The Cybersecurity Capability Gap

1 JUNE 2025

Denisa Cepoiu

Introduction

The European Union (EU) is becoming increasingly exposed to cybersecurity threats that target both its civilian infrastructure and military security regimes. Cybersecurity refers to the protection of information networks, key infrastructures, and digital assets from malicious activity that disrupts social and government functioning. Rising geopolitical tensions have increased the frequency of malicious activity, which can range from ransomware assaults on healthcare systems to coordinated cyber operations against key infrastructure (Dekker et al., 2025). Recognising the changing threat landscape, the EU has implemented extensive regulatory measures such as the NIS2 Directive, the Cyber Resilience Act, and the Strategic Compass to improve cyber resilience and collective defence (European Commission, 2022). However, major competence gaps remain between these strategic goals and their operational implementation. While the EU has succeeded at developing legal and normative frameworks, it faces challenges in translating these frameworks into operational capabilities, particularly in terms of speed, interoperability, and deterrence (Carrapico & Barrinha, 2017; Sliwinski, 2014).

This review essay evaluates scholarly and policy perspectives to examine these capability gaps. The essay will first present the governance structures responsible for the EU's cyber-related regulations; then it will dive into concrete cyber capability gaps, both in terms of the civilian aspect and the military aspect; finally, the essay will offer a brief comparative perspective to major players in the cyber stage—NATO, Russia, and China. The essay observes recurring themes of institutional fragmentation, competing national interests, skill shortages, and the EU's normative preference for regulation over aggressive action. By employing ideas from both academic and policy sources, this essay aims to show that unless these weaknesses are addressed systematically, the EU risks remaining strategically vulnerable in an increasingly contested digital space.

Conceptual Framework

A thorough assessment of the EU's cyber capabilities gaps requires a solid understanding of core cybersecurity concepts and the theoretical foundations that underpin this discussion. Cybersecurity broadly refers to the safeguarding of information systems, networks, and digital data against harmful threats such as illegal access, destruction, and disruption. Cyber defence expands on this notion by emphasising both passive security measures and active defensive operations aimed at countering cyber threats before or during a cyber assault (Ducaru et al., 2024). Cyber resilience refers to a system's or society's ability to maintain vital functions and recover quickly after a cyber incident (Dekker et al., 2024). Finally, offensive cyber capabilities refer to acts aimed at disrupting, degrading, or destroying an adversary's information systems, either proactively or reactively. In contrast to cybersecurity and cyber defence, which are primarily reactive, offensive cyber operations are proactive.

The European Union's self-perception as a "civilian power" has a significant impact on its cybersecurity strategy. The EU had placed great value on regulatory frameworks, diplomatic commitment, and the promotion of international norms over military solutions, even in security sectors (Carrapico & Barrinha, 2017). However, scholars such as Sliwinski (2014) argue that the EU's liberal intergovernmental framework, which stresses member states' sovereignty, provides barriers to further integration in defence-related cyber activity. Hence, the looming threat of cyberattacks, which are frequently orchestrated by states such as Russia or China, calls into question the efficacy of a solely regulatory strategy.

The Governance of the EU's Cyber Capabilities

Institutional fragmentation significantly weakens the European Union's cybersecurity governance. This concept refers to the distribution of responsibilities, mandates, and competencies across several EU entities and member states in the absence of adequate centralised oversight. The European Union Agency for Cybersecurity (ENISA), the Cybersecurity Service for the Union (CERT-EU), Europol, and national Computer Security Incident Response Teams (CSIRTs) all play roles in cybersecurity, but their tasks overlap, and their performance varies (Dekker et al., 2025; European Commission, 2022). For example, ENISA concentrates on advisory and normative tasks such as developing standards and conducting risk assessments, but it lacks the operational capabilities required for incident management and cyber defence. Meanwhile, CERT-EU's role is limited to protecting EU institutions rather than coordinating member states responses.

Furthermore, member states frequently prioritise national interests over collective EU action, particularly in sensitive areas like cyber intelligence and military operations (Iancu, 2024). This tendency intensifies the fragmentation at the governance level, challenging coordinated attribution of

cyberattacks and collective response actions. Thus, institutional fragmentation not only impairs the EU's cyber defence but also undermines trust among member states, creating a systemic vulnerability that adversaries might exploit. To strengthen governance, voluntary coordination must be replaced by binding commitments to share threat information, conduct joint exercises, and respond collectively.

Concrete Gaps in Cybersecurity Capabilities

Civilian cybersecurity capabilities in the EU demonstrate certain weaknesses, which expose vital infrastructure and services to systemic cyber risk. Capability gaps are inadequacies in basic cyber hygiene, incident response readiness, vulnerability management, and technical resilience across multiple sectors. ENISA's NIS360 Report (2025) depicts critical weaknesses in healthcare, transportation, energy, banking, and information and communications technology (ICT) sectors, where security maturity is still imbalanced. For example, the healthcare industry's reliance on old systems and insufficient incident response planning has made it a regular target of ransomware attacks, with potentially fatal implications.

The Cyber Resilience Act and NIS2 Directive seek to address these weaknesses by establishing baseline cybersecurity standards, breach reporting requirements, and supply chain risk assessments (European Commission, 2022). However, Kamara (2024) criticises these legislative measures for placing disproportionate compliance obligations on small and medium-sized businesses, which frequently lack the means to achieve high cybersecurity standards. Small and medium-sized enterprises make up a considerable percentage of Europe's digital economy, and their cyber vulnerability ripples throughout bigger supply chains.

Furthermore, Hernández (2024) emphasises that the EU's digital sovereignty remains fragile because of its reliance on non-European vendors for essential technologies such as cloud computing, semiconductors, and telecommunications. This dependence creates strategic weaknesses that regulatory measures alone cannot address. The European Commission (2025) underlines that establishing operational resilience necessitates not just stronger laws but also significant investment in indigenous technical capabilities, public-private collaborations, and cross-sector threat intelligence sharing.

Sector-specific capability gaps are especially worrying, given the increasing sophistication of adversarial strategies. Advanced Persistent Threats (APTs) that target financial systems, healthcare networks, and energy grids are specifically designed to take advantage of these gaps in readiness (Mueller et al., 2023). As long as sectors are fragmented in their preparation for cyber incidents, the EU's overall civilian resilience will be insufficient to resist or mitigate catastrophic cyberattacks. Bridging civilian capability gaps calls for a holistic approach that includes legislative coordination, targeted

investments, personalised support for small and medium-sized enterprises, and constant threat monitoring and adaptation.

Visualisation 1

An additional impediment to fulfilling the European Union's cyber resilience goals is the shortage of cybersecurity personnel. Workforce shortages are best defined as the difference between the demand for competent and specialised cybersecurity-schooled experts and the restricted supply available within member states and EU institutions. According to Catal and co-authors (2022), over 300,000 cybersecurity posts remain unfilled across Europe, exposing serious risks in public administrations, vital infrastructure sectors, and commerce. Almeida (2025) further emphasises that present educational programs frequently fail to meet industry needs, focusing on theory rather than real, applicable skills.

Additionally, Hernández (2024) contends that varied certification standards across member states hinder cross-border labour mobility, making it harder to deploy competent experts quickly. The Cyber Solidarity Act calls for improvements in cross-border cyber training and cooperative exercises, but implementation is still in its early stages (Dewi & Nugrahani, 2024). This mismatch between policy ambition and workforce preparation jeopardises the EU's capacity to implement cyber-related frameworks like the NIS2 Directive or the Cyber Resilience Act.

Given the lack of investment in cybersecurity education, certification systems, and cross-sector professional development programs, the EU's regulatory cyber frameworks remain underutilised. As a result, the shortage in cyber experts is not only an operational issue but also a weakness that could be exploited by malicious actors to undermine European cybersecurity.

Regarding the cyber side of the EU, its cyber capabilities are still fragmented, underdeveloped, and mostly defensive, limiting the EU's ability to strike effectively in cyberspace. Military cyber capabilities include the structures, doctrines, and resources required to secure military assets, project force, and support missions via digital means. The 2022 EU Cyber Defence Policy calls for "full-spectrum capabilities," but it leaves offensive operations and strategic cyber deterrence largely up to individual member states (European Commission, 2022).

Mueller and co-authors (2023) show that during the Russia-Ukraine war, effective cyber operations required strong integration of military, information, and digital warfare domains—a paradigm the EU has yet to replicate. According to Katagiri (2024), inside the EU, the political sensitivity surrounding cyberspace militarisation has stalled efforts to build unified offensive guidelines, cooperative exercises, or centralised cyber commands.

Furthermore, Hernández (2024) critiques the lack of designated cyber units in several European armed services, claiming that ad hoc cyber defensive measures are insufficient to face persistent, well-coordinated adversary

attacks. Without the establishment of structured, interoperable military cyber units capable of supporting CSDP missions and NATO operations, the EU's aspiration to be a credible digital security provider will remain unfulfilled. Military cyber deficiencies significantly impair the EU's ability to project force or defend its strategic autonomy.

Developing offensive cyber capabilities poses additional significant strategic, legal, and normative difficulties to the EU. Offensive cyber operations involve pre-emptively or reactively disrupting or destroying hostile information systems. Despite offensive cyber capabilities being increasingly regarded as crucial to credible deterrence measures, the EU has historically avoided using such tools because of legal limits and political considerations (Ducaru et al., 2024).

Taillat (2024) suggests that conceptual difficulties about what constitutes a "cyberattack" versus "cyberwarfare" make it difficult to define red lines and proportional responses within the EU framework. The Tallinn Manual and NATO's cyber defence policies provide some direction, but the EU has not formally established comparable doctrines (Ducaru et al., 2024). Furthermore, Miadzvetskaya (2024) observes that while the EU has implemented cyber sanctions regimes, it lacks the practical tools to undertake direct action against its possible adversaries in cyberspace. Without a clear offensive posture, the EU risks remaining a "soft target" for ongoing low-intensity cyber operations that erode strategic stability. Thus, resolving offensive cyber capability deficiencies is more than just a technological challenge; it is also a matter of the EU's determination to redefine its identity as a civilian power in a disputed digital space.

Visualisation 2

A Comparative Analysis: EU vs. NATO, China, and Russia

When comparing the EU to other prominent players within cyberspace, some strategic vulnerabilities in both civilian and military cybersecurity stand out. For instance, NATO has designated cyberspace as an operational domain and established a dedicated Cyber Operations Centre to coordinate member reactions to major cyber crises (Ducaru et al., 2024). NATO also has collective defence mechanisms in place, such as Article 5, which can theoretically be implemented in the event of a serious cyberattack. In contrast, the EU's cybersecurity architecture continues to be a mix of sectoral legislation and non-binding frameworks, making it difficult to ensure timely and coordinated responses across member states.

Meanwhile, China has established a cyber sovereignty strategy that combines digital monitoring, civil-military cooperation, and the development of indigenous technology to maintain state control over its digital infrastructure (Sliwinski, 2014). Hernández (2024) underlines that China's strategy allows for integrated offensive and defensive operations, establishing it as a considerable actor in the cyber stage. Similarly, Russia has exhibited strong

skills in hybrid cyber operations, particularly during its war against Ukraine, wherein cyberattacks support traditional military activities (Mueller et al., 2023). On the other hand, the EU's commitment to multilateral principles, privacy, and market openness is becoming an obstacle to the establishment of a coordinated and effective cyber policy. According to Bendiek and Bund (2024), while the EU excels at regulation, it falls short of its competitors in terms of quick coordination and deterrence. Without better integration of civilian and military cyber capabilities and a stronger doctrinal commitment to active defence, the EU risks falling further behind.

So, when taking a comparative look at the EU and its main competitors in cyberspace, it becomes apparent that the EU needs to move beyond its existing regulatory framework and toward more unified and operationally capable cybersecurity governance.

Diverging Perspectives in Literature and Policy

There is a significant difference between academic literature and EU policy directives on the bloc's cybersecurity trajectory. On the one hand, academics argue that the EU should continue to support international cyber rules, diplomacy, and capacity-building rather than creating military cyber capabilities that could jeopardize its identity as a civilian-centric union (Carrapico & Barrinha, 2017; Taillat, 2024). Hence, scholars advocate for strengthening the EU's normative impact by promoting cyber-peace efforts, investing in digital rights protections, and encouraging multistakeholder governance. On the other hand, without an effective cyber deterrence, the EU could remain vulnerable to asymmetric cyber threats which fall short of conventional warfare. According to Ducaru and co-authors (2024), cyber deterrence involves not just legal instruments but also the practical capacity to impose sanctions on enemies. However, such tactics remain politically controversial in the EU because member states have different legal and ethical limits when it comes to cyber operations (Backman, 2022).

Furthermore, scholars such as Bygrave (2024) consider that the fragmentation of EU cybersecurity law, which includes several rules, directives, and national transpositions, generates compliance issues and undermines bloc-wide policy coherence. Miadzvetskaya (2024) expresses concern about the efficacy of EU cyber sanctions due to the lack of direct enforcement tools. These opposing viewpoints reflect a deeper strategic concern inside the EU: whether to maintain its civilian-centric identity or adapt to an evolving geopolitical landscape that has moved within the realm of cyber. Resolving this contradiction is important to the EU's strategic coherence and relevance in the digital age.

Conclusion

The EU's cybersecurity infrastructure has ongoing flaws that limit its efficacy as both a civilian and military cyber actor. Fragmented governance

structures, undeveloped offensive capabilities, sectoral vulnerabilities, and labour shortages all contribute to a security posture that is more aspirational than practical. Despite policy improvements when it comes to frameworks such as the Cyber Resilience Act, NIS2 Directive, and Cyber Solidarity Act, implementation is inconsistent; important functions like collective cyber defence and quick threat response lack institutional backing. Thus, to address these capability gaps, the EU must balance its intrinsic moral obligations with the strategic considerations raised by an increasingly aggressive cyberspace. By complementing the strength of its policy frameworks with practical skills, the EU can strengthen its resilience, protect digital sovereignty, and establish itself as a credible cybersecurity actor on a global scale.

Bibliography:

Almeida, F. (2025). Comparative analysis of EU-based cybersecurity skills frameworks. Computers & Security, 151(104329). https://doi.org/10.1016/j.cose.2025.104329

Backman, S. (2022). Risk vs. threat-based cybersecurity: the case of the EU. European Security, 32(1), 85–103. https://doi.org/10.1080/09662839.2022.2069464

Bendiek, A., & Bund, J. (2024). Hardening norms and networks: Europe's cyber defence posture. Intereconomics, 59(4), 198–203. https://doi.org/10.2478/ie-2024-0041%0A

Bygrave, L. A. (2024). The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes. Computer Law & Security Review, 56(106071). 1–8. https://doi.org/10.1016/j.clsr.2024.106071

Catal, C., Ozcan, A., Donmez, E., & Kasif, A. (2022). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. Education and Information Technologies, 28(2), 1809–1831. https://doi.org/10.1007/s10639-022-11261-8

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

Dekker, M., Skritaite, J., Philippou, E., Naydenov, R., & ENISA. (2025). ENISA NIS360 2024: ENISA cybersecurity maturity & criticality.

Dewi, A.S., & Nugrahani, H.S.D. (2024). Strengthening EU cyber resilience: A critical analysis of the Cyber Solidarity Act's legislative framework. Islamic World and Politics, 8(2). 182–195. https://doi.org/10.18196/jiwp.v8i2.115

Ducaru, S. D., Caradaică, M., & Costea, A.-M. (2024). Can a cyberattack become an act of war? European and trans-atlantic perspectives. Romanian Journal of European Affairs, 24(1), 21–45. https://doaj.org/article/3a91c691e51d438299c0c9f4ff4bf338

European Commission. (2022). Joint communication to the European Parliament and the Council: EU Policy and Cyber Defense. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022JC0049

European Commission. (2025). Joint White Paper for European Defence Readiness 2030. https://defence-industry-space.ec.europa.eu/document/download/30b50d2c-49aa-4250-9ca6-27a0347cf009_en?filename=White%20Paper.pdf

Iancu, N. (2024). A national security perspective on strengthening e.u. civilian-defence cybersecurity synergy: A systemic approach. In Proceedings of the International Conference on Cybersecurity and Cybercrime (pp. 22-34). https://www.ceeol.com/search/chapter-detail?id=1282657

Kamara, I. (2024). European cybersecurity standardisation: a tale of two solitudes in view of Europe's cyber resilience. Innovation the European Journal of Social Science Research, 37(5), 1441–1460. https://doi.org/10.1080/13511610.2024.2349626

Katagiri, N. (2025). The rise of offensive cyber and reality of European digital policy. European Politics and Society, 1–18. https://doi.org/10.1080/23745118.2025.2483813

Miadzvetskaya, Y. (2024). EU sanctions in response to cyber-attacks as crime-based emergency measures. Computer Law & Security Review, 54(106010). 1–11. https://doi.org/10.1016/j.clsr.2024.106010

Hernández, E. O. (2024). Towards the autonomous defence capabilities of the European Union: Upgrading cyber defence policy. Global Policy, 15(Suppl. 8). 57–62. https://doi.org/10.1111/1758-5899.13412

Mueller, G. B., Jensen, B., Valeriano, B., Maness, R. C., & Macias, J. M. (2023). Cyber Operations during the Russo-Ukrainian War. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war

Sliwinski, K. F. (2014). Moving beyond the European Union's Weakness as a Cyber-Security Agent. Contemporary Security Policy, 35(3), 468–486. https://doi.org/10.1080/13523260.2014.959261

Taillat, S. (2024). Conceptualizing cyberwarfare. In T. Stevens & J. Devanny (Eds.), Research Handbook on Cyberwarfare (pp. 34–51). Edward Elgar Publishing Limited. https://doi.org/10.4337/9781803924854.00009

DOI 10.69790/epis-rep-spd/98364

EPIS