and exposing the potential vulnerability of the EU's critical infrastructure, the situation in the Middle East, involving an increased risk of terrorist attacks and real attempts to disseminate terrorist content via online platforms and networks (COM(2024) 198 final), have all reinforced the need to intensify transnational collaboration. The EU has also been active in engaging in cooperation with non-EU partners to pursue common interests in cybersecurity policy, e.g. the EU–US Cyber Dialogue (December 2023), the EU–Ukraine dialogue on exchanging best practices and situational awareness, launching the EU's Cyber Dialogues with India, Japan, the Republic of Korea, Brazil, the United Kingdom, the EU–Latin America and the Caribbean Dialogue, Regulatory Dialogue between the EU and Western Balkans, the EU–NATO Structured Dialogue on Cyber Security and Defence. As stressed by Renda (2022), the EU has directed its efforts towards promoting non-binding cybersecurity rules and standards in third countries, particularly in terms of increasing global

resilience for maintaining resilience across Europe. The European Union has a very strong cooperation with NATO, but without any military doctrine or cyber command of its own in the context of cyber warfare. Nevertheless, the EU has included cyber defence in the scope of its cybersecurity policy (JOIN/2022/49 final). On the one hand, it reflects the importance of cyber defence in the context of taking holistic and adequate cybersecurity measures; on the other hand, for the EU Member States and non-Community partners, it can be treated as a harbinger of a larger European cybersecurity 'project' (Małecka, 2021, p. 87), or the beginning of a revision of the role of the Common Security and Defence Policy or changes in the division of competences in the EU. EU action can serve as a global example of an active approach by an international organisation which is not concerned with military or defence issues, on matters related to the implementation of cybersecurity both internally and externally.

CONCLUSIONS

An in-depth analysis of the cybersecurity strategy together with related documents as well as normative acts allows not only to show the complexity of the structure and legal framework, but also to articulate an interdisciplinary approach to cybersecurity in the EU. It has evolved over time from the economic dimension, taking into account technical infrastructure, and then building digital resilience and citizen awareness. The EU has taken significant steps towards strengthening the security of supply and product chains, enhancing solidarity at EU level and increasing its capacity to better detect, prepare for and respond to cyber threats and incidents. The EU's actions and legal regulations address many aspects of building a cybersecurity system; however, it is a complex and sophisticated process, limited by the scope of EU competences or differences in the temporal implementation of legal regulations by the Member States. There are also concerns about further development in terms of keeping up with relevant activities in other areas, e.g. the implementation of cybersecurity in the context of AI development. Due to varying organisational and cultural conditions, socio-economic development levels as well as the desirability of the existence of specific international organisations or

economic communities, the solutions implemented in the European Union must not be treated as universal and feasible in other regions of the world. However, the EU's experience in undertaking transnational cooperation for active and proactive cybersecurity measures is a sphere of verifying the effectiveness of specific solutions, especially those in the economic dimension, which can serve as a source of (both positive and negative) inspiration for other organisations and economic communities. Further, there are recommendations among researchers suggesting that it would be desirable to set not only national but also international standards regulating the various aspects of cyberspace (Jacuch, 2021), or to recognise a new right to cybersecurity in EU law (Chiara, 2024). Assessing the efficiency of the legal regulations and solutions implemented in the EU in a longer-term perspective, taking into account statistical data, as well as its activity in relations with third countries, may constitute a direction of further research on the development of cybersecurity.

References

Adamiec, D., Branna, J., Dziewulak, D., Firlej, N., Groszkowska, K., Karkowska, M., & Żołądek, Ł. (2021). Informacja na temat legislacji dotyczącej systemu cyberbezpieczeństwa w wybranych państwach Unii Europejskiej (Belgia, Czechy, Estonia, Francja, Holandia, Niemcy, Szwecja). *Zeszyty Prawnicze Biuro Analiz Sejmowej*, *3*, 280–314. DOI: 10.31268/ZPBAS.2021.61

Bockett, D. (2017). Virtual Theory: Integrating Cybersecurity into International Relations Theory. *International Journal of Interdisciplinary Global Studies*, *12*(4), 15–30. DOI: 10.18848/2324-755X/CGP/v12i04/15-30

Brandão, A.P., & Camisão, I. (2022). 'Playing the Market Card: The Commission's Strategy to Shape EU Cybersecurity Policy'. *JCMS: Journal of Common Market Studies*, *60*(5), 1335–1355.

Brandon V., & Maness, R.C. (2015). *Cyber War Versus Cyber Realities. Cyber Conflict in the International System*. Oxford: Oxford University Press.

Chałubińska-Jentkiewicz, K., Radoniewicz, F., & Zieliński, T. (Eds.) (2022). *Cybersecurity in Poland: Legal aspects*. Cham: Springer.

Chiara, P.G. (2024). Towards a right to cybersecurity in EU law? The challenges ahead. *Computer Law & Security Review*, *53*. DOI: 10.1016/j.clsr.2024.105961

Council of the European Union (2018). EU Cyber Defence Policy Framework (2018 update) (14413/18, November 19, 2018).
Cybersecurity Ventures (2024). *Top 10 Cybersecurity Predictions and Statistics For 2024*. https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/ (accessed on 24th February 2025).
ENISA (2017). *Overview of Cybersecurity and Related Terminology, Version 1.* Heraklion: ENISA Publications.
European Commission (2013). *Cybersecurity strategy of the European Union: An open, safe and secure cyberspace* (JOIN(2013) 1 final, February 7, 2013).
European Commission (2015a). *European agenda on security* (COM(2015) 185 final).
European Commission (2015b). *A digital single market strategy for Europe* (COM(2015) 192 final)
European Commission (2020a). *Communication from the Commission on the EU Security Union Strategy* (COM(2020) 605 final).
European Commission (2020b). *Joint communication to the European Parliament and the Council: The EU's cybersecurity strategy for the digital decade* (JOIN/2020/18 final).
European Commission (2022). *Joint Communication to the European Parliament and the Council: EU Policy on Cyber Defence* (JOIN/2022/49 final).
European Commission (2024). *Seventh progress report on the implementation of the EU Security Union Strategy* (COM(2024) 198 final).
European Commission (2025a). *European action plan on the cybersecurity of hospitals and healthcare providers* (COM(2025) 10 final).
European Commission (2025b). *Proposal for a Council Recommendation for an EU Blueprint on cybersecurity crisis management* (COM/2025/66 final).
European Commission (2025c). *State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future* (COM(2025) 290 final).
European Commission, & European External Action Service (2016). *Joint framework on countering hybrid threats – a European Union response* (JOIN(2016) 18 final).
European Commission. (2024). *Commission Guidelines for Providers of Very Large Online Platforms and Very Large Online Search Engines on the Mitigation of Systemic Risks for Electoral Processes Pursuant to Article 35(3) of Regulation (EU) 2022/2065* (C/2024/3014).
European Court of Auditors (2019). *Challenges to effective EU cybersecurity policy*. https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_en.pdf.
European External Action Service (2016). *Shared vision, common action. A stronger Europe. A global strategy for the European Union's foreign and security policy*. Publications Office. DOI: 10.2871/9875

European Parliament and Council of the European Union (2019). *Regulation (EU) 2019/881 of 17 April 2019 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)*. Official Journal of the European Union, L 151, 15–69.

European Parliament and Council of the European Union (2022). *Directive (EU) 2022/2555 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)*. Official Journal of the European Union, L 333, 80–152.

European Parliament and Council of the European Union (2024). *Regulation (EU) 2025/38 of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)*. Official Journal of the European Union, L 2025/38.

European Parliament and Council of the European Union (2024). *Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)*. Official Journal of the European Union, L 2024/2847.

European Parliament and the Council of the European Union (2016). *Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. Official Journal of the European Union, L 194, 1–30.

European Parliament and the Council of the European Union (2016). Regulation (EU) 2016/679 of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Official Journal of the European Union, L 119, 1–88.

Farrand, B., Carrapico, H., & Turobov, A. (2024). The new geopolitics of EU cybersecurity: Security, economy and sovereignty. *International Affairs, 100*(6), 2379–2397. DOI: 10.1093/ia/iiae231

Galinec, D., Možnik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: national level strategic approach. *Automatika: Journal for Control, Measurement, Electronics, Computing & Communications*, *58*(3), 273–286. DOI: 10.1080/00051144.2017.1407022

General Secretariat of the Council (2017, 9th October). *Draft implementing guidelines for the framework on a joint EU diplomatic response to malicious cyber activities: Approval of the final text* (Document No. 13007/17). Council of the European Union.

Interpol (2021). National cybercrime strategy guidebook. https://www.interpol.int (accessed on 24th February 2025).

Jacuch, A. (2021). Comparative Analysis of Cybersecurity Strategies. European Union Strategy and Policies. Polish and Selected Countries Strategies. *Online Journal Modelling the New Europe*, *37*, 102–121. DOI: 10.24193/OJMNE.2021.37.06

Lan, T., & Inkster, N. (2020). International governance of/in cyberspace. In E. Tikk & M. Kerttunen (Eds.) *Routledge Handbook of International Cybersecurity* (pp. 79–93). Abingdon: Routledge.

Renda, K.K. (2022). The Development of Eu Cybersecurity Policy: From a Coordinating Actor to a Cyber Power? *Ankara Review of European Studies (ARES) / Ankara Avrupa Çalışmaları Dergisi (AAÇD)*, *21*(2), 467–495. DOI: 10.32450/aacd.1226890

Rupp, C. (2024). *Navigating the EU cybersecurity policy ecosystem: A comprehensive overview of legislation, policies and actors*. https://www.interface-eu.org/publications/navigating-the-eu-cybersecurity-policy-ecosystem (accessed on 24th February 2025).

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more presentative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*(2), Article 8, 53–74. DOI: 10.15394/jdfsl.2017.1476

Senol, M., & Karacuha, E. (2020). Creating and implementing an effective and deterrent national cyber security strategy. *Journal of Engineering*, 1–19. DOI: 10.1155/2020/5267564

Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: a historical and conceptual review. *International Journal of Information Security*, *23*(3), 1695–1719. DOI: 10.1007/s10207-023-00811-x

von Solms, B. & von Solms, R. (2018). Cybersecurity and information security – what goes where? Information and Computer Security, *26*(1), 2–9. DOI: 10.1108/ICS-04-2017-0025

Wang, X. (2023). Decoupling trade and cybersecurity. A way to recalibration? *Asian Journal of WTO & International Health Law & Policy*, *18*(1), 39–88.

Weiss, J., Perkins, E., & Walls, A. (2013). Definition: Cybersecurity. https://www.gartner.com/en/documents/2510116/ (accessed on 24th February 2025).