DOI: 10.47743/eurint-2025-FOC • November 2025 • VOLUME 12

European cybersecurity challenges and policy gaps. The Estonian experience in cybersecurity

Andreea Cosmina Foca ✉
Alexandru Ioan Cuza University of Iași, Iași, Romania

Abstract: Following the COVID-19 pandemic, the European Union has strengthened its cybersecurity policies to address the growing threats generated by increased digital dependence, including attacks on critical infrastructures, individuals, and businesses. While notable progress has been made, fragmentation remains a major challenge. Legal and regulatory advancements, such as the NIS2 Directive, the Cyber Resilience Act, and DORA, have harmonized standards and reduced disparities among Member States. Horizontal fragmentation between EU institutions and agencies has improved through strengthened ENISA competences and cooperation mechanisms like CERT-EU, the CSIRTs network, and CyCLONe, yet overlapping mandates and the absence of a central coordinating authority persist. Vertical fragmentation, involving the EU, Member States, and the private sector, remains pronounced, as sovereign prerogatives and limited information-sharing hinder coherence. This study evaluates the EU's post-pandemic cybersecurity framework, identifies structural and institutional challenges, and draws lessons from Estonia's cybersecurity model using qualitative analysis of EU strategies, ENISA and Europol reports, and academic literature.

Keywords: malicious use of technological advancements, European institutions, European cybersecurity policy, Estonian cybersecurity policies

Introduction

The advancement of the Internet has facilitated accelerated growth in the global economy, enabling faster information exchange, global trade, and the digitalization of services. In parallel, developments in information and communication technology (ICT) have interconnected billions of devices worldwide, thereby expanding cyberspace into new domains of economic, social, and personal interest for users. The widespread adoption of cloud computing, artificial intelligence, and digitally connected devices has catalysed profound transformations in governance, commerce, healthcare, education, and daily social

✉ PhD Student, Alexandru Ioan Cuza University of Iași, Iași, Romania; email: focaandreea11@gmail.com

interactions, reshaping the way societies operate and individuals engage with technology (Muggah, 2021). However, this expansion has also amplified the attack surface for cybercriminals, increasing the frequency and sophistication of cyber threats. Modern attackers exploit technological vulnerabilities, such as insecure software, network misconfigurations, and weak authentication systems, while simultaneously taking advantage of human behavioural weaknesses through phishing, social engineering, and manipulation of trust.

A new challenge has emerged for free societies: democracies must find ways to strike a balance between allowing Internet freedom on one hand and maintaining adequate early warning and monitoring systems on the other (Herzog, 2011). The post-Covid-19 crisis has led to a greater dependence on digital solutions, exposing many of its vulnerabilities to state and non-state actors who have begun to exploit them. The COVID-19 pandemic precipitated a long-anticipated tipping-point in digital transformation (Muggah, 2021). Unfortunately, this period has led to an increase in cyber incidents at a rate never seen before. Meanwhile cybercrime, especially ransomware, has also increased exponentially (Muggah, 2021). As the consequences of cyberattacks and other malicious activities have increasingly affected multiple policy domains—including critical infrastructure, finance, healthcare, and public administration—cybersecurity has emerged as a central priority on the European Union's policy agenda. Recognizing the pervasive risks posed by digital threats, the EU has sought to strengthen its regulatory and institutional frameworks to protect citizens, businesses, and public institutions from cybercrime and systemic vulnerabilities. Simultaneously, the European Commission has placed Europe's digital transformation at the centre of its strategic agenda, emphasizing the necessity of ensuring that the growth of digital services, cloud computing, artificial intelligence, and interconnected devices is accompanied by robust cybersecurity safeguards.

This study seeks to address several interrelated research questions. First, it examines the extent to which the European Union has succeeded in developing a coherent cybersecurity policy framework in the post-pandemic period. Second, it investigates the main institutional, political, and structural challenges that hinder the implementation of a unified cybersecurity strategy. Third, the research analyzes the impact of vertical fragmentation (relationships between the EU, Member States, and the private sector) and horizontal fragmentation (relationships among EU institutions and agencies) on the coherence of cybersecurity governance. Fourth, it explores the role of trust and divergent policy priorities among Member States in shaping EU cybersecurity policies. Finally, the study considers the Estonian model to identify lessons and best practices that may be transferable at the EU level.

The objectives of the study are closely aligned with these questions. They include evaluating the coherence of EU cybersecurity policies post-COVID-19, identifying barriers affecting European cybersecurity governance, analyzing vertical and horizontal relationships within the EU governance architecture, and

investigating how trust and differences in priorities among Member States influence policy coherence. In addition, the study aims to examine the Estonian experience to extract lessons and policy recommendations applicable to the broader EU context.

The research addresses multiple policy dimensions. The institutional and governance dimension focuses on cooperation among EU institutions and specialized agencies. The national and comparative dimension examines the involvement of Member States, highlighting differences between larger and smaller states. The sectoral (public–private) dimension explores interactions with private actors essential for critical infrastructure protection. The normative and strategic dimension considers EU directives, regulations, and cybersecurity strategies. The trust and solidarity dimension analyses how mutual trust and information sharing between states and institutions affect policy effectiveness. Finally, the lessons and best practices dimension investigates the Estonian model and its potential applicability to other EU Member States. Together, these research questions, objectives, and policy dimensions provide a comprehensive framework for assessing the EU's cybersecurity governance and identifying avenues for improving coherence and effectiveness.

1. Methodology

The study adopts a qualitative research design, relying primarily on document and policy analysis. It draws on official EU documents, strategies, regulations, and communications, as well as reports from relevant agencies such as ENISA and Europol. In addition, academic literature and think-tank studies provide the analytical framework for understanding both the achievements and the limitations of the EU's cybersecurity governance. A comparative element is incorporated through the case study of Estonia, widely regarded as a pioneer in cybersecurity policy within the EU. The Estonian experience is examined in order to extract insights and policy lessons that may be relevant for other Member States and for the Union as a whole. This approach allows for both a descriptive mapping of existing EU instruments and actors in the cybersecurity domain, and a critical assessment of their coherence and effectiveness.

However, the study also presents certain limitations. First, the reliance on document analysis and the absence of primary empirical data may reduce the depth of understanding regarding the practical experiences of the actors involved. Second, the official sources consulted may be shaped by an institutional perspective, emphasizing achievements while downplaying challenges. Furthermore, the choice of Estonia as a case study, although relevant due to its pioneering role, raises issues of transferability, as its specific context does not necessarily reflect the realities of other Member States. Finally, the rapid evolution of policies and the cybersecurity landscape limits the durability of the conclusions, which may require frequent updates.

2. Literature review. The gradual evolution of the cybersecurity regulatory framework

To understand the evolution of EU cybersecurity policy, it is important to highlight the key developments in the legal and institutional frameworks that have underpinned its growth. Initially, the European Commission's primary focus was on economic integration and the protection of the single market, rather than on cybersecurity per se. In this context, information and communication technologies have been widely recognized as fundamental to economic growth. Beyond their technological advantages, ICTs pose notable risks, as reflected in international discussions on cybersecurity and the growing concerns over computer- and network-based crimes. Information and communication technologies were presented as both the Single Market's future, but also its Achilles' heel, as their abuse by foreign powers and individual criminals could seriously undermine economic development, distorting the functioning of the internal market (European Commission 1993) (Carrapico & Farrand, 2024). This approach emphasizes the essential role of ICT protection in supporting economic growth. In this context, the European security discourse on these challenges, which initially emerged under the Justice and Home Affairs Pillar, has gradually shaped the EU's approach to cybersecurity. By the mid-1990s, European institutions were already expressing a sense of urgency in addressing illegal and harmful content on the Internet (European Council 1996), as well as the use of information technologies by organised criminals (Council of the European Union 1997) (Carrapico & Farrand, 2024). The EU has soon become a key leader in cybersecurity, developing a comprehensive cybersecurity strategy and policies that emphasize public-private collaboration, leveraging private sector responsibility for information infrastructure and recognized expertise.

It is worth noting that security dynamics continue to be shaped by international events, including regional conflicts, cyberattacks, and terrorist operations, which increasingly rely on information and communication technologies for planning and execution. The EU Cybersecurity Strategy (EUCSS), adopted in 2013, was the first comprehensive document to address the wide range of cyber threats. The strategy introduced a comprehensive approach to cyber security, including cyber threats as a new risk to European security. The document aimed to protect the internal market by combating cybercrime, strengthening the resilience of network and information systems, and securing critical information infrastructures.

The strategy has also a legislative proposal to strengthen the security of information systems in the EU. The proposal highlighted the need for Member States and the private sector to adopt appropriate strategies to combat cyber threats and to facilitate information sharing between the public and private sectors, as well as among Member States, although the document itself is not legally binding. It reflects the awareness that coordination across a range of policy areas in Europe is necessary to respond to the challenges of cybersecurity (Vela, 2021). The EUCSS also defines

national and EU-level entities responsible for ensuring cyber security and emphasizes the need to strengthen national cybersecurity capabilities, including the development and operation of Computer Emergency Response Teams (CERTs). The EUCSS will require each MS to possess a well-functioning, national-level computer emergency response team (CERT) and a competent authority to speak on behalf of the country in discussions on the European level (Vela, 2021). Given that CERTs did not have a legal framework, informal operation was achieved by sharing data without knowing what data they could or could not share across borders.

Another significant achievement was the NIS Directive (EU) 2016/1148, which established a unified level of security for networks and information systems, as these systems are vital for critical sectors of a society. This directive provides, in particular, further clarifications on operators of essential services and relevant digital service providers. In this regard, they must apply security elements and report incidents. The proposal strengthens and streamlines security and reporting requirements for companies by imposing a risk management approach, which provides a minimum list of basic security elements that have to be applied (Sciacca, 2020). The document also describes the national framework that should be adopted by each Member State regarding the security of network and information systems. In this regard, Member States had the obligation to introduce a national strategy and to designate national competent authorities and the computer security incident response teams (CSIRTs).

Due to the rapid technological advancements and intense transactions on the internet, the volume of personal data collected and shared has grown substantially. Private companies and public authorities are using personal data on an unprecedented scale to carry out their activities, thus underlining the urgent need for adequate security measures to protect personal information against destruction, loss, alteration, disclosure or unauthorized access. In response to these new challenges, the General Data Protection Regulation (EU) 679/2016 required all businesses, whether acting as data controllers or processors, to ensure the security of personal data processing. In particular, it mandates that the controller, by the use of appropriate technical and organisational measures, shall ensure that only personal data that are necessary for the purpose are processed (Sciacca, 2020). Moreover, the controller shall ensure that by default personal data are not made accessible, without the individual's intervention, to an indefinite number of natural persons (Sciacca, 2020).

The EU Cybersecurity Act (Regulation EU 2019/881) strengthened the ENISA authority and expanded its mandate to new tasks. The Act granted ENISA a permanent mandate and gave it more resources and new tasks, including the implementation of an EU cybersecurity certification framework for ICT products (Fahey, 2024). The act also authorized the agency to enhance operational cooperation at the EU level by assisting Member States in managing cybersecurity incidents and supporting the EU in the event of large-scale cross-border cyberattacks and crises. The first objective of the regulation is to establish a certification scheme

about the cybersecurity features of ICT products, ICT services and ICT processes to tackle the current fragmentation of the internal market (Sciacca, 2020). CE marking indicates that a product has been assessed by the manufacturer and deemed to meet EU safety, health and environmental protection requirements (Fahey, 2024).

The impact of the COVID-19 crisis on EU cybersecurity policy resulted not in a rupture but in the continuation of existing strategies, this time emphasizing the role of social platforms in spreading disinformation and undermining the legitimacy of certain institutions and democracy. Thus, while the private sector proves to be a reliable partner in protecting cyberspace, social platforms provide sources of insecurity, being considered a challenge to EU security. Following the COVID-19 pandemic, the EU's cybersecurity policy continued to evolve, furthering digital transformation while strengthening security measures to enhance digital security, resilience, and cooperation among Member States. Many lessons have been learned, with the key realization that rapid digitalization has considerably increased security standards, making cybersecurity a top priority. To continue to develop society and promote economic prosperity through digitalization, government leaders, businesses, and end users must recognize the essential role of cybersecurity in this process. Additionally, the threat posed by cybercriminal activities in the online environment compels the EU to take decisive and urgent action to safeguard the digital market. The EU is aware of these risks, not only with respect to the direct potential damages but also with the loss of trust in the digital market, which could lead to more serious repercussions (Sciacca, 2020). In the contemporary European security context, the EU acknowledges that effective security depends on a strong cybersecurity strategy.

In light of this, the EU Cybersecurity Strategy, introduced in late 2020, sought to ensure the security of critical sectors of the economy and society, including energy networks, aviation systems, and space programmes. Particularly, the strategy stresses the significance of preventing foreign manipulation of elections and protecting press freedom (Renda, 2022). At the same time, the strategy addresses the development of new technologies, such as quantum communications infrastructure, encryption, 5G and future generations of mobile networks, as well as artificial intelligence. All these technologies must be developed and produced as designed and made in Europe technologies by European companies that are not dependent on high-risk suppliers (Renda, 2022). Lastly, the strategy acknowledges the EU's efforts to protect global cyberspace, to support non-binding international norms, rules and principles on responsible state behaviour, and its role in facilitating international cooperation, including bolstering third-country cybersecurity capabilities. The new Cybersecurity Strategy also allows the EU to step up leadership on international norms and standards in cyberspace, and to strengthen cooperation with partners around the world to promote a global, open, stable and secure cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values (European Commission, 2020).

The NIS Directive (NIS 2), updated in 2023 (Directive (EU) 2022/2555 of the European Parliament and of the Council), strengthened cyber resilience across critical public and private sectors, while enforcing specific cybersecurity requirements. Thus, it expanded the number of regulated sectors from 7 to 18, including digital services, critical manufacturing, utilities, and postal services. At the same time, the directive represents the EU's first comprehensive cybersecurity legislation that protects vital services within the European community. The entities concerned and their management bodies were required to implement measures in accordance with the directive by a certain date. The directive also mandates the establishment of a network of Computer Security Incident Response Teams (CSIRTs) in each EU Member State to oversee and respond to cyber threats, vulnerabilities, and incidents at the national level; to provide early warnings and disseminate information to the entities involved and therefore provide assistance in this regard. EU Member States can request ENISA's assistance in setting up their CSIRTs and must ensure their national CSIRTs' active involvement in the CSIRTs Network (Rupp, 2024). The CSIRTs Network provides a forum for cooperation and developing a coordinated response to cross-border cybersecurity incidents (Rupp, 2024).

The Digital Operational Resilience Act (DORA) (Regulation (EU) 2022/2554) strengthens cybersecurity in the financial sector, ensuring banks, insurance companies, and financial institutions can withstand cyberattacks. The DORA Regulation establishes a proportionality principle, requiring that rules on ICT risk management, incident reporting, operational resilience testing, and third-party risk management be applied in proportion to the financial entity's size, risk profile, and the complexity of its activities (Rupp, 2024). In late 2023, the EU adopted the Regulation on institutional cybersecurity, obliging Union entities to implement internal frameworks for managing, governing, and controlling cybersecurity risks. The regulation obliges each Union entity to carry out cybersecurity assessments, following which they must develop cybersecurity plans. In effect, the cybersecurity risk-management measures „shall ensure a level of security of network and information systems across the entirety of the ICT environment commensurate to the cybersecurity risks posed" (Art. 8 (1)) (Rupp, 2024).

In October 2024, the European Commission adopted the Cyber Resilience Act (CRA), setting cybersecurity requirements for products containing digital elements, to ensure their security throughout their lifecycle. The Act aims to ensure that products bearing the 'CE marking' comply with a minimum level of cybersecurity requirements (Fahey, 2024). CE marking indicates that a product has been assessed by the manufacturer and deemed to meet EU safety, health and environ-mental protection requirements (Fahey, 2024). The Cyber Resilience Act addresses the insufficient level of cybersecurity in many products, and the difficulties consumers and businesses face when trying to identify products that are cybersecure. The CRA introduces mandatory cybersecurity requirements for manufacturers and retailers, governing the planning, design, development, and maintenance of such products

(European Commission, 2025). This regulation will give the Commission considerable powers, under the heading of market surveillance and enforcement, including deeming products as non-compliant with the regulation and as presenting a significant cybersecurity risk based on an ENISA assessment (Carrapico & Farrand, 2024).

In December 2024, the European Commission adopted the Cyber Solidarity Act (CSA) (Regulation (EU) 2025/38) in order to enhance resilience and response to cyber threats. The document aims to establish a cybersecurity unit, supported by member states, to enhance the detection, analysis, and response to cyber incidents. It also includes the creation of an urgent response mechanism for cybersecurity incidents and the establishment of an EU cybersecurity reserve, made up of contractual providers, ready to intervene in the event of a cybersecurity incident. Article 1 of the proposed Cyber Solidarity Act explicitly includes in its objectives reinforcing 'the competitive position of industry and services in the Union cross the digital economy and contributing to the Union's technological sovereignty in the area of cybersecurity' (European Commission, 2023, p. 22), reinforcing the regulatory mercantilist position adopted by the Commission in this field (Carrapico & Farrand, 2024). This means that the EU seeks to reduce its dependence on external technologies (for example, from the United States or China) and instead to develop and rely on its own solutions.

Furthermore, the EU has advanced its cybercrime agenda by reinforcing Europol's European Cybercrime Centre (EC3) and introducing legislation on digital evidence. Additionally, cyber diplomacy has significantly increased in recent years, becoming a central component of the European Union's (EU) cybersecurity policies. Cyber diplomacy as part of cybersecurity policies involves a collective effort to implement a unified diplomatic response to malicious cyber activities. In this context, the EU's cyber diplomacy toolbox is particularly noteworthy, as it introduces, for the first time, a coordinated diplomatic response to malicious cyber activities. The measures included within the Toolbox are meant to be „complementary to existing and continuous cyber diplomacy engagement to advance conflict prevention, cooperation and stability in cyberspace" and can be carried out „individually or jointly, in coordination or in parallel, and where appropriate in cooperation with international partners" (Rupp, 2024). Also, cyber defence policy advocates for investments in cyber defense capabilities and aims to enhance coordination and cooperation between the EU's military and civilian cyber communities. In accordance, the Council regards the EU Policy on Cyber Defence as an enabler for „the EU and its Member States to strengthen their ability to protect, detect, defend and deter, making appropriate use of the whole range of defensive options available to the civilian and military communities for the broader security and defence of the EU, in accordance with international law, including human rights law and international humanitarian law" (Rupp, 2024).

The EU also engages in high-level cooperation with NATO through the NATO Defence Innovation Accelerator (DIANA), an initiative that collaborates with top researchers and entrepreneurs across the Alliance to develop technologies aimed at safeguarding NATO populations. The NATO Defence Innovation Accelerator seeks to increase the participation of innovative companies based in NATO member countries. These companies are developing deep technology solutions to respond to pressing security challenges related to energy & power, sensing & surveillance, data & information security, human health & performance, and critical infrastructure & logistics (NATO, 2024). Under the DIANA programme, companies gain funding, training, and access to specialized environments for testing and improving their technological solutions.

In conclusion, the European Union has shown a clear ambition to enhance its ability to project cybersecurity norms on the international stage, while simultaneously striving to present a cohesive position in global fora in coordination with the United States. Like the US, the EU is also increasingly interested in nudging international cybersecurity developments (Fahey, 2024). Their engagement has been concentrated mainly within the framework of the Council of Europe, because of the long-standing deadlock at the UN in recent years, stemming from disagreements among major powers on issues such as state responsibility in cyberspace, the applicability of international law, and norms for offensive cyber operations (e.g., differences between the US, EU, Russia, and China). The EU's continued efforts to strengthen European cyber capabilities are a key component of its cybersecurity strategy, thus contributing to regional stability. Along with these, the Union actively promotes the security and stability of international cyberspace by leveraging its cyber diplomacy toolbox, engaging in diplomatic initiatives with global partners, and employing legal instruments such as the sanctions regime to deter and respond to malicious cyber activities.

2.1. Horizontal and vertical dynamics within the EU's cybersecurity field

Horizontal fragmentation arises from structural and functional overlaps among different EU institutions and agencies, which complicates cohesive cybersecurity governance. Agencies such as ENISA (EU Agency for Cybersecurity), Europol's EC3 (European Cybercrime Centre), and CERT-EU have overlapping but distinct responsibilities, potentially leading to redundancy, inefficiencies, and inter-agency competition. The absence of a central coordinating authority with overarching responsibility for cybersecurity at the EU level further exacerbates these challenges, as there is no single entity tasked with ensuring strategic alignment across institutions. Moreover, cybersecurity intersects multiple policy areas—including justice, internal affairs, defense, the digital market, and data protection—yet coordination across these „silos" is often limited. This fragmentation can hinder rapid response to emerging threats, delay policy implementation, and reduce the

overall coherence and effectiveness of the EU's cybersecurity framework, leaving gaps that may be exploited by attackers and undermining public trust in digital infrastructures.

Carrapico and Barrinha (2017), in their article „The EU as a coherent actor in the field of (cyber)security?", highlight the difficulties the European Union faces in achieving coherence in cybersecurity governance, emphasizing both vertical and horizontal dimensions. Vertical challenges stem from the need to coordinate cybersecurity policies between the EU, Member States, and the private sector, where issues of national sovereignty and uneven capacities impede the consistent implementation of measures across the Union. Horizontal challenges, on the other hand, are linked to insufficient communication and coordination among EU institutions, agencies, and Member States. The authors emphasize the importance of addressing contradictions between policies, responsibilities, and instruments to enhance coherence and effectiveness in the EU's cybersecurity governance.

In this view, the NIS Directive, adopted by the European Commission in 2016, is the EU's first cybersecurity legislation and serves as a legally binding instrument on cybersecurity policy. In the NIS Directive, the EU legislature acknowledges the importance of imposing not only obligations on the Member States' authorities, but also on the private sector, notably the providers of essential services mentioned in Annex II of the Directive and the providers of digital services mentioned in Annex III of the Directive (Verhelst & Wouters, 2020). In light of the above, the NIS Directive represents the most significant advancement in strengthening coordination between EU institutions and Member States. The NIS Directive (Directive (EU) 2016/1148) appears to further contribute to this by bringing together the European Commission, Member States and ENISA as members of the new Cooperation Group, which has been created to offer strategic guidance and facilitate cooperation between Member States on information security (Carrapico & Barrinha, 2017).

Following this, the cooperation agreement between the European Union Agency for Cybersecurity (ENISA) and the European Cybercrime Centre (EC3), signed in 2019, elevated the level of coordination within the EU. Key issues addressed included defining what constitutes a cyber incident and establishing a systematic information-sharing framework to combat cybercrime. In this context, Carrapico and Barrinha (2017) emphasize the need to eliminate contradictions in policies, responsibilities, and instruments. They argue that various EU bodies, including the European Commission, ENISA, and EC3, should collaborate synergistically. Moreover, the authors highlight that overlapping mandates among these institutions can create inefficiencies and hinder coherent action, making it essential to clarify roles and ensure that coordination mechanisms effectively complement rather than duplicate each other.

The EU's approach to cyberspace is still fractured despite these accomplishments, as it is a developing policy field with too many complicated issues. There are coordination problems between, but also within institutions, which

are related to the historical evolution of the different cybersecurity areas, as well as the perception that each area still experiences different separate challenges (Carrapico & Barrinha, 2017). Moreover, cybersecurity intersects a wide range of policy domains—including justice, internal affairs, defense, the digital market, and data protection—each governed by distinct legal frameworks, institutional mandates, and strategic priorities. This multidimensional nature of cybersecurity creates challenges in aligning objectives, procedures, and resources across sectors. Coordination across these areas is often hindered by institutional silos, differing threat perceptions, and varying levels of technical expertise, which can lead to overlapping responsibilities, delays in decision-making, and inconsistencies in policy implementation.

Vertical fragmentation refers to the coordination challenges between the European Union, Member States, and the private sector in managing cybersecurity. One of the main obstacles is national sovereignty: cybersecurity remains largely considered a matter of national security, and Member States are often reluctant to delegate authority or harmonize policies at the EU level. This reluctance can slow down the implementation of common strategies and create inconsistencies in preventive and response measures across the Union. Additionally, there are significant differences in national capacities: while some Member States have developed sophisticated cyber defense infrastructures, others face resource constraints and limited technical expertise, leading to uneven implementation of EU directives and standards. Public–private coordination also remains insufficient. As most critical infrastructures are owned or operated by private entities, the lack of systematic information-sharing and joint risk management between governments and private actors reduces overall resilience and creates vulnerabilities that can be exploited in cross-border cyber incidents.

In the vertical dimension—encompassing relationships between Member States and EU institutions, as well as interactions with the private sector—a gradual increase in coherence has been observed in response to the intensification of cyberattacks. Several factors have contributed to this trend, including the rapid growth of internet users and digital services, the significant societal and economic impacts of cyberattacks, and the rising prevalence of cybercrime. These developments have created strong incentives for Member States and EU institutions to enhance coordination, align policies, and engage more effectively with private-sector actors to mitigate risks and strengthen overall cybersecurity resilience across the Union. More recently, the increasing use of cyber tools by nation-states to disrupt elections and other democratic processes has further strengthened the EU's commitment to improving cybersecurity.

Despite these successes, Carrapico and Barrinha identify that the lack of coherence at the vertical level is largely driven by difficulties in alignment and collaboration. In the relationship between Member States and EU institutions, the primary coordination challenge lies in the European Commission's limited capacity

to persuade Member States of the necessity for deeper integration in cybersecurity. The reluctance of Member States to grant the EU greater authority over cyber activities constrains the Union's overall coherence in this field. Nevertheless, while coordination challenges persist between Brussels and Member States, the primary responsibility for cybersecurity governance appropriately remains with the Member States. This approach acknowledges the importance of national sovereignty and the critical coordinating role that each country plays in addressing cyber threats within its own territory, while still emphasizing the need for effective collaboration at the EU level.

Vertical fragmentation in the EU's cybersecurity governance is significantly shaped by issues of sovereignty and uneven capacities. Member States are cautious in delegating authority to EU institutions, as cybersecurity is considered a core aspect of national security, and there is concern that deeper integration could undermine sovereign control over sensitive operations. Also, states are often afraid of sharing information that could compromise the economic interests of their companies or, given the significant secrecy that still surrounds cybersecurity operations, of sharing too much operational information (Carrapico & Barrinha, 2018). In this regard, smaller EU member states often lack both resources and expertise in cybersecurity, while larger EU states are reluctant to have cybersecurity priorities set for them by the European Commission. Additionally, some countries are not prepared to make substantial financial investments in developing cybersecurity infrastructure, not because they lack interest, but because cybersecurity is not currently a high policy or budgetary priority relative to other national concerns.

Additionally, conflicts of interest have also been observed in public–private interactions, as the public sector prioritizes security and risk mitigation, whereas private actors often emphasize efficiency, profitability, and competitive advantage (Carrapico & Barrinha, 2017). Thus, while the public sector prioritizes security and the protection of critical infrastructures, the private sector often emphasizes efficiency and profitability, seeking to maintain a competitive advantage. These differing priorities can create tensions in the implementation of cybersecurity measures, complicate information-sharing, and hinder the development of coherent strategies that effectively balance risk management with operational and commercial considerations. The more attractive financial prospects in the private sector make it challenging for public institutions to attract and retain professionals with cybersecurity expertise (Spanou, 2021). This disparity in incentives can undermine trust between public and private partners, which is crucial for effective information-sharing, particularly regarding the reporting and disclosure of cyberattacks at the national level (Carrapico & Barrinha, 2017).

2.2. Additional challenges for European cybersecurity policies

Beyond the theoretical framework proposed by Helena Carrapico and André Barrinha regarding the coherence of European cybersecurity policy, it can be argued that global political and social developments play an equally significant role in shaping these dynamics. Such external factors contribute to both vertical and horizontal fragmentation within the EU's cybersecurity architecture, affecting coordination between Member States, EU institutions, and the private sector, as well as among the various EU agencies themselves. The Russo-Ukrainian war has had a significant impact on the European Union's security policy, including its approach to cybersecurity. The conflict has accelerated efforts to strengthen defense and security cooperation among Member States, highlighting the need for rapid and coordinated responses to emerging threats, including cyberattacks originating from state or state-affiliated actors. In particular, the risk of cyberattacks targeting critical infrastructure—such as energy, transportation, and communication systems—has increased, emphasizing the importance of resilience and information-sharing between governments and the private sector.

The hybrid war started by Russia, as long as it continues, this will destabilize European security. For the foreseeable future, this threat landscape will be dominated by risks connected to the Kremlin's cyber operations (Kaushik, 2024). Since the outset of Russia's war, several European countries have been victims of cyberattacks launched by cyber-organized groups that support the Kremlin's revisionist policy. The attacks targeted the countries' critical infrastructure, namely satellite networks and the energy grid. Hybrid campaigns and influence operations carried out by Russian malign actors, which have historically especially targeted Central and Eastern Europe (CEE), are likely to continue as the EU maintains its support for Ukraine (Kaushik, 2024).

The role of China in conducting state-affiliated cyberattacks is extensively documented and acknowledged by experts and international observers. Chinese aligned Advanced Persistent Threat (APT) groups have been active for quite some time, regularly targeting government entities, as well as private companies in the engineering, telecom, and aerospace sectors, in a bid to steal classified information (Kaushik, 2024). While their activities are global, they frequently focus on countries with advanced technological capabilities and critical infrastructure, including the United States, members of the European Union, Japan, and Australia. These operations aim to exfiltrate classified information, intellectual property, and sensitive technological data, thereby advancing China's strategic and economic objectives. Within the European context, the persistent activity of these APT groups underscores the vulnerabilities of EU institutions and companies to state-aligned cyber threats, highlighting the urgent need for robust cybersecurity measures, enhanced public–private cooperation, and coordinated responses across At the same time, China's ambition to become a global leader in emerging technologies—such

as 5G, artificial intelligence, and quantum computing—places pressure on the EU to accelerate the development of its own digital capabilities and to safeguard critical infrastructure from dependency on foreign technology. In addition, the proliferation of disinformation campaigns, including deepfake content and online influence operations, poses significant challenges to public trust and democratic resilience within Europe.

In this context, emerging technologies, especially AI and machine learning, have great potential to improve cybersecurity capabilities. In this situation, artificial intelligence can identify threats and vulnerabilities, predict threats and risks, and be incorporated into incident response capabilities to accelerate response times. An increasing number of companies, such as IBM, Google and Microsoft, have started advertising and showcasing ways in which AI can be used to enhance cybersecurity (Car & Marcelin, 2024). However, hostile actors could use artificial intelligence algorithms to launch automated cyberattacks and disseminate false information. According to ENISA, AI systems are becoming particularly powerful in social engineering techniques thanks to their ability to mimic human interaction (Car & Marcelin, 2024). These challenges are made worse by the growing calls for European cybersecurity financing. Additionally, there is a sizable disparity in priority accorded to cybersecurity within EU Member States, contributing to uneven cybersecurity capabilities across the EU and exacerbating security vulnerabilities across European networks (Kaushik, 2024).

Beyond these factors, the size and complexity of cyberspace, which makes it even harder to pinpoint specific attackers, present another obstacle for European cybersecurity policy. As a result, attackers utilize various tactics and tools to evade detection and deceive investigators. For example, attackers use false flags – employing techniques, tools, and/or languages associated with other threat actors/nations – to mislead investigators and may spoof IP addresses to make it seem as though an attack originated from a different location (Kaushik, 2024).

3. Case study - the Estonian cybersecurity policy model

The Estonian model is widely regarded as an effective cybersecurity policy thanks to its holistic approach, which places strong emphasis on investment in education and developing cyber skills. Estonia has incorporated cybersecurity into its academic programs, developed a robust local cyber ecosystem, assisted small cybersecurity companies to increase their knowledge and facilitate information exchange. Furthermore, it promoted cooperation between the public and private sectors, adopted cybersecurity procedures in both private businesses and educational institutions, and put important laws in place to protect data and the privacy of its citizens. Experts also stress the importance of the fact that Estonia's cybersecurity prioritisation is premised on scientific research and analysis rather than being dependent on changing political whims (Kaushik, 2024).

The success story begins following the cyberattacks of 2007, with Estonia being the victim of the world's first coordinated cyberattack against a state that was allegedly committed by Russian-backed hackers. The attacks targeted various organizations in the country, including the parliament, banks, ministries, newspapers, and broadcasters, serving as a catalyst for the nation's digital transformation. The cyber-terrorist attacks were executed via globally dispersed botnet networks composed of „zombie" computers. The hackers hijacked computers—including many home PCs—in places like Egypt, Russia, and the United States and used them in a „swarming" DDoS strategy (Herzog, 2011). With this sudden awakening of the world, the cyberattacks on Estonia became a pivotal moment in enhancing the nation's security infrastructure for the long term. Shortly after the attacks, the Estonian government endorsed the first national-level cybersecurity strategy focused on the protection of critical information infrastructure (Pernik, 2021).

Estonia has developed a comprehensive cybersecurity infrastructure that involves multiple institutions working collaboratively to ensure national resilience and societal preparedness. Central to this system is the Estonian Information System Authority (RIA), responsible for national cybersecurity policies and the protection of critical digital services, alongside the Cyber Defense Unit of the Estonian Defence League, a volunteer-based organization providing operational support in cyber defense. Estonian Information System Authority can conduct risk analyses of critical information infrastructures and impose extra-judicial fines for insufficient actions on operators of essential services or digital service providers (Kohler, 2020). The Cyber Defense Unit is an innovative model for the involvement of volunteers in national cyber defence. Also, the Estonian Defence League is a voluntary defense organization with about 16,000 members (Kohler, 2020). Over the past decade, Estonia has become home to numerous cybersecurity organizations that have earned international recognition. NATO was the most effective framework for Estonia in boosting its status as a cyber authority, as Tallinn is home to NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE), which serves as a key hub for cyber defense research, training, and international collaboration. The CCDCOE facilitated the Tallinn Manual I and II, describing how international law can apply to cyberspace (Crandall, 2024). CCDCOE also hosts annual multinational exercises such as Locked Shields and Crossed Swords. The former is the largest and most complex international live-fire cyber defense exercise in the world, which is run on the NATO Cyber Range in Tartu operated by the EK (Estonian Defence Forces) (Kohler, 2020). Estonia has become a hub for cybersecurity innovation, many leading cybersecurity companies have either been founded by Estonians or established offices in the country, contributing to the development of cutting-edge security solutions and fostering collaboration between the private sector, government institutions, and research organizations. Notable examples include Malwarebytes,

Symantec, and CyberCube, which illustrate the country's growing influence in the global cybersecurity landscape.

Equally important is the fact that Estonia has incorporated cybersecurity education into its academic curriculum from an early stage, fostering a highly skilled workforce. Higher education institutions offer undergraduate and graduate programs in computer science, cybersecurity, and digital technologies, complemented by specialized courses and international certifications that enable continuous professional development.

Tallinn University of Technology (TalTech), Estonia, offers cybersecurity bachelor's, master's, and doctoral degrees that are all taught in English. In this academic context, TalTech's Center for Digital Forensics and Cyber Security enhances cyber competence and emphasizes research and education in cybersecurity. Also, Estonia consistently collaborates with global tech leaders to keep its education system at the cutting edge of innovation. Thanks to the programs offered by TalTech, some graduates pursue careers with the police and border guard to combat cybercrime, others join the Defense Forces, while some transition to the private sector, specializing in cybersecurity-related work. Furthermore, the Center for Digital Forensics and Cyber Security at TalTech aims to establish itself as the premier institution for Master's and Doctoral studies in cybersecurity across the Baltics and Nordic countries. Today, Estonia is taking another pioneering step by integrating AI into high school education, ensuring that the next generation is equipped to navigate and shape the future (Holm, 2025). By teaching young people how to leverage AI for their benefit, we are strengthening their digital competence and fostering a new generation of cyber security experts who can anticipate and counter emerging threats (Holm, 2025).

Participation in international exercises, such as NATO's Locked Shields, allows professionals to refine their skills in complex attack and defense scenarios. Also, the presence of leading cybersecurity companies, including Malwarebytes, Symantec, and CyberCube, further enhances expertise through collaboration, knowledge transfer, and exposure to cutting-edge technologies. Estonia collaborates with private companies and international partners to strengthen cyber defenses and information-sharing. As a result of these developments, Estonia has established a robust national cybersecurity ecosystem, underpinned by strong collaboration between government institutions and private sector actors, particularly startups and technology firms. This partnership not only facilitates the development of cutting-edge cybersecurity solutions but also promotes innovation, knowledge transfer, and the continuous professional growth of cybersecurity specialists, reinforcing the country's position as a global leader in digital security. For instance, private cybersecurity companies often collaborate with government agencies to share expertise, improve threat detection systems, and strengthen national cybersecurity defenses. Estonia collaborates extensively with international partners, including NATO and the European Union, particularly in the fields of cybersecurity and

defense. This cooperation encompasses joint research initiatives, participation in multinational cyber exercises, sharing of threat intelligence, and the development of common standards and best practices, thereby enhancing both national and regional resilience against evolving cyber threats. Additionally, Estonia collaborates with other EU member states to combat cybercrime, actively participating in the European Cybercrime Centre (EC3) at Europol and contributing to coordinated efforts to prevent and respond to online threats and cyberattacks.

Estonia's e-governance system—which encompasses digital IDs, e-voting, and a wide range of secure online services—is supported by a secure and resilient digital infrastructure. This robust framework ensures the integrity, confidentiality, and availability of digital services, enables efficient and transparent interactions between citizens and the state, and provides a strong foundation for implementing advanced cybersecurity measures that protect both personal data and critical national systems. Estonia developed institutions such as the e-Governance Academy which is responsible for training and educating administrative representatives and officials from different countries. Estonia developed the e-Governance Academy (eGA) to train and educate government officials and administrative representatives from various countries, transferring knowledge and best practices in digital transformation, e-governance, digital democracy, and national cybersecurity. Since its inception, eGA has been recognized as a pioneer in implementing development cooperation projects, transferring best practices in e-governance and digital transformation to various countries. Projects carried out in Ukraine currently listed on their website go back to 2014 and cover several topics such as boosting e-governance solutions, improving cybersecurity readiness in Ukrainian public officials, and building cyber defence capabilities (Crandall, 2024).

Estonia has been a pioneer in integrating blockchain technology into its digital infrastructure, particularly for enhancing cybersecurity, data integrity, and e-governance. Blockchain is applied in areas such as the national digital ID system, healthcare records, and data exchange between public institutions, ensuring that critical information remains tamper-proof while enabling efficient and trustworthy interactions between citizens and the state. Thus, in public services, such as the Land Registry and Business Registry, blockchain maintains secure, tamper-proof records of property ownership and company registrations. In the healthcare system, it is used to securely track patient data and prevent unauthorized modifications. Additionally, blockchain plays a key role in cybersecurity and data protection, securing national databases and safeguarding citizen identity data. In finance and banking, it enhances transaction security, and in the legal and judicial system, it enhances security, transparency, and efficiency. These implementations have positioned Estonia as a global leader in blockchain-driven digital governance and cybersecurity innovation. As a result of having proven its capacity and preparedness to successfully counter cyber threats, Estonia has increased public trust in state institutions. Through proactive cybersecurity measures, transparent communication, and collaboration

with private and international partners, Estonia has reinforced its digital resilience, assuring citizens that their data and digital services remain secure. Estonia now boasts one of the highest levels of public trust in government, proof of our transparent and citizen-centric digital society (Holm, 2025).

3.1. Statistical data on cyber incidents in the last 2 years in Estonia

Estonia has experienced a significant rise in cybercrime incidents over 2023 and 2024, reflecting broader global trends influenced by geopolitical tensions and the increasing sophistication of cyber threats. The escalation in cyber threats has been influenced by major global events, such as Russia's aggression in Ukraine since February 2022 and the Hamas-Israel conflict that reignited in October 2023. In this regard, armed conflicts often stimulate an intensification of cyber operations conducted by states or state-affiliated actors, as they seek to disrupt critical infrastructure, gather intelligence, or project power in the digital domain. These tensions led to increased ideological hacktivism, with denial-of-service attacks targeting Estonia's government, financial, transport, and media sectors. In Estonian cyberspace, one of the largest and most visible indirect effects of Russia's full-scale invasion of Ukraine, which began in February 2022, was a fourfold increase in distributed denial-of-service (DDoS) attacks (Information System Authority, National Cyber Security Center, 2024). This surge reflects broader regional cyber tensions, as Estonia, due to its historical and strategic position, often becomes a target for politically and ideologically motivated cyber operations linked to conflicts in Eastern Europe.

In 2023, according to the Estonian Information Systems Authority (RIA), 3.314 impactful cyber incidents were recorded, representing a 24% increase compared to 2022. We saw – and will surely continue to witness – a growth in ideological 'hacktivism' expressed in denial-of-service attacks against the government, financial, transport, and media sectors (Information System Authority, 2024). DDoS attacks surged, with 484 incidents in 2023—a 60% increase from the previous year (139 of the attacks had an impact). The damage was generally limited to a short period of downtime or slower response on a website or service, but a few cases were more serious (Information System Authority, National Cyber Security Center, 2024). It is important to emphasize that some of these incidents were the result of human error or technical malfunctions, rather than malicious cyberattacks.

The cybersecurity incidents involved data leaks, as a result of which attackers infiltrated the systems of a higher education institution in Estonia, compromising the personal data of students and graduates. According to the Estonian Information System Authority, a notable data breach was the incident involving the genetic testing company Asper Biogene, where attackers accessed and downloaded sensitive medical and personal data of approximately 10,000 individuals. Various forms of fraud have recorded significant increases, recalling that 546 fraud incidents were

recorded, a 250% increase over the previous year. Data provided by the Police and Guard Board show that Estonians were defrauded of at least 8.3 million euros (Information System Authority, National Cyber Security Center, 2024). Some scammers posed as police officers, claiming to help victims avoid fraud, asking for personal information, while others pretended to be interested buyers on Facebook Marketplace, trying to extract sensitive information from sellers.

Ransomware attacks have also been recorded, mainly targeting relatively large and financially stable companies, perceived as being able to pay significant ransoms. We also saw criminals use IT and accounting service providers to obtain access to bigger, wealthier clients and implant ransomware that encrypts data (Information System Authority, National Cyber Security Center, 2024). Also, zero-day vulnerabilities in software that remain unaddressed by developers in a timely manner present attractive targets for attackers, who recognize the potential for significant financial gain. Not lastly, the Estonian Information System Authority reported that one-third of phishing attack recipients are deceived by the scam, with 10-20% of victims ultimately providing the requested information. These incidents highlight a significant vulnerability in terms of user awareness and digital hygiene in the country.

In 2024, Estonia experienced a marked escalation in cyber threats, with the number of significant cyber incidents doubling compared to the previous year. The Estonian Information System Authority (RIA) reported 6.515 such incidents, up from 3.314 in 2023. Regarding the cyber incidents, in 2024 two-thirds of the incidents involved phishing and scam websites, with 4.224 cases detected—2.5 times more than the previous year, highlighting a significant rise in social engineering attacks. Additionally, in 2024, distributed denial-of-service (DDoS) attacks reached unprecedented levels, overwhelming public-sector websites for several hours and producing approximately three billion malicious requests. Some websites experienced short-term outages or slowdowns, but none of the attacks caused severe damage (Information System Authority, National Cyber Security Center, 2025). Estonia also recorded 68 data leak incidents, almost twice as many as last year. The most serious cyberattack was on the company Allium UPI, which affected more than 700.000 people. Attackers gained access to this system and successfully stole nearly 700,000 personal identification numbers, more than 400,000 email addresses, and tens of thousands of phone numbers and home addresses (Information System Authority, National Cyber Security Center, 2025).

According to the Estonian Information System Authority, 624 significant fraud incidents were recorded last year, up from 546 in 2023. This rise is largely attributed to the growing prevalence of investment scams and banking fraud, which continue to exploit public trust and digital vulnerabilities. Invoice fraud has become a relatively common type of scam in which fraudsters send a fake invoice to an organisation under the guise of a legitimate business partner (Information System Authority, National Cyber Security Center, 2025). Ransomware attacks decreased in

2024, with around 10 ransomware incidents reported, fewer than in previous years. In this context, two Estonian schools were hit by ransomware attacks: only one had backups to restore its data, while the other suffered more severe disruption. In nearly one-third of cases, attackers gained access to systems through Remote Desktop applications that were protected by weak passwords and lacked additional security measures such as VPNs, two-factor authentication, IP-based restrictions, logging and monitoring (Information System Authority, National Cyber Security Center, 2025).

Zero-day vulnerabilities continue to be exploited by attackers within the systems used to manage the agency's computers and devices, with over 40.000 security vulnerabilities reported last year. Some agencies fail to apply essential system updates for managing their computers and devices, increasing vulnerability. This vulnerability is also observed in both public and private sector organizations. Cybercriminals also continued to target devices with older, known vulnerabilities, often exploiting them for ransomware attacks or adding them to botnets (Information System Authority, National Cyber Security Center, 2025). As in previous years, numerous critical vulnerabilities were discovered in web content management systems and e-commerce software (Information System Authority, National Cyber Security Center, 2025).

4. Discussion

Despite being targeted by multiple cyberattacks over the past two years, Estonia maintains a strong cybersecurity posture and is consistently ranked among the most cyber-resilient nations in the world. The country's strong digital defenses and proactive measures continue to set the standard for cybersecurity procedures around the globe. According to data provided by specialists in the field, the proactive measures taken by Estonian institutions to mitigate cyber threats, their early recognition and subsequent investments in building a secure digital infrastructure have made Estonia a successful model of cybersecurity policy for other European states. The lessons of the Estonian model show that a good relationship between the public-private sector and academia is essential for the proper management of cybersecurity risks. Estonia has taken bold steps to ensure that cyber security awareness extends beyond government and industry to the entire population (Holm, 2025). Considering that we all use gadgets on a daily basis to make our lives easier, it is essential that we become more mindful and vigilant about the risks we encounter in cyberspace. The use of these commonplace gadgets without cybersecurity safeguards and consumers' lack of attention to detail, on the other hand, makes room for bad actors who, without necessarily intending to harm us personally, can use our devices as tools to create botnets or, worse, to serve organized crime and destabilize democratic and peaceful societies. This is why we need people who will bring cyber hygiene into general education as a skill that everybody must have if they are going to be owners of electronic equipment (Spanou, 2001). Investments should prioritize

education, with the goal of creating programs that improve students' cybersecurity skills and encourage research in the field of cybersecurity, while also supporting the private sector by helping small companies provide specialized expertise in the field. As the continent prepares to defend itself, it must take a holistic approach, integrating technological security with public awareness and trust (Holm, 2025).

Conclusions

The study's objectives align closely with its research questions, focusing on evaluating the coherence of EU cybersecurity policies post-COVID-19, identifying governance barriers, analysing vertical and horizontal institutional relationships, and examining how trust and divergent priorities among Member States influence policy effectiveness. The Estonian experience serves as a comparative case to extract lessons and best practices applicable to the broader EU context. These objectives engage multiple policy dimensions, including institutional cooperation, national variation between larger and smaller Member States, public–private interactions, normative and strategic frameworks, trust and solidarity, and the transfer of lessons from successful national models. Theoretical claims regarding multilevel governance and fragmentation are supported by evidence that inconsistent coordination, misaligned priorities, and limited trust undermine a fully cohesive EU cybersecurity policy, while Estonia's proactive and integrated approach highlights pathways for improving resilience and coherence.

Methodologically, the study relies on qualitative document and policy analysis, drawing on official EU and national documents, agency reports, and scholarly literature. While this allows for a detailed mapping of policies, actors, and instruments, it limits insight into operational practices and real-time challenges, suggesting that conclusions are interpretive rather than empirically validated. Despite these limitations, the findings point to prioritized EU-level actions: strengthening vertical and horizontal coordination, enhancing trust and information sharing, integrating national best practices such as Estonia's cyber resilience and awareness campaigns, promoting sectoral public–private cooperation, harmonizing legal and strategic instruments, and developing EU-wide education and workforce initiatives. Together, these measures address the institutional, national, sectoral, strategic, and trust dimensions of cybersecurity governance, offering a roadmap for increasing policy coherence and effectiveness across the Union.

References

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

Carrapico, H., & Farrand, B. (2024). Cybersecurity trends in the European Union: Regulatory mercantilism and the digitalisation of geopolitics. *Journal of Common Market Studies*, *62*(Annual Review), 147–158. https://doi.org/10.1111/jcms.13654

Carrapico, H., & Barrinha, A. (2018). *How coherent is EU cybersecurity policy?* LSE European Politics and Policy (EUROPP) Blog. https://blogs.lse.ac.uk/europpblog/

Car, P., & Marcelin, T. (2024, April 25). *Artificial intelligence and cybersecurity*. Think Tank – European Parliament. https://epthinktank.eu/2024/04/25/artificial-intelligence-and-cybersecurity/

Crandall, M. (2024). Understanding Estonia's cyber support for Ukraine. *Applied Cybersecurity & Internet Governance*, *3*(1), 1–13. https://doi.org/10.60097/ACIG/190396

Directive (EU) 2016/1148 of the European Parliament and of the Council 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 194/119, September. http://data.europa.eu/eli/dir/2016/1148/oj

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union, L 333, 80–152. http://data.europa.eu/eli/dir/2022/2555/2022-12-27

European Commission. (2020). *New EU cybersecurity strategy and new rules to make physical and digital critical entities more resilient* [Press release]. https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_20_2391/IP_20_2391_EN.pdf

European Commission. (2023, April 18). *Proposal for a regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents (COM(2023) 209 final, 2023/0109 (COD)).* European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023PC0209

European Commission. (2025). *Cybersecurity policies*. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

Fahey, E. (2024). The evolution of EU–US cybersecurity law and policy: On drivers of convergence. *Journal of European Integration*, *46*(7), 1073–1088. https://doi.org/10.1080/07036337.2024.2411240

Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security*, *4*(2), 49–60. https://doi.org/10.5038/1944-0472.4.2.3

Holm, P. (2025). *Estonia's bold approach to cyber security: A holistic model for Europe*. e-Estonia.com. https://e-estonia.com/estonias-cyber-security-model-for-europe/.

Information System Authority, National Cyber Security Center. (2024). *Cyber security in Estonia 2024* (pp. 1–60). Information System Authority. https://www.ria.ee/en/news/cyber-security-estonia-2024

Information System Authority, National Cyber Security Center. (2025). *Cyber security in Estonia 2025* (pp. 1–60). Information System Authority. https://www.ria.ee/sites/default/files/documents/2025-02/Cyber-security-in-Estonia-2025.pdf

Kaushik, A. (2024). *Shaping the next EU Commission's priorities: Addressing cybersecurity challenges and policy gaps* (pp. 1–8). GLOBSEC. https://www.globsec.org/sites/default/files/2024-08/Shaping%20the%20Next%20EU%20Commission%27s%20Priorities-%20Addressing%20cybersecurity%20challenges%20and%20policy%20gaps%20chapter.pdf

Kohler, K. (2020). *Estonia's National Cybersecurity and Cyberdefense Posture* (CSS Cyberdefense Report). Zürich: Center for Security Studies, ETH Zurich. https://doi.org/10.3929/ethz-b-000438276

Muggah, R. (2021). The COVID-19 pandemic precipitated a long-anticipated tipping-point in digital transformation. *European Cybersecurity Journal*, *7*(1), 1–91. https://ik.org.pl/wp-content/uploads/2023/11/ECJ_vol7_issue1_final-1.pdf

NATO. (2024). Over 70 companies chosen to join NATO's 2025 accelerator programme for defence innovation. https://www.nato.int/cps/en/natohq/news_231338.htm?selectedLocale=en

Pernik, P. (2021). Cyber deterrence: A case study on Estonia's policies and practice (Hybrid CoE Paper 8, pp. 1–28). Hybrid CoE. https://www.hybridcoe.fi/wp-content/uploads/2021/10/20211012_Hybrid_CoE_Paper_8_Cyber_deterrence_WEB.pdf

Renda, K. K. (2022). The development of EU cybersecurity policy: From a coordinating actor to a cyber power? *Ankara Avrupa Çalışmaları Dergisi*, *21*(2), 467–495. https://dergipark.org.tr/en/download/article-file/2863171

Regulation (EU) 2016/679 of the European Parliament and of the Council 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. http://data.europa.eu/eli/reg/2016/679/oj

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). Official Journal of the European Union, L 151, 15–69. http://data.europa.eu/eli/reg/2019/881/oj

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 (Text with EEA relevance). Official Journal of the European Union, L 333, 1–79. http://data.europa.eu/eli/reg/2022/2554/oj

Regulation (EU) 2025/38 of the European Parliament and of the Council 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, OJ L, 2025/38. http://data.europa.eu/eli/reg/2025/38/oj

Rupp, C. (2024). *Navigating the EU cybersecurity policy ecosystem: A comprehensive overview of legislation, policies and actors.* Interface, Cybersecurity Policy and Resilience Programme.

Sciacca, G. (2020). *Cybersecurity in the EU: An introduction*. UNED's Jean Monnet Chair. https://blogs.uned.es/digitaleconomy/wp-content/uploads/sites/253/2022/01/Cybersecurity-in-the-EU-an-introduction.pdf

Spanou, D. (2021). Cybersecurity – the heart of the EU security strategy. In Strategic perspectives on cybersecurity management and public policies. *European Cybersecurity Journal*, *7*(1), 1–91. https://ik.org.pl/wp-content/uploads/2023/11/ECJ_vol7_issue1_final-1.pdf

Verhelst, A., & Wouters, J. (2020). Filling global governance gaps in cybersecurity: International and European legal perspectives. *International*

Organisations Research Journal, 1–26. https://doi.org/10.17323/1996-7845-2020-02-07

Vela, J. (2021). *The development of the EU Cyber Security Strategy and its importance* (pp. 1–3). Finabel, The European Land Force Commanders Organisation. https://finabel.org/info-flash-the-development-of-the-eu-cyber-security-strategy-and-its-importance/