EXAMINING THE EU POLICIES AND CORPORATE RELATIONS THROUGH A CYBERSECURITY LENS

Oana-Alexandra SARCEA (MANEA)
National University of Political Studies and Public Administration
Bucharest/Romania

Ana-Maria COSTEA
National University of Political Studies and Public Administration
Bucharest/Romania

Alexandra ZBUCHEA
National University of Political Studies and Public Administration
Bucharest/Romania

Abstract
The present paper integrates a broad analysis of European Union policies and their synergy with private corporations through a cybersecurity filter. As the digital landscape evolved, the EU has implemented a series of regulations and directives aimed at sustaining cybersecurity across member states. Various EU regulations establish strict requirements for cyber resilience and data protection. The analysis explores how these policies affect private corporations, emphasizing the impact on operational practices and compliance challenges. The paper examines the joint frameworks established between the EU and private sector entities, such as information-sharing initiatives and public-private partnerships. A bibliometric analysis was conducted to highlight the connections between the key terms used in the study. This analysis allows understanding of the interferences between the cybersecurity-related EU framework and private companies operating in the EU.

Keywords
Bibliometric analysis; cybersecurity; EU policies; private corporations.

1. INTRODUCTION

Cybersecurity is paramount for the European Union (EU), having a critical impact not only at the geopolitical level but also on economic development (European Council 2023). The issue is increasingly more sensitive since all aspects of the EU operations and EU citizens' lives rely increasingly more on digital technologies, which cyber threats increased (World Economic Forum 2024).

Cybersecurity is critical to protect the digital economy, which is a wide part of the European economy (UNCDF, 2022). The European economy is deeply integrated with digital systems; it becomes dependent on its digital infrastructure. Even more, sensitive domains, such as energy, finance, or transportation, rely on this digital infrastructure. This phenomenon has brought progress and reliability to many associated processes but also made all these systems more vulnerable to all sorts of threats. In this framework, the financial costs of cybercrime increased, both in terms of direct costs but also in terms of reputation and trust in European institutions and policies (Eling et al. 2023, 431). There is also a positive aspect of these evolutions. There is increased concern and investment in innovation and sustainable development of the digital infrastructure, as well as better cooperation and integration in this field across the Union. Additionally, EU strategies emphasize education, training, and upskilling to face cybersecurity better than ever, especially considering increasing and diverse threats.

In this way, the EU aims to enhance its digital sovereignty, reducing the dependence on non-EU technologies, as well as the agenda of big corporations. It aims to develop and protect its own infrastructure, and cybersecurity policies and measures aim to minimize the risks associated with external providers. In this manner, the critical infrastructure could be protected. Not only the critical

infrastructure, such as energy grids, are aimed by the EU policies but also other sectors, through specific measures (European Parliament 2024).

Promoting public trust and data protection are other essential facets. Public adoption of European digital systems, such as e-government, e-commerce, and digital payments, is related to actors' confidence in the cybersecurity of the European Union and member states. The strict and early regulations of the EU related to personal data protection not only highlight the EU's commitment to ensuring cybersecurity but also set European citizens' expectation level for early and effective policies in other domains.

Therefore, cybersecurity is not only a technical aspect but also a fundamental strategic element. Protecting digital infrastructure, ensuring economic resilience, safeguarding privacy, and strengthening geopolitical stability depend on strong and adequate cybersecurity measures and their effective implementation. A very important component is the role and interferences related to big corporations, which can affect the well-being of the EU and its citizens in many ways. With this framework in mind, the present study aims to enhance understanding of cybersecurity-related EU vulnerabilities and the associated policy and practical frameworks, particularly focusing on the relationship between the European Union and corporate entities as pictured by academic mainstream research.

Relevance to the research topic consists of identifying key themes and gaps in the main academic literature by a bibliometric analysis, namely a VOSviewer analysis. It can reveal key themes within the body of research related to European policy, corporate governance, and cybersecurity. This might include topics like data privacy, cyber policy, compliance requirements, or cross-border security standards. VOSviewer's network analysis contributes to mapping interdisciplinary connections in a topic that spans multiple fields (e.g., law, corporate governance, cybersecurity, and public policy); it can effectively show how these fields interact. For instance, it may reveal connections between cybersecurity and corporate policy or map how different EU countries approach cyber regulations. Another important benefit of this analysis would be tracking policy and technology trends. As cybersecurity policies rapidly evolve,

VOSviewer can show how specific keywords or topics have gained traction over time.

The approach consists of a three-step methodology. Firstly, an examination of cybersecurity is considered, by analysing the definitions of cybersecurity, as well as its historical evolution from basic system protection to comprehensive frameworks addressing global and geopolitical cyber threats. Secondly, the study explores the EU cybersecurity policies and frameworks, especially considering its complex relationships with businesses. The last part includes a bibliometric investigation focused on assessing corporate impact and engagement associated with the EU policies in the field of cybersecurity:

The analysis concludes by discussing the opportunities and ongoing challenges in aligning EU policies with corporate cybersecurity needs, recommending a balanced approach that ensures robust security while helping economic growth and innovation. This study underscores the importance of adaptive and dynamic policy frameworks in addressing cybersecurity threats' evolving and complex nature in the present digital age.

2. UNDERSTANDING CYBERSECURITY. A FOCUSED LITERATURE REVIEW

To better understand how to face cybersecurity-related vulnerabilities, it is important to understand this concept. Table 1 presents part of the cybersecurity definitions, selected considering their practical relevance.

Table 1. Cybersecurity definitions

Cybersecurity visions	Description
Admass et al. 2024, 7	Cybersecurity is the protection of societies, individuals, systems, organizations, and technologies from unusual activity. Maintaining the integrity, confidentiality, and availability of computer resources owned by one

	organization or connected to another organization's network is also part of cybersecurity.
Cains et al. 2021, 1650	The compilation of tools, security concepts, policies, security safeguards, risk management approaches, guidelines, actions, best practices, training, assurance, and technologies that can be used to defend the cyber environment and organization with user's assets. Organization and user's assets carry connected computing devices, infrastructure, personnel, applications, telecommunications systems, services, and the totality of transmitted and/or stored information in the cyber environment.
Gutzwiller et al. 2024, 7	Cybersecurity is the practice of safeguarding networks, computing systems, and data from loss of confidentiality, availability, or integrity. Cybersecurity approaches often ignore the end user, but the field itself frequently directly involves human cognition and perception.

Source: Authors' research

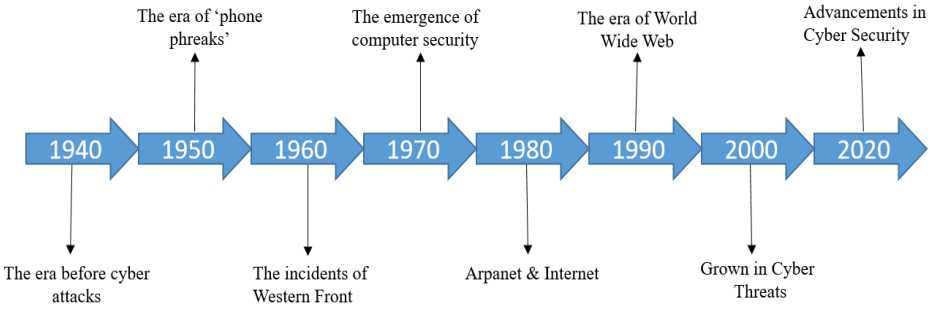
In 2013, the EU's cybersecurity approach was formalized in the Cybersecurity Strategy - European Commission, High Representative of the European Union for Foreign Affairs and Security Policy (EUR-Lex 2023). It aims to ensure a resilient and secure digital environment by protecting critical infrastructure and enhancing digital sovereignty. It integrates regulatory frameworks, public-private partnerships, and investments in innovation to counter cyber threats and foster global leadership in setting cybersecurity standards. The cybersecurity strategy of the European Union is based on an open, safe, and secure cyberspace (Farrand and Carrapico 2022, 443). The EU policies for cybersecurity related to private companies are the following: NIS Directive (Directive on Security of Network and Information Systems), NIS2 Directive, Cybersecurity Act, GDPR

(General Data Protection Regulation), Digital Operational Resilience Act (DORA) and eIDAS Regulation (Electronic Identification, Authentication, and Trust Services). They are complex documents, sometimes balancing contradictory interests. For instance, the NIS2 Directive safeguards the digital economy while upholding the fundamental rights of citizens.

Carrapico and Barrinha highlight that nowadays, in terms of the political dimension, cybersecurity is among the EU's most important priorities, with cybersecurity elements being mainstreamed into other EU policies (European Commission 2015). The framework set by the EU, as well as the cooperation network designed, determine collaborations that are crucial in growing a merged approach to threat response coordination and intelligence. The cybersecurity framework in the EU is permanently evolving as policy measures ultimately lead to adjustments and changes to the legal landscape and vice versa. The outlines of this landscape have also changed due to its flexibility, if not ambiguity, inserted in the very term "cybersecurity," which involves both advantages and disadvantages. (Fuster and Jasmontaite 2020, 73).

Cybersecurity evolved over time, as Figure 1 represents a timeline for the past 80 years splitting into decades for a better cybersecurity historical understanding. It can be observed that in the past 24 years, the grown and advancements in cybersecurity took place.

Figure 1. The general cybersecurity history timeline

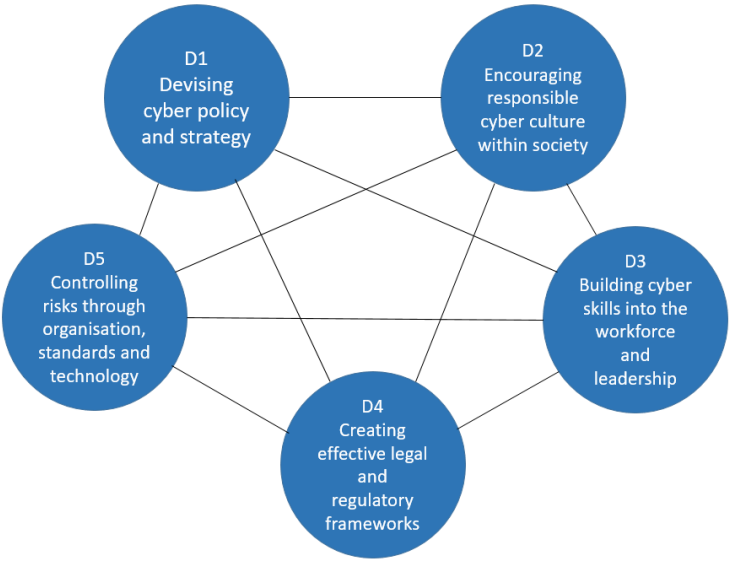


Source: Authors' research based on NIST (National Institute of Standards and Technology - US) and McKinsey studies

It has evolved from basic measures to protect individual systems to sophisticated frameworks and structures targeting global threats. From antivirus software and firewalls, we register today a complex security network that continues evolving as the cyber risks and attacks grow. All the digital advancements, such as cloud computing or artificial intelligence, have brought valuable opportunities but also new vulnerabilities. Various types of attacks, such as ransomware or phishing campaigns, increased, and they are not sponsored anymore by individuals, organizations, and even states (Guiora 2017, 7). Sometimes, the aims are purely economic, and some other times are political, targeting critical EU infrastructure. Therefore, the cybersecurity approach must deal not only with technical aspects but also with human and geopolitical factors.

Cybersecurity capacity models allow for the coherent development and monitoring of cyber capacities and their maturity across different dimensions of interest. Few models have been developed for this purpose and are being applied for the moment internationally to observe the capacity building of organizations, companies and even entire countries. For instance, the United States NIST's cybersecurity framework is a coordinated and open process that attempts to improve the country's critical infrastructure cybersecurity. One of the most used general cybersecurity capacity models is the Cybersecurity Capability Maturity Model (CMM), University of Oxford 2016, developed by the Global Cyber Security Capacity Centre (GCSCC). The model wraps cybersecurity capacity building comprehensively (CSDP 2017). It considers the cybersecurity capacity over five dimensions, as encompassed in Figure 2.

Figure 2. Cybersecurity Capability Maturity Model



Source: Authors' representation after GCSCC, University of Oxford

This model, displaying five core components, presents two main traits. We observe a holistic integration of policies, culture, regulation, and technology. There is also a global collaboration between interconnected frameworks. Also, this model allows balancing reventive and reactive measures in case of cybersecurity breaches.

In order to be able to analyse the corporate relations and the public-private partnerships, we firstly have to look at EU's approach towards cybersecurity in general, which are its core principles, its strategic documents and the competences that the organisation has.

3. THE EU'S BROAD FRAMEWORK ON CYBERSECURITY

The EU has been one of the most active organizations in establishing a robust cybersecurity framework in response to the increasing digital threats. Also, it is

one of the international leaders regarding the regulation of both digital and cyberspace, being the promoter of the individual rights that people have online, but also the responsibilities that the private companies hold over the data they collect, archive, sell, etc. As crucial initiatives and strategies have been implemented to enhance the region's security and resilience, it is a considerable challenge to discuss in depth all approaches, as well as their evolution in time, the present difficulties and future-oriented perspectives. Therefore, we highlight five fundamental initiatives that together could describe the European holistic approach to cybersecurity:

The Digital Compass and Connectivity. This initiative was adopted in 2021, outlining the EU's ambitions for digital transformation (European Commission 2021). In 2024, internet connectivity reached around 90% coverage in the context where this growth has narrowed the rural-urban digital divide significantly since 2007 (Statista 2024). This high level of development opened room for new opportunities like instant communication, less time-consuming bureaucracy, online education, and banking. However, at the same time, new threats arose from cyberspace.

Cybersecurity policy development: The EU's Strategic Compass for Security and Defence (2022), adopted the following year from the previous policies, emphasizes the importance of addressing cybersecurity threats as one of the most pressing threats to the entire Union. More specifically, the European decision-makers have adopted an upgraded EU Policy on Cyber Defence (2022) that will emphasize the EU's need to create a resilient framework that will mitigate all online threats. Another programmatic document in this regard is represented by the NIS 2 Directive (2022), which was introduced to establish a high standard level of cybersecurity across member states. This initiative was more than required since we cannot realistically believe that we can be part of a resilient system without ensuring we have the same cybersecurity standards. Additionally, in 2022, the EU adopted the Cyber Resilience Act, within which one of the major problems that the EU was confronting is represented by the "insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner" (European Commission 2022).

Public awareness and education: ENISA (the European Union Agency for Cybersecurity) (2024) has been pivotal in raising awareness through campaigns for schools, universities, end users, companies, the public sector, etc. One of the most visible initiatives in this regard would be the European Cybersecurity Month (ECSM), an annual event that is dedicated to specific target groups each year and has been organized since 2012. Since then, the number of participating states has increased beyond the EU's physical borders (e.g., the Republic of Moldova) (ENISA 2021). Also, this event reunites both public and private actors since Public-Private partnerships are essential for a credible, resilient society (Costea 2023, 115). In terms of quantifiable results, the campaign from 2021 achieved significant results, reaching an audience of over 20 million people, more than double the 8.8 million reached in 2020. Furthermore, over 70% of EU Member States believe that these campaigns have positively influenced the reduction of cyber incidents (ENISA 2021).

Educational programs: ENISA is also involved in education programs. Under the Digital Education Action Plan (2021-2027) (European Commission 2020), all EU member states have been developing initiatives to enhance digital skills and competencies, evidenced by the active educational programs in various countries (for example, Romania and Croatia that involve the public sector; Estonia, Ireland and Finland that established partnerships with universities, or France, Malta and Sweden that have developed these types of activities with the help of civil society (ENISA 2022, 9-21). All these activities are essential since, according to the above-mentioned statistics, the internet coverage is rather high, and "in 2022, 96 % of young people in the EU made daily use of the internet, compared with 84 % for the whole population" (Eurostat 2023). In terms of digital skills, in 2021 "young people between the age of 16 and 29 [are] reporting basic or above basic overall digital skills. Country shares range from 93 % in Finland, 92 % in Malta, 89 % in Croatia and 87 % in Greece and the Netherlands to 49 % and 46 % in Bulgaria and Romania" (Eurostat 2023).

Regulatory measures: There are numerous European regulations addressing in practical terms this topic. As already mentioned, the GDPR has set a precedent in data protection at the international level, empowering individuals with rights over their personal data and contributing to the EU's reputation as a normative

power in cybersecurity. Through it, the persons from the EU territory have the right to know how private companies use their data, and can demand their data erased, facts that are unique at the international level (Regulation (EU) 2016/679). Other good practice examples are the NIS Directive (2016), the EU's first comprehensive cybersecurity law, requiring member states to improve national cybersecurity capabilities and ensure the security of essential services, and the NIS2 Directive (2022), which extended the former's application. Another critical measure is the Cybersecurity Act (2019), which, among other aspects, introduced an EU certification framework for ICT products and services to meet high cybersecurity standards.

Thus, the EU's approach to cybersecurity is a perfect example of a collaborative strategy that involves both member states and candidate countries, private and public authorities, to create a unified strategy in an interconnected cyberspace. The European cybersecurity strategy operates within a dynamic framework designed to address the complexities of a rapidly evolving digital landscape as well as harmonizing cybersecurity standards with the EU at every level – state, organizational and citizen levels. Still, digital literacy and ensuring uniform implementation of the regulations and policies in each member state remain significant challenges (Marin and Castaneda 2023, 1091). Also, as evidence is showing, the EU member states are rather far from having the same private-public partnerships development level, fact that can affect the resilience of the entire organization (Costea 2023, 120).

4. CYBERSECURITY APPROACH FOR EU'S RELATIONSHIP WITH COMPANIES

When considering a cybersecurity framework for the EU's relationship with companies, several key aspects should be considered: the regulatory standards imposed by the EU to all actors operating in the EU, which are higher than in other political and economic spaces (European Commission 2024), incident reporting and accountability, public-private partnerships, upgrading cybersecurity skills, cyber risk management. Overall, the EU's regulatory

framework and implemented measures ensure not only the European market's integrity but also increase its global competitiveness.

All measures presented above also significantly influence the activity of the companies operating in the EU, which have to comply and even notify relevant national authorities if an incident occurs (see NIS2, for instance – European Commission 2023). Some specific directives focus on strategic sectors. For example, the Digital Operational Resilience Act focuses on the financial sector and supports its actors to face and recover from cyberattacks (EUR-Lex, 2022). Special attention is given by the EU to online services, aiming to protect not only these platforms, but primarily citizens from all sorts of fraud and cyberattacks. The main approaches are regulated through the Digital Services Act (European Commission 2024) and Digital Markets Act (European Commission 2023). This last initiative sets the criteria for corporations to become "gatekeepers" – influential digital business platforms being subject to stricter rules to ensure fair competition (European Commission 2020). For instance, Alphabet, Amazon, Apple, Meta, Booking, Byte Dance, and Microsoft are gatekeepers under EU regulations (European Commission 2024). Another initiative aiming to regulate the services sector is the Electronic Identification, Authentication, and Trust Services Regulation (eIDAS) (European Commission 2024) which is meant to ensure secure digital interactions.

This regulatory framework, especially the NIS2 Directive, also sets requirements for companies to report cybersecurity incidents (Bruder at al. 2024, 3). By encouraging sensitive issues disclosure, the EU contributes to improving not only the awareness and the protection against threats but also fosters a culture of transparency and accountability. Still, a weakness of this system relies on the desire of companies not to report such issues in order not to face trust decline and challenges.

The EU does not stop in imposing specific standards and approaches but also offers help to businesses. For instance, the EU cooperated with companies to increase their security and resilience, including SMEs or along the supply chain (European Council 2024). As mentioned, the EU policies also contribute to workforce-related skills development, as in the Digital Education Action Plan (European Commission 2020).

Last, but not least, the EU regulates and/or works directly with the activity of giant corporations, such as Meta or Apple, to ensure the (cyber)security of the EU systems, states, and citizens. Some corporations align voluntarily with various regulations, some others negotiate or resist. For instance, Meta and Apple did not sign the EU Pact for AI, while more than 100 important companies signed the document (Morucci 2024, 2).

Many digital giants, in their desire to maximize their already huge profits, pose different types of security threats at the country level. Therefore, various states and supra-statal structures, such as the US or the EU, impose bans and additional regulations designed especially for these companies. For instance, considering their security threats, TikTok or X (former Tweeter) faces all sorts of restrictions in the EU, US, or other countries (da Silva and Buschschluter 2024; Berico and Wells 2024; Jamali 2024). Misinformation is a significant motive but not the only one related to these initiatives (Schulten 2023, 3). Extremism and terrorist concerns determine states and the EU to impose some limits on these companies (Kroet 2024, 3) and to fine organizations or even sanction individuals (as in the case of Telegram's owner – see Tidy 2024, Davies 2024). Voices are challenging these approaches, fearing an attack on free speech and business freedom (Jamali 2024, 4). Another issue of concern is the development of controlled markets, and the EU is enforcing antitrust rules against such companies (European Commission 2024). Another sensitive issue that tightened the relationships between the giant digital companies and the EU is related to protecting its citizens (for instance, Meta and X have been charged with misleading their customers under the European regulation – see – Ravia and Hammer 2024). Privacy concerns have also been grounds for specific regulation aiming the digital giants (Paul 2023, 2).

5. BIBLIOMETRIC ANALYSIS. METHODOLOGY

For a deeper understanding of the existing patterns of research and themes of interest in the area of EU cybersecurity policies in the context of corporate business, a bibliometric analysis using VOSviewer has been employed. Firstly,

the most relevant papers on the subject have been searched in two reputable databases, Scopus and Web of Science using similar search terms.
In the context of research on European policies, corporate relationships, and cybersecurity, VOSviewer can help identify trends, patterns, and relationships within a large body of academic literature or other documented data sources. The methodology involves data collection, bibliometric mapping, and network visualization.

Scopus: (ALL ("European Union") AND ALL (cybersecurity) AND ALL (legislation) AND ALL (business)) – which yielded 643 results.
Wos: "European Union" (All Fields) and cybersecurity (All Fields) and legislation (All Fields) and business (All Fields) – which yielded 6 results.

The two resulting datasets have been imported into Zotero reference management software, merged, deduplicated, and reviewed for thematic accuracy. After these actions, 639 documents were employed in the VOSviewer analysis.
In VOSviewer, a map based on bibliographic data has been created to be subjected to a keyword co-occurrence analysis. A thesaurus file has been utilized to reduce redundancy. The merged keywords can be seen in Table 2.

Table 2. Replaced keywords from the bibliometric analysis

Label	Replace by
cyber security	cybersecurity
security	cybersecurity
general data protection regulations	GDPR
law	laws and legislation
ai	artificial intelligence
crime	cybercrime
privacy	data privacy

The minimum number of occurrences has been set to 10 for higher accuracy. Two generic keywords, "current" and "human," have been further eliminated from the analysis. Finally, the bibliometric analysis resulted in 21 items divided into three clusters, further analysed in this paper's next section.

6. FINDINGS AND DISCUSSION

The resulting figure (Figure 3) shows the network the analysed co-occurring keywords created. The total number of links between these 21 terms is 134, representing a quite high level of interconnectedness between the terms. They have a link strength of 584, which is significant considering the network size of 21, meaning that there is solid research connecting various thematic aspects of this research area, and these connections are consistent across the current literature. It can be observed that the terms are highly interconnected across clusters, meaning that the research in this area is multidisciplinary and focuses on a broader conceptual picture.

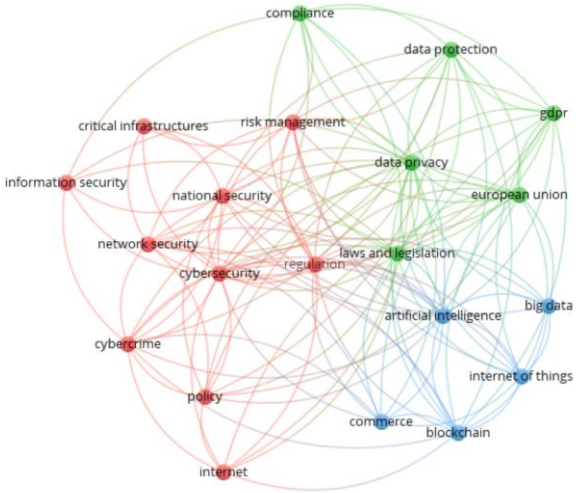
Analysing research results for the used keywords reveals several core clusters of academic interest and interconnections between topics. Typically, VOSviewer visualizes such research landscapes by forming clusters based on co-occurrence and citation patterns, allowing us to identify which fields are most closely connected. For instance, "cybersecurity," "network security," and "cybercrime" are likely to form a dense cluster, reflecting a well-developed body of research focused on protecting digital infrastructures and combatting cyber threats. This cluster is highly relevant in discussions of "national security," as the need for countries to safeguard critical infrastructure from cyber threats has fuelled research on integrating cybersecurity into broader national defence strategies.

The keyword "GDPR" often links closely with "data privacy" and "European Union," forming another distinct but interrelated cluster. Research in this area explores compliance frameworks, privacy-enhancing technologies, and the regulatory impact of GDPR on data management practices. With the European Union setting a global standard for data protection, studies often examine the role of GDPR in shaping data governance across different industries.

Furthermore, this cluster frequently overlaps with "AI" and "big data," as the rise of these technologies has introduced new challenges in handling personal data, prompting research on ethical and legal frameworks to guide their responsible use.

"Blockchain" often appears in discussions related to "AI," "big data," and "risk management," although it is somewhat less integrated with traditional security topics like network security or cybercrime. Research in this area focuses on blockchain's potential for enhancing transparency, integrity, and trust, particularly in sectors like finance and supply chain management, where risk management is a priority. Studies also address how blockchain could reinforce data privacy through decentralized frameworks (Wylde et al. 2022, 127), presenting an alternative to traditional centralized data storage approaches, which often face vulnerabilities. Overall, the VOSviewer analysis highlights the multidisciplinary nature of these topics, showing how research in digital security, regulation, and emerging technologies converges to address complex issues in a highly interconnected digital environment.

Figure 3. Outcome after keywords searching and cumulated analysis



Source: VOSviewer

Table 3 shows how the keywords are divided into clusters. At first glance, the first cluster seems to focus on cybersecurity policies and regulations, specific aspects, and needed infrastructure. The green cluster focuses on compliance and legislation around GDPR, data protection, and privacy, and the blue cluster focuses on the digital aspect, domains, and business applicability of cybersecurity policies and legislation.

Table 3. VOSviewer clusters

Red Cluster	Green Cluster	Blue Cluster
critical infrastructures	compliance	artificial intelligence
cybercrime	data privacy	big data
cybersecurity	data protection	blockchain
information security	European Union	commerce
internet	GDPR	internet of things
national security	laws and legislation	
network security		
policy		
regulation		
risk management		

The red cluster is the biggest, with the highest number of highly interconnected keywords. It focuses on cybersecurity concerns at various levels. This cluster centres around the "cybersecurity term," highlighting the increasing worries about cybercrime in the current internet era. It can be said that today, people and businesses have a double existence, one in the physical world and one in the digital world. Just as in the physical world, specific threats to the integrity of businesses and individuals may also arise in the virtual world of the digital realm. This is why it needs to be subject to similar (but adapted to its specifics) policies, laws, and regulations. The presence in this cluster of terms such as "policy," "regulation," and "risk management" indicates a preoccupation in this direction - to create a suitable governance structure in the cybersecurity area. They suggest a focus on developing frameworks, laws, and strategies to manage

and mitigate cyber risks at organizational and national levels. The presence of "national security" terms is worth noting, which signifies that cybersecurity is now an essential component of overall national defence. The "critical infrastructure" term might signify both the infrastructure critical to businesses and nations that is essential to be secure from a cybernetic point of view as well as from a physical point of view. However, it may also point to critical infrastructures to enable consistent cybersecurity. In the same context, "information security" and "network security" terms represent the technical aspects of protecting data and systems, pointing towards the emphasis put on improving the technical capabilities for safeguarding digital assets.

The green cluster is deeply related to EU laws and legislation around data protection. It focuses on compliance with GDPR (General Data Protection Regulation) and adherence to global data protection standards. "Data privacy" and "data protection" are important keywords, highlighting the persistent interest in protecting personal information in the current digital age. GDPR is an important aspect for every business, especially for those with intense digital activity with cross-border operations. To comply with legal standards, companies across domains and countries must establish strong cybersecurity systems that protect data from being stolen, inappropriately shared, or used for unethical reasons.

Finally, the blue cluster concentrates on emerging technologies and the digital economy. The "artificial intelligence," "big data," "blockchain," and "internet of things" terms in this cluster may refer to different evolving business areas in the digital economy that would be potentially subject to cyber threats, so suitable security systems need to be developed for them, which is a strong branch of research, of big interest for both academia and corporate actors. On the other hand, the presence of these keywords may indicate exploration of these cutting-edge technologies as important component parts or enablers of cybersecurity systems. The "commerce" term presence in this cluster suggests a focus on regulating and ensuring security for ongoing (and constantly evolving) business activity across the European Union and beyond. As commerce is now happening in a high proportion online, it is of significant interest for companies to have strong securing systems in place, from data protection to payment

protection, logistics, and delivery records, as well as financial documents that are all traced digitally, especially for large companies/corporations.

7. CONCLUSIONS

Integral to the EU's cybersecurity strategy, private corporations face major obligations to ensure the protection of critical infrastructure and personal data. The study highlights the binary role of these entities as both targets of cyber threats and as pivotal players in safeguarding digital ecosystems. The paper identifies the key areas where EU policies intersect with corporate cybersecurity strategies, including incident reporting, risk management, and adopting cybersecurity standards. Apart from these large provisions, there are all kinds of decisions and more blunt interactions with companies through which certain operations are limited to them, considering the security of citizens and the states of the EU.

The Union's approach to cybersecurity is a comprehensive, dynamic framework that aligns with both economic growth and innovation while addressing the increasingly sophisticated cyber threats. Through a mix of regulatory measures, policy development, and public-private collaboration, the EU aims to create a secure digital environment that enables innovation and fosters economic prosperity. However, balancing the regulatory requirements for cybersecurity with the need to promote growth and innovation in the corporate sector presents several challenges and opportunities.

Harmonized cybersecurity standards across the EU benefit businesses by fostering a uniform operative level, increasing consumer confidence, and enabling cross-border operations without excessive regulatory burdens. This can lead to more competitive digital industries within the EU and globally. By setting high standards for data protection, the EU creates a safer environment for businesses to operate, increasing consumer trust and driving innovation in privacy-preserving technologies. The GDPR is seen as a global benchmark, helping EU companies maintain a competitive edge in international markets. GDPR compliance can significantly burden businesses, particularly regarding

the resources required for legal counsel, audits, and data protection measures. Additionally, as digital technologies advance, so do cybercriminals' tactics, requiring continuous adaptation of security practices to protect personal data. Similar challenges and opportunities might arise from other regulations of the EU.

Balancing economic growth with (cyber)security is challenging. To encourage businesses to invest in cybersecurity, the EU could offer financial incentives such as tax breaks or subsidies for companies adopting best cybersecurity practices or undergoing third-party security audits. This would help offset compliance costs and make it easier for businesses to align with EU cybersecurity standards. Also, enlarging educational efforts might bring long-term benefits on various levels.

REFERENCES

- Admass, Wasyihun S., Munaye, Yirga Y., Diro, Abebe A. 2024. "Cyber security: State of the art, challenges and future directions" *Cyber Security and Applications*, vol 2. https://doi.org/10.1016/j.csa.2023.100031.
- Bruder, Ana, Hadnes, Beck, Benjamin, Yaros, Oliver, Sarpong, Rudigel, Ksinsik, Amelie. 2024. "New Eu Cyber Rules (NIS2) Take Effect; Implementing Rules Adopted". *Mayer/Brown*. Accessed on November 20, 2024.https://www.mayerbrown.com/en/insights/publications/2024/10/new-eu-cyber-rules-nis2-take-effect-implementing-rules-adopted.
- Cains, Mariana G., Liberty, Flora, Taber, Danica, King, Zoe, Henshel, Diane S. 2021. "Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation." *Risk Analysis*. https://doi.org/10.1111/risa.13687.
- Carrapico, Helena, Barrinha, Andre. 2018. "European Union cyber security as an emerging research and policy field." *European Politics and Society* 19(3): 299-303. https://doi.org/10.1080/23745118.2018.1430712.
- Costea, Ana Maria. 2023. "Private-Public Partnerships in cyber space as deterrence tools. The trans-atlantic view." *Europolity* 17(2): 111-134. http://doi.org/10.25019/europolity.2023.17.2.4.

- Davies, Pascale. 2024. "Who is Pavel Durov, the Telegram co-founder arrested in France?". *EuroNews*. Accessed on 19.11.2024. https://www.euronews.com/next/2024/08/26/who-is-pavel-durov-the-telegram-co-founder-arrested-in-france.
- Eling, Martin, Elvedi, Mauro, Falco, Greg. 2023. "The Economic Impact of Extreme Cyber Risk Scenarios." *North American Actuarial Journal* 27(3): 429-443. https://doi.org/10.1080/10920277.2022.2034507.
- ENISA. 2021. *European Cybersecurity Month 2021 - Deployment report.* Accessed on January 2024. https://www.enisa.europa.eu/publications/european-cybersecurity-month-2021-deployment-report.
- ENISA. 2022. *Cybersecurity Education Initiatives in the EU Member States.* Accessed on 15.08.2024. https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states.
- ENISA. 2024a. *About ENISA*. Accessed on 10.01.2024. https://www.enisa.europa.eu/about-enisa/regulatory-framework.
- ENISA. 2024b. "European Cybersecurity month." Accessed on 20.08.2024. https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/european-cybersecurity-month.
- EUR-Lex. 2013. *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee Of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Accessed on 11.11.2024. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001.
- EUR-Lex. *2016. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data*. Accessed on 20.08.2024. https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html.
- EUR-Lex. 2019. *Regulation (EU) 2019/881 of the European Parliament and of the Council 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).* Accessed on 19.11.2024. https://eur-lex.europa.eu/eli/reg/2019/881/oj.
- EUR-Lex. 2022. *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU)*

No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. Accessed on 19.11.2024. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554.

- European Commission. 2021. *COM(2021) 118 final. Communication from the Commission to the Eropean Parliament, the Coluncil, the European Econommic and Social Committee and the Committee of the Regions. 2030 Digital Compass: the European way for the Digital Decade*. Accessed on 15.08.2024. https://eur-lex.europa.eu/resource.html?uri=cellar:12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02/DOC_1&format=PDF.
- European Commission. 2022a. *Cyber Resilience Act*. Accessed on 15.08.2024. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
- European Commission. 2022b. *Joint Communication, EU Policy on Cyber Defence.* Accessed on 15.08.2024. https://www.european-cyber-defence-policy.com/.
- European Commission. 2023a. "A Europe fit for the digital age. Empowering people with a new generation of technologies." Accessed on 19.11.2024. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en.
- European Commission. 2023b. *DESI dashboard for the Digital Decade (2023 onwards).* Accessed on 19.11.2024. https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts.
- European Commission. 2023c. *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. Accessed on 19.11.2024. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.
- European Comission. 2024a. "Commission fines Meta €797.72 million over abusive practices benefitting Facebook Marketplace.", Nov. 14, 2024. Accessed on 19.11.2024. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5801.
- European Commission. 2024b. *Digital Education Action Plan (2021-2027).* Accessed on 19.11.2024. https://education.ec.europa.eu/focus-topics/digital-education/action-plan.
- European Commission. 2024c. *eIDAS Regulation*. Accessed on 19.11.2024. https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation
- European Comission. 2024d. "Gatekeepers." Accessed on19.11.2024. https://digital-markets-act.ec.europa.eu/gatekeepers_en#:~:text=On%206%20September%202023%20the,Digital%20Markets%20Act%20(DMA).

- European Commission. 2024e. "New rules to boost cybersecurity of the EU institutions enter into force.", Jan. 8, 2024. Accessed on 19.11.2024. https://commission.europa.eu/news/new-rules-boost-cybersecurity-eu-institutions-enter-force-2024-01-08_en.
- European Commission. 2024f. *The Digital Services Act package*. Accessed on 19.11.2024. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.
- European Council. 2023. *Cybersecurity: how the EU tackles cyber threats.* Accesssed on 19.11.2024. https://www.consilium.europa.eu/en/policies/cybersecurity/
- European Council. 2024. *How the EU responds to crises and builds resilience.* Accessed on 19.11.2024. https://www.consilium.europa.eu/en/policies/eu-crisis-response-resilience/.
- European Parliament. 2024. *Fact Sheets on the European Union*. Accessed on 20.11.2024. https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe.
- European Parliamentary Research Service. 2017. "*Cybersecurity in the EU Common Security and Defence Policy (CSDP). Challenges and risks for the EU.*". Scientific Foresight Unit. https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf
- European Parliamentary Research Service. 2020. *Directive on security of network and information systems (NIS Directive). EU cybersecurity policy*. Ex-Post Evaluation Unit. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/654198/EPRS_BRI(2020)654198_EN.pdf#:~:text=The%20NIS%20Directive%20%28Directive%20on%20security%20of%20network,policy%20and%20in%20particular%20the%20EU%27s%20cybersecurity%20strategies.
- European Union. 2022. *A Strategic Compass for Security and Defence. For a European Union that protects its citizens, values and interests and contributes to international peace and security.* Accessed on 15.08.2024. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf.
- Eurostat. 2023. *Being young in Europe today - digital world.* Accessed on 10.08.2024. https://ec.europa.eu/eurostat/statistics-

explained/index.php?title=Being_young_in_Europe_today_-_digital_world&oldid=564756.

- Farrand, Benjamin, Carrapico, Helena. 2022. "Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity." *European Security* 31(3): 435-453. https://doi.org/10.1080/09662839.2022.2102896.
- Feingold, Spencer, Beato, Filipe. 2024. "Cybersecurity rules saw big changes in 2024. Here's what to know". *World Economic Forum*, Oct. 17, 2024. Accessed on 11.11.2024. https://www.weforum.org/stories/2024/10/cybersecurity-regulation-changes-nis2-eu-2024/.
- Guiora, A. N. 2017. *Cybersecurity: geopolitics, law, and policy*. Routledge.
- Gutzwiller, Robert S, Fugate, Sunny J, Lukos, Jamie R., Wiegand, Karl. 2024. "A novel visual interface enables human detection of malware in portable document format." *Journal of Cybersecurity*, 10(1). https://doi.org/10.1093/cybsec/tyae016.
- Gonzalez, Fuster, Gloria, Jasmontaite, Lina. 2020. "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights." In: Christen, M., Gordjin, B., Loi, M. (eds) *The Ethics of Cybersecurity*, The International Library of Ethics, Law and Technology, vol. 21, 97-115. Springer: Cham. https://doi.org/10.1007/978-3-030-29053-5_5.
- Kari, Paul. 2023. "Meta's Threads app launches across EU in blow to competitor X." The Guardian, Dec. 14, 2023. Accessed on 29.11.2024. https://www.theguardian.com/technology/2023/dec/14/threads-launches-europe-meta-twitter.
- Kroet, Cynthia. 2024. "The online platforms now have three months to report back about the measures they took to take down illegal content". *EuroNews*, Nov. 14, 2024. Accessed on 19.11.2024. https://www.euronews.com/next/2024/11/14/tiktok-x-meta-exposed-to-terrorist-content-irish-regulator.
- Marin, Victoria I., Castaneda, Linda. 2023. "Developing Digital Literacy for Teaching and Learning." In: Zawacki-Richter, O., Jung, I. (eds.) *Handbook of Open, Distance and Digital Education*, 1089-1108. Springer: Singapore. DOI:10.1007/978-981-19-2080-6_64.
- Morucci, Noemi. 2024. "More than 100 companies signed EU Pact for AI. Meta and Apple missing from the list". *EU News,* Sept. 25, 2024. Accessed

on 19.11.2024. https://www.eunews.it/en/2024/09/25/more-than-100-companies-signed-eu-pact-for-ai-meta-and-apple-missing-from-the-list/.

- NISS 2 Directive. 2022. Accessed on 15.09.2024. https://www.nis-2-directive.com/.
- Pranckutė, Raminta. 2021. "Web of Science (WoS) and Scopus: The Titans of Bibliographic Information in Today's Academic World" *Publications* 9(1): 12. https://doi.org/10.3390/publications9010012.
- Ravia, Haim, and Hammer, Dotan. 2024. "European Commission Charges Meta and X with Violations of Online Services Laws". *Pearl Cohen*. Accessed on 29.11.2024. https://www.pearlcohen.com/european-commission-charges-meta-and-x-with-violations-of-online-services-laws/.
- Schulten, Lucia. 2023. "The European Union has voiced concerns over disinformation related to the Israel-Hamas conflict spreading in Europe. The EU Commission has put social media platforms X, Instagram, Facebook and TikTok on notice". *DW*, October 13, 2023. Accessed on 19.11.2024. https://www.dw.com/en/eu-warns-x-meta-and-tiktok-over-israel-hamas-disinformation/a-67081766.
- Statica. 2024. "Annual level of internet access among households in cities, towns & suburbs, and rural areas in the European Union from 2007 to 2022". Accessed on 15.08.2024. https://www.statista.com/statistics/1370388/eu-digitalization-level-household-internet-access-rural-urban/#statisticContainer.
- Tidy, Joe. .2024. "Telegram: 'The dark web in your pocket'". *BBC*, August 31, 2024. Accessed on 19.11.2024. https://www.bbc.com/news/articles/cdey4prn3e1o.
- United Nations Capital Development Fund (UNCDF). 2022. *The role of cybersecurity and data security in the digital economy.* Accessed on 11.11.2024. https://policyaccelerator.uncdf.org/all/brief-cybersecurity-digital-economy.
- Wylde, Vinden, Rawindaran, Nisha, Lawrence, John, Balasubramanian, Rushil, Prakash, Edmond, Jayal, Ambikesh, Khan, Imtiaz, Hewage, Chaminda, Platts, Jon. 2022. "Cybersecurity, Data Privacy and Blockchain: A Review". *SN Computer Science* 3: 127. https://doi.org/10.1007/s42979-022-01020-4.