The European Cybersecurity Framework: Challenges, Legal Aspects and Regulations

PhD. candidate **Leonidas SOTIROPOULOS**[1]

Abstract

This article analyzes the European Union's cybersecurity evolution, tackling the dual imperatives of fostering technological advancement and ensuring systemic resilience amid rising cyber risks. Centered on the question "How do EU legislative and institutional adaptations safeguard digital sovereignty, critical infrastructure, and cross-border coordination?", it employs dogmatic legal analysis to evaluate supranational laws (NIS 1/2, Cyber Resilience Act, DORA), institutional upgrades (ENISA, CERT-EU), and policy innovations. The paper's objectives are: Transitioning from fragmented policies to a unified "cyber shield"; balancing regulatory rigor with adaptive enforcement; identifying gaps in mitigating human-centric threats and cloud vulnerabilities. The article begins with cyberspace's conceptual foundations and EU regulatory milestones. Subsequent parts dissect ENISA's capacity-building initiatives, NIS 2's expanded sectoral coverage, and the Cyber Solidarity Act's crisis-response mechanisms. Case studies on ransomware and election interference highlight systemic vulnerabilities. The conclusion underscores integration (unified threat detection), innovation (AI defenses, quantum encryption), and inclusivity (global partnerships) as pillars for maintaining Europe's leadership in ethical digital governance. By prioritizing workforce development, AI-driven solutions, and transnational collaboration, the EU seeks to establish a global standard for a resilient cybersecurity framework

Keywords: *cyber-security, NIS 2, ENISA, cyber threats.*

JEL Classification: K24, K33

DOI: https://doi.org/10.62768/ADJURIS/2025/3/04

Please cite this article as:
Sotiropoulos, Leonidas, „The European Cybersecurity Framework: Challenges, Legal Aspects and Regulations", in Devetzis, Dimitrios, Dana Volosevici & Leonidas Sotiropoulos (eds.), *Digital Lawscapes: Artificial Intelligence, Cybersecurity and the New European Order*, ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, 2025, p. 57-71.

[1] Leonidas Sotiropoulos - European University of Cyprus, LL.M in Shipping Law (Cardiff University), LLB in Law (Aristotle University of Thessaloniki in Greece), ORCID: 0009-0004-1596-7887, leon.sotiropoulos@gmail.com.

1. Introduction

The rapid evolution of cyberspace—a concept rooted in mid-20th-century cybernetics and popularized by William Gibson's vision of a "consensual hallucination"[2] — has transformed from a theoretical abstraction into a cornerstone of modern societal infrastructure.[3] As defined in the EU's Cybersecurity Act (Regulation 2019/881)[4], this domain encompasses the interconnected networks enabling global communication, commerce, and governance, yet its borderless nature exposes systemic vulnerabilities to increasingly sophisticated threats. A cyber threat was identified as any potential circumstance, event, or action that could destroy, disrupt, or otherwise adversely affect network and information systems, their users, or other individuals. These definitions are also referenced in the NIS 2 Directive, which we will discuss in detail below. Against this backdrop, the European Union faces a critical juncture: balancing technological innovation with the imperative to protect digital sovereignty, secure critical infrastructure, and harmonize cross-border defenses.

Basically, the term cyberspace was defined many years ago as the amorphous, hypothetical "virtual" world created by connections between computers, internet-enabled devices, servers, routers, and other elements of the internet infrastructure. However, unlike the internet itself, cyberspace is the realm generated by these connections. It exists, according to some, beyond and without any specific nation-state. The word cyberspace is a combination of the prefix "cyber-" and the word "space."[5] The word "space" refers to a place or area and, in the context of cyberspace, denotes the virtual world within computer networks. This world is accessible through computers and other electronic devices and can be used for various purposes, such as communication, entertainment, commerce, and education. It is, therefore, an ever evolving and expanding domain, likely to play an increasingly significant role in our lives in the coming years.

The term cyberspace has existed for decades, dating back to the 1940s

[2] See analytically at Sabine Heuser (2003). "William Gibson's Construction of Cyberspace". In *Virtual Geographies*. Leiden, The Netherlands: Brill. https://doi.org/10.1163/9789004334373_005. Also, at Arulmurugan, S., and Jinnah, A.M.A., (2021). „The Cyberpunk Elements in William Gibson's Neuromancer". *Journal of Language and Linguistic Studies*, 17(3), 2558-2565.

[3] In the 1980s, novelist William Gibson combined the prefix with space in his novel "Neuromancer," creating the term as we know it today. Gibson defined cyberspace as "...a consensual hallucination experienced daily by billions of operators, in every nation... A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data."

[4] 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).

[5] The prefix "cyber-" originates from the Greek word "kybernetes," meaning governor or pilot, and implies foresight and control.

when MIT mathematician Norbert Wiener coined the term "cybernetics." Wiener borrowed the ancient Greek adjective "kybernetikos," meaning governing, piloting, or skilled at the helm, to describe the futuristic idea that one day we would have self-regulating computer systems operating solely through feedback. In his book "Cybernetics or Control and Communication in the Animal and the Machine"[6], the term was used to refer to the control of complex systems in the animal world and mechanical networks, particularly self-regulating control systems. Since then, cyberspace has been used by politicians, scholars, artists, and spies. It has been associated with concepts ranging from warfare to everyday online shopping, signifying both opportunities and threats.[7]

This article examines how the EU's legislative and institutional adaptations — spanning regulatory modernization, capacity-building mechanisms, and crisis-response frameworks — collectively address these challenges while navigating the tension between regulatory rigor and operational flexibility. Methodologically, the analysis employs a dogmatic legal framework to dissect supranational instruments such as the NIS 2 Directive, the Digital Operational Resilience Act (DORA), and the Cyber Resilience Act, while contextualizing their implementation through technical assessments of emerging threats (e.g., AI-enhanced ransomware) and geopolitical evaluations of cybersecurity as a tool for global leadership. Diverging from prior studies that compartmentalize technical, legal, or policy dimensions, this work adopts an integrative tripartite lens. First, it scrutinizes the technical realities of cloud vulnerabilities and hybrid warfare tactics, exemplified by the 2023 surge in state-sponsored election interference. Second, it evaluates the legal ramifications of expanded sectoral coverage under NIS 2, which now mandates cybersecurity protocols for entities ranging from energy grids to pharmaceutical manufacturers. Third, it analyzes the geopolitical implications of the EU's Cyber Solidarity Act, positioning cybersecurity as both a defensive mechanism and a vehicle for asserting normative influence in global digital governance.

The paper's originality lies in its systematic synthesis of three often-disconnected domains: legislative evolution, institutional interoperability, and threat actor innovation. By tracing the EU's transition from fragmented national policies to the envisioned "cyber shield" paradigm, it reveals how regulatory instruments like DORA's 24-hour incident reporting requirements coexist with adaptive governance structures such as AI-driven Security Operations Centres (SOCs). Concurrently, the article identifies persistent gaps, particularly in mitigating human-centric risks — evidenced by social engineering attacks compromising 68% of EU critical infrastructure breaches in 2024 — and supply chain

[6] Norbert Wiener, *Cybernetics or Control and Communication in the Animal and the Machine,* MIT Press, 1948.

[7] James Shires and Max Smeets (2017), *The Word Cyber Now Means Everything — and Nothing At All*, https://slate.com/technology/2017/12/the-word-cyber-has-lost-all-meaning.html#:~:text=In%20the%201980s%2C%20novelist%20William,and%20laymen%2C%20artists%20and%20spies

vulnerabilities exacerbated by third-party IoT device integration.[8]

Ultimately, this article contends that the EU's cybersecurity strategy hinges on three pillars: integration of threat intelligence across member states, innovation in quantum encryption and AI-driven anomaly detection, and inclusivity through partnerships with non-EU CERTs and Global South nations. By prioritizing workforce development programs to address the cybersecurity talent shortfall by 2026 and institutionalizing ethical AI governance frameworks, the EU aims to establish a global benchmark for resilient digital ecosystems.[9] These efforts not only safeguard Europe's critical infrastructure but also position the bloc as a normative architect in the contested arena of global cyber diplomacy.

2. The European Cyber-Legislative Evolution

2.1. The European Cybersecurity Framework: Historical Context

The history of cybersecurity in the European Union (EU) is characterised by a growing awareness of the importance of digital security, reflected in evolving regulations and continuous efforts towards collaboration and reciprocity among member states. Among the early (and highly significant) initiatives of the EU was the timely recognition of the need to target an adequate level of cybersecurity, with the first step being the establishment of the European Network and Information Security Agency (ENISA) in 2004. ENISA (renamed the European Union Agency for Cybersecurity in 2019) essentially took on the task of improving network and information security across the EU, providing guidance and recommendations for the development and oversight of infrastructures and systems, depending on their criticality to both the European economy and the protection of fundamental rights of Europeans.

The European Commission early on introduced regulatory interventions, largely formulated through supranational legal instruments, aiming to achieve a unified approach and implementation across member states. The Commission published the first European cybersecurity strategy in 2013, outlining a vision for a secure and resilient cyberspace and aiming to "make the EU's digital environment the safest in the world." This was followed by Directive 2013/40/EU on attacks against information systems. Subsequent strategies and frameworks, such as the EU's 2020 cybersecurity strategy, aimed to further strengthen the EU's stance in cyberspace.

[8] https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf, accessed on 10.05.2025.

[9] Lee A. Bygrave (2025), „The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes", *Computer Law & Security Review*, Volume 56, 106071, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2024.106071.

In 2016, the Network and Information Security (NIS) Directive[10] was issued, marking the first EU-wide legislation to establish principles and aim to ensure a common level of cybersecurity across critical sectors such as energy, transport, finance, and healthcare. Additionally, Regulation (EU) 2019/881[11] introduced cybersecurity certification schemes. Member states were required to transpose this Directive into their national legislation. On 15 September 2021, Ursula von der Leyen announced in her State of the Union address that Europe, where cyber defence tools are being developed,[12] needs a European Cyber Defence Policy,[13] including legislation on common standards based on a new European Cyber Resilience Act,[14] which addresses horizontal cybersecurity requirements for products with digital elements. "If everything is connected, everything can be hacked. Given that resources are scarce, we must pool our forces. And we must not only be satisfied with addressing the threat in cyberspace but also strive to become leaders in cybersecurity. It should be here in Europe where cyber defence tools are developed, which is why we need a European Cyber Defence Policy, including new legislation on common standards based on a new European Cyber Resilience Act."

Greece for instance, has already taken a series of significant initiatives in response to international and EU requirements, shaping a secure environment for new technologies and increasing the trust of citizens and businesses in digital applications and services for the benefit of the economy and society. The issuance of Ministerial Decision 1027/2019 (Government Gazette B' 3739) on the framework of obligations for Operators of Essential Services (OES) and Digital Service Providers (DSP) marked a critical step forward in creating the network of relationships between self-regulation and oversight, essential for ensuring an adequate level of cybersecurity in critical infrastructures and services. As highlighted in the latest edition of the National Cybersecurity Strategy, "*continuous adaptation, prevention, and timely response to the challenges of an ever-changing environment form the strongest foundation for the effective shaping of a comprehensive strategy to address cyberattacks [...] and make it necessary to immediately*

[10] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

[11] 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).

[12] Kasper, A., Mölder, H. (2020). „The EU's Common Security and Defence Policy in Facing New Security Challenges and Its Impact on Cyber Defence". In: Ramiro Troitiño, D., Kerikmäe, T., de la Guardia, R., Pérez Sánchez, G. (eds.) *The EU in the 21st Century*. Springer, Cham. https://doi.org/10.1007/978-3-030-38399-2_15.

[13] Bendiek, Annegret (2012): *European cyber security policy*, SWP Research Paper No. RP 13/2012, Stiftung Wissenschaft und Politik (SWP), Berlin, https://www.swp-berlin.org/publikation/european-cyber-security-policy, accessed on 10.05.2025.

[14] https://www.european-cyber-resilience-act.com/, accessed on 10.05.2025.

evaluate and provide feedback on the strategic planning for the country's cybersecurity."[15] Moreover, the issuance of the NIS 2 Directive, which will replace the NIS Directive (hereafter referred to as NIS 1 for distinction), and the imminent publication of the Greek implementation framework will evidently require a reassessment of the NIS 1 criteria as we move towards a much broader scope of application of its obligations, extending beyond the critical infrastructure operators covered by NIS 1.

2.2. ENISA: Institutional Backbone of EU Cybersecurity

The European Union Agency for Cybersecurity (ENISA)[16] actively contributes by providing expertise, guidelines, and recommendations to member states to strengthen their capabilities in the field of cybersecurity. The main ways to achieve its objectives include:

- **Collaboration and information sharing.**

- **Strengthening communities:** As ENISA emphasises, cybersecurity is a shared responsibility.[17] Europe aims to create a cross-sectoral framework for collaboration without exclusions. For this reason, ENISA has developed the **EU Cybersecurity Institutional Map** to identify and promote key stakeholders.

- **Cybersecurity policy:** According to ENISA, cybersecurity policy should not be limited to a specialised community of technical experts in cyberspace but should encompass a wide range of policy areas and initiatives.

- **Capacity building:** The demand for knowledge and skills in cybersecurity exceeds supply. The EU must invest in building capacities and talents in cybersecurity at all levels, from non-specialists to highly skilled professionals.

- **Trusted solutions:** In the process of evaluating the security of digital solutions and ensuring their reliability, a common approach must be adopted to balance the needs of society, the market, the economy, and cybersecurity. The establishment of a neutral entity acting transparently will increase customer trust in digital solutions and the broader digital environment.

- **Proactiveness:** Through a structured process enabling dialogue among stakeholders, decision-makers and policymakers will be able, on the one hand, to define strategies for timely mitigation, improving the EU's resilience to cybersecurity threats, and, on the other hand, to find solutions to emerging challenges.

- **Knowledge:** The driving force of cybersecurity is information and knowledge, necessitating a continuous process of collecting, organising, summarising, analysing, disseminating, and preserving information and knowledge about cybersecurity.

[15] See https://mindigital.gr/wp-content/uploads/2022/11/E%CE%9D-NATIONAL-CYBER-SECURITY-STRATEGY-2020_2025.pdf, accessed on 10.05.2025.

[16] https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_en, accessed on 10.05.2025.

[17] Definition of Cybersecurity Gaps and overlaps in standardization, v1.0 | December 2015.

The reality is that the complexity of risks associated with information and communication technologies (ICT) is constantly increasing, and the frequency of incidents in cyberspace is rising alongside their potentially significant negative impacts.[18] Moreover, due to the interconnectedness of critical sectors of the economy and state structures, ICT-related incidents may cause potential systemic effects. For this reason, managing the so-called ICT risk is of fundamental importance for an organisation to achieve its strategic, corporate, and operational objectives and safeguard its reputation. The general objectives of cybersecurity (should) include the following: availability, integrity (which may include authenticity and non-repudiation of data), and confidentiality.

Cybercrime includes all criminal offences committed using computers and communication networks. When the internet is used, it is referred to as cybercrime.[19] Cybercrime via the internet primarily targets data access, illegal data trafficking, financial exploitation, or extortion of the data controller and can take the form of a generalised cyberattack aimed at disabling or disrupting networks to weaken a market or demand ransom (ransomware).[20] However, cybersecurity does not primarily refer to cybercrime, which falls under the jurisdiction of the Cybercrime Prosecution, but rather to its broader form, which concerns critical state infrastructures, electronic communications, physical security of infrastructures, economic activity in critical market sectors, and, ultimately, the State itself.

2.3. Legislative Framework and Modernization - the Evolution of EU Cybersecurity Framework

The NIS Directive (NIS 1),[21] adopted in 2016, laid the foundation for a unified approach to cybersecurity across the European Union. It mandated Member States to develop national strategies for safeguarding critical network and information systems, established a Cooperation Group to facilitate cross-border collaboration, and created a network of Computer Security Incident Response

[18] See analytically, Ramjee Prasad, Vandana Rohokale (2020). *Cyber security: the lifeline of information and communication technology*. Cham, Switzerland: Springer International Publishing, p. 74.

[19] Dupont, B., Fortin, F., & Leukfeldt, R. (2024). „Broadening our understanding of cybercrime and its evolution." *Journal of Crime and Justice*, *47*(4), 435–439. https://doi.org/10.1080/0735648X.2024.2323872.

[20] See Andrew Jenkinson, (2022). *Ransomware and Cybercrime* (1st ed.). CRC Press. https://doi.org/10.1201/9781003278214. Also, Sarah Gordon & Richard Ford (2006), „On the definition and classification of cybercrime". *Journal in Computer Virology* 2, 13–20. https://doi.org/10. 1007/s11416-006-0015-z.

[21] Charlotte Ducuing, „Understanding the rule of prevalence in the NIS directive: C-ITS as a case study", *Computer Law & Security Review*, Volume 40, 2021, 105514, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2020.105514.

Teams (CSIRTs) to address cyber threats.[22] Crucially, it imposed security obligations on operators of essential services (e.g., energy, transport) and digital service providers, requiring them to adopt robust safeguards and report incidents promptly. While groundbreaking, NIS 1's limited sector coverage and fragmented enforcement highlighted the need for modernization in an era of escalating cyber risks.

In response, the NIS 2 Directive,[23] effective since January 2023, expands and strengthens this framework.[24] It broadens the scope to include 13 critical sectors — up from 11 under NIS 1 — such as public administration, space, and wastewater management. Digital service providers, including online marketplaces and cloud platforms, now face stricter compliance requirements. NIS 2 introduces enhanced risk management protocols, mandating organizations to conduct comprehensive cybersecurity assessments, implement mitigation measures like supply chain audits, and report incidents to National Cybersecurity Authorities (NCAs) within 24 hours. New obligations include cybersecurity training for employees, public awareness campaigns, and formal incident response plans. All Member States transposed NIS 2 into national law, replacing NIS 1 entirely.

The Digital Operational Resilience Act (DORA),[25] targeting the financial sector, mandates stringent ICT risk management for banks, insurers, and fintech firms. It requires regular stress testing, third-party vendor oversight, and real-time incident reporting to ensure operational continuity during cyberattacks.[26] Parallelly, the EU Cyber Resilience Act addresses vulnerabilities in connected devices (e.g., smart appliances, IoT systems).[27] Manufacturers must now embed cybersecurity features during product design, disclose vulnerabilities transparently, and

[22] See characteristically, Pauline Meyer & Sylvain Métille (2023), „Computer security incident response teams: are they legally regulated? The Swiss example". *International Cybersecurity Law Review* 4, 39–60. https://doi.org/10.1365/s43439-022-00070-x.

[23] Niels Vandezande, „Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor", *Computer Law & Security Review*, Volume 52, 2024,105890, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2023.105890.

[24] Paula Contreras (2023). „The Transnational Dimension of Cybersecurity: The NIS Directive and Its Jurisdictional Challenges". In: Cyril Onwubiko, Pierangelo Rosati, Aunshul Rege, Arnau Erola, Xavier Bellekens, Hanan Hindy, Martin Gilje Jaatun, *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media*. Springer Proceedings in Complexity. Springer, Singapore. https://doi.org/10.1007/978-981-19-6414-5_18.

[25] Neumannová, Anita, Edward W. N. Bernroider & Christoph Elshuber (2023). „The Digital Operational Resilience Act for Financial Services: A Comparative Gap Analysis and Literature Review". In: Maria Papadaki, Paulo Rupino da Cunha, Marinos Themistocleous, Klitos Christodoulou (eds.) Information Systems. EMCIS 2022. Lecture Notes in Business Information Processing, vol 464. Springer, Cham, pp. 327–341, https://doi.org/10.1007/978-3-031-30694-5_40.

[26] Dirk Clausmeier (2023), „Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA)". *International Cybersecurity Law Review* 4, 79–90. https://doi.org/10.1365/s43439-022-00076-5.

[27] See Pier Giorgio Chiara, „The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements." *International Cybersecurity Law Review* 3, 255–272 (2022). https://doi.org/10.1365/s43439-022-00067-6.

comply with EU-wide certification schemes before releasing goods to the market.

Regulation 2023/2841, effective since January 2024, establishes a Cybersecurity Governance Framework for EU institutions. It tasks the newly formed Cybersecurity Advisory Board (IICB) with overseeing compliance, while expanding the role of CERT-EU (the EU's central cyber incident response body) to coordinate threat intelligence sharing and crisis management. Together, these measures aim to harmonize standards, foster cross-border collaboration, and preempt emerging threats like AI-driven attacks or ransomware targeting critical infrastructure.

The EU's legislative push — spearheaded by NIS 2, DORA, and the Cyber Resilience Act — reflects a paradigm shift from reactive to proactive cybersecurity. By unifying reporting standards, broadening sectoral coverage, and institutionalizing cross-border cooperation, the bloc seeks to fortify its digital ecosystem against evolving threats. For businesses, this translates to heavier compliance burdens but also opportunities to build trust through demonstrable cyber resilience.

3. Operational Dynamics & Strategic Responses

3.1. Cybersecurity Challenges and Threat Landscape

Growing anxieties over the security of digital infrastructure and the vast quantities of data circulating across digital systems and subsystems have reached unprecedented levels, with trends indicating a persistent upward trajectory. The European Union's intensified focus on collaborative frameworks, legislative reforms, and the establishment of resilient cybersecurity architectures highlights its commitment to fortifying a secure digital environment for member states.

According to the European Union Agency for Cybersecurity (ENISA), cybersecurity challenges now threaten the foundational pillars of democratic Europe, extending beyond isolated sectors or organisations reliant on digital infrastructure. In its most recent analysis of evolving cyber threat trends, ENISA underscores a disturbing shift: cyberattacks increasingly target individuals in positions of influence, including employees in critical roles, politicians, government officials, journalists, and activists. Attackers predominantly deploy spear-phishing emails and exploit social media platforms to infiltrate systems. Notable tactics include[28]:

- Malicious advertising campaigns, where counterfeit websites masquerade as legitimate applications, enabling attackers to hijack system boot processes and bypass security protocols.

[28] Peter Swire, DeBrae Kennedy-Mayo, Drew Bagley, Sven Krasser, Avani Modak, and Christoph Bausewein. (2024). "Risks to Cybersecurity from Data Localization, Organized by Techniques, Tactics and Procedures." *Journal of Cyber Policy* 9 (1): 20–51. doi: 10.1080/23738871.2024.2384724.

- Exploitation of cloud infrastructure misconfigurations, a method that not only compromises cloud-based storage, networks, and systems but also extends to cloud management consoles, granting attackers broad control over operational environments.

In 2024 Cyber threats intensified globally, marked by a 35% surge in ransomware (40% targeting healthcare/education) and 25% more phishing campaigns, with AI-generated emails boosting success rates by 50%. Critical infrastructure (energy/transportation) faced 70% of incidents, while IoT device attacks rose 60% and AI-driven threats comprised 20% of advanced attacks. Data breaches cost averaged $4.5M (+15% YoY), with human error causing 30%. Sector-specific risks spiked: financial attacks (+50%, exploiting APIs) and healthcare breaches (+40%, targeting patient data). State-sponsored attacks grew 30%, focusing on espionage, with Europe hit by 25% of global incidents. These trends demand urgent AI-augmented defenses, infrastructure hardening, and international cooperation.[29]

Furthermore, the escalating frequency of cloud-based vulnerabilities[30] underscores systemic risks, as misconfigured environments offer attackers opportunities to disrupt operations or exfiltrate sensitive data. Elections, as a cornerstone of democratic processes, face heightened risks due to attacks on public administration and essential service providers. Meanwhile, the trend toward human-centric targeting — using psychologically manipulative tactics against high-profile individuals — reflects adversaries' growing sophistication in exploiting social dynamics.

Initiatives such as the NIS 2 Directive and the Cyber Resilience Act exemplify the bloc's efforts to address these challenges through harmonised security standards, stringent compliance mandates, and enhanced cross-border collaboration.[31] However, the rapidly evolving threat landscape demands continuous innovation in defensive technologies, investment in workforce training, and strengthened public-private partnerships to safeguard Europe's digital future.

3.2. Cyber-Strategic Initiatives and Institutional Coordination

The European Cybersecurity Competence Centre and Network (ECCC),[32] established under a 2021 Regulation, represents a cornerstone of the

[29] https://ciras.enisa.europa.eu/, accessed on 10.05.2025.

[30] FNU Jimmy, (2024). „Cyber security Vulnerabilities and Remediation Through Cloud Security Tools". *Journal of Artificial Intelligence General Science (JAIGS)* ISSN:3006-4023, 2(1), 129–171. https://doi.org/10.60087/jaigs.v2i1.102.

[31] Philipp Eckhardt & Anastasia Kotovskaia (2023), „The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive". *International Cybersecurity Law Review* 4, 147–164. https://doi.org/10.1365/s43439-023-00084-z.

[32] Sebastian Suciu & Andreea-Larisa Cirjan (2022). „The European Cybersecurity Competence Centre-One More Step towards Supranationalism". *Perspective Politice*, vol. XV, no. 1-2, pp. 57-73, DOI: 10.25019/perspol/22.15.4.

EU's strategy to bolster cybersecurity capabilities. Headquartered in Bucharest, the ECCC collaborates with National Coordination Centres (NCCs) across member states to drive innovation, industrial policy, and resilience. By pooling resources from the EU, member states, and private industry, the Centre focuses on developing shared technological priorities for critical sectors such as public administration, energy, and SMEs. Its mission extends beyond infrastructure protection to fostering cross-border collaboration among researchers, industry leaders, and public institutions, ensuring Europe maintains its competitive edge in cybersecurity technologies while safeguarding democratic institutions and economic stability.[33]

The Cyber Europe 2024 exercise, scheduled for June 2024, exemplifies the EU's proactive approach to crisis preparedness. As the 7th iteration of pan-European cybersecurity drills, it simulates a scenario involving geopolitical tensions at the EU's borders, including foreign state interference and coordinated attacks on energy infrastructure.[34] Secondary targets include digital service providers and public administration systems, reflecting growing concerns over hybrid threats to critical infrastructure. These exercises, building on lessons from Cyber Europe 2020, aim to refine incident response protocols and strengthen coordination among ENISA, national agencies, and private stakeholders.

The CERT-EU, now rebranded as the Cybersecurity Service for EU Institutions, has expanded its mandate to become a central hub for threat intelligence sharing and incident response. Its upgraded role includes providing advisory services to EU bodies, analyzing emerging threats, and coordinating cross-institutional responses to cyber incidents.[35] This evolution underscores the EU's commitment to protecting its own governance structures from increasingly sophisticated attacks, particularly those targeting sensitive political or operational data.[36]

[33] Aljosa Pasic (2022), „Governance Mesh Approach for Cybersecurity Ecosystem", *Information & Security: An International Journal,* vol. 53, no. 1: 105-130, https://doi.org/10.11610/isij.5308.

[34] Darlington Eze Ekechukwu, & Peter Simpa (2024). „The future of cybersecurity in renewable energy systems: A review, identifying challenges and proposing strategic solutions". *Computer Science & IT Research Journal*, *5*(6), 1265–1299.DOI: 10.51594/csitrj.v5i6.1197R. Also see Rauno Pirinen, Paresh Rathod, Emilia Gugliandolo, Kevin Fleming, Nineta Polemi, "Towards the Harmonisation of Cybersecurity Education and Training in the European Union Through Innovation Projects," *2024 IEEE Global Engineering Education Conference (EDUCON)*, Kos Island, Greece, 2024, pp. 1-9, doi: 10.1109/EDUCON60312.2024.10578867.

[35] Pythagoras Petratos, (2014). „Cybersecurity in Europe: Cooperation and Investment." In: Elias G. Carayannis, David F. J. Campbell, Marios Panagiotis Efthymiopoulos, (eds.), *Cyber-Development, Cyber-Democracy and Cyber-Defense.* Springer, New York, p. 279-301, https://doi.org/10.1007/978-1-4939-1028-1_11.

[36] Christian Calliess, Ansgar Baumgarten (2020). „Cybersecurity in the EU the example of the financial sector: a legal perspective". *German Law Journal*, 21(6), 1149-1179. Also see Odermatt, J. (2018). „The European Union as a Cybersecurity Actor". In: Blockmans, S. & Koutrakos, P. (Eds.), *Research Handbook on EU Common Foreign and Security Policy.* (pp. 354-373). Cheltenham, UK: Edward Elgar Publishing. ISBN 9781785364075 doi: 10.4337/9781785364082.00026.

The EU Cyber Solidarity Act (2023), proposed in April 2023, introduces a multi-layered framework to enhance collective resilience. Central to this initiative is the European Cybersecurity Shield, a network of interconnected Security Operations Centres (SOCs) leveraging AI and data analytics to detect threats in real time.[37] Funded through the Digital Europe Programme, these SOCs — including three cross-border consortia involving 17 member states and Iceland — form a distributed early-warning system. Complementing this infrastructure is a **Cybersecurity Reserve**, a pool of pre-vetted private response teams available to assist member states during large-scale incidents, and a **Mutual Assistance Framework** enabling states to request or provide cross-border support during crises.

Strategic priorities under these initiatives focus on achieving **technological sovereignty** by reducing reliance on non-EU cybersecurity solutions, fostering homegrown innovation through public-private partnerships, and addressing hybrid threats through stress-testing critical sectors like finance and healthcare. By aligning the ECCC's research capabilities, CERT-EU's operational expertise, and the Cyber Solidarity Act's response mechanisms, the EU aims to create a unified "cyber shield"[38] capable of anticipating disruptions, mitigating attacks, and ensuring rapid recovery — a vital component of its broader digital single market and geopolitical resilience agenda.[39]

4. Conclusion

The European Union's cybersecurity framework has transitioned from fragmented national policies to a cohesive, forward-looking strategy marked by legislative milestones like the NIS 2 Directive, DORA, and the Cyber Resilience Act, which prioritize harmonized regulations, cross-border collaboration, and technological sovereignty. Central to this evolution are institutional advancements such as the European Cybersecurity Competence Centre (ECCC) and the Cyber Solidarity Act, which pool resources and expertise to counter state-sponsored threats and critical infrastructure vulnerabilities. Despite progress, challenges persist, including AI-driven ransomware, supply chain exploits, and workforce shortages, compounded by the need for consistent implementation of directives across member states. Looking ahead, the EU aims to integrate initiatives like the Cybersecurity Shield and DORA for seamless threat response, innovate

[37] Pier Giorgio Chiara and Laura Bartoli, *Unveiling EU Cybersecurity Law Turf Battles: The Case of the EU Cyber Solidarity Act Proposal*. Available at SSRN: https://ssrn.com/abstract =4719533 or http://dx.doi.org/10.2139/ssrn.4719533.

[38] Anna-Maria Osula (2022). „Building Cyber Resilience: The Defensive Shield for the EU". In: Gertjan Boulet, Michael Reiterer, Ramon Pacheco Pardo (eds.) *Cybersecurity Policy in the EU and South Korea from Consultation to Action. New Security Challenges*. Palgrave Macmillan, Cham. pp. 179–196, https://doi.org/10. 1007/978-3-031-08384-6_9.

[39] Izabela Oleksiewicz, Mustafa Emre Civelek, (2023). „Where are the changes in EU cybersecurity legislation leading?". *Humanities and Social Sciences*, *30*(4-part 1), 183-197.

through AI-driven defenses and quantum-resistant encryption, and strengthen global partnerships to combat transnational cybercrime. By embedding cybersecurity into digital transformation agendas and balancing regulatory rigor with adaptive governance, the bloc seeks to set a global standard for resilient, ethical digital ecosystems capable of mitigating 21st-century threats.

Bibliography

1. Arulmurugan, S. and A.M.A. Jinnah (2021). „The Cyberpunk Elements in William Gibson's Neuromancer". *Journal of Language and Linguistic Studies*, 17(3), 2558-2565.
2. Bendiek, Annegret (2012): *European cyber security policy*, SWP Research Paper No. RP 13/2012, Stiftung Wissenschaft und Politik (SWP), Berlin, https://www.swp-berlin.org/publikation/european-cyber-security-policy, accessed on 10.05.2025.
3. Bygrave, Lee A. (2025), „The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes", *Computer Law & Security Review*, Volume 56, 106071, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2024.1060 71.
4. Calliess, Christian & Ansgar Baumgarten (2020). „Cybersecurity in the EU the example of the financial sector: a legal perspective". *German Law Journal*, 21 (6), 1149-1179.
5. Chiara, Pier Giorgio & Laura Bartoli, *Unveiling EU Cybersecurity Law Turf Battles: The Case of the EU Cyber Solidarity Act Proposal*. Available at SSRN: https://ssrn.com/abstract=4719533 or http://dx.doi.org/10.2139/ssrn.47 19533.
6. Chiara, Pier Giorgio, „The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements." *International Cybersecurity Law Review* 3, 255–272 (2022). https://doi.org/10.1365/s43439-022-00067-6.
7. Clausmeier, Dirk (2023), „Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA)". *International Cybersecurity Law Review* 4, 79–90. https://doi.org/10.1365/s43439-02 2-00076-5.
8. Contreras, Paula (2023). „The Transnational Dimension of Cybersecurity: The NIS Directive and Its Jurisdictional Challenges". In: Onwubiko, Cyril, Pierangelo Rosati, Aunshul Rege, Arnau Erola, Xavier Bellekens, Hanan Hindy & Martin Gilje Jaatun, *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media*. Springer Proceedings in Complexity. Springer, Singapore. https://doi.org/10.1007/978-981-19-6414-5_ 18.
9. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.
10. Ducuing, Charlotte, „Understanding the rule of prevalence in the NIS directive: C-ITS as a case study", *Computer Law & Security Review*, Volume 40, 2021, 105514, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2020.1055 14.

11. Dupont, Benoît, Francis Fortin & Rutger Leukfeldt (2024). „Broadening our understanding of cybercrime and its evolution." *Journal of Crime and Justice*, 47(4), 435–439. https://doi.org/10.1080/0735648X.2024.2323872.
12. Eckhardt, Philipp & Anastasia Kotovskaia (2023), „The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive". *International Cybersecurity Law Review* 4, 147–164. https://doi.org/10.1365/s43439-023-00084-z.
13. Ekechukwu, Darlington Eze & Peter Simpa (2024). „The future of cybersecurity in renewable energy systems: A review, identifying challenges and proposing strategic solutions". *Computer Science & IT Research Journal*, *5*(6), 1265–1299. DOI: 10.51594/csitrj.v5i6.1197R.
14. Gordon, Sarah & Richard Ford (2006), „On the definition and classification of cybercrime". *Journal in Computer Virology* 2, 13–20. https://doi.org/10.1007/s11416-006-0015-z.
15. Heuser, Sabine (2003). "William Gibson's Construction of Cyberspace". In *Virtual Geographies*. Leiden, The Netherlands: Brill. https://doi.org/10.1163/9789004334373_ 005.
16. Jenkinson, Andrew (2022). *Ransomware and Cybercrime* (1st ed.). CRC Press. https://doi.org/10.1201/9781003278214.
17. Jimmy, FNU (2024). „Cyber security Vulnerabilities and Remediation Through Cloud Security Tools". *Journal of Artificial Intelligence General Science (JAIGS)* ISSN:3006-4023, 2(1), 129–171. https://doi.org/10.60087/jaigs.v2i1.102.
18. Kasper, A., H. Mölder (2020). „The EU's Common Security and Defence Policy in Facing New Security Challenges and Its Impact on Cyber Defence". In: Ramiro Troitiño, D., Kerikmäe, T., de la Guardia, R., Pérez Sánchez, G. (eds.) *The EU in the 21st Century*. Springer, Cham. https://doi.org/10.1007/97 8-3-030-38399-2_15.
19. Meyer, Pauline & Sylvain Métille (2023), „Computer security incident response teams: are they legally regulated? The Swiss example". *International Cybersecurity Law Review* 4, 39–60. https://doi.org/10.1365/s43439-022-000 70-x.
20. Neumannová, Anita, Edward W. N. Bernroider & Christoph Elshuber (2023). „The Digital Operational Resilience Act for Financial Services: A Comparative Gap Analysis and Literature Review". In: Maria Papadaki, Paulo Rupino da Cunha, Marinos Themistocleous, Klitos Christodoulou (eds.) *Information Systems.* EMCIS 2022. Lecture Notes in Business Information Processing, vol 464. Springer, Cham, pp. 327–341, https://doi.org/10.1007/97 8-3-031-30694-5_40.
21. Odermatt, J. (2018). „The European Union as a Cybersecurity Actor". In: Blockmans, S. & Koutrakos, P. (Eds.), *Research Handbook on EU Common Foreign and Security Policy.* (pp. 354-373). Cheltenham, UK: Edward Elgar Publishing. ISBN 9781785364075 doi: 10.4337/9781785364082.00026.
22. Oleksiewicz, Izabela & Mustafa Emre Civelek, (2023). „Where are the changes in EU cybersecurity legislation leading?". *Humanities and Social Sciences*, *30*(4-part 1), 183-197.
23. Osula, Anna-Maria (2022). „Building Cyber Resilience: The Defensive Shield for the EU". In: Gertjan Boulet, Michael Reiterer, Ramon Pacheco Pardo (eds.) *Cybersecurity Policy in the EU and South Korea from Consultation to Action. New Security Challenges.* Palgrave Macmillan, Cham. pp. 179–196, https://doi.

org/10. 1007/978-3-031-08384-6_9.

24. Pasic, Aljosa (2022), „Governance Mesh Approach for Cybersecurity Ecosystem”, *Information & Security: An International Journal,* vol. 53, no. 1: 105-130, https://doi.org/10.11610/isij.5308.
25. Petratos, Pythagoras (2014). „Cybersecurity in Europe: Cooperation and Investment.” In: Carayannis, Elias G., David F. J. Campbell, Marios Panagiotis Efthymiopoulos, (eds.), *Cyber-Development, Cyber-Democracy and Cyber-Defense.* Springer, New York, p. 279-301, https://doi.org/10.1007/978-1-4939-10 28-1_11.
26. Pirinen, Rauno, Paresh Rathod, Emilia Gugliandolo, Kevin Fleming & Nineta Polemi, "Towards the Harmonisation of Cybersecurity Education and Training in the European Union Through Innovation Projects," *2024 IEEE Global Engineering Education Conference (EDUCON)*, Kos Island, Greece, 2024, pp. 1-9, doi: 10.1109/EDUCON60312.2024.10578867.
27. Prasad, Ramjee & Vandana Rohokale (2020). *Cyber security: the lifeline of information and communication technology*. Cham, Switzerland: Springer International Publishing.
28. 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).
29. Shires, James and Max Smeets (2017), *The Word Cyber Now Means Everything — and Nothing At All*, https://slate.com/technology/2017/12/the-word-cyber-has-lost-all-meaning.html#:~:text=In%20the%201980s%2C%20novelist%20 William,and%20laymen%2C%20artists%20and%20spies.
30. Suciu, Sebastian & Andreea-Larisa Cirjan (2022). „The European Cybersecurity Competence Centre-One More Step towards Supranationalism”. *Perspective Politice*, vol. XV, no. 1-2, pp. 57-73, DOI: 10.25019/perspol/22.15.4.
31. Swire, Peter, DeBrae Kennedy-Mayo, Drew Bagley, Sven Krasser, Avani Modak and Christoph Bausewein. (2024). “Risks to Cybersecurity from Data Localization, Organized by Techniques, Tactics and Procedures.” *Journal of Cyber Policy* 9 (1): 20–51. doi: 10.1080/2373 8871.2024.2384724.
32. Vandezande, Niels, „Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor”, *Computer Law & Security Review*, Volume 52, 2024,105890, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2023.105890.
33. Wiener, Norbert, *Cybernetics or Control and Communication in the Animal and the Machine,* MIT Press, 1948.