Deloitte. | EUPC

CYBER DEFENCE IN EUROPE

Building Resilience through Innovation in Uncertain Times

May 2025

Table of Contents

Table of Figures

Table of Tables

1. EXECUTIVE SUMMARY

Boost EU cyber defence with targeted innovation projects

In an increasingly fragmented international arena, defence has reemerged as a critical component of both international and national discourses. The President of the European Commission, Ursula von der Leyen, unveiled on March 4, 2025, the EU's "**ReArm Europe Plan**." This defence package aims to mobilize nearly **EUR 800 billion** to kick off "an era of rearmament" for Europe and augment its defence expenditures.[1]

In light of the latest technological advancements and the growing relevance of the "fifth domain"[2] – namely, cyberspace – it is imperative to not only respond to evolving tactics and techniques of malicious actors but also to strategically direct innovation efforts towards the development of long-term EU cyber defence capabilities and the enhancement of European strategic autonomy.

Therefore, this paper investigates the potential benefits of innovation for cyber defence and the importance of robust governance mechanisms to drive these initiatives. In particular, we highlight best practices from the EU and its Member States while identifying potential gaps, redundancies, and inefficiencies across the following four analytical perspectives: technology, policy, governance, and capabilities.

Key Takeaways

➢ A TECHNOLOGY PERSPECTIVE

Technological advancements are crucial for developing robust cyber defence capabilities, with **dual-use technologies** offering significant potential for innovation to give the EU a strategic advantage. The reduction of barriers between civil and military sectors will promote the adoption of dual-use technologies, help foster R&D, and ultimately strengthen the EU's industrial base.

➢ A POLICY PERSPECTIVE

In the absence of a unified and coordinated strategy, current efforts focus on harmonising and simplifying the EU legislative landscape shaped throughout the previous mandates of the European Commission[3]. In this regard, the current **European Commission's goals** and the **Competitiveness Compass** are examined in depth.

➢ A GOVERNANCE PERSPECTIVE

Strong mandates beget effective governance mechanisms and policy instruments that translate policy guidelines into actionable results. That is why cooperation among key EU stakeholders and robust **funding mechanisms** are vital for the success of cyber defence programs. In addition, EU-UK and EU-NATO dialogue are identified as critical components of successful cyber governance.

➢ A CAPABILITY PERSPECTIVE

[1] Von der Leyen. (2025, March 4). Press statement by President von der Leyen on the defence package. https://ec.europa.eu/commission/presscorner/detail/sv/statement_25_673

[2] EDA. (n.d.). Cyber. https://eda.europa.eu/what-we-do/capability-development/cyber

[3] To deep dive on the current EU digital and cyber legislative landscape, please refer to the Deloitte EUPC Digital Playbook. Deloitte. (2025, January 17). EUPC Digital Playbook. https://www.deloitte.com/content/dam/assets-zone2/be/en/docs/about/2024/eupc-digital-playbook.pdfhttps://www.deloitte.com/mt/en/services/consulting-risk/analysis/digital-playbook-summary.html

Best practices from Finland, France, and Estonia demonstrate successful cyber defence innovation initiatives, with empirical analysis of these countries' approaches showing best practices in addressing gaps, redundancies, and inefficiencies at the EU level.

2. NAVIGATING UNCERTAINTY

Deloitte.

Achieving strategic autonomy for the EU and positioning the bloc as a global innovator

Key Takeaways

➢ CLOSING THE INNOVATION GAP

Technological sovereignty is of paramount importance for EU security. Thus, the EU will focus on innovation, investing in technologies such as supercomputing, semiconductors, IoT, and quantum computing. However, this effort must be underpinned by a clearly defined, European unified innovation strategy to guide investments and coordinate actions across Member States.

➢ ESTABLISHING CREDIBLE DETERRENCE

Credible deterrence has become key for an EU less reliant on the US military and defence shield. To achieve EU strategic autonomy and resilience, a **cohesive rearmament program**, alongside investments in emerging technologies to enhance cyber defence capabilities, is pivotal. In order to avoid duplication of efforts across Member States, cyber defence initiatives must be guided by a clear, EU-wide innovation strategy[4] enabling coordination and promoting a unified approach.

In recent years, the international geopolitical landscape has been marked by a series of significant crises, including those in the Middle East,[5] ongoing tensions in the Asia-Pacific[6] region, and Russia's aggression against Ukraine.[7] The latter continues to disrupt European stability, institutions, and citizens, also by the means of cyber-enabled warfare.[8] Furthermore, the 2024 US elections, which culminated in the re-election of President Donald Trump, have introduced fresh uncertainties into transatlantic cooperation[9], including with regard to economic relations (e.g., tariffs), cross-border collaboration, and security guarantees.

These evolving dynamics have contributed to a security and geopolitical environment where traditional and non-traditional threats increasingly intersect. A salient feature of the current geopolitical context is the proliferation of **hybrid threats**, which are defined as harmful activities perpetrated by State and non-State actors to undermine the stability of States and institutions through a variety of means, including cyberattacks, disinformation campaigns, and economic influence or coercion, often combined.[10] With regards to cybersecurity, there has been an escalation of cyberattacks targeting civilian and military critical

[4] Draghi, M. (2024, September 9). The Draghi Report: A competitiveness strategy for Europe (Part A). https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en#paragraph_47059

[5] International Rescue Committee. (2023, 15 December). Crisis in the Middle East: What is happening? https://www.rescue.org/article/crisis-middle-east-what-happening

[6] The International Institute for Strategic Studies (IISS). (2024). Asia-Pacific Regional Security Assessment 2024. https://www.iiss.org/publications/strategic-dossiers/asia-pacific-regional-security-assessment-2024/

[7] Duguin, S., Pavlova, P. (September 2023). The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict. *EU Parliament, Directorate General for External Policies*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf

[8] Mueller, G. B. et al. (2023, July 13). Cyber Operations during the Russo-Ukrainian War. *Centre for Strategic & International Studies*. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war

[9] Von der Leyen, U. (2025, January 21). Davos 2025: Special Address by Ursula von der Leyen, President of the European Commission. https://www.weforum.org/stories/2025/01/davos-2025-special-address-by-ursela-von-der-leyen-president-of-the-european-commission/

[10] Hybrid Centre of Excellence (Hybrid CoE). (n.d.). Hybrid threats as a concept. https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

infrastructures that have resulted in significant economic losses.[11] In light of these challenges, the role of security and defence is set to become more prominent in the political agendas of the EU and its Member States.

The 2024-2029 European Commission has therefore initiated measures to address these geopolitical challenges, as evidenced by the establishment of "**a new era for European Defence and Security**" among the European Commission priorities.[12] Specifically, the Union will support Member States to rebuild, replenish, and transform national armed forces, including through investments in high-end capabilities in critical areas such as cyber. The European Commission's initiative to establish a European Defence Union,[13] bolstered by a strengthened partnership between the EU and NATO, is a fundamental facet thereof.

The goals of this new strategy are to enhance Member States' national security apparatuses, as well as to establish credible deterrence. Thus, the pursuit of technological sovereignty has become critical. Technological sovereignty can be understood as the ability and competence of a State to ensure reliable access to critical technologies and its components without being structurally dependent on third countries.[14] Ensuring access to critical resources (e.g., rare earth elements), as well as securing stretched supply chains, is pivotal to avoid possible EU's dependencies on a limited number of stakeholders,[15] and closing the innovation gap with the US and China.[16]

To address these technological challenges, the 2024-2029 European Commission has announced "**a new plan for Europe's sustainable prosperity and competitiveness**."[17] Specifically, the European Commission intends to increase the EU's productivity and competitiveness by investing in technologies such as supercomputing, semiconductors, the Internet of Things (IoT), genomics, quantum computing, and space technology, ultimately positioning the EU as a leader in AI innovation.

Cybersecurity, and in particular cyber defence, will play a key role in safeguarding EU interests, as it is at the intersection of defence, critical infrastructure protection, and emerging technologies. The newly introduced portfolio of Executive Vice-President Henna Virkkunen, titled "**Tech Sovereignty, Security, and Democracy**,"[18] highlights the intersection between and mutual importance of defence capabilities and technological capacity, emphasizing their role for Europe's future resilience. Developing and strengthening the EU's cyber defence capabilities and leveraging emerging technologies will drive the EU's efforts to be a global innovator rather than a global regulator.

[11] The cost of a data breach targeting critical infrastructures has increased by USD 1.26 million. ENISA. (2024). ENISA Threat Landscape 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[12] European Commission. (2024). Commission's priorities. https://commission.europa.eu/priorities-2024-2029_en

[13] European Commission. (2024). A new era for European Security and Defence. https://commission.europa.eu/priorities-2024-2029/security-and-defence_en

[14] Jakob, E. (2024). Technology sovereignty of the EU: needs, concepts, pitfalls and ways forward. Fraunhofer-Institut für System- und Innovationsforschung ISI. https://ec.europa.eu/assets/rtd/srip/2024/ec_rtd_srip-report-2024-chap-08.pdf

[15] Lipke, A., et al. (2024, May 29). Trust and trade-offs: How to manage Europe's green technology dependence on China. European Council of Foreign Relations. https://ecfr.eu/publication/trust-and-trade-offs-how-to-manage-europes-green-technology-dependence-on-china/

[16] Draghi, M. (2024, September 9). The Draghi Report: A competitiveness strategy for Europe (Part A). https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en#paragraph_47059

[17] European Commission. (2024). A new plan for Europe's sustainable prosperity and competitiveness. https://commission.europa.eu/priorities-2024-2029/competitiveness_en

[18] EU Parliament. Confirmation hearings of the Commissioners-designate. Henna Virkkunen – Executive Vice-President for Tech Sovereignty, Security and Democracy. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762455/EPRS_BRI(2024)762455_EN.pdf

3. A TECHNOLOGY PERSPECTIVE

Deloitte.

Strengthening national security through AI and Quantum Technologies

Key Takeaways

- SAFEGUARDING EUROPEAN INTERESTS THROUGH CYBER DEFENCE INNOVATION

  Reduced barriers between civil and military domains require fostering dual-use innovations, specifically targeting AI and quantum technologies development. Dual-use technologies will impact governments' abilities to counteract malicious cyber activities and boost overall cyber defence.

- MEASURING CYBER DEFENCE INNOVATION THROUGH TANGIBLE METRICS

  It is crucial for the EU to define tangible metrics, such as adoption rates of advanced technologies (i.e., AI, quantum), that measure cyber defence innovation's **progress** and **impacts**. However, it is crucial to expand such metrics beyond the "outcome" dimension and integrate "input" and "process" variables to measure innovation holistically once a unified innovation strategy has been defined.

Cybersecurity and cyber defence are two inherently interconnected concepts, and both aim to protect digital environments from malicious cyber activities. However, within shared objectives, some distinctions have characterized the two concepts.

On the one hand, cybersecurity mainly refers to the protection of civilian infrastructures from cyber intrusions and cybercrime. Furthermore, national cybersecurity policies are generally publicly available and aim to ensure resilience and security against cyber threats. Following the quadruple helix model[19] and the ITU guidelines[20], the development of national cybersecurity policies entails the participation of a wide stakeholder community, which brings together government agencies, private sector entities, academia, and civil society to merge diverse expertise and provide a comprehensive policy. Additionally, these strategies adopt a risk-management approach to identify, assess, and prioritize risks, enabling effective resource allocation and continuous risk mitigation.

On the other hand, cyber defence is a core component of a country's national **security policy**. It often falls within the mandate of defence departments or ministries and focuses on protecting national interests against malicious cyber operations, including military and State-sponsored cyber activities. As they deal with national security issues and national cyber defence policies are generally classified[21].

To summarise, while cybersecurity has traditionally covered broader, civilian-focused measures to prevent cyber threats, cyber defence has focused on military and strategic aspects, strengthening national security in cyberspace.

[19] Carayannis, E., Campbell, D. F. J. (2009, January). "'Mode 3 and Quadruple Helix," 207; Carayannis and Campbell, Mode 3 Knowledge Production. International Journal of Technology Management 46(3/4). https://www.researchgate.net/publication/240295704_'Mode_3'_and_'Quadruple_Helix'_Toward_a_21st_century_fractal_innovation_ecosystem

[20] International Telecommunication Union (ITU). 2021. Guide to Developing a National Cybersecurity Strategy. *Strategic Engagement in Cybersecurity. 2nd Edition.* *https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2021-ncs-guide.pdf*

[21] Cordey, S., & Dewar, R. S. (2019). National Cyberdefence Policy Snapshots. *Centre for Security Studies (CSS) ETH Zürich.* https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/centre-for-securities-studies/pdfs/Cyber-Reports_National_Cybersecurity_and_Cyberdefence_Policy_Snapshots_Collection_2.pdf

Today, the boundaries between cybersecurity and cyber defence are blurred, as the complexity of cyber threats demands an integrated approach where civilian and military capabilities reinforce each other. This is envisaged, for instance, by the active cyber defence doctrine. Active cyber defence can be defined as "the proactive detection, analysis and mitigation of network security breaches in real-time combined with the use of aggressive countermeasures deployed outside the victim network[22]," and, according to the UK National Cyber Security Centre (NCSC), its aim is to "Protect the majority of people in the UK from the majority of the harm caused by the majority of the cyber-attacks the majority of the time." The active cyber defence doctrine thus embodies the growing convergence of cybersecurity and cyber defence, illustrating how a comprehensive response is essential to address the complex nature of modern cyber threats.

This paper employs established innovation frameworks, including the quadruple helix model[23] and the four types of innovation delineated by the Harvard Business Review[24] to analyse innovation in the domain of cyber defence[25]. Unlike other frameworks emphasising granular aspects of innovation, the four types of innovation framework provides a more comprehensive approach by classifying innovation into distinct types: disruptive, breakthrough, sustaining, and incremental. In the context of cyber defence, this distinction allows for consideration of how the EU can approach innovation not merely at a technical level but also through a broader, strategic lens. This lens allows consideration of how different types of innovation contribute to strengthening national security, enabling the EU to address emerging threats and improve existing capabilities through coordination among stakeholders from government, industry, academia, and civil society.

In addition to the innovation strategies mentioned above, it is worth considering the potential impact of frugal innovation on cyber defence. By encouraging innovation through affordable, off-the-shelf technologies[26], frugal innovation can encourage the deployment of dual use technologies. Indeed, by prioritizing accessibility, cost-effectiveness, and adaptability, frugal innovations can be readily applied across both civilian and military sectors. A technology initially developed for civilian use can meet military or security needs through minimal adaptation, or the other way around, fostering innovation spillovers and reducing costs.

Building on this conceptual framework, the paper considers cyber defence innovation as the process of creating, developing, and deploying technologies, strategies, and policies to improve the resilience and effectiveness of cyber defence systems.

It is worth noticing that emerging technologies and related innovations impact both **defensive** and **offensive capabilities**, but types of innovation might vary depending on the target capability. The reason lies in the

[22] Dewar, R., S. (2014). The "Triptych of Cyber Security": A Classification of Active Cyber Defence. *6th International Conference on Cyber Conflict.* https://ccdcoe.org/uploads/2018/10/d1r1s9_dewar.pdf

[23] Campbell, D. F. J., Carayannis, E. (2009, January). Mode 3' and Quadruple Helix: Toward a 21st century fractal innovation ecosystem. *International Journal of Technology Management*, 46 (3/4). https://www.researchgate.net/publication/240295704_%27Mode_3%27_and_%27Quadruple_Helix%27_Toward_a_21st_century_fractal_innovation_ecosystem

[24] Satell, G. (2017, June 21). The 4 Types of Innovation and the Problems They Solve. *Harvard Business Review*. https://hbr.org/2017/06/the-4-types-of-innovation-and-the-problems-they-solve

[25] Yat-Kwan Wong, E., Hutton, K. R. (2018, July 18). Thinking Outside-the-Box for Cyber Defence: Introducing an Innovation Framework for the 21st Century. https://www.researchgate.net/publication/329179669_Thinking_Outside-the-Box_for_Cyber_Defence_Introducing_an_Innovation_Framework_for_the_21st_Century

[26] Radjou, N., Prabhu, J., Ahuja, S. (2012). Jugaad Innovation: Think Frugal, Be Flexible, Generate Breakthrough Growth. https://books.google.it/books/about/Jugaad_Innovation.html?id=GU24XFLPAv0C&redir_esc=y ; Prabuh, J. (2018, April 16). Frugal Innovation. https://www.jbs.cam.ac.uk/2018/frugal-innovation/

inherent asymmetry of cyber operations: while attackers can operate independently with minimal resources and need to identify a single vulnerability to disrupt systems, defenders face the challenging task of securing systems against a widening attack surface and a huge amount of known and unknown vulnerabilities. Consequently, cyber offense capabilities predominantly rely on disruptive innovation that leverages low-cost, high-impact solutions exploiting vulnerabilities in existing systems. In contrast, defensive solutions (e.g., intrusion prevention systems) often require significant investment in research and development, thus falling into the domains of breakthrough and sustaining innovations.[27]

In the following, practical examples of how innovation and emerging technologies are shaping cyber defence are provided. Given the increasing relevance of dual use technologies for national security and technological sovereignty,[28] the analysis also offers an overview of such technologies and their relevance to cyber defence. Subsequently, the paper delves into critical technologies within the dual-use category, specifically focusing on AI and quantum technologies.

3.1. Dual-use Technologies

Dual-use technologies are pivotal for advancing Europe's cyber defence. Among others, they include AI, quantum, advanced cryptography, advanced robotics, and unmanned aircraft systems (UAS). For example, AI, advanced encryption algorithms, and quantum computing are critical for protecting civilian infrastructures like financial systems, healthcare networks, and communications, as well as related economic sectors. In contrast, these technologies also play a crucial role in military operations. Indeed, possible scopes of applicability in the military domain include securing classified information, coordinating logistics, and enhancing situational awareness.

Public-private partnerships and synergies play a crucial role in harnessing dual-use innovation as they depend on collaboration between governments, private sector, academia, and research institutions. By leveraging such synergies, the EU can reduce its dependency on critical technologies and reinforce its **Defence Technological and Industrial Base** (**EDTIB**),[29] ensuring greater resilience and strategic autonomy in the face of evolving threats. Indeed, the EU currently **depends on third countries** for more than **80%** of its digital products, services, infrastructure, and intellectual property, especially with regards to the semiconductor sector.[30]

R&D activities and technology transfer between the military and civilian domains still face hurdles. Currently, EU funding mechanisms and programs such as **Horizon Europe** and the **European Defence Fund** (**EDF**) suffer from the inability to overcome the repurposing of civilian products and services to military purpose, or the other way around. In brief, civilian and defence R&D efforts currently operate in isolation, with minimal, if any, opportunities for cross-sector spillovers. Even though such separation may address ethical concerns about militarizing civilian technologies, it is increasingly clear that defence capabilities need robust civil

[27] Ibidem

[28] Dual-use technology – Cross-sector cooperation in the cybersecurity sector. https://cybersecforum.eu/wp-content/uploads/2024/12/Dual-use-technology-%E2%80%93-cross-sector-cooperation-in-the-cyber-security-sector.pdf

[29] EDTIB is a framework aimed at developing a competitive, collaborative, and integrated European defence industry to enhance security and economic growth. It focuses on strengthening cooperation, avoiding duplication, ensuring interoperability, and fostering innovation across Member States. EU Parliament. The EU's Defence Technological and Industrial Base. https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2020)603483

[30] Draghi. M. (2024, September 9). The Draghi report on EU competitiveness. https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en#paragraph_47059

security measures to safeguard the EU's resilience.[31] Hence, the need for funding programs and governance structures that promote synergies between civil and defence research.

3.1.1. Focus on AI in Cyber Defence

Cyber defence systems increasingly call for breakthrough technologies capable of improving data analytics, countering advanced and sophisticated threats, and strengthening threat projection and scenario analysis. Indeed, the exponential growth in the flow of digital information has created significant challenges in managing and structuring data. Data overload poses a concrete threat to cyber defence systems and capabilities, as it can hinder their ability to detect, analyse, and respond to cyber threats in a timely manner. As the volume of data increases, so does the complexity of distinguishing between normal activity and potential malicious behaviour, increasing the risk of delayed responses. Furthermore, AI-enabled cyberattacks have increased the sophistication of malicious actors' techniques, complicating traditional threat landscapes.

AI technologies are expected to provide some solutions to strengthen cyber defence and foster innovation. As observed by the **European Defence Agency** (**EDA**),[32] AI systems leveraging machine learning and deep learning[33] are proving effective in performing predictive analysis with potential applications in cyber situation awareness, decision-support systems, malware detections, and data correlation, just to name a few.

AI technologies are likely to impact cyber defence both at the network and infrastructure level. The former might benefit from AI's ability to perform real-time analysis and adapt to evolving threats enabling self-configuring networks. By simplifying the identification of vulnerabilities and enabling immediate responses to cyberattacks, AI-enabled systems strengthen network resilience and threat prevention. From the infrastructure perspective, AI applications such as **Intent-Based Network Security** (**IBNS**) with self-adaptive capabilities might represent a shift toward more autonomous and resilient cyber defence mechanisms.

By automating complex processes such as threat detection, response coordination, and vulnerability management, complementing human expertise, AI can significantly strengthen the ability of cyber defence systems to mitigate risks and safeguard critical assets. Hence, investing in the development and deployment of AI technologies is crucial to impact cyber defence and address the escalating challenges posed by digital information and the increasing sophistication of cyber threats.

As AI innovation accelerates, states are increasingly developing governance frameworks, but most of them exclude security and defence applications. The **United Nations Institute for Disarmament Research** (**UNIDIR**) has launched guidelines to address this gap, aiming to help States responsibly develop, deploy, and review AI strategies in security and defence.[34] The framework introduces procedural and substantive guidelines.

[31] European Commission (2024, January 24). WHITE PAPER On options for enhancing support for research and development involving technologies with dual-use potential. https://research-and-innovation.ec.europa.eu/system/files/2024-01/ec_rtd_white-paper-dual-use-potential.pdf

[32] EDA. Artificial Intelligence (AI) Enabled Cyber Defence. *European Defence Matters*. Issue 14. https://eda.europa.eu/webzine/issue14/cover-story/artificial-intelligence-(ai)-enabled-cyber-defence

[33] Machine learning is a field of computer science that trains a program or system to perform tasks without explicit instructions, by using algorithms to process large amounts of data, identify patterns, and make accurate predictions

Deep learning is a subset of machine learning that uses special algorithmic structures (i.e., neural networks), inspired by the human brain. It focuses on automating more complex tasks, such as image recognition, language translation, or speech-to-text transcription. Source: AWS. (n.d.). Qual è la differenza tra machine learning e deep learning?. https://aws.amazon.com/it/compare/the-difference-between-machine-learning-and-deep-learning/

[34] Afina, Y. (2024). Draft Guidelines for the Development of a National Strategy on AI in Security and Defence. Geneva, Switzerland: *UNIDIR*. https://unidir.org/publication/draft-guidelines-for-the-development-of-a-national-strategy-on-ai-in-security-and-defence/

The procedural guidelines emphasize the importance of defining objectives, roles, and expected outcomes, engaging in consultations with stakeholders from different sectors, assessing geopolitical, legal, ethical, and technical factors, as well as establishing oversight and accountability mechanisms. The substantive guidelines delve into considerations regarding ethical and practical integration of AI into security and defence, including responsible data practices, machine learning's risks, compliance with international law, and the need of robust emergency response planning and capacity building.

3.1.2. Focus on Quantum Technologies in Cyber Defence

By leveraging quantum mechanics to enhance capabilities in secure communication, threat detection, and computational power, quantum technologies are expected to impact cyber defence in the next decades.

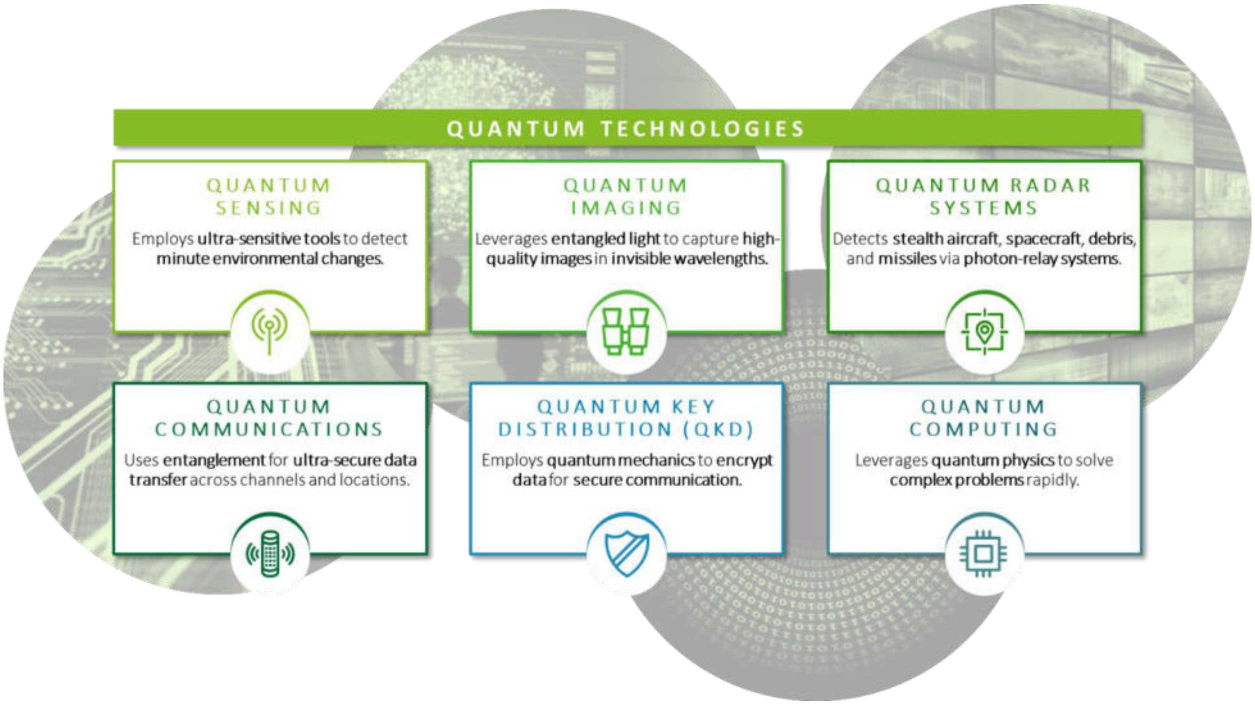

QUANTUM TECHNOLOGIES
QUANTUM SENSING
Employs ultra-sensitive tools to detect minute environmental changes.
QUANTUM IMAGING
Leverages entangled light to capture high-quality images in invisible wavelengths.
QUANTUM RADAR SYSTEMS
Detects stealth aircraft, spacecraft, debris, and missiles via photon-relay systems.
QUANTUM COMMUNICATIONS
Uses entanglement for ultra-secure data transfer across channels and locations.
QUANTUM KEY DISTRIBUTION (QKD)
Employs quantum mechanics to encrypt data for secure communication.
QUANTUM COMPUTING
Leverages quantum physics to solve complex problems rapidly.

Figure 1 Quantum technology types and examples

First, as quantum computing leverages high processing capabilities to improve the efficiency and effectiveness of AI algorithms used to counter complex cyber threats, quantum computing is intertwined with AI.[35] The **synergy** between these two technologies creates a virtuous **cycle of innovation**, where advancements in quantum technologies drive AI development, and AI, in turn, maximizes the positive impact of quantum systems tackling evolving cyber defence challenges.

Second, quantum technologies are set to **overcome traditional encryption techniques**, securing communications at unprecedented levels. For instance, Quantum Key Distribution (QKD) are expected to enable ultra-secure communication channels by establishing an alarming mechanism that informs communicators as soon as any attempt at interception occurs. Military communications can benefit from such technologies, reducing the likelihood of interception.

[35] EDA. Artificial Intelligence (AI) Enabled Cyber Defence. *European Defence Matters*. Issue 14. https://eda.europa.eu/webzine/issue14/cover-story/artificial-intelligence-(ai)-enabled-cyber-defence

However, quantum technologies also pose a significant threat to current cryptographic systems, as quantum computing could potentially break widely used encryption methods[36]. This issue is particularly relevant also in the short-term as adversaries may intercept and store encrypted, aiming to decrypt it as soon as quantum computers will be available with a tactic known as "harvest now, decrypt later."[37] For this reason, organizations like NIST are already working to standardize quantum-resistant public-key cryptographic algorithms[38].

Beyond the military domain, quantum technologies can also enhance the protection of sensitive data and digital infrastructures in the civil domain through the development of new cryptographic techniques. An example is represented by the **EU Quantum initiative "EuroQCI"**,[39] which aims to enable "ultra-secure, quantum encrypted, space-based communication between government institutions and critical infrastructures"[40] (e.g., data centres, governmental institutions, energy grids) integrating quantum-based systems into existing communication infrastructures.

Third, quantum sensors are set to impact threat detection techniques as their sensitivity allows the identification of electromagnetic anomalies. This feature enables quantum sensors to uncover unauthorized devices or suspicious activities within secure networks.

3.2. Measuring Cyber Defence Innovation: How To?

In order to ensure that innovation in cyber defence does not remain an abstract concept, it is crucial for the EU and its Member States to define indicators that capture both the progress and impact of innovation efforts. In order to do so, the EU could rely on a variety of approaches.

Quantitative metrics, such as the number of patents filed or the adoption rates of advanced technologies, are used for establishing baselines and monitoring innovation progress by offering insights into national and sectoral innovation capabilities. Such metrics are adopted, for instance, by the EU Commission to track the progresses of the **EU State of the Digital Decade**.[41]

Nevertheless, quantitative metrics are frequently based solely on output metrics – namely, indicators that measure the tangible results of innovation efforts. This approach risks providing an incomplete view of the innovation landscape. In order to address potential shortcomings, the EU needs to first define a unified innovation strategy framework and taxonomy to ensure consistency and avoid fragmentation across Member States. Such framework and taxonomy can rely on existing approaches such as the four types of

[36] Parker, E. (2023, September 13). When a Quantum Computer Is Able to Break Our Encryption, It Won't Be a Secret. *RAND.* https://www.rand.org/pubs/commentary/2023/09/when-a-quantum-computer-is-able-to-break-our-encryption.html

[37] NIST. (n.d.) What Is Post-Quantum Cryptography? https://www.nist.gov/cybersecurity/what-post-quantum-cryptography

[38] NIST. (n.d.) Post-Quantum Cryptography. https://csrc.nist.gov/projects/post-quantum-cryptography

[39] EU Commission. The European Quantum Communication Infrastructure (EuroQCI) Initiative. https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

[40] EU Commission. Quantum Technologies. (n.d.) https://defence-industry-space.ec.europa.eu/eu-space/research-development-and-innovation/quantum-technologies_en

[41] The Report on the state of the Digital Decade measures the EU Member States and the EU performance against quantitative metrics regarding digital infrastructure (e.g., number of quantum computers in the EU), digital transformation of business (e.g., percentage of enterprises that registered AI take-up and number of EU Unicorns), digital skills (e.g., percentage of individuals with basic digital skills and number of ICT specialists employed), and digital public services (e.g., score of digital public services for citizens and businesses). The Report on the state of the Digital Decade 2024 has been published in July: EU Commission. (2024, July 2). Report on the state of the Digital Decade 2024. https://digital-strategy.ec.europa.eu/en/library/report-state-digital-decade-2024

innovation[42] or frugal innovation.[43] Subsequently, based on the innovation strategy defined, the EU has to identify a set of quantitative and qualitative metrics to measure innovation performance.

Considering quantitative metrics, it is crucial to pursue a balanced assessment across input, process, and output metrics. While the input ones assess the preconditions necessary for innovation success (e.g., the allocation of financial resources), process metrics capture the dynamics that characterize the innovation funnel (e.g., average time from idea generation to first revenue)[44], thus providing visibility into the efficiency of innovation pipelines. Effective cyber defence innovation metrics should integrate input, process, and output metrics to shift the focus from isolated outcome measurements to a more comprehensive consideration of the innovation lifecycle.

To complement quantitative metrics, performance-based funding models – such as those used in EU programmes like Horizon Europe or the European Defence Fund (EDF) – tie financial support to the achievement of predefined innovation milestones. This approach aims to ensure that funded projects deliver tangible results and resources are allocated efficiently.

Furthermore, encouraging public-private partnerships (PPPs) to co-develop innovation benchmarks allows for the inclusion of diverse stakeholder priorities and fosters a shared understanding of innovation objectives. An example is represented by Partnership AI, which launched the **Global Task Force for Inclusive AI** in 2023. Such Task Force brings together experts from academia, industry, civil society, and policymaking to define a framework for ethical and inclusive stakeholder engagement in AI development. For instance, the **Guidelines for Participatory and Inclusive AI**[45] address critical challenges, such as algorithmic bias, while aligning innovation goals with societal priorities. The objective is to encourage the development of AI systems that meet ethical and inclusive standards and drive responsible innovation.[46]

Finally, real-world testing of innovative solutions – through stress tests, simulations, or testbeds – provides an evidence-based method to evaluate the operational effectiveness of new technologies, measuring the performance of innovative solutions in real-world scenarios[47].

These approaches offer a multifaceted toolkit for assessing innovation in a way that balances quantitative and qualitative metrics while also considering real-world implications. A well-integrated combination of these approaches can ensure that innovation translates into concrete outcomes within the field of cyber defence.

[42] Satell, G. (2017, June 21). The 4 Types of Innovation and the Problems They Solve. *Harvard Business Review*. https://hbr.org/2017/06/the-4-types-of-innovation-and-the-problems-they-solve

[43] Radjou, N., Prabhu, J., Ahuja, S. (2012). Jugaad Innovation: Think Frugal, Be Flexible, Generate Breakthrough Growth. https://books.google.it/books/about/Jugaad_Innovation.html?id=GU24XFLPAv0C&redir_esc=y ; Prabuh, J. (2018, April 16). Frugal Innovation. https://www.jbs.cam.ac.uk/2018/frugal-innovation/

[44] Skipso. (n.d). What are the best instruments to measure the innovation funnel?. https://www.skipso.com/resources/what-are-the-best-instruments-to-measure-the-innovation-funnel#:~:text=Input%20%E2%80%93%20Process%20%E2%80%93%20Output&text=For%20example%2C%20the%20average%20time,number%20of%20new%20customers%2C%20etc.

[45] Park, T. (2024, September 17). Stakeholder Engagement for Responsible AI: Introducing PAI's Guidelines for Participatory and Inclusive AI. *Partnership AI*. https://partnershiponai.org/stakeholder-engagement-for-responsible-ai-introducing-pais-guidelines-for-participatory-and-inclusive-ai/

[46] Partnership AI. (n.d.). Global Task Force for Inclusive AI. https://partnershiponai.org/global-task-force-for-inclusive-ai/

[47] Arntzen, S. et al. (2019, October). Testing Innovation in the Real World. Real-world testbeds. https://media.nesta.org.uk/documents/Testing_innovation_in_the_real_world.pdf

4. A POLICY PERSPECTIVE

Establishing a Harmonised EU Cyber (Defence) Innovation Framework

Key Takeaways

- **2024-2029 EU GOALS FOR INNOVATION, COMPETITIVENESS, AND SECURITY**

  During the 2024-2029 mandate, the European Commission will focus on strengthening its competitiveness and innovation capabilities and harmonising its approach across the Member States along three pillars: **closing** the **innovation gap** with the US and China, developing a joint roadmap for decarbonization and competitiveness, and **increasing security** and reducing excessive dependencies.

- **2019-2024 EU ACHIEVEMENTS FOR AN EUROPEAN STRATEGIC AUTONOMY**

  Throughout the 2019-2024 mandate, the European Commission has enhanced cyber defence by **investing** in emerging technologies, **standardizing** products for greater resilience, expanding the EU defence industrial base, and fostering closer cooperation between civil and military sectors, Member States, and EU institutions.

There are a wide range of EU cybersecurity legislation, policies and frameworks that encompass the entirety of the Union's ambitions from both a civil and military perspective. The **EU's Cyber Defence Policy Framework** (**CDPF**) fosters interconnectedness between civil and military domains through key bodies such as the **EU Cyber Defence Coordination Centre** (**EUCDCC**).

The section offers, firstly, a review of the **2024-2029 European Commission agenda** to increase EU strategic autonomy and technological sovereignty, with a specific focus on new proposed **regulations** for **innovation** and **research** in the EU. Herein, relevant legislation and policy initiatives around cybersecurity and cyber defence are cited that have served as "enabling factors" to the current state of EU innovation in cyber defence.[48]

4.1. Towards a Harmonised EU Regulatory Framework for Cyber (Defence) Innovation

The Union plays a pivotal role in promoting the development of EU cyber capabilities, both civilian and military, through a vast corpus of **digital** and **cyber legislation**. The following timeline provides an overview of all the key documents that are currently shaping and that will shape cyber defence innovation in the EU, showing synergies and interconnections.

[48] Csernatoni, R. (2022). The EU's hegemonic imaginaries: from European strategic autonomy in defence to technological sovereignty. https://www.tandfonline.com/doi/epdf/10.1080/09662839.2022.2103370?needAccess=true

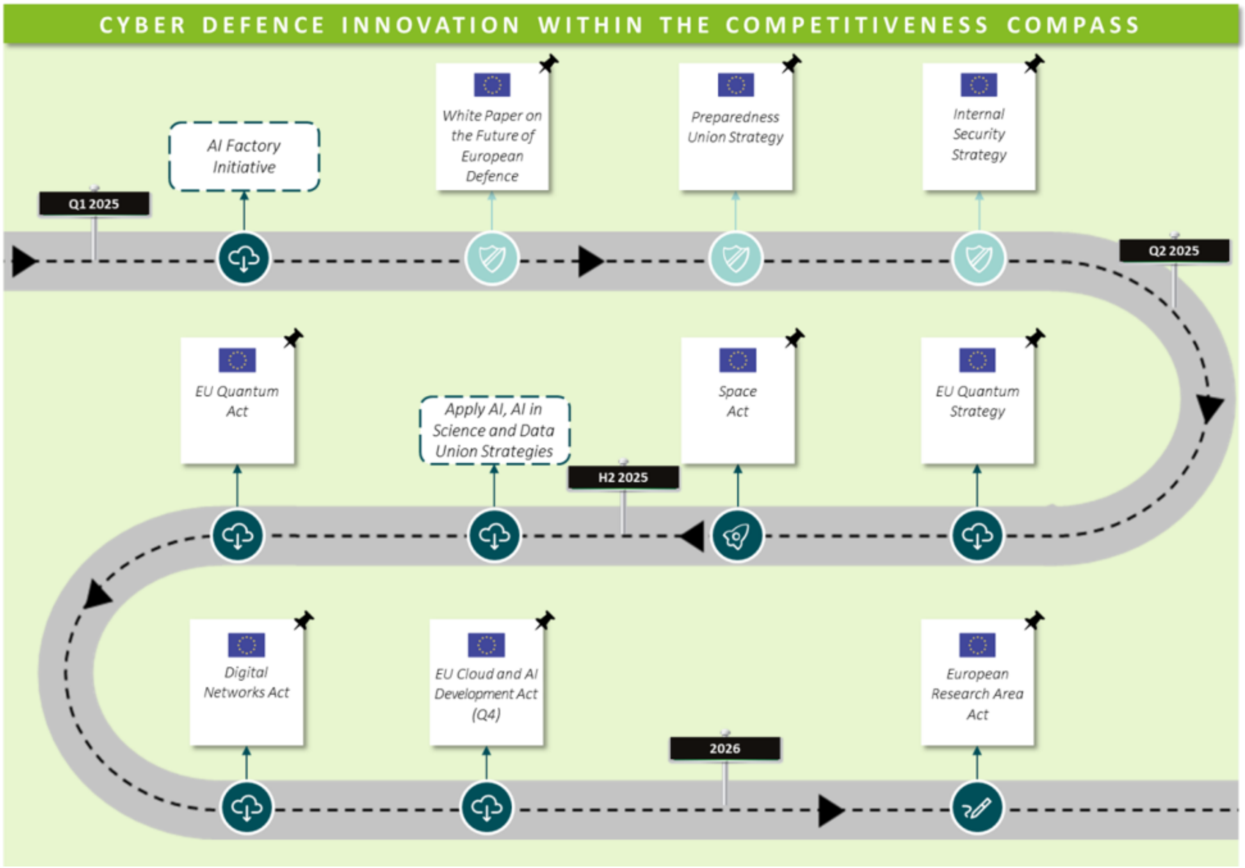

CYBER DEFENCE INNOVATION WITHIN THE COMPETITIVENESS COMPASS
Q1 2025
AI Factory Initiative
White Paper on the Future of European Defence
Preparedness Union Strategy
Internal Security Strategy
Q2 2025
EU Quantum Act
Apply AI, AI in Science and Data Union Strategies
H2 2025
Space Act
EU Quantum Strategy
Digital Networks Act
EU Cloud and AI Development Act (Q4)
2026
European Research Area Act

Figure 2 European Commission 2024-2029 Competitiveness Compass initiatives related to cyber innovation

Building on the **2019-2024 European Commission achievements**,[49] the new challenge posed to the European Commission regards focusing the digital, cybersecurity, and cyber defence agendas on innovation, effectively achieving a harmonised EU framework for cyber innovation.

As anticipated in the introduction, the **2024-2029 European Commission**, led by President von der Leyen, has outlined its seven key priorities[50] for the upcoming legislative term. With regards to cyber defence, such priorities include:

- a new plan for Europe's sustainable prosperity and competitiveness;
- a new era for European Defence and Security;
- protecting our democracy, upholding our values;
- a global Europe: Leveraging our power and partnerships.

The first major initiative of the new European Commission is the **Competitiveness Compass**, published on January 29, 2025.[51] The Compass is built on the three pillars of the Draghi report[52] "The future of European

[49] For a detailed analysis, refer to paragraph *4.2.*

[50] European Commission. (2024). Commission's priorities. https://commission.europa.eu/priorities-2024-2029_en

[51] European Commission. (January 29, 2025). Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of Regions. A competitiveness Compass for the EU. https://commission.europa.eu/document/download/10017eb1-4722-4333-add2-e0ed18105a34_en

[52] Draghi, M. (2024, September 9). The Draghi Report: A competitiveness strategy for Europe (Part A). https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en#paragraph_47059

competitiveness – A competitiveness strategy for Europe." The first is closing the innovation gap with the US and China. The second is a joint roadmap for decarbonization and competitiveness. The third is increasing security and reducing excessive dependencies.

To complement these pillars, the Competitiveness Compass outlines two fundamental requirements for stronger policy support: simplifying and accelerating regulations to reduce complexity and enhance flexibility and improving coordination between EU and national policies. While the first and the third pillars have direct implications for cyber defence innovation, the second one – a joint roadmap for decarbonization and competitiveness **–** falls outside the scope of this paper.

Under the first pillar, closing the innovation gap, Europe's competitiveness strategy prioritizes research and innovation, placing science and technology at the core of the economy. The plan focuses on fostering investment, enhancing cooperation, and creating conditions for researchers to thrive and acquire new skills. With a targeted approach to transformative innovation, the strategy seeks to advance Europe's competitiveness while meeting key goals for security, sustainability, and economic growth in a clean and digital economy. According to the first pillar, the EU is set to encourage innovation among both Small and Medium-sized Enterprises (SMEs) and big companies. While the former will benefit from an EU start-up and scale-up strategy, the latter will be supported in the adoption of AI and robotics through a "Apply AI" initiative[53]. Furthermore, the development of new technologies is expected to be supported by the development of action plans targeting, for instance, advanced materials and quantum, as well as by a unified set of rules across the 27 Member States. Considering the simultaneous push towards R&D and defence, the development and adoption of cyber defence technologies could benefit from a fertile innovation environment. As strengthened research and innovation capabilities can contribute to the achievement of technological sovereignty and strategic autonomy, reducing dependencies on external technologies, effective support towards the European industrial competitiveness will be pivotal to fulfil the current EU agenda.

Technological sovereignty and strategic autonomy are also key objectives of the third pillar of the Competitiveness Compass, namely increasing security and reducing excessive dependencies. In this regard, the establishment of new clean trade and investment partnerships to ensure the supply of raw materials, along with updated public procurement rules that prioritize EU interests in critical sectors and strategic industries, represent two key policy measures with significant implications for the advancement of cyber defence technologies[54].

The EU has proposed several regulations aiming to harmonise the way innovation is tackled across the EU. On October 2024, in "**The future of European competitiveness – A competitiveness strategy for Europe"**, Mario Draghi recommended the adoption of a new **EU Cloud and AI Development Act** aimed at enhancing European high-performance computing (HPC), quantum capabilities and infrastructure, dedicated to the training and fine-tuning of AI models. The Act will also aim to harmonise EU's cloud architecture requirements and procurement processes and coordinating priority initiatives to scale up private involvement and financing through an EU-wide framework. Additionally, the new Act will look into identifying priority AI applications to incentivize development in pivotal sector, harmonising AI sandbox regimes and General Data Protection Regulation (GDPR) implementation.

[53] EU Commission (n.d.). Strengthening European competitiveness. https://commission.europa.eu/topics/eu-competitiveness_en

[54] EU Commission (n.d.). Strengthening European competitiveness. https://commission.europa.eu/topics/eu-competitiveness_en

During the plenary on 16 December 2024 the **Commissioner Ekaterina Zaharieva** has presented a plan for a **European Innovation Act**[55] to the European Parliament in Strasbourg. The Act will strengthen the innovation ecosystem by simplifying and streamlining EU's regulatory framework, tackling EU's underdeveloped financial market by mobilizing more private capital to enhance access to funding and investment opportunities, and supporting testing of new solutions and technologies. Lastly, it will foster the growth of skills and talent, which are fundamental for the development of innovative products and solutions. The plan presented by Commissioner Zaharieva focuses on existing but underutilized and fragmented tools, in order to maximize their usage and reduce the burden of innovation costs. In 2025 an extensive public consultation will be launched, to gather feedback and input across the Union. Lastly, another step, critical in translating EU innovation into competitiveness by retaining talent within the EU, will be represented by the **European Research Area Act**.

Furthermore, the EU Commission is set to address regulatory fragmentation also with regards to AI and quantum technologies, as demonstrated by the announcement of within the Competitiveness Compass scope[56]. On the one hand, the European AI Continent Action Plan focuses on the development of AI factories[57], and on the announced EU Cloud and AI Development Act. Such efforts aim to boost AI and cloud infrastructure by supporting AI Gigafactories for training large-scale models and setting minimum standards for cloud services across the EU, also complementing efforts in chip design and manufacturing, particularly for advanced AI chips.

On the other hand, building upon the **Chips Act**[58], the announced **Quantum Strategy** and **Quantum Act** aim to harmonise EU and national programs, and foster investment in pan-European quantum computing, communication, and sensing infrastructure.

Finally, the EU Commission has announced the **European Research Area Act**, which is expected to strengthen and harmonise R&D investments across the EU, aligning strategic priorities and increasing R&D investment up to the 3% GDP target[59].

Considering the role of AI quantum technologies to strengthen cyber capabilities, cyber defence innovation could benefit from such pan-European approach towards emerging technologies.

While regulatory harmonisation and strategic planning are essential to foster cyber (defence) innovation, the availability of adequate and sustainable financing mechanisms remains a critical enabler. The upcoming negotiations on the Multiannual Financial Framework (MFF) will be pivotal in determining the extent to which the EU can support its ambitions in cyber innovation. As the Union seeks to close the innovation gap and enhance its strategic autonomy, the allocation of resources to digital and defence-related R&D will be a litmus test of its political will.

[55] EU Parliament. (2024, December 16). A European Innovation Act: lowering the cost of innovating in Europe. *Verbatim report of proceedings.* https://www.europarl.europa.eu/doceo/document/CRE-10-2024-12-16-ITM-018_EN.html

[56] European Commission. (January 29, 2025). Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of Regions. A competitiveness Compass for the EU. https://commission.europa.eu/document/download/10017eb1-4722-4333-add2-e0ed18105a34_en

[57] EU Commission. (n.d.) AI Factories. https://digital-strategy.ec.europa.eu/en/policies/ai-factories

[58] Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe's semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act) (Text with EEA relevance). https://eur-lex.europa.eu/eli/reg/2023/1781/oj/eng

[59] European Commission. (January 29, 2025). Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of Regions. A competitiveness Compass for the EU. https://commission.europa.eu/document/download/10017eb1-4722-4333-add2-e0ed18105a34_en

The MFF debate will not only shape the future of flagship programmes such as Horizon Europe, the Digital Europe Programme, and the European Defence Fund, but also determine the level of coherence and ambition in funding cross-cutting initiatives that support dual-use technologies. In this context, cyber innovation—situated at the intersection of digital transformation and security—requires a dedicated and well-resourced approach. Ensuring that cyber capabilities are adequately financed will be essential to operationalise the objectives set out in the Competitiveness Compass and the forthcoming European Innovation Act.

As the EU advances its cyber defence agenda, securing sustainable and strategic financing will be essential. While discussions around introducing new own resources and expanding EU debt instruments and – building on the precedent of NextGenerationEU[60] – are gaining momentum, these alone may not suffice. The scale and speed of innovation required in cyber technologies demand a more agile and collaborative approach. In this context, public-private partnerships (PPPs) emerge as a cornerstone of the EU's innovation financing strategy. By mobilising private capital, sharing risk, and fostering co-development between industry and public institutions, PPPs can accelerate the deployment of cutting-edge cyber capabilities.

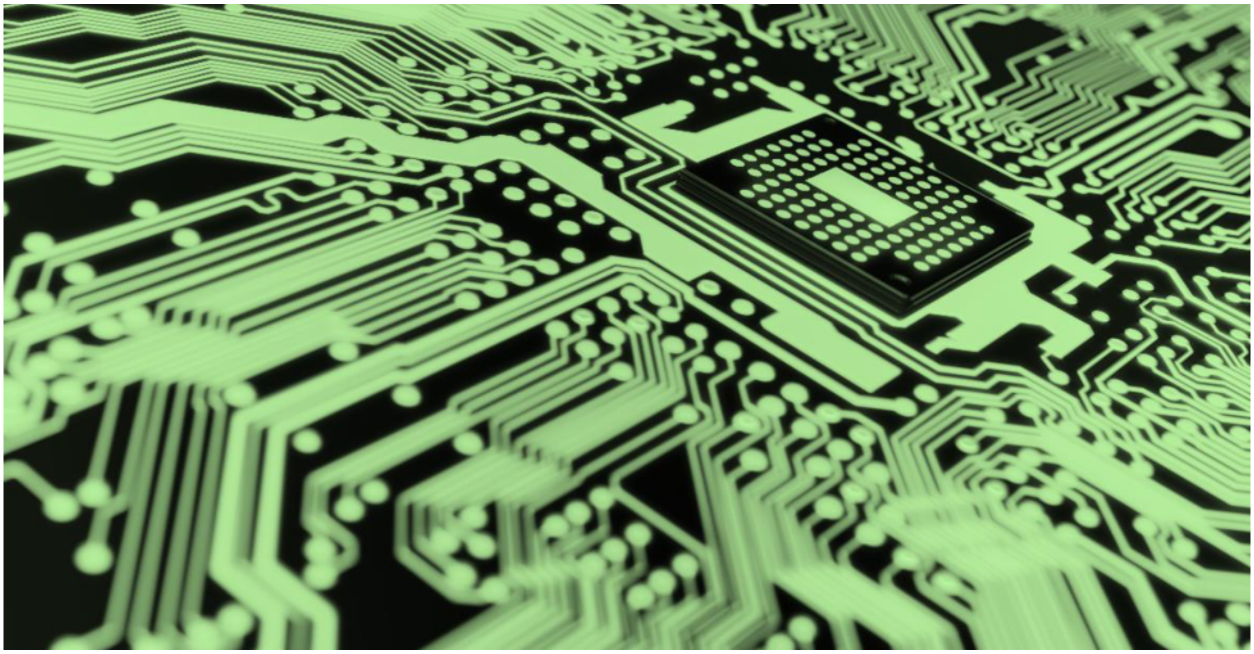
4.2. 2019-2024 EU Achievements Regarding the European Strategic Autonomy and Technological Sovereignty

The 2019-2024 European Commission key efforts around cyber defence have been directed to the following four key points:

- Enhancement of the **Union's cyber capabilities**, including through the development of emerging technologies (e.g., quantum computing, AI) and capacity building;
- **Standardization** of products and services, in order to reach elevated levels of resilience and interoperability;
- Broadening and maximization of the **EU's investments** to enlarge the European defence and technological industrial base;
- Improved **cooperation between civil and military domains**, as well as enhanced collaboration among Member States, EU institutions, bodies, and agencies.

The ensuing analysis includes relevant strategic, legislative, and policy initiatives around cybersecurity and cyber defence that have served as "enabling factors" to the current state of EU innovation in cyber defence, building and reinforcing concepts such as, but not limited to, European strategic autonomy and technological sovereignty.

1. [60] EU Commission. (2020, May 27). Recovery plan for Europe. https://commission.europa.eu/strategy-and-policy/recovery-plan-europe_en



Throughout the 2019-2024 EU Commission mandate, the EU demonstrated strong commitment towards the progression of its digital landscape, as evidenced by the development of the **Europe's Digital Decade** under the objective of "A Europe fit for the digital age." In particular, the EU developed an overarching strategy to achieve a sustainable and secure digital transformation, creating a playing field for the adoption of new technologies.

Furthermore, the EU focused on shaping and enhancing its regulatory framework targeting security. In July 2020, for instance, the EU adopted the **Union's Security Strategy 2020-2025** to respond to increasingly complex threats, addressing the importance of security in cyberspace. In this regard, the **EU Cybersecurity Strategy for the Digital Decade**[61] represents a cornerstone. The Strategy, which was published at the end of 2020, focuses on three main areas:

- Resilience, Technological Sovereignty, and Leadership;
- Building Operational Capacity to Prevent, Deter, and Respond;
- Advancing a Global and Open Cyberspace Cooperation.

In the first area, "Resilience, Technological Sovereignty, and Leadership", EU efforts aim to enhance the resilience of infrastructures and critical services. A key initiative in this regard is the reform of EU rules governing the security of Network and Information Systems (NIS), culminating in the adoption of the **NIS2 Directive** (2022),[62] which came into force on 17 January 2023. Additional efforts under this area are directed to the creation of a network of Security Operations Centres (SOCs) at the European level powered by AI under the **Cyber Solidarity Act** (CSA),[63] proposed in April 2023. In order to strengthen the technological

[61] EU Commission. (2020, December 16). The EU's Cybersecurity Strategy for the Digital Decade. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

[62] EU Parliament, the Council of the EU. (2022, December 14). 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 No 910/2014 and Directive 2018/1972, and repealing Directive 2016/1148. https://eur-lex.europa.eu/eli/dir/2022/2555

[63] EU Parliament, the Council of the EU. (2024, November 20). 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 cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act) https://data.consilium.europa.eu/doc/document/PE-94-2024-INIT/en/pdf

sovereignty of the EU and its Member States, the EU also envisaged a strategic initiative to support SMEs and raise cyber-security skills and capabilities within the framework of **Digital Innovation Hubs**.

Other strategic initiatives launched during the 2019-2024 EU Commission mandate include regulatory measures for an Internet of Secure Things and higher cybersecurity investments for the Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres (CCCN), as well as the establishment of ultra-secure communication infrastructures harnessing quantum technologies, and the completion of the 5G Toolbox implementation.

The second area "Building Operational Capacity to Prevent, Deter, and Respond", focuses on EU capabilities to prevent, deter, and respond to accidental or deliberate cyber incidents. The EU communities that are responsible for preventing, discouraging, deterring, and responding to cyber threats, and that are mostly impacted by this area, are NIS authorities (e.g., CSIRTs), law enforcement and judicial authorities, cyber diplomacy bodies, and cyber defence entities. Among the key strategic initiatives that the EU should deploy in this area, it is worth mentioning the establishment of a Joint Cyber Unit (JCU). Leveraging progresses achieved by the NIS Cooperation Group and the CyCLONe Network, JCU is set to enable cooperation among EU Member States and EU institutions, bodies and agencies, as well as foster resources and capabilities' sharing mechanisms.

Another relevant strategic initiative regards the boosting of EU cyber defence capabilities through the review of the CDPF and the development of an EU "Military Vision and Strategy on Cyberspace as a Domain of Operations" for **Common Security and Defence Policy** (**CSDP**) military missions and operations. The EU should, for instance, foster further cooperation among Member States on cyber defence research, innovation and capability development, also leveraging the **Permanent Structured Cooperation** (**PESCO**) and the EDF.

The third area "Advancing a Global and Open Cyberspace Cooperation", focuses **European engagement and leadership** in the international standardisation processes, reinforcing EU participation to international and European standardisation bodies. Such process is pivotal in complementing the EU traditional regulatory efforts in areas such as AI, cloud, quantum computing, and quantum communication.

In line with the 2020 EU Cybersecurity Strategy, the **European External Action Service** (**EEAS**) has directed its efforts to strengthen EU defence capabilities, including the Union's cyber posture and cyber intelligence capacities. A step towards the aforementioned ambition has been taken with the adoption by the Council in March 2022 of the **Strategic Compass for Security and Defence**.[64] The Strategic Compass aims at strengthening security and defence by 2030, enhancing strategic autonomy, unity, and cooperation with NATO and the UN and regional partners (e.g., OSCE, AU and ASEAN) and bilateral partners, while addressing global threats and supporting international peace. The Strategic Compass sets out four work strands, each completed by concrete actions, so that the EU will:

- **act** more quickly and decisively when facing crises;
- **secure** its citizens against fast-changing threats;
- **invest** in the capabilities and technologies needed;

[64] European External Action Service. (2022). Strategic Compass for Security and Defence. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

- **partner** with others to achieve common goals.

In particular, the Strategic Compass recognizes cyberspace as a field for strategic competition, highlighting that all actors are facing a growing dependence on digital technologies. Therefore, the concrete actions to be undertaken until 2030 under the work strand "secure citizens against fast-changing threats" include investments in shared analysis capabilities (e.g., situational awareness, strategic foresight). For instance, such a work strand includes the strengthening of an Early Warning System and the development of state-of-the-art European technical equipment, infrastructure, and expertise for enhanced secure communications.

Furthermore, in order to harmonise existing tools countering hybrid threats, cyberattacks and foreign information manipulation and interference, existing EU tools will be unified under a broader **EU Hybrid Toolbox**. At the same time, the **EU Cyber Diplomacy Toolbox** will be strengthened, supporting to the JCU efforts in this domain.

As part of the initiatives aiming to reinforce the EU cybersecurity posture and boost resilience under the Strategic Compass,[65] it is worth mentioning the **EU Cyber Defence Policy,**[66] which encourages a coordinated effort in protecting, detecting, defending, and deterring cyberattacks, as well as the proposal for the **CSA** and the adoption of the **Cyber Resilience Act**.

Other specific actions within the cyber domain under the work strand, "invest in the capabilities and technologies needed", include the development and intensive use of new technologies, notably quantum computing, AI and Big Data. Investments in such fields should be supported by EU funding instruments, such as the EDF.

The EEAS is directing collective investments in defence innovation by combining civil, space, and defence research while developing new standards for next generation technologies. Therefore, a **Defence Innovation Hub** within the EDA, in partnership with the European Commission and in coordination with the European innovation Council and the EDF, has been established on 17 May 2022 under the name Hub for EU Defence Innovation (HEDI).[67] The HEDI works closely with the European Commission's **EU Defence Innovation Scheme** to support SMEs, start-ups, and research organisations to encourage the uptake of innovative solutions in defence domain. In February 2024 the Strategic Technologies for Europe Platform has been established, to further support the EU technological sovereignty and investments in critical technologies. Further actions have been undertaken under the **Observatory of critical technologies** for civil-defence-space industries to identify and prevent future gaps and dependencies and related risks.

In the end of 2022, building on the EU CDPF adopted on 18 November 2014 by the European Council and solicited by the Russia's military aggression against Ukraine, the **EU Policy on Cyber Defence** has been published. The Policy represents a further step towards the ambitious strategy drafted by the EU Cybersecurity Strategy for Defence and the Strategic Compass for Security and Defence. Its **four focus areas** reflect those outlined by the Strategic Compass and, in order to achieve its strategic ambition, the Policy will deploy initiatives such as the construction of an EU Cyber Defence Coordination Centre (EUCDCC) for

[65] European External Action Service. (2024, March). Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence. https://www.eeas.europa.eu/sites/default/files/documents/2024/StrategicCompass_2ndYear_Report_0.pdf#page=14&zoom=100,0,0

[66] High Representative of the Union for Foreign Affairs and Security Policy. (2022, November 10). Joint Communication to the European Parliament and the Council EU Policy on Cyber Defence. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022JC0049

[67] European Defence Agency. (n.d.). Hub for Eu Defence Innovation (HEDI). https://eda.europa.eu/what-we-do/research-technology/hedi

enhanced situational awareness and the establishment of an operational network for Military Computer Emergency Response Teams (milCERTs), the MICNET.

Furthermore, cooperation between civilian and military standardization bodies for the development of harmonised standards for dual-use products will be fostered and EU-NATO cooperation in cyber defence training, education, situational awareness and exercises will be strengthened. Finally, in terms of capability development, the Policy leads the way for a technology roadmap for critical cyber technologies for the EU to assess the level of dependencies, along with the development of Emerging Disruptive Technologies (EDTs) Strategic Assessment.

The EU CSA constitutes one more element of the Union's objective to establish EU cyber resilience capabilities, whilst concomitantly strengthening cooperation mechanisms. The text, approved by the Council on 2 December 2024, aims to support detection and awareness of significant or large-scale cybersecurity threats and incidents, bolster preparedness and solidarity at EU level through an EU-level cybersecurity reserve with services from trusted private providers, and contribute to a safe and secure digital landscape for citizens and businesses through testing of critical entities. The objectives will be implemented through the following actions:

- The deployment of a pan-European infrastructure of National Cyber Hubs, the **European Cybersecurity Alert System**, to build and enhance common detection and situational awareness capabilities;
- The creation of a **Cyber Emergency Mechanism** to support Member States in preparing for, responding to an immediate recovery from significant and large-scale cybersecurity incidents, gradually building an **EU Cybersecurity Reserve** with incident response services from trusted providers ready to intervene. Support for incident response shall also be made available to European institutions, bodies, offices and agencies of the Union (EUIBAs);
- The establishment of a **Cybersecurity Incident Review Mechanism** for the **European Union Agency for Cybersecurity** (**ENISA**) to review and assess specific significant or large-scale incidents.

Another step toward fostering cyber defence innovation has been taken with the establishment in 2019 of the **Cybersecurity Act,**[68] a framework for the certification of products, processes, and services. Building on the 2020 EU Cybersecurity Strategy and EU Security Union Strategy, further efforts in this field have led in 2024 to the adoption of the **Cyber Resilience Act** (**CRA**). The CRA aims to safeguard consumers and businesses buying products, both hardware and software, that are connected either directly or indirectly to another device or to a network, namely Products with Digital Elements (PDEs). In particular, CRA creates the conditions for the development of secure PDEs by introducing mandatory cybersecurity requirements for economic operators governing the planning, design, development, and maintenance of such products. The regulation aims to ensure that cybersecurity is taken into account throughout the entire supply chain and lifecycle of PDEs, as well as sets rules on market surveillance. While the CRA entered into force on 10 December 2024, the main obligations introduced by the CRA will apply from 11 December 2027. However, as stated by Art. 2, Par. 7 of the Regulation,[69] this set of controls and requirements do not apply to products

[68] EU Parliament, the Council of the EU. (2019, April 17). 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) https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

[69] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) https://eur-lex.europa.eu/eli/reg/2024/2847/oj

developed or modified exclusively for national security or defence purposes or to products specifically designed to process classified information.

Recent EU strategic efforts also include the **European Defence Industrial Strategy** (**EDIS**) presented in March 2024. The objective of the strategy is to enhance the defence industrial capacity by 2035, encouraging investment in the EDTIB and including initiatives such as the EUR 1.5 billion **European Defence Industry Programme** (**EDIP**). EDIP consists of a voluntary legal framework to boost Member States' cooperation on defence equipment.[70]

[70] European Parliament. Think Thank. (2024, 16 September). Briefing. European defence industrial strategy. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2024)762402

5. A GOVERNANCE PERSPECTIVE

Governance is Key to Enhancing the EU Cyber Defence Innovation Ecosystem, Streamlining Funding Mechanisms, and Strengthening Strategic Partnerships

Key Takeaways

- ### "CORE" AND "SUPPORTING" ORGANISATIONS WITHIN THE EU CYBER DEFENCE INNOVATION ECOSYSTEM

  The EU cyber defence innovation ecosystem is a diverse **network** of organisations with varying governance structures and roles. Collectively, these organisations promote and develop European defence R&D and cyber defence innovation. The ecosystem comprises two categories of organisations: "core" driving innovation through legislative, cooperative, and financial governance, and "supporting", facilitating the functioning of the overall ecosystem.

- ### HARMONISING EU FUNDING MECHANISMS AND STRENGTHENING STRATEGIC PARTNERSHIPS FOR MORE AND BETTER INNOVATION

  The EU policy framework has to be supported by sound **policy instruments** and strategic partnerships. In fact, funding and investment mechanisms, such as the Strategic Technologies for Europe Platform (STEP) initiative, are critical for supporting R&D, enhancing capabilities, and facilitating cross-border cooperation, particularly for SMEs. Moreover, the EU has to reinforce its multifaceted **cooperation** with NATO through structured dialogues, joint exercises, and information-sharing frameworks to bolster cyber defence innovation.

This paragraph provides a high-level overview[71] of the EU's institutions, agencies, and entities that comprise the European cyber defence innovation ecosystem. The paragraph also illustrates the funding mechanisms sustaining cyber defence innovation efforts at both European and Member States' levels, as well as the EU's role as a global actor engaging with strategic partners to foster cyber defence innovation. The EU governance landscape is characterised by fragmentation; by analysing key EU stakeholders involved in cyber defence and existing cooperation initiatives, the text highlights the necessity for the EU to promote strong mandates to advance coherent cyber defence programs. The analysis demonstrates that collaboration among stakeholders from academia, public institutions, private industry, and civil society will drive innovation more effectively and profitably. The reduction of barriers to entry in the defence market and the extension of investment programmes are identified as key activities. Finally, the EU-NATO and EU-UK dialogue will help achieve stable, well-coordinated, and secure cyber defence.

[71] The analysis is a non-exhaustive mapping of the key European institutions, entities, and agencies that are shaping the European cyber defence innovation landscape.

5.1. The EU Cyber Defence Innovation Ecosystem: Core and Supporting Entities

The Union's cyber defence innovation ecosystem encompasses multiple organisations that play a distinct role in promoting and developing European defence R&D and, more specifically, its subcategory, defence Research & Technology (R&T).

The EU cyber defence innovation ecosystem can be categorized into two distinct groups of organisations. The first category comprises **"core" organisations** that drive cyber defence innovation through different kinds of governance: "legislative", "cooperation" and "financial" modes.[72] The second one includes **"supporting"** or **"enabling" organisations** that contribute to the EU's overall cyber defence innovation ecosystem.

CORE ENTITIES

Among the entities characterized by a "legislative mode" governance, at the core there is the European Commission.[73] The European Commission plays a pivotal role in shaping the EU's legislative landscape. Particularly, in the following domains, it:

- proposes and enforces relevant **legislation** on cybersecurity, cyber defence and innovation issues;
- coordinates and establishes **investment platforms** and **programs** for cyber defence innovation to foster economic growth and competitiveness;
- promotes **Public-Private Partnerships** (PPPs) and **cooperation** between Member States and EU institutions to build a European Defence Union.

To further bolster defence innovation within the EU, the European Commission's Directorate-General for Defence Industry and Space (DG DEFIS) has adopted and oversees a dedicated instrument, the EU Defence Innovation Scheme (EUDIS). The EUDIS aims to reduce barriers to entry for SMEs in the defence sector.

Another key organisation in the field of cyber defence innovation is the EEAS. The EEAS, established on July 8, 2010, prioritizes peace, security, and defence of the EU in its agenda. As highlighted in paragraph *4.1 Towards a Harmonised EU Regulatory Framework for Cyber* (Defence) Innovation, the EEA directs its efforts toward the implementation of the **Strategic Compass for Security and Defence** and the **EU Cybersecurity Strategy**. On the other hand, a key structure with a "coordination mode" governance established on July 12, 2004, under the CSDP to enable the European Union to act as a global security actor, is the **EDA.**[74] The EDA's primary function is to facilitate coordination among Member States on security and defence issues, including cyber defence innovation. Specifically, the EDA:

- assists Member States in developing and improving their defence capabilities and stimulating defence R&T to strengthen the European defence industry;
- facilitates the development of capabilities that underpin the Common Security and Defence Policy of the Union;

[72] Helwig , N. and Iso-Markku, T. (2024, July). The EU's different modes of defense governance: More European defense, but how?, *CESifo*. https://www.cesifo.org/en/publications/2024/article-journal/eu-different-modes-defense-governance

[73] European Commission. (2024). Commission's Priorities. https://commission.europa.eu/priorities-2024-2029_en

[74] European Defence Agency. (n.d.). Cyber. https://eda.europa.eu/what-we-do/capability-development/cyber

- supports EU cooperation by creating coherence between the Cyber activities of the EDA, the ENISA, the Computer Emergency Response Team for the EU institutions (CERT-EU), and the European Cyber Crime Centre (EC3)/Europol.

Additionally, since 2022, the **HEDI**[75] has been established within the EDA to provide Member States with a platform to stimulate and facilitate cooperation on defence innovation, ensuring synergies with the European Commission and coherence with NATO innovation initiatives.

Finally, the **"financial mode"** governance group of entities includes funding initiatives such as the **EDF** in 2017, and the **EDIP** proposed by the Commission meant to add another EUR 1.5 billion to use for common procurement as well as for defence industrial initiatives.

SUPPORTING ENTITIES

"**Supporting**" or "**enabling**" actors comprise various entities of different nature that contribute to the EU's cyber defence innovation initiatives and overall ecosystem. Among them are the European Computer Emergency Response Teams, such as **CERT-EU**, established to support and enhance the security of the European Union's digital infrastructure, as well as **MilCERT**, specialized units within military organizations responsible for handling cybersecurity incidents and threats affecting military networks and systems. EU **Member States** and their **National Cybersecurity Agencies** are responsible for developing and implementing national cybersecurity strategies, coordinating responses to cyber threats, and enhancing the overall cybersecurity posture within their respective countries. The **industry** and **private sector**, represented by companies and organizations, as well as start-ups, contribute to cyber defence through innovation, development of cybersecurity technologies, and collaboration with public sector entities to share threat intelligence and best practices. **Research institutions**, **accelerators**, and **universities** drive innovation through research and development in cyber defence, provide education and training to build a skilled workforce, and foster collaboration between academia, industry, and government to advance cyber defence capabilities. Lastly, **international organizations**, such as NATO, work collaboratively with the EU to address cyber threats and share intelligence to enhance global cyber defence.

5.2. Bolstering EU Cyber Defence Innovation through Funding

As previously outlined in paragraph **4. A POLICY PERSPECTIVE**, the EU has developed numerous strategies, frameworks, and initiatives targeting innovation and cyber defence. To ensure the effective implementation of these strategies and the ultimate benefit they will provide to the EU and its Member States, the establishment of sound funding mechanisms to support stakeholders are required. To this end, the EU has established several funding programs to sustain efforts in this domain.

A first funding mechanism is represented by the European Investment Bank (EIB). Even though defence is not the main focus of EIB, the organisation has decided to double its investments in this sector, doubling investments from EUR 1 billion to EUR 2 billion by 2025, potentially benefitting cyber defence innovation initiatives. Relevantly, such investments are not expected to target purely military projects as they are excluded from the current lending policy of EIB.[76]

[75] European Defence Agency. (n.d.). Hub for Eu Defence Innovation (HEDI). https://eda.europa.eu/what-we-do/research-technology/hedi

[76] Soler. P. (2025, January 30). European Investment Bank to invest €95bn in 2025, but only €2bn for defence. *Euronews*. https://www.euronews.com/my-europe/2025/01/30/european-investment-bank-to-invest-95bn-in-2025-but-only-2bn-for-defence

A first example is the **Multiannual Financial Framework (MFF),**[77] which encompasses the EU's **long-term budget** and ensures that EU expenditures are aligned with its resources over a period of at least five years. Long-term budgets benefit projects and programs by providing solid, future-proof funding structures enabling R&D efforts.

Just before reaching its midpoint,[78] the sixth MFF (2021–2027) has been subject to its first-ever revision, which was presented on June 20, 2023, by the European Commission, endorsed by EU leaders on February 1, 2024, and approved by the EU Parliament on February 27, 2024. The strategic importance of sustaining EU defence and innovation is reflected by changes applied to the MFF. On the one hand, the budget allocated to the modernization of the EU through research and innovation, fair climate and digital transitions, preparedness, recovery, and resilience exceeds 50% of the total amount of the long-term budget.[79] On the other hand, the revision included a proposal, adopted by the European Commission in 2024, for a **regulation** establishing a **Strategic Technologies for Europe Platform** (**STEP**)[80] to maintain a European edge over critical and emerging technologies.

The STEP initiative entails an additional allocation of EUR 1.5 billion for defence investments.[81] The primary objective of the initiative is to mobilize and allocate funding across a total of 11 EU programs,[82] targeting investments in the following domains:

- digital technologies and deep-tech innovation (e.g., microelectronics, quantum computing, AI);
- clean and resource-efficient technologies;
- biotechnologies and biomanufacturing.

A distinctive trait of STEP consists of the requirements set to access funding. Specifically, the proposed technologies need to meet at least one of the following criteria. First, the proposed technologies have to have innovative elements, namely "bring to the internal market an innovative, emerging, and cutting-edge element with significant economic potential."[83] Secondly, they have to reduce EU strategic dependencies.

In contrast with other EU funding programs, such as Horizon Europe, which target civilian projects, STEP does not preclude interdependencies and exchanges between civilian and military technologies. As many projects encompassing innovative, emerging, and cutting-edge elements have dual-use potential, STEP could enable progress in cyber defence. Furthermore, STEP criteria reflect the EU's intention to foster innovation while responding to the impending need for a strengthened EU industrial base and EU-developed technologies.

[77] EU Parliament. (n.d.) Fact Sheets on the European Union. Multiannual financial framework. https://www.europarl.europa.eu/factsheets/en/sheet/29/multiannual-financial-framework

[78] EU Commission. (n.d.) 2021-2027 long-term EU budget & NextGenerationEU. https://commission.europa.eu/strategy-and-policy/eu-budget/long-term-eu-budget/2021-2027_en

[79] Ibid

[80] EU. (2024, February 29). Regulation (EU) 2024/795 of the European Parliament and of the Council of 29 February 2024 establishing the Strategic Technologies for Europe Platform (STEP), and amending Directive 2003/87/EC and Regulations (EU) 2021/1058, (EU) 2021/1056, (EU) 2021/1057, (EU) No 1303/2013, (EU) No 223/2014, (EU) 2021/1060, (EU) 2021/523, (EU) 2021/695, (EU) 2021/697 and (EU) 2021/241. https://eur-lex.europa.eu/eli/reg/2024/795/oj/eng

[81] EEAS. (2024, March). ANNUAL PROGRESS REPORT on the Implementation of the Strategic Compass for Security and Defence https://www.eeas.europa.eu/sites/default/files/documents/2024/StrategicCompass_2ndYear_Report_0.pdf

[82] Refer to paragraph 5.2 a detailed overview of such mechanisms.

[83] EU. (2024, May 13). About the Strategic Technologies for Europe Platform (STEP). https://strategic-technologies.europa.eu/about_en

Considering innovation in the defence sector, another European Commission’s funding instrument is the EDF.[84] Entirely dedicated to R&D in defence, the EDF supports companies in Member States, including SMEs, in developing innovative and interoperable defence technologies and equipment through competitive and collaborative projects. The European Commission directly implements the EDF, with possible delegation to entrusted entities, and collaborates closely with Member States representatives (i.e., the Network of European Defence Fund National Focal Points, NFPs), the EDA, and the EEAS. NFPs support the implementation of the EDF by advising applicants on administrative procedures, as well as facilitating partnerships among stakeholders operating in different Member States.

With a budget of nearly **EUR 8 billion** established by the **MFF 2021-2027**, the **EDF** allocates **EUR 2.7 billion** for **collaborative defence research** and **EUR 5.3 billion** for **collaborative capability development projects**. Despite these economic efforts, it is worth noticing that the funding allocated to the EDF dropped from EUR 13 billion to EUR 8 billion during the budget negotiations, possibly impacting the scope and effectiveness of selected projects.

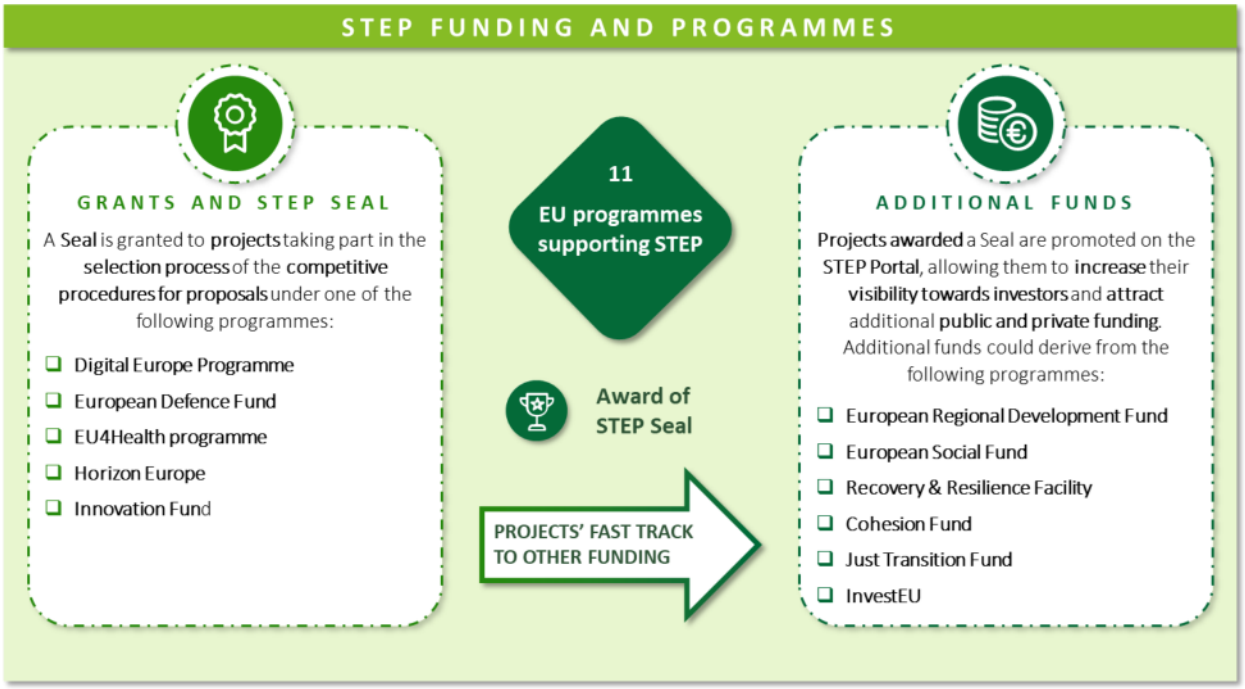
Implemented via annual work programs structured into 34 categories (i.e., including cyber), the EDF aligns with the Union's security and defence interests, the CSDP,[85] and the Capability Development Plan (CDP).[86] Moreover, the EDF considers regional and international priorities, such as those expressed by NATO. On 30 January 2025, the European Commission adopted the fifth annual Work Program under the EDF,[87] with more than **EUR 1 billion** allocated to **defence collaborative R&D** projects. Cyber R&D, together with naval combat, underwater warfare, simulation and training, and advanced passive and active sensors, is set to receive around EUR 40 million under the announced annual Work Program.

[84] European Commission. (n.d.) EDF | Developing tomorrow's defence capabilities. https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en

[85] EEAS. The Common Security and Defence Policy. https://www.eeas.europa.eu/eeas/common-security-and-defence-policy_en

[86] EDA. EU Capability Development Plan. https://eda.europa.eu/what-we-do/all-activities/activities-search/capability-development-plan

[87] EU Commission. (2025, January 30). More than €1 billion from the European Defence Fund to develop next generation defence technologies and innovation. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_376



STEP FUNDING AND PROGRAMMES

GRANTS AND STEP SEAL

A **Seal** is granted to **projects** taking part in the **selection process** of the **competitive procedures for proposals** under one of the following programmes:

- □ Digital Europe Programme
- □ European Defence Fund
- □ EU4Health programme
- □ Horizon Europe
- □ Innovation Fund

11 EU programmes supporting STEP

Award of STEP Seal

PROJECTS' FAST TRACK TO OTHER FUNDING

ADDITIONAL FUNDS

Projects awarded a Seal are promoted on the **STEP Portal**, allowing them to **increase** their **visibility towards investors** and **attract** additional **public and private funding**. Additional funds could derive from the following programmes:

- □ European Regional Development Fund
- □ European Social Fund
- □ Recovery & Resilience Facility
- □ Cohesion Fund
- □ Just Transition Fund
- □ InvestEU

Figure 3 Step Funding and Programmes

As the EU has established mechanisms to facilitate synergies among funding programs, an increase of the EDF is expected to impact STEP, which will support projects aimed at enhancing the skills required to develop and manufacture critical technologies, safeguarding and strengthening their value chains.

Among the EDF instruments, the EUDIS explicitly aims to reinforce defence innovation in the EU[88] by reducing entry barriers into the defence domain for SMEs and supporting them in accessing the EDF. Managed by the DG DEFIS, the EUDIS is mainly **funded** by **EDF** (around **EUR 1.46 billion**) but also gathers funding from other public and private sources (around **EUR 400-500 million**). Among its key features, EUDIS supports SMEs in migrating their innovation from the civil to the defence domain, facilitates access to private funding (e.g., venture capital and private equity funds), and enters SMEs into thematic innovation hubs.[89] The focus on SMEs is relevant as, according to EU official estimates,[90] about **2,500 SMEs operate** in the **defence industry** across the EU and play a key role in defence **supply chains**. Nevertheless, such supply chains are often limited to national borders, making cross-border cooperation complicated even among EU Member States. Hence, there is a need for programs supporting SMEs and encouraging cross-border cooperation. Considering their goals, EUDIS and the EDF can play a role in these domains.

The EU funding programs targeting defence are not limited to European Commission-led initiatives. An example is represented by HEDI, managed by EDA. Although **HEDI funding** (around **EUR 60k per year**) is not comparable to those of the EDF and EUDIS, it allocates economic resources for defence innovation prizes,

[88] EU. (n.d.). EU Defence Innovation Scheme (EUDIS). https://eudis.europa.eu/index_en

[89] EUDIS. (2024). Factsheet. https://eudis.europa.eu/document/download/3d382c48-1dec-4de0-97bf-15bbabea7024_en?filename=20240312%20-%20EUDIS%20factsheet%20v11.pdf

[90] EU Commission(n.d.). Defence SMEs. https://defence-industry-space.ec.europa.eu/eu-defence-industry/defence-smes_en

proof-of-concept of innovative ideas, and other initiatives aimed at promoting and encouraging defence[91] rather than directly supporting projects throughout their whole lifecycle.

The existence of funding mechanisms supporting innovation reflects the EU political will to support Member States and businesses investing in defence innovation. Nevertheless, the issue of defence within the EU is not merely political. Instead, it lies in transforming such political will into action and tangible results. Questions regarding the sufficiency of the budget, coordination among funding mechanisms, and the willingness of Member States to cooperate are open and will define the success or failure of European efforts in cyber defence innovation.

5.3. Engaging in Cyber Defence Innovation through Cooperation

In addition to its legislative framework and funding programs, the EU, in its capacity as a global player, engages with strategic partners to foster cyber defence innovation. The EU-NATO cooperation serves as a case in point. From structured dialogues to joint cyber defence exercises, the EU-NATO cooperation is multifaceted and encompasses crisis management, capability development, and defence against hybrid threats,[92] including cyber.

In this regard, the EU and NATO launched their first **Structured Dialogue on Cyber**[93] in October 2024, with the aim to enhancing cooperation on cybersecurity and cyber defence. A second meeting has been scheduled for 2025. The 2024 Dialogue focused on the enhancement of coordination to bolster the two organisations' capacity to detect, deter, and defend against cyberattacks, with a particular focus on enhancing cyber resilience and protection of critical infrastructures, as well as effective cyber crisis

[91] Möhring, J. (2024, September 23). EUDIS, HEDI, DIANA What's Behind Three Defence Innovation Acronyms?. Security Studies Centre. https://www.ifri.org/en/memos/eudis-hedi-diana-whats-behind-three-defence-innovation-acronyms

[92] NATO. (2024, December 3). Relations with the European Union. https://www.nato.int/cps/in/natohq/topics_49217.htm

[93] EEAS. (2024, October 4). European Union and NATO hold the first Structured Dialogue on Cyber. https://www.eeas.europa.eu/eeas/european-union-and-nato-hold-first-structured-dialogue-cyber-0_en

management. Notably, opportunities to align the EU and NATO's respective cyber defence frameworks and instruments were part of the discussions, indicating the possibility of further cooperation in this domain.

The EU and NATO are also involved on a series of pragmatic initiatives and projects targeting cyber defence. For instance, their collaboration encompasses training, research, exercises, and frameworks for information sharing. With regard to exercises, the EU and NATO participate in the cyber defence exercises organized by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). The CCDCOE employs an interdisciplinary approach to cyber defence, encompassing areas such as technology, operations, strategy, and law.[94] Differently, the **Technical Arrangement on Cyber Defence** between the NATO Cyber Security Centre and the CERT-EU consists of a framework for the sharing of information and best practices.[95]

In addition to cooperative mechanisms fostering cybersecurity and cyber defence, NATO is equipped with its own programs to support innovation. A notable example is the **NATO Defence Innovation Accelerator for the North Atlantic** (**DIANA**), whose mission is to identify and develop dual-use, deep-tech solutions and accelerate dual-use innovation capacity across the Alliance by providing support to innovators and their ideas from the early stages to maturity.[96] This mission highlights the significance of synergies between the civilian and military innovation spheres, a synergy whose relevance is increasingly clear also to the EU.

DIANA's governance widely differs from the traditional EU initiatives and funding mechanisms. While the EDF and EUDIS are directly managed by EU institutions, bodies, and agencies, DIANA constitutes a separate NATO entity with a separate legal and financial framework overseen by a board with members from academia, the private sector, or the government of NATO Member States.[97] Furthermore, DIANA is also funded by the **NATO Innovation Fund** (**NIF**), a separate venture capital where Member States can invest. As dual-use technologies are the main focus of DIANA, its managing team is composed of civilian and military experts.

In order to facilitate the development of an effective cyber defence innovation strategy, the EU needs to strengthen its programs and collaboration with external stakeholders while taking inspiration from other models, even beyond its borders. Nevertheless, considering that cooperation in cyber defence innovation means cooperation in a strategic and critical sector, the EU needs to cultivate its relations conscious of the current volatile geopolitical context. In spite of these shared initiatives, the EU and NATO relations will strongly depend on the convergence of their strategic interests and agreement among their Member States over the next few years. Therefore, while keeping NATO as a strategic partner and continuing its efforts to strengthen their collaboration, the 2024-29 European Commission aims to build a European Defence Union. Thus, a relation of cooperation and not dependency could be the one pursued by the EU[98]: open to shared initiatives but capable of ideating, developing, and deploying its own cyber defence solutions.

[94] CCDCOE. About us. https://ccdcoe.org/

[95] NATO. (2024, July 30) Cyber Defence. https://www.nato.int/cps/en/natohq/topics_78170.htm#:~:text=The%20Technical%20Arrangement%20on%20Cyber,information%20and%20sharing%20best%20practices

[96] DIANA. (n.d.). About. https://www.diana.nato.int/about-diana.html

[97] Möhring, J. (2024, September 23). EUDIS, HEDI, DIANA What's Behind Three Defence Innovation Acronyms?. Security Studies Centre. https://www.ifri.org/en/memos/eudis-hedi-diana-whats-behind-three-defence-innovation-acronyms

[98] European Commission. (2024). A new era for European Security and Defence. https://commission.europa.eu/priorities-2024-2029/security-and-defence_en

6. A CAPABILITY PERSPECTIVE

Deloitte.

EU National Cyber Defence Innovation Use Cases

Key Takeaways

- FINLAND'S CENTRALIZED APPROACH

  Finland's robust cyber innovation ecosystem is **government-led**, with initiatives like the National Cyber Strategy and Defence Innovation Network Finland (DEFINE)[99] promoting cooperation and development in emerging technologies.

- ESTONIA'S MARKET-ORIENTED STRATEGY

  Estonia's defence innovation is **driven** by **industry** and **supported** by the **Ministry of Defence** (MoD),[100] with initiatives like the Research and Innovation Policy and the Defence and Security Industry Innovation Cluster.

- FRANCE'S CENTRALIZED GOVERNANCE MODEL

  France's cyber defence innovation is **led** by the **Minister of Defence**, supported by strong governance structures, and substantial investments in AI and emerging technologies, exemplified by the Future Combat Air System (FCAS) program.[101]

The EU context is being influenced and influences the cyber defence innovation posture of Member States. In order to gain a better understanding of the cyber defence innovation capabilities deployed by Member States, this paragraph will focus on specific use cases of three (3) European countries.

6.1. Use Cases Methodology

The strategic benchmarking analysis aims to compare best practices among a panel of countries, in order to identify areas of improvement across different areas and sub-areas.

PANEL SELECTION

The identification of these countries has been achieved through the implementation of a set of criteria. The primary criterion adopted pertains to the identification of twelve (12) Member States that have the highest innovation performance among the EU innovation landscape through the European Innovation Scoreboard (EIS).[102] The innovation performance score of each country, also called the summary innovation index (SII), is calculated based on 32 indicators capturing a broad range of activities and factors related to innovation. The innovation ranking is divided in four groups, each country is assigned to a performance group based on its innovation performance relative to the EU average in 2024. The first group encompasses the **Innovation Leaders**, whose innovation score is greater than 125% of the EU average. The second group includes the **Strong Innovators**, or countries that have an innovation score between 100% and 125% of the EU average in 2024. The third group is composed by **Moderate Innovators**, whose innovation score is between 70% and 100% of the EU average. Lastly, the fourth group encompasses the **Emerging Innovators**, or countries with

[99] DEFINE. (n.d.). What is DEFINE? https://www.definefinland.fi/en/what-is-define/

[100] Republic of Estonia. Ministry of Defence. (n.d.). Homepage. https://www.kaitseministeerium.ee/en

[101] Airbus. (2023, 20 November). Future Combat Air System (FCAS) - Enter the Internet of Military Things. https://www.airbus.com/en/newsroom/stories/2023-11-future-combat-air-system-fcas-enter-the-internet-of-military-things

[102] European Commission. (n.d.). European Innovation Scoreboard. https://projects.research-and-innovation.ec.europa.eu/en/statistics/performance-indicators/european-innovation-scoreboard/eis-2024#/eis

an innovation score below 70% of the EU average. In order to select the Member States that demonstrated the highest performance in the field, the Innovation Leaders, encompassing four (4) countries, and the Strong Innovators, encompassing eight (8) countries, groups have been considered.

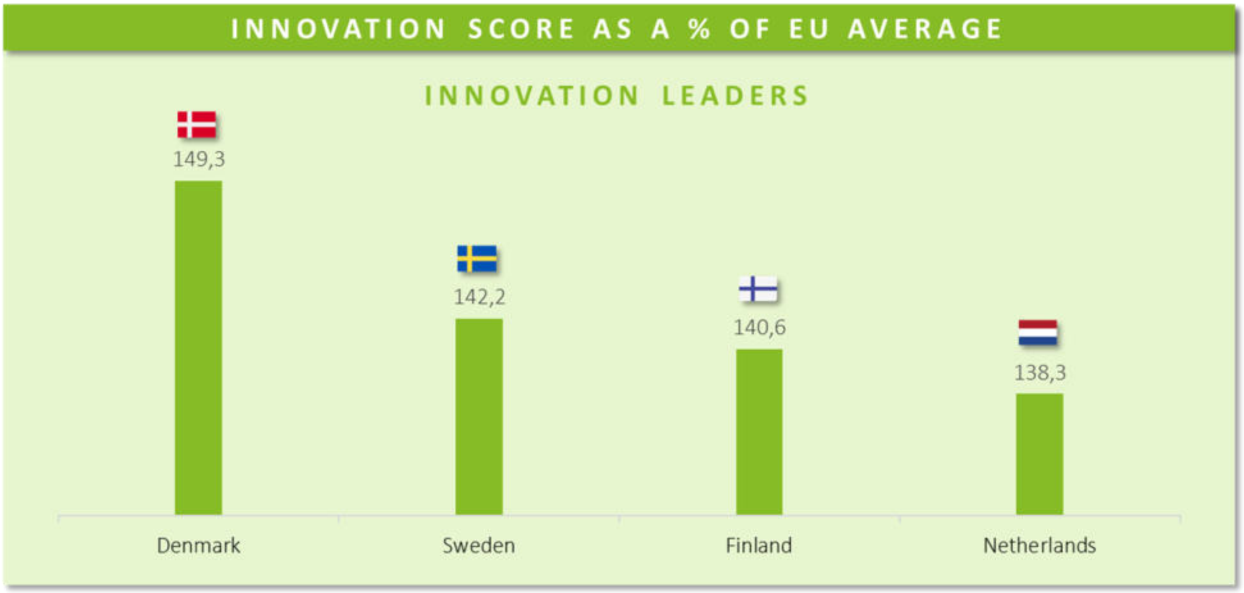


Figure 4 First criterion adopted for the panel selection (Part 1)

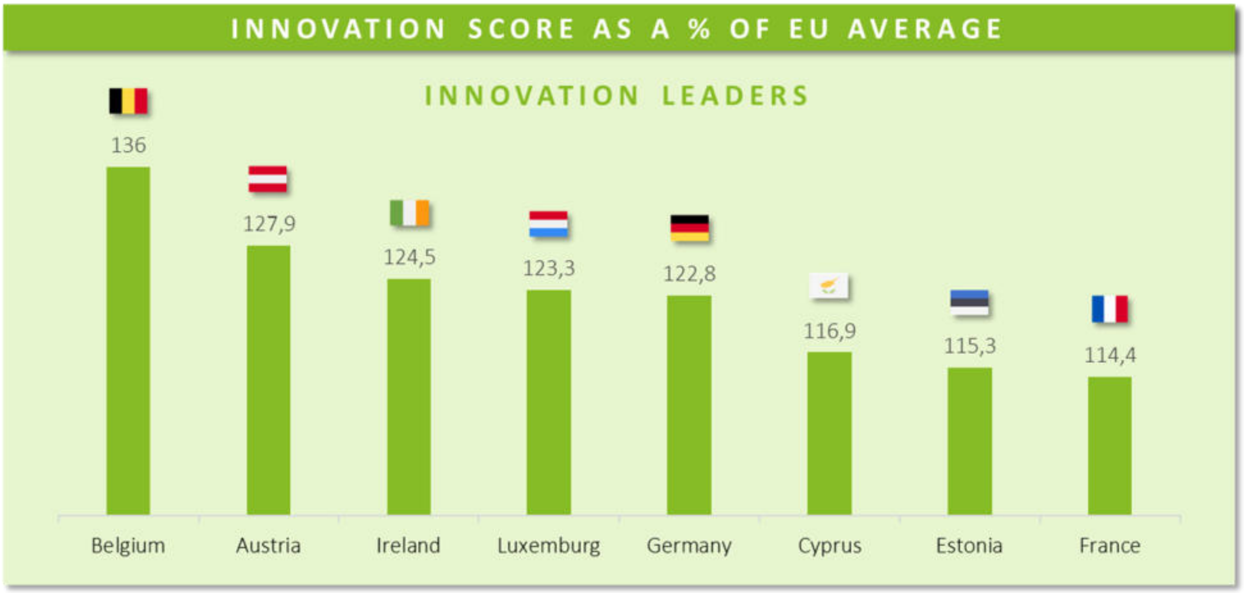


Figure 5 First criterion adopted for the panel selection (Part 2)

Whilst the current iteration of the EIS captures the overall innovation performance of Member States, it does not provide an in-depth analysis of innovation performance across diverse industry sectors, resulting in an incomplete representation of national innovation capabilities. For instance, countries that rank highly on the EIS may not necessarily excel in the defence and security sectors. It is imperative that this limitation is addressed in order to develop more targeted and effective innovation policies that leverage regional strengths and foster sector-specific advancements.

In order to address this shortcoming, in the context of the present analysis, an additional criterion for the selection of the panel has been adopted. The second criterion regard the identification of three (3) States to be considered as use cases by **cross-checking** data from the **EIS** and the **Military expenditure** as a percentage of GDP developed by Stockholm International Peace Research Institute (SIPRI)[103] and adopted by the World Bank.[104] The following data refer to 2023, the latest measurement available.

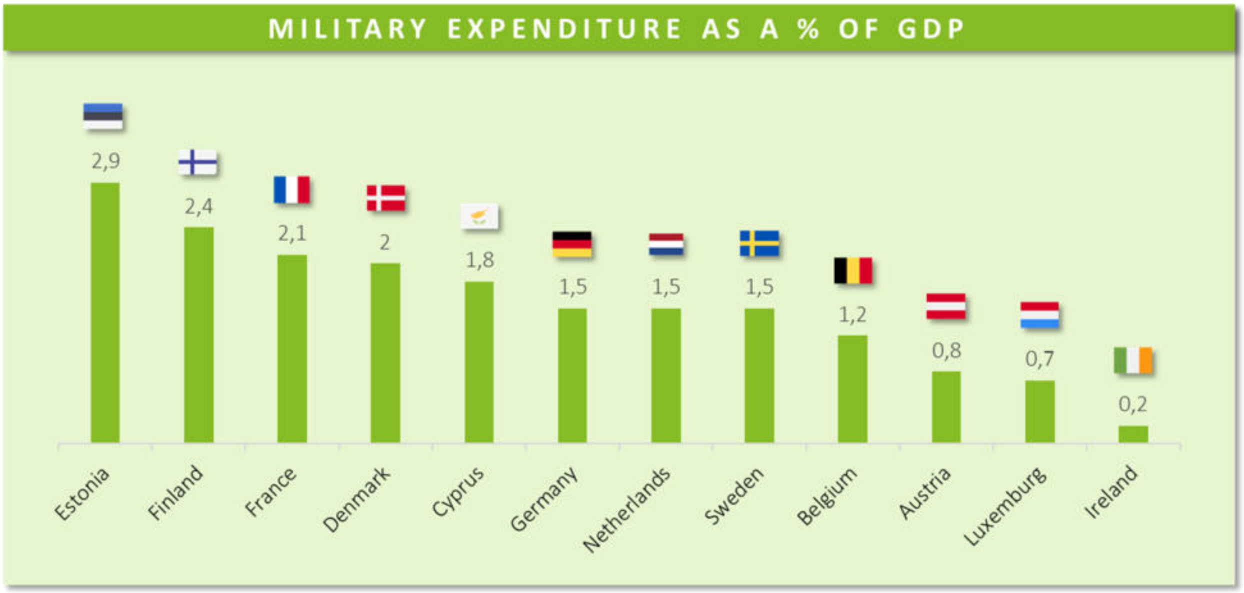


Figure 6 Second criterion adopted for panel selection

Therefore, the resulting countries for the benchmarking analysis are Finland, Estonia, and France.

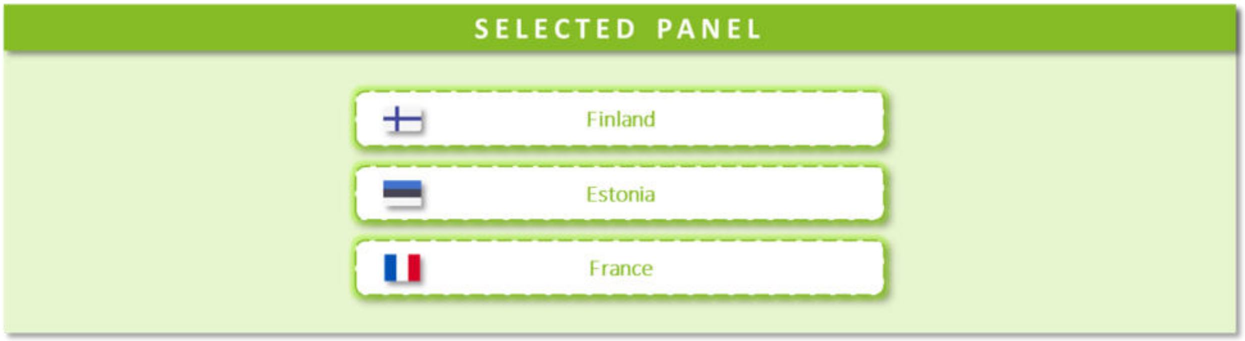


Figure 7 Selected panel

AREAS OF ANALYSIS

The analysis has been conducted on Finland, Estonia, and France considering three (3) different areas.

[103] SIPRI. (n.d.) Military Expenditure Database. https://www.sipri.org/databases/milex

[104] World Bank. (n.d.) Military expenditure (% of GDP). https://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS

- A **Governance Perspective** is comprised of three (3) sub-areas:
  - **national ecosystem**, which includes government, private sector, academia and civil society entities dealing with cyber defence innovation;
  - **funding**, which includes an analysis of financial resources allocated for cyber defence innovation; and
  - **cooperation**, which includes an examination of collaborative efforts between various stakeholders of the national ecosystem, both domestically and internationally, to enhance cyber defence capabilities;
- A **Policy Perspective** encompasses an overview of the national regulatory landscape around cyber defence innovation;
- Finally, a **Technology Perspective** encompasses an overview of the main national cyber defence innovation objectives and how they are implemented.

Flagship initiatives have been identified under the area of analysis as they might be applicable at the EU-level to solve gaps, redundancies, and inefficiencies.

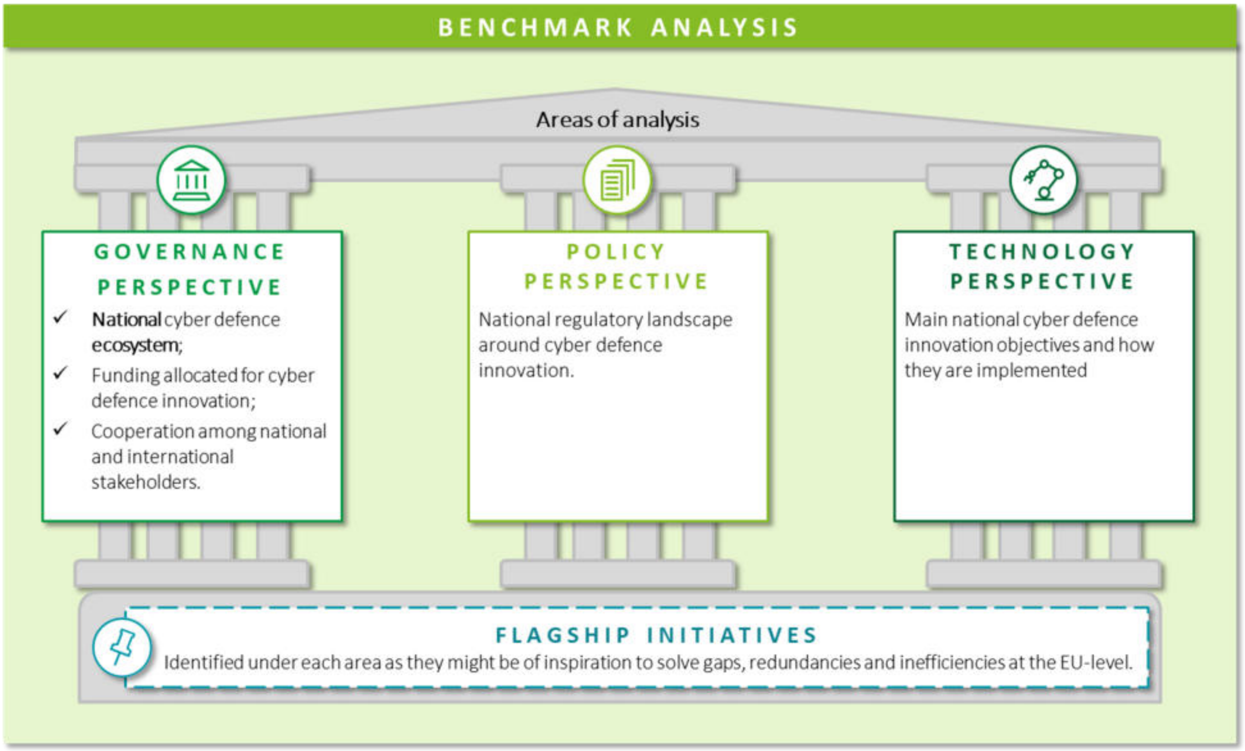

BENCHMARK ANALYSIS
Areas of analysis
GOVERNANCE PERSPECTIVE
✓ National cyber defence ecosystem;
✓ Funding allocated for cyber defence innovation;
✓ Cooperation among national and international stakeholders.
POLICY PERSPECTIVE
National regulatory landscape around cyber defence innovation.
TECHNOLOGY PERSPECTIVE
Main national cyber defence innovation objectives and how they are implemented
FLAGSHIP INITIATIVES
Identified under each area as they might be of inspiration to solve gaps, redundancies and inefficiencies at the EU-level.

Figure 8 Areas of analysis

6.2. Use Cases Key Results

This section provides an overview of the main outcomes of the benchmarking analysis regarding cyber defence innovation practices in Finland, Estonia, and France. The objective is to discuss insights and **best practices** from the three (3) countries of the panel.

6.2.1. Use Case 1: Finland

Finland's Robust Cyber Innovation Ecosystem Centralized and Government-Led

Finland, the first country analysed for the purpose of this paper, is considered as an Innovation Leader by the EIS, and has a **military expenditure** that amounts to **2.4% of its total GDP**, as per **SIPRI**[105] data from 2023.

Finland's approach for cyber defence and technological innovation stands out as effective, primarily due to its comprehensive **National Cyber Strategy 2024-2035**.[106] This strategy, as a political commitment, integrates the concept of cyber defence alongside cybersecurity, recognizing cyber defence as a crucial component and distinguishing between the two. Given the acknowledgement of cyber defence and the strong commitment to R&D, Finland is able to promote cooperation and development in emerging and disruptive technologies in the field of cyber defence.

A key initiative, the DEFINE,[107] highlights Finland's effort in cooperating and advancing innovation in cyber defence and dual-use technologies. DEFINE acts as a hub for defence and security innovation, uniting government entities, funding initiatives, military experts, leading companies, research institutions, and startups. The **Riihimäki area** is notable for its strategic focus on high-level defence and security industry networks, creating a unique ecosystem for developing cutting-edge solutions. **DEFINE's accelerator program**[108] supports the development of advanced technologies, including AI, cybersecurity, and autonomous systems, addressing both military and commercial market needs.

Focus on DEFINE[109]

The DEFINE[110] is an initiative that underscores Finland's commitment to advancing innovation in cyber defence and dual-use technologies. It serves as a hub for defence and security innovation, leveraging the unique ecosystem of the Riihimäki area. In particular, DEFINE's three (3) months accelerator program[111] actively supports the development of advanced technologies by providing resources, mentorship, and connections to enter global markets. DEFINE enhances Finland's cyber defence capabilities and technological sovereignty, positioning the country as a ***leader in cyber defence innovation*** *within the EU and NATO.*

[105] SIPRI. (n.d.). Military Expenditure Database. https://www.sipri.org/databases/milex

[106] Prime Minister's Office. (2024). Finland's Cyber Security Strategy 2024–2035. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165893/VNK_2024_13.pdf?sequence=1&isAllowed=y

[107] DEFINE. (n.d.). What is DEFINE? https://www.definefinland.fi/en/what-is-define/

[108] DEFINE. (n.d.). DEFINE Accelerator backed by Redstone. https://www.definefinland.fi/en/define-accelerator/

[109] DEFINE. (n.d.). What is DEFINE? https://www.definefinland.fi/en/what-is-define/

[110] Ibidem

[111] DEFINE. (n.d.). DEFINE Accelerator backed by Redstone. https://www.definefinland.fi/en/define-accelerator/

6.2.2. Use Case 2: Estonia

Estonia's Market-Oriented Defence Innovation Driven by Industry and Supported by the MoD

Estonia, the second country analysed for the purpose of this paper is considered as a Strong Innovator by the EIS and has a **military expenditure** that amounts to **2.9% of its total GDP**, as per **SIPRI**[112] data from 2023. This percentage is the **highest** recorded among the selected **panel**.

The strong collaboration between the MoD[113] and R&D sector and research institutes to bolster national defence outlines Estonia's successful approach to cyber defence and technological innovation. The **Research and Innovation Policy 2022**[114] published by the Estonian MoD encompasses several strategic objectives: implementing research and innovation policies to achieve governance goals, focusing R&D activities on developing advanced technologies and integrating prototypes into military units, and supporting the sustainability of Military Sciences through collaborative R&D projects with universities and research institutions. Additionally, the policy aims to provide a platform for international activities by establishing centres of excellence in cyber and electronic warfare, participating in EU, and NATO research cooperation initiatives to enhance R&D and innovation in the defence industry.

A notable outcome of this synergy is the **Estonian Defence and Security Industry Innovation Cluster**,[115] which acts as a facilitator and network for international cooperation and export. This cluster enhances collaboration between Estonian companies, R&D institutions, and clients, promoting innovation in the defence and security industry and developing new, highly competitive products. Estonia's integrated approach ensures that it remains a leader in cyber defence and technological advancement.

Focus on Estonian Defence and Security Industry Innovation Cluster[116]

*The Estonian Defence and Security Industry Innovation Cluster[117] is a key component of Estonia's cyber defence strategy, fostering innovation through collaboration among academic institutions, research labs, SMEs, large industries, and public organisations. The cluster enhances Estonia's capability to develop advanced cybersecurity solutions focusing on areas such as **drones**, **autonomous unmanned ground vehicles**, **IT cyber-digital solutions**, and **AI-assisted software**. It is closely linked with European initiatives, and NATO's objectives as well. Specifically, considering Estonia's **involvement** in the **NATO CCDCOE** in Tallinn, the Cluster serves to support and strengthen knowledge exchange and innovation within the alliance.*

[112] SIPRI. (n.d.). Military Expenditure Database. https://www.sipri.org/databases/milex
[113] Republic of Estonia. Ministry of Defence. (n.d.). Homepage. https://www.kaitseministeerium.ee/en
[114] Republic of Estonia. Ministry of Defence. (2022). Research and Innovation Policy in the Ministry of Defence’s Field of Governance. https://www.ksk.edu.ee/en/files/2024/03/Research-and-Innovation-Policy-of-the-Ministry-of-Defence-Field-of-Governance-1.pdf
[115] Estonian Defence and Aerospace Industry Association. (n.d.). About Cluster. https://defence.ee/cluster-and-members/
[116] Ibidem
[117] Ibidem

6.2.3. Use Case 3: France

France's Centralized Cybersecurity and Cyber Defence Governance Model Led by the MoD

France, the third country analysed for the purpose of this article is considered as a Strong Innovator by the EIS and has a **military expenditure** that amounts to **2.1% of its total GDP**, as per **SIPRI**[118] data from 2023.

French innovation in cyber defence is eased by a robust governance structure that integrates efforts from both the public and private sectors, aligning with France's highly centralized political framework. In June 2023, the French National Assembly passed the **2024-2030 military programming bill**,[119] which includes four articles that enhance the **prerogatives** of **ANSSI**,[120] the French cybersecurity agency, to respond to severe cyber threats by developing a leading cyber defence, supported by **EUR 4 billion** in funding. The bill acknowledges the importance of technological advances and innovation, recognizing the synergies between government and external entities such as innovative companies, universities, and research institutes, and allocates **EUR 10 billion** for innovation. Consequently, France has a well-defined implementation of its goals and strategies through projects specializing in emerging technologies. One notable example is the **FCAS Program**,[121] which, in collaboration with Germany and Spain, designs an air defence system.

More significantly for cyber defence, France is making substantial investments in AI to establish itself as the leading European ecosystem for AI development, with applications extending to cyber defence. This comprehensive approach ensures that France remains at the forefront of cyber defence and technological innovation.

Thales and Dassault Aviation for FCAS Program (with Airbus and Indra)[122]

*The FCAS program[123] is a cornerstone of innovation in cyber defence for France and Europe, aiming to develop an advanced air defence system that enhances **Europe's strategic autonomy** and **technological sovereignty**. By integrating cutting-edge cyber defence technologies, this initiative aims at protecting and securing the interconnected systems that form the backbone of modern air combat operations. The FCAS program includes the development of secure communication networks, advanced AI-driven threat detection systems, and resilient cybersecurity measures to safeguard critical data and operational integrity. Specifically, it advances technological innovation in cyber defence by leveraging the expertise of leading defence companies such as Thales[124] and Dassault Aviation.[125] The importance of this program lies in its ability to provide a robust and secure defence infrastructure, strengthening the overall security posture of France and its European allies.*

[118] SIPRI. (n.d.) Military Expenditure Database. https://www.sipri.org/databases/milex

[119] JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE. (2023, 2 August). LOI no 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047914986

[120] The Editorial Team. (2023, 6 September). Military programming bill: strengthening of Anssi approved. INCYBER. https://incyber.org/en/article/military-programming-bill-strengthening-of-anssi-approved/

[121] Airbus. (2023, 20 November). Future Combat Air System (FCAS) - Enter the Internet of Military Things. https://www.airbus.com/en/newsroom/stories/2023-11-future-combat-air-system-fcas-enter-the-internet-of-military-things

[122] Ibidem

[123] Ibidem

[124] Thales. (n.d.). About Thales. https://www.thalesgroup.com/en/global/group

[125] Dassault Aviation. (n.d.). Homepage. https://www.dassault-aviation.com/fr/

7. CONCLUSION

Deloitte.

Prioritizing Cyber Defence in EU Policy Plans: Reinforcement, Rearmament, and Funding Initiatives

Key Takeaways

Drawing upon the analysis conducted, it may be beneficial for the EU to:

➢ TECHNOLOGY AND POLICY INTEGRATION

Continue **reducing barriers** between civil and military technologies to encourage dual-use innovations, such as AI and quantum, aiming for technological sovereignty and reducing dependencies on third countries.

➢ SINGLE INNOVATION TAXONOMY

Define and adopt a shared **taxonomy** regarding innovation to align efforts, guide investment priorities, and foster a cohesive approach to defence capability building across Member States while avoiding fragmentation and duplication of efforts.

➢ UNIFIED INNOVATION STRATEGY

Define a unified and coordinated innovation **strategy** while supporting cyber defence through **updated** and **harmonised legislation** that not only enhances security but also fosters innovation. By establishing clear, uniform regulations across Member States, the EU could rely on a set of policy instruments that encourage the development of innovative cyber defence technologies.

➢ EFFECTIVE GOVERNANCE MECHANISMS

Establish a **centralised governance mechanism** to support cyber defence and ensure alignment among its institutions and Member States, expand investment programs, and enhance collaboration among diverse public and private stakeholders; equally critical are **deeper EU-NATO** dialogues and **EU-UK cyber** dialogues.

➢ LEVERAGING NATIONAL BEST PRACTICES

Build upon the efforts and best practices of its **27 Member States** to shape an effective cyber defence strategy and ecosystem. By identifying and integrating successful national approaches at the EU level, the EU can enhance its cyber defence while prioritising **EU-sponsored initiatives** over fragmented national efforts.

Being "a new era for European Defence and Security" one of the European Commission's priorities, it is of paramount importance for the EU to consider cyber defence innovation at the heart of its forthcoming policy plans and collective defence strategy. This paper analysed cyber defence innovation through four perspectives: technology, policy, governance, and capability. All of them contribute to a stronger, harmonised, and **unified EU cyber defence innovation strategy**.

A TECHNOLOGY PERSPECTIVE

Building on its current efforts to reduce barriers between civil and military technologies, it may be beneficial for the EU to continue encouraging the development of dual-use technologies, with a particular emphasis on AI and quantum. Given the nature of cyber defence technologies and the blurred lines separating civil and military applications, **innovation spillovers** between these domains could result **reduced duplication of efforts**, increased synergies, and support for the enhancement of defence capabilities.

Furthermore, innovation and R&D efforts focused on developing an industrial base for product development within the EU's borders could lead the EU to become a **technology exporter** rather than an importer, thereby reducing its technological dependencies on third countries. This ambitious long-term objective could serve as the focal point for EU efforts and initiatives targeting cyber defence innovation to meet **technological sovereignty**.

Finally, it could be beneficial for the EU to adopt a unified taxonomy regarding innovation to align efforts, guide investment priorities, and foster a cohesive approach to defence capability building while ensuring a shared approach to **measuring** cyber defence innovation.

A POLICY PERSPECTIVE

It may be beneficial for the EU to define a unified and coordinated innovation strategy to achieve European strategic autonomy while strengthening its efforts at sustaining innovation by adapting its **research** and **innovation laws** and **policies** to increase research spending. However, it is also recommendable that efforts be made to facilitate access to such **funding,** including for SMEs. In this regard, the **European Research Area Act** and the **European Innovation Act** are expected to define the effectiveness of the newly established European Commission's vision towards innovation.

As announced through the Competitiveness Compass, the EU aims to:

- harmonise current regulations;
- foster regulatory simplification;
- limit potential regulatory overlaps.

Given that EU efforts in the policy domain will not solely focus on new pieces of legislation, a **streamlined approach** to an innovation policy framework has the potential to deploy policy instruments beyond traditional funding programs (e.g., innovation hubs and cyber defence competitions).

A GOVERNANCE PERSPECTIVE

It would be beneficial for the EU to focus on enhancing common governance mechanisms, investment programs, and collaboration initiatives towards a comprehensive EU collective defence. Given the current fragmented cyber defence landscape, the following key takeaways are observed:

- Effective **governance** relies on **stakeholders** with **strong mandates** to propose and advance coherent cyber defence programs;
- Expansion of **investment programs** supporting innovators throughout the product development lifecycle, along with programs reducing barriers of entry to the defence market, could strengthen cyber defence innovation;
- Enhanced **collaboration** among **stakeholders** from academia, civil society, the public (e.g., EU institutions), and the private sector (e.g., industry), as well as **cooperation** among **Member States**, EU institutions, bodies, and agencies, would be paramount in supporting cyber defence innovation.

Beyond the EU's borders, deepening EU-NATO dialogues, as well as EU-UK cyber dialogues,[126] could represent an opportunity to strengthen EU interoperability with critical allies. Cooperation with the UK, a non-EU Member State with a state-of-the-art cyber defence strategy,[127] is especially promising, especially considering both bodies' **shared agenda** on a variety of geopolitical issues, such as the war in Ukraine and the consequent threats to regional stability, as well as the changing US policy towards the EU.

A CAPABILITY PERSPECTIVE

The EU's composite nature must be viewed as an advantage. Leveraging **best practices** from its 27 Member States, the EU has at its disposal a plethora of virtuous models to follow and adopt at the EU level. Four characteristics stand out from the benchmarking analysis of Finland, Estonia, and France:

- **Cyber defence figures centrally** in national policies and strategies, resulting in targeted allocating of resources to innovate and enhance cyber defence systems to protect national interests against cyber threats;
- Cyber defence innovation ecosystems of Finland, Estonia, and France are all characterised by a **robust governance structure** with clear roles and mandates assigned to cyber defence stakeholders, resulting in increased security capabilities, the development of emerging technologies, and trans-national initiatives across Europe;
- **Cooperation** among national stakeholders from government, industry, academia, and civil society highlights the importance of **promoting synergies** throughout the innovation lifecycle.

To achieve **strategic autonomy**, the EU could benefit from maximising innovation potential and avoiding duplication of efforts. **Cooperation** is the magic word. Piecemeal endeavours at the level of EU Member States might only perpetuate the existing fragmented landscape.

WHAT IS NEXT?

In **uncertain times**, the primary option for the EU may be to advance its security interests as one bloc. This is doubly true when it comes to potential threats in cyber defence. Now could be the time for the EU to strengthen its cyber defence apparatus and make it resilient to hybrid threats within the broader context of a **shared EU defence**. The challenge is evident, and the political will is present: now could be the time for the EU to transform this political will into a cohesive approach that encompasses technology, policy, governance, and capability perspectives to deliver results as a unified entity operating beyond the monetary and economic union.

[126] EU Commission (2024, December 9). Cyber: EU and UK hold Second Cyber Dialogue. https://digital-strategy.ec.europa.eu/en/news/cyber-eu-and-uk-hold-second-cyber-dialogue

[127] UK Government. (2022, May 9). Cyber Resilience Strategy for Defence. https://www.gov.uk/government/publications/cyber-resilience-strategy-for-defence

8. ANNEXES

Deloitte.

8.1. Focus on the Use Cases: A Strategic Benchmark Analysis

FOCUS ON A GOVERNANCE PERSPECTIVE

In the Tables below, an Overview of the National Cyber Defence Innovation Ecosystems, Funding and Cooperation Mechanisms.

NATIONAL CYBER DEFENCE INNOVATION ECOSYSTEMS		
Finland	**Estonia**	**France**
Finland's governance of cyber defence involves a structured approach that integrates both government and private-public partnerships. The government, primarily through the MoD,[128] plays a crucial role in shaping national defence policy, ensuring national security, and fostering both national cooperation with public and private entities as well as international cooperation in defence matters with a strong specialization within EU and NATO partnerships. It is worth to mention the NORDEFCO[129] alliance between Nordic countries (Denmark, Finland, Iceland, Norway and Sweden) in security and defence matters. At the governmental level, Finland's Government actively supports R&D though various agencies and	Estonia's cyber defence governance for the field of research and innovation is presented in the related Research and Innovation Policy from 2022.[141] The tasks related to research and innovation are distributed among the MoD and its institutions, such as the Estonian Defence Forces, including the Estonian National Defence College,[142] Republic of Estonia Centre for Defence Investments,[143] the Estonian Defence League,[144] the Estonian War Museum[145] and CR14.[146] In particular, the MoD, as part of its tasks, guides and manages the research and innovation policy, ensuring coherence with defence industry policy, and coordinates cross-sectoral, inter-governmental, and international cooperation, including budgeting and resource	France's approach to innovation in cyber defence is characterized by a robust governance structure that integrates both public and private sector efforts, consistent with France's highly centralized political structure. The French Cyber Defence Strategy primarily focuses on defensive measures, aiming to improve robustness and resilience across its information systems and networks and the MoD[148] plays a central role, directing substantial public investments through strategic initiatives such as the French Military Programming Act 2024-2030.[149] Public-private partnerships are particularly significant in France's cyber defence strategy. Major companies such as Thales[150] and Dassault Aviation[151] collaborate closely with government

[128] Ministry of Defence. (n.d.). Homepage. https://www.defmin.fi/en
[129] NORDEFCO. (n.d.). About NORDEFCO. https://www.nordefco.org/the-basics-about-nordefco
[141] Republic of Estonia. Ministry of Defence. (2022). Research and Innovation Policy in the Ministry of Defence's Field of Governance. https://www.ksk.edu.ee/en/files/2024/03/Research-and-Innovation-Policy-of-the-Ministry-of-Defence-Field-of-Governance-1.pdf
[142] Estonian Military Academy. (n.d.). Homepage. https://www.ksk.edu.ee/en/
[143] Estonian Centre for Defene Investments. (n.d.). Homepage. https://www.kaitseinvesteeringud.ee/en/
[144] KAITSELIIT. (n.d.). Estonian Defence League. https://www.kaitseliit.ee/en/edl
[145] Estonian War Museum. (n.d.). Homepage. https://esm.ee/
[146] CR14. (n.d.). Homepage. https://www.cr14.ee/
[148] Ministère des Armées. (n.d.). Homepage. https://www.defence.gouv.fr/
[149] Gras, O., (2023, 19 September). FRENCH MILITARY PROGRAMMING ACT 2024-2030. Eurodefence. https://www.eurodefence.fr/articles/143351-french-military-programming-act-2024-2030
[150] Thales. (n.d.). About Thales. https://www.thalesgroup.com/en/global/group
[151] Dassault Aviation. (n.d.). Homepage. https://www.dassault-aviation.com/fr/

NATIONAL CYBER DEFENCE INNOVATION ECOSYSTEMS		
Finland	**Estonia**	**France**
Ministries, such as the Research and Innovation Council,[130] an advisory body whose objectives are developing research and innovation policy, presenting initiatives for national strategy choices, and preparing and presenting initiatives related to research and innovation policy and proposals for the allocation of R&D funding. Alongside, different Ministries, such as the Ministry of Employment and the Economy[131] or the MoD oversee partnerships and protects and cooperates with Business Finland[132] and VTT,[133] a state-owned research institute. Research is additionally implemented with the cooperation between the Ministry of Education and Culture[134] alongside with universities. Private-public partnerships are also essential to Finland's cyber defence strategy, such as the partnership between the Finnish Defence Forces C5 Agency[135] and Suomen Erillisverkot Oy[136] and Government ICT Centre Valtori[137] to produce and maintain network services with which the Defence Forces engage in cooperation with other	allocation, to enhance Estonia's defence capabilities and competitiveness. It also supports strategic studies, development projects, and intellectual property protection, while monitoring and organizing the implementation of these policies. MoD's institutions are also entrusted with vital tasks regarding research and innovation. The private sector in Estonia can also be considered a crucial part of the governance structure. For instance, the Estonian Defence Industry Association (EKTL)[147] that represents leading defence and security industry companies in Estonia spearheads the implementation of the national defence innovation strategy by driving the Estonian defence innovation model and is supported by the MoD.	entities to advance key defence program and technological innovations.[152]

[130] Finnish government. (n.d.). Research and Innovation Council. https://valtioneuvosto.fi/en/research-and-innovation-council
[131] Ministry of Economic Affairs and Employment. (n.d.). Homepage. https://tem.fi/en/frontpage
[132] Business Finland. (n.d.). About us. https://www.businessfinland.fi/en/for-finnish-customers/about-us/in-brief
[133] VTT. (n.d.). What is VTT? https://www.vttresearch.com/en/about-us/what-vtt
[134] Ministry of Education and Culture. (n.d.). Homepage. https://okm.fi/en/frontpage
[135] The Finnish Defence Forces. (n.d.). Finnish Defence Forces C5 Agency. https://puolustusvoimat.fi/en/about-us/c5-agency
[136] Erillisverkot. (n.d.). Homepage. https://www.erillisverkot.fi/en/
[137] Valtori. Government ICT Centre. (n.d.). Homepage. https://valtori.fi/en/frontpage
[147] Estonian Defence and Aerospace Industry Association. (n.d.). Homepage. https://defence.ee/
[152] Airbus. (2023, 20 November). Future Combat Air System (FCAS)- Enter the Internet of Military Things. https://www.airbus.com/en/newsroom/stories/2023-11-future-combat-air-system-fcas-enter-the-internet-of-military-things

NATIONAL CYBER DEFENCE INNOVATION ECOSYSTEMS		
Finland	Estonia	France
authorities. Moreover, initiatives like DEFINE,[138] the Digital Defence Ecosystem (DDE)[139] and Nordic Defence Innovation Foundry[140] bring together military, industry, academic experts and potential investors to develop dual-use technologies that serve both military and civilian needs.		

Table 1 A Governance Perspective: National Cyber Defence Innovation Ecosystems

[138] DEFINE. (n.d.). What is DEFINE? https://www.definefinland.fi/en/what-is-define/

[139] Digital Defence Ecosystem. (n.d.). Members. https://www.digitaldefence.fi/#members

[140] Nordic Defence Innovation Foundry. (n.d.). Homepage. https://www.nordic-defence.com/

NATIONAL FUNDING MECHANISMS FOR CYBER DEFENCE INNOVATION		
Finland	Estonia	France
In Finland, funding for cyber defence initiatives is primarily public, with substantial government investment. The MoD[153] is the central authority responsible for allocating resources and implementing national cyber defence policies, while innovation funds are primarily co-managed by other Ministries such as the Ministry of Education and Culture,[154] the Ministry of Employment and the Economy,[155] as well as state-owned research centres such as VTT and funding agencies such as Business Finland. State-owned institutions and initiatives like DEFINE, VTT[156] and the Finnish Defence Research Agency[157] receive government support to advance research and development in cybersecurity, cyber defence and related technologies such as dual-use technologies,	In Estonia, funding for cyber defence initiatives is a balanced mix of public and private investments, with significant contributions from both sectors. The government, primarily through the MoD, plays a pivotal role in funding and overseeing national cyber defence strategies. Public funding supports key entities such as the Cyber Defence Unit[159] within the Estonian Defence League[160] and the Cyber Command,[161] which are essential for maintaining national security and cyber situational awareness. Additionally, initiatives like the CR14 Foundation[162] provide cyber range solutions and support research and development in cybersecurity,[163] Private sector involvement is also substantial, with companies like Plural[164] and SmartCap[165] investing in innovative defence	In France, funding for cyber defence initiatives is predominantly public, driven by substantial government investment and strategic direction. The MoD plays a crucial role in allocating resources, as evidenced by the French Military Programming Act 2024-2030,[167] which earmarks significant budgetary allocations to enhance cyber defence capabilities. Public initiatives such as the Campus Cyber[168] and the Call for Projects "Development of critical innovative cyber technologies"[169] are supported by public authorities, illustrating the government's commitment to fostering innovation in cybersecurity. While private companies like Thales[170] and Dassault Aviation[171] are integral to the ecosystem, contributing through technological development and strategic partnerships, the

[153] Ministry of Defence. (n.d.). Areas of Expertise. Security. https://www.defmin.fi/en/areas_of_expertise/security#730f3b7a

[154] Ministry of Education and Culture. (n.d.). Homepage. https://okm.fi/en/frontpage

[155] Ministry of Economic Affairs and Employment. (n.d.). Homepage. https://tem.fi/en/frontpage

[156] VTT. (n.d.). What is VTT? https://www.vttresearch.com/en/about-us/what-vtt

[157] The Finnish Defence Forces. (n.d.). Finnish Defence Research Agency Divisions. https://puolustusvoimat.fi/en/about-the-research-agency

[159] Kaska, K., Osula, A.-M., Stinissen, LTC J. (2013). The Cyber Defence Unit of the Estonian Defence League. Legal, Policy and Organisational Analysis. https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf

[160] KAITSELIIT. (n.d.). Estonian Defence League. https://www.kaitseliit.ee/en/edl

[161] Republic of Estonia. Defence Forces. (n.d.). Land Forces. Cyber Command. https://mil.ee/en/landforces/cyber-command/

[162] CR14. (n.d.). Homepage. https://www.cr14.ee/

[163] Republic of Estonia. Ministry of Defence. (2022). Research and Innovation Policy in the Ministry of Defence's Field of Governance. https://www.ksk.edu.ee/en/files/2024/03/Research-and-Innovation-Policy-of-the-Ministry-of-Defence-Field-of-Governance-1.pdf

[164] Plural. (n.d.). The peers. https://pluralplatform.com/the-peers/

[165] Smartcap. (n.d.). About us. https://smartcap.ee/about-us/

[167] Gras, O., (2023, 19 September). FRENCH MILITARY PROGRAMMING ACT 2024-2030. Eurodefence. https://www.eurodefence.fr/articles/143351-french-military-programming-act-2024-2030

[168] Campus Cyber. (n.d.). Homepage. https://campuscyber.fr/

[169] Campus Cyber. (2025, 26 February). Candidatez à l'Appel à Projets « Développement de Technologies Cyber Innovantes Critiques ». https://campuscyber.fr/candidatez-a-lappel-a-projets-developpement-de-technologies-cyber-innovantes-critiques/

[170] Thales. (n.d.). About Thales. https://www.thalesgroup.com/en/global/group

[171] Dassault Aviation. (n.d.). Homepage. https://www.dassault-aviation.com/fr/

NATIONAL FUNDING MECHANISMS FOR CYBER DEFENCE INNOVATION		
Finland	Estonia	France
cybersecurity for AI and quantum computing and encryption. Additionally, the Nordic Defence Innovation Foundry[158] is a non-profit organisation which support innovative startups and research teams to connect with potential private investors and organisations in the Military, Law Enforcement, Cyber Security, Critical Infrastructure, Crisis Management, and Space sectors.	technologies and startups, but also coalition of investors and founder as Darkstar,[166] These private-public partnerships are integral to Estonia's cyber defence governance, ensuring that both public oversight and private sector innovation contribute to a robust and comprehensive cybersecurity framework.	primary funding and strategic oversight remain under public control. This public funding is closely linked with governance structures, ensuring that national security priorities are met while leveraging private sector expertise and innovation to build a comprehensive and robust cyber defence framework.

Table 2 A Governance Perspective: National Funding Mechanisms for Cyber Defence Innovation

[158] Nordic Defence Innovation Foundry. (n.d.). Homepage. https://www.nordic-defence.com/
[166] Darkstar. (n.d.). Homepage. https://darkstar.ee/

BOLSTERING CYBER DEFENCE INNOVATION THROUGH NATIONAL AND INTERNATIONAL COOPERATION

Finland	Estonia	France
In March 2024, the Prime Minister's Office launched a project to develop an operating model for government security management, aligned with the National Cyber Security Strategy 2024-2035.[172] This initiative, which emphasizes robust national and international cooperation, saw contributions from public and private sectors, scientific communities, and NGOs. Nationally, the Finnish Defence Forces partnered with Suomen Erillisverkot Oy[173] and Government ICT Centre Valtori[174] to enhance network services,[175] while VTT led a quantum encryption network project[176] in collaboration with Suomen Erillisverkot Oy, Cinia Oy,[177] and CSC – IT Centre.[178] This project aims to build a public test network in the Helsinki Metropolitan Area for quantum encryption	Estonia's approach to innovation in cyber defence is marked by robust cooperation within the military and among international partners. The MoD[183] leads efforts to integrate advanced technologies such as AI and quantum computing into national defence strategies. This is achieved through active collaboration with international partners within the EU and NATO frameworks, including participation in EDA projects and PESCO initiatives. Estonia fosters strong public-private partnerships and emphasizes the importance of education and R&D in advancing cyber defence technologies. The Estonian Defence and Security Industry Innovation Cluster[184] brings together academic institutions, research labs, SMEs, and large industries to drive	France works closely with other EU Member States in PESCO projects to pool resources, share expertise, and develop interoperable systems. France cooperates on the European level with countries like Germany and Spain for the FCAS project.[188] French legislative frameworks (e.g., French Military Programming Act 2024–2030[189]) also foster cooperation for innovation in cyber defence. The involvement of public authorities like ANSSI,[190] DGE,[191] DGA,[192] SGPI,[193] and BPI France[194] in building initiatives such as the Call for Projects "Development of critical innovative cyber technologies"[195] as well as the support the French

[172] Prime Minister's Office. (2024). Finland's Cyber Security Strategy 2024–2035. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165893/VNK_2024_13.pdf?sequence=1&isAllowed=y

[173] Erillisverkot. (n.d.). Homepage. https://www.erillisverkot.fi/en/

[174] Valtori. Government ICT Centre. (n.d.). Homepage. https://valtori.fi/en/frontpage

[175] The Finnish Defence Forces. (n.d.). Finnish Defence Forces C5 Agency. https://puolustusvoimat.fi/en/about-us/c5-agency

[176] Erillisverkot. (2023, May 16). Construction of the quantum encryption network begins in Finland https://www.erillisverkot.fi/en/construction-of-the-quantum-encryption-network-begins-in-finland/

[177] Cinia. (n.d.). Homepage. https://www.cinia.fi/en/

[178] CSC. (n.d.). Homepage. https://csc.fi/en/

[183] Ministry of Defence. (n.d.). Homepage. https://www.kaitseministeerium.ee/en

[184] Estonian Defence and Aerospace Industry Association. (n.d.). About Cluster. https://defence.ee/cluster-and-members/

[188] Airbus. (2023, 20 November). Future Combat Air System (FCAS)- Enter the Internet of Military Things. https://www.airbus.com/en/newsroom/stories/2023-11-future-combat-air-system-fcas-enter-the-internet-of-military-things

[189] Gras, O., (2023, 19 September). FRENCH MILITARY PROGRAMMING ACT 2024-2030. Eurodefence. https://www.eurodefence.fr/articles/143351-french-military-programming-act-2024-2030

[190] ANSSI. (n.d.). Homepage. https://cyber.gouv.fr/

[191] Ministre de l'Économie, des Finances et de la Souveraineté industrielle et numérique. (n.d.). Direction générale des Entreprises. https://www.entreprises.gouv.fr/

[192] Ministère des Armées. (n.d.). Direction Générale de l'Armement. https://www.defence.gouv.fr/dga

[193] Gouvernement. (n.d.). Secrétariat général pour l'investissement (SGPI). https://www.info.gouv.fr/organisation/secretariat-general-pour-l-investissement-sgpi

[194] BPI France. (n.d.). Homepage. https://www.bpifrance.fr/

[195] Campus Cyber. (2025, 26 February). Candidatez à l'Appel à Projets « Développement de Technologies Cyber Innovantes Critiques ». https://campuscyber.fr/candidatez-a-lappel-a-projets-developpement-de-technologies-cyber-innovantes-critiques/

BOLSTERING CYBER DEFENCE INNOVATION THROUGH NATIONAL AND INTERNATIONAL COOPERATION		
Finland	Estonia	France
technologies. Additionally, the Digital Defence Ecosystem[179] aims to foster innovation in defence technologies by connecting leading Finnish defence and technology companies with research institutes. Internationally, Finland engages in various collaborations, including NORDEFCO's COPA CAPA[180] activities on advanced defence technologies, the DEFINE accelerator[181] in Riihimäki to scale defence and security innovations, NATO's DIANA[182] initiative for next-generation technologies, and participation in EDA and PESCO projects to bolster its defence and cybersecurity capabilities.	innovation in cybersecurity and defence technologies.[185] The CR14 Foundation,[186] established by the MoD, supports research and development in cybersecurity, providing advanced cyber range solutions. Additionally, Estonia's Research and Innovation Policy 2022[187] promotes applied research in AI, emerging technologies, and quantum computing, facilitating collaboration among experts from academia, industry, and government.	MoD and the Agence de l'Innovation de Défense[196] show towards structures designed to respond to the defence technological needs (e.g., Interdisciplinary Centre for Defence and Security (CIEDS))[197] bear witness to the French public authorities' commitment in cyber defence innovation initiatives.

Table 3 A Governance Perspective: Bolstering Cyber Defence Innovation through National and International Cooperation

[179] Digital Defence Ecosystem. (n.d.). Homepage. https://www.digitaldefence.fi/

[180] NORDEFCO. (n.d.). COPA Capabilities. https://www.nordefco.org/COPA-Capabilities2

[181] DEFINE. (n.d.). DEFINE Accelerator backed by Redstone. https://www.definefinland.fi/en/define-accelerator/

[182] DIANA. (n.d.). Homepage. https://www.diana.nato.int/

[185] Talinn. (n.d.). Defence- and Security Cluster. https://www.tallinn.ee/en/clustersinestonia/defence-and-security-cluster

[186] CR14. (n.d.). Homepage. https://www.cr14.ee/

[187] Republic of Estonia. Ministry of Defence. (2022). Research and Innovation Policy in the Ministry of Defence's Field of Governance. https://www.ksk.edu.ee/en/files/2024/03/Research-and-Innovation-Policy-of-the-Ministry-of-Defence-Field-of-Governance-1.pdf

[196] Ministère des Armées. (n.d.). Agence de l'innovation de défense. https://www.defence.gouv.fr/aid

[197] Institut Polytechnique de Paris. (n.d.). CIEDS- Interdisciplinary Centre for Defence and Security. https://www.ip-paris.fr/en/cieds

FOCUS ON A POLICY PERSPECTIVE

In the Tables below, an Overview of the National Cyber Defence Innovation Laws, Strategies, and Policies.

NATIONAL CYBER DEFENCE INNOVATION LAWS, STRATEGIES AND POLICIES		
Finland	Estonia	France
In Finland's National Cybersecurity Strategy 2024-2035,[198] cyber defence is considered alongside with cyber security and focuses on enhancing its cyber defence posture and investing in R&D in emerging technologies: • Within "Pillar I: Competence, Technology and RDI," Finland leverages the benefits of emerging and disruptive technologies, ensuring integrated security in devices, software, and services. The strategy aims to protect cybersecurity knowledge capital and achieve self-sufficiency in critical cryptographic technology. Additionally, Finland seeks to create an attractive RDI environment and promote the competitiveness of businesses in the cybersecurity sector, while fully utilizing opportunities for cooperation and funding through the EU and NATO. "Pillar III: Cooperation" emphasizes aligning Finland's cybersecurity and cyber defence objectives with those of the EU and NATO.	Estonia's approach to innovation in cyber defence is outlined in the Research and Innovation Policy 2022[199] of the MoD. It fosters applied research in cyber defence including AI, emerging technologies, quantum computing, the development of Centres of excellence and participation to international programs within EU and NATO. The policy includes four objectives: • Objective 1: Implementation of research and innovation policies to meet the strategic objectives of the area of governance. • Objective 2: Solutions in the field of deterrence, early warning, force generation and defence capabilities. • Objective 3: Supporting the sustainability of Military Sciences. • Objective 4: Platform for international activities, including output for the defence industry.	France's approach to innovation in cyber defence is outlined in the French Military Programming Act 2024–2030,[200] which sets the objective to "develop a leading cyber defence" placing a significant emphasis on innovation in cyber defene by investing in R&D in advanced technologies within the military. Moreover, as a follow up of the first phase of the Strategy ("AI for humanity"), a National Strategy for AI 2022-2025[201] was adopted in November 2021, and it is built upon two main pillars. The first one, "IA-Cluster" has the goal to transform French training and research centres into international hubs of AI expertise; while the second pillar, "AI Booster", focuses on supporting the digital transformation of French SMEs and to facilitate AI integration into small companies. Furthermore, France supports the growth of the AI ecosystem at the national level through a public-private partnership, also focusing on cyber defence technologies.

[198] Prime Minister's Office. (2024). Finland's Cyber Security Strategy 2024–2035. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165893/VNK_2024_13.pdf?sequence=1&isAllowed=y

[199] Republic of Estonia. Ministry of Defence. (2022). Research and Innovation Policy in the Ministry of Defence's Field of Governance. https://www.ksk.edu.ee/en/files/2024/03/Research-and-Innovation-Policy-of-the-Ministry-of-Defence-Field-of-Governance-1.pdf

[200] Gras, O., (2023, 19 September). FRENCH MILITARY PROGRAMMING ACT 2024-2030. Eurodefence. https://www.eurodefence.fr/articles/143351-french-military-programming-act-2024-2030

[201] Krasavina, A., (2023, 8 August). France- National Strategy for AI. Digital Skills & Jobs Platform. https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/france-national-strategy-ai

NATIONAL CYBER DEFENCE INNOVATION LAWS, STRATEGIES AND POLICIES		
Finland	**Estonia**	**France**
- "Pillar IV: Response and Countermeasures" introduces a cyber defence doctrine that provides national operating principles for responding to state-sponsored threats and threats against national security. The strategy includes an implementation plan, acknowledged by the Finnish MoD, detailing development measures to achieve these objectives. Prioritized measures include participating in cybersecurity cooperation, cybercrime prevention, and cyber defence, supporting partner countries, achieving self-sufficiency in critical cryptographic technologies, and preparing for the quantum threat by 2030.	Each objective has indicators (e.g., Number of international research and development projects involving universities and/or companies (cumulative) and respective baselevel from 2021 and target levels to be reached by 2025 (e.g., 5) and 2030 (e.g., 8).	

Table 4 A Policy Perspective: National Cyber Defence Innovation Laws, Strategies and Policies

FOCUS ON A TECHNOLOGY PERSPECTIVE

In the Table below, an Overview of how National Cyber Defence Innovation Objectives are Implemented through National Projects.

NATIONAL CYBER DEFENCE INNOVATION PROJECTS		
Finland	Estonia	France
Finland is at the forefront of advancing cyber defence technologies through a series of strategic initiatives. A notable project is the quantum encryption network[202] led by Suomen Erillisverkot Oy,[203] Cinia Oy,[204] and CSC – IT Centre for Science,[205] in partnership with the Finnish Defence Forces C5 Agency.[206] This project is developing a public test network in the Helsinki Metropolitan Area to introduce and test quantum encryption technologies, with plans to connect to the EU-wide network. AI is another key focus, with a dedicated NORDEFCO working group fostering Nordic cooperation in AI.[207] The DEFINE supports the development of defence and dual-use technologies through its DEFINE Accelerator,[208] a 3-month	Estonia is developing several advanced technologies to enhance its cyber defence and innovation capabilities. The EKTL[211] has established the Estonian Defence and Security Industry Innovation Cluster,[212] which focuses on the development of drones, autonomous unmanned ground vehicles, IT cyber-digital solutions, and AI-assisted software technologies. This cluster is driving significant innovation, particularly in the area of autonomous unmanned ground vehicles. Regarding cybersecurity, Estonia coordinates the CRF[213] within the PESCO project, which can be used for creating innovative cybersecurity products and services, including AI solutions and the	France is an active actor in projects designed to support European defence capabilities and technological sovereignty. Besides participation in various PESCO projects under the area of CYBER, C4ISR (e.g., ACCESS[219]), France, with its manufacturers Dassault Aviation,[220] Safran,[221] and Thales[222] is involved, along with Germany and Spain in projects such as FCAS.[223] FCAS aims to design an air defence system, which includes a New-Generation Fighter (NGF), Remote Carriers (RCs) that can operate in conjunction with the NGF, and Combat Cloud that will enable seamless communication and data sharing between the NGF, RCs, and other assets.

[202] Erillisverkot. (2023, May 16). Construction of the quantum encryption network begins in Finland. https://www.erillisverkot.fi/en/construction-of-the-quantum-encryption-network-begins-in-finland/

[203] Erillisverkot. (n.d.). Homepage. https://www.erillisverkot.fi/en/

[204] Cinia. (n.d.). Homepage. https://www.cinia.fi/en/

[205] CSC. (n.d.). Homepage. https://csc.fi/en/

[206] The Finnish Defence Forces. (n.d.). Finnish Defence Forces C5 Agency. https://puolustusvoimat.fi/en/about-us/c5-agency

[207] NORDEFCO. (n.d.). COPA Capabilities. https://www.nordefco.org/COPA-Capabilities2

[208] DEFINE. (n.d.). DEFINE Accelerator backed by Redstone. https://www.definefinland.fi/en/define-accelerator/

[211] Estonian Defence and Aerospace Industry Association. (n.d.). Homepage. https://defence.ee/

[212] Estonian Defence and Aerospace Industry Association. (n.d.). About Cluster. https://defence.ee/cluster-and-members/

[213] PESCO. (n.d.). PESCO Projects. Cyber Ranges Federations (CRF). https://www.pesco.europa.eu/project/cyber-ranges-federations-crf/

[219] PESCO. (n.d.). PESCO Projects. Arctic Command & Control Effector and Sensor System (ACCESS). https://www.pesco.europa.eu/project/arctic-command-control-effector-and-sensor-system-access/

[220] Dassault Aviation. (n.d.). Homepage. https://www.dassault-aviation.com/fr/

[221] Safran. (n.d.). Homepage. https://www.safran-group.com/

[222] Thales. (n.d.). About Thales. https://www.thalesgroup.com/en/global/group

[223] Airbus. (2023, 20 November). Future Combat Air System (FCAS)- Enter the Internet of Military Things. https://www.airbus.com/en/newsroom/stories/2023-11-future-combat-air-system-fcas-enter-the-internet-of-military-things

NATIONAL CYBER DEFENCE INNOVATION PROJECTS		
Finland	**Estonia**	**France**
program involving the Finnish Defence Forces, leading companies, research institutes, and startups. Additionally, the DIANA has established an accelerator and two test centres in Finland, in collaboration with the VTT research centre,[209] focusing on next-generation communication systems, 6G technology, cybersecurity, quantum, and space technologies. Finland is also actively participating in NORDEFCO-led projects,[210] including the Counter-UAS project to address unmanned aerial systems threats, a permanent working group enhancing Nordic cooperation in cyber defence, and a study group exploring swarming technologies for operational efficiencies and cost savings. Furthermore, Ground Anti Access Area Denial (GA2AD) projects aim to develop	cybersecurity of cyber-physical systems like 5G. Additionally, the state-owned investment company SmartCap[214] manages a new fund[215] dedicated to investing in military-use and dual-use technologies. AI solutions for detection systems aimed at tracking and intercepting unmanned systems are being developed through a bootcamp organized by Darkstar,[216] a coalition of founders, builders, and investors. Furthermore, Estonia's commitment to enhancing defence, intelligence, and national security systems is exemplified by the investment fund Plural's[217] participation in a EUR 450 million funding round for the German AI company Helsing.[218]	In addition, the French company Thales[224] proactively engages in innovation and talent acquisition through Thales Research & Technology (TRT),[225] which serves as a hub for innovation, building partnerships with industrial and scientific communities, and attracting skilled science graduates to enhance Thales' expertise. Finally, actors such as the French hub CAMPUS CYBER[226] are conducting activities related to cyber defence innovation in technology. CAMPUS CYBER has issued a Call for Projects[227] with the aim to support the development of disruptive cybersecurity technologies. Public authorities, such as DGA[228] were involved in its co-construction. Another actor on the French scene, the Institut Polytechnique de Paris,[229] has created "CIEDS - Interdisciplinary Centre for Defence and Security"[230]

[209] VTT. (2024, March 14). NATO accelerator and two test centres to be established in Finland. https://www.vttresearch.com/en/news-and-ideas/nato-accelerator-and-two-test-centres-be-established-finland#:~:text=Finland%20is%20now%20part%20of,the%20civil%20and%20defence%20sectors.

[210] NORDEFCO. (n.d.). COPA Capabilities. https://www.nordefco.org/COPA-Capabilities2

[214] Smartcap. (n.d.). About us. https://smartcap.ee/about-us/

[215] Invest in Estonia. (2025, January). Estonia unveils €100M Defence Industry Fund, speeding up military innovations. https://investinestonia.com/estonia-unveils-e100m-defence-industry-fund-speeding-up-military-innovations/

[216] Darkstar. (n.d.). Homepage. https://darkstar.ee/

[217] Plural. (n.d.). The peers. https://pluralplatform.com/the-peers/

[218] Kahn, M. (2025, February 21). Estonia's tech investors take defence into their own hands as Russian threat looms. Reuters. https://www.reuters.com/business/aerospace-defence/estonias-tech-investors-take-defence-into-their-own-hands-russian-threat-looms-2025-02-21/

[224] Thales. (n.d.). About Thales. https://www.thalesgroup.com/en/global/group

[225] Thales. (n.d.). Research and Technology. https://www.thalesgroup.com/en/global/innovation/research-and-technology

[226] Campus Cyber. (n.d.). Homepage. https://campuscyber.fr/

[227] Campus Cyber. (2025, 26 February). Candidatez à l'Appel à Projets « Développement de Technologies Cyber Innovantes Critiques ». https://campuscyber.fr/candidatez-a-lappel-a-projets-developpement-de-technologies-cyber-innovantes-critiques/

[228] Ministère des Armées. (n.d.). Direction Générale de l'Armement. https://www.defence.gouv.fr/dga

[229] Institut Polytechnique de Paris. (n.d.). Homepage. https://www.ip-paris.fr/en

[230] Institut Polytechnique de Paris. (n.d.). CIEDS- Interdisciplinary Centre for Defence and Security. https://www.ip-paris.fr/en/cieds

NATIONAL CYBER DEFENCE INNOVATION PROJECTS		
Finland	**Estonia**	**France**
systems that deny free use of areas with minimal risk to own soldiers.		in 2021. It CIEDS benefits from strong support from the French MoD and the Agence de l'Innovation de Défense.[231] Its research areas include, among others, cybersecurity and digital security, robotics and AI, imaging and modelling for systems engineering, quantum technologies, detection of biological and chemical threats and care of the combatant, management of defence innovation and technological sovereignty and defence strategy.

Table 5 A Technology Perspective: National Cyber Defence Innovation Projects

[231] Ministère des Armées. (n.d.). Agence de l'innovation de défense. https://www.defence.gouv.fr/aid

8.2. Focus on Finland, Estonia, and France Participation in PESCO Projects (Area Cyber, C4ISR)

PESCO projects (area CYBER, C4ISR)		Country		
Project Name	Project Description	Finland	Estonia	France
Arctic Command & Control Effector and Sensor System (ACCESS)[232]	*ACCESS aims to create a knowledge base and concept for scalable, multifunctional transceivers. The project explores developing systems where a single, centrally controlled piece of equipment offers improved performance and reliability at reduced weight and cost.*	Coordinates	Participates	Participates
Cyber Ranges Federations (CRF)[233]	*CRF aims to enhance European Cyber Ranges by federating national Cyber Ranges into a larger cluster for cyber-related R&D and sharing R&D to facilitate standardization.*	Participates	Coordinates	Participates
European Secure Software defined Radio (ESSOR)[234]	*ESSOR aims to improve interoperability in land, maritime, and air communications by developing European Software Defined Radios (SDR). It focuses on creating waveforms to meet specific needs and ensuring their interoperability through a custodianship centre.*	Participates	-	Coordinates
Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT)[235]	*CRRT's mission is to assist Member States and other parties in responding to cyber incidents and enhancing cyber resilience. The long-term goal is to develop a common cyber toolkit for multinational rapid response teams.*	-	Participates	-
Robust Communication Infrastructure and Networks (ROCOMIN)[236]	*The ROCOMIN project aims to enhance studies and initiatives within EDA/EDF/PESCO projects. It seeks to develop an AI-driven tool to manage and adapt communication and network infrastructure, ensuring timely, safe, and secure communications.*	Participates	-	Participates

[232] PESCO. (n.d.). PESCO Projects. Arctic Command & Control Effector and Sensor System (ACCESS). https://www.pesco.europa.eu/project/arctic-command-control-effector-and-sensor-system-access/

[233] PESCO. (n.d.). PESCO Projects. Cyber Ranges Federations (CRF). https://www.pesco.europa.eu/project/cyber-ranges-federations-crf/

[234] PESCO. (n.d.). PESCO Projects. European Secure Software defined Radio (ESSOR). https://www.pesco.europa.eu/project/european-secure-software-defined-radio/

[235] PESCO. (n.d.). PESCO Projects. Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT). https://www.pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/

[236] PESCO. (n.d.). PESCO Projects. Robust Communication Infrastructure and Networks (ROCOMIN). https://www.pesco.europa.eu/project/robust-communication-infrastructure-and-networks-rocomin/

PESCO projects (area CYBER, C4ISR)		Country		
Automated Modelling, Identification and Damage Assessment of Urban Terrain (AMIDA-UT)[237]	*AMIDA-UT is a project using a digital 3D mapping system to identify urban targets. It involves drones with multisensory payloads, vehicle/soldier-attached sensors, and space-based sensors. Data is collected and sent to a land-based station for processing, potentially using cloud computing and AI, to create digital models of terrain and building structures autonomously.*	-	-	Participates
Strategic C2 System for CSDP Missions and Operations (EUMILCOM)[238]	*EUMILCOM aims to develop a command-and-control system capable of conducting multiple simultaneous operations with various forces worldwide, independently or in cooperation with NATO.*	-	-	Participates
European High Atmosphere Airship Platform (EHAAP) – Persistent Intelligence, Surveillance and Reconnaissance (ISR) Capability (EHAAP)[239]	*EHAAP aims to achieve operational capability using a System of Systems approach. It will provide advanced dual-use capabilities such as communication relay, missile warning, surveillance, reconnaissance, fire coordination, navigation, weather monitoring, electronic countermeasures, missile defence, and air-to-ground strike capabilities.*	-	-	Participates
Cyber and Information Domain Coordination Centre (CIDCC)[240]	*CIDCC aims to support EU missions and operations in the cyber and information domain, plan and conduct EU CID operations, and enhance EU CSDP resiliency. The Cyber and Information Domain integrates cyberspace, the electromagnetic environment, and the cognitive environment.*	-	-	Participates

Table 6 Finland, Estonia, and France Participation in PESCO Projects (Area Cyber, C4ISR)

[237] PESCO. (n.d.). PESCO Projects. Automated Modelling, Identification and Damage Assessment of Urban Terrain (AMIDA-UT). https://www.pesco.europa.eu/project/automated-modelling-identification-and-damage-assessment-of-urban-terrain-amida-ut/

[238] PESCO. (n.d.). PESCO Projects. Strategic C2 System for CSDP Missions and Operations (EUMILCOM). https://www.pesco.europa.eu/project/strategic-c2-system-for-csdp-missions-and-operations/

[239] PESCO. (n.d.). PESCO Projects. European High Atmosphere Airship Platform (EHAAP) – Persistent Intelligence, Surveillance and Reconnaissance (ISR) Capability (EHAAP). https://www.pesco.europa.eu/project/european-high-atmosphere-airship-platform-ehaap-persistent-intelligence-surveillance-and-reconnaissance-isr-capability/

[240] PESCO. (n.d.). PESCO Projects. Cyber and Information Domain Coordination Centre (CIDCC). https://www.pesco.europa.eu/project/cyber-and-information-domain-coordination-centre-cidcc/

8.3. Acronyms & Abbreviations

Acronym, Abbreviation	Description
ACCESS	Arctic Command & Control Effector and Sensor System
AI	Artificial Intelligence
AMIDA-UT	Automated Modelling, Identification and Damage Assessment of Urban Terrain
ASEAN	Association of Southeast Asian Nations
AU	African Union
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CDP	Capability Development Plan
CDPF	Cyber Defence Policy Framework
CERT-EU	Computer Emergency Response Team for the EU institutions
CIDCC	Cyber and Information Domain Coordination Centre
CIEDS	Interdisciplinary Centre for Defence and Security
CRA	Cyber Resilience Act
CRF	Cyber Ranges Federations
CRRT	Cyber Rapid Response Teams and Mutual Assistance in Cyber Security
CSA	Cyber Solidarity Act
CSDP	Common Security and Defence Policy
CSIRT	Computer Security and Incident Response Team
DDE	Digital Defence Ecosystem
DEFINE	Defence Innovation Network Finland
DG DEFIS	Directorate-General for Defence Industry and Space
DIANA	NATO Defence Innovation Accelerator for the North Atlantic

Acronym, Abbreviation	Description
EC3	European Cyber Crime Centre
EDA	European Defence Agency
EDF	European Defence Fund
EDIP	European Defence Industry Programme
EDIS	European Defence Industrial Strategy
EDT	Emerging Disruptive Technologies
EDTIB	EU Defence Technological and Industrial Base
EEAS	European External Action Service
EHAAP	European High Atmosphere Airship Platform
EIB	European Investment Bank
EIS	European Innovation Scoreboard
EKTL	Estonian Defence Industry Association
ENISA	European Network and Information Security Agency
ESSOR	European Secure Software defined Radio
EU	European Union
EUCDCC	EU Cyber Defence Coordination Centre
EUDIS	EU Defence Innovation Scheme
EUIBAs	European institutions, bodies, offices, and agencies of the Union
EUMILCOM	Strategic C2 System for CSDP Missions and Operations
EuroQCI	European Quantum Communication Infrastructure
FCAS	Future Combat Air System
GA2AD	Ground Anti Access Area Denial
GDPR	General Data Protection Regulation

Acronym, Abbreviation	Description
GII	Global Innovation Index
HEDI	Hub for EU Defence Innovation
HPC	High-performance computing
IBNS	Intent-Based Network Security
IoT	Internet of Things
ISR	Persistent Intelligence, Surveillance and Reconnaissance
IT	Operational Technology
JCU	Joint Cyber Unit
LEAs	law enforcement agencies
MFF	Multiannual Financial Framework
MICNET	Military Computer Emergency Response Team Operational Network
milCERTs	Military Computer Emergency Response Teams
MoD	Ministry of Defence
NATO	North Atlantic Treaty Organisation
NCSC	National Cyber Security Centre
NFPs	Network of European Defence Fund National Focal Points
NGF	New-Generation Fighter
NIF	NATO Innovation Fund
NIS	Network and Information Systems
NORDEFCO	alliance between Nordic countries (Denmark, Finland, Iceland, Norway, and Sweden)
OSCE	Organisation for Security and Co-operation in Europe
OT	Information Technology
PDEs	Products with digital element

Acronym, Abbreviation	Description
PESCO	Permanent Structured Cooperation
PPPs	Public-Private Partnerships
QKD	Quantum Key Distribution
R&D	Research and Development
R&T	Research & Technology
RCs	Remote Carriers
ROCOMIN	Robust Communication Infrastructure and Networks
SII	Summary Innovation Index
SIPRI	Stockholm International Peace Research Institute
SMEs	Small and Medium-sized Enterprises
SOCs	Security Operations Centres
STEP	Strategic Technologies for Europe Platform
UAS	Unmanned Aircraft Systems
UN	United Nations
UNIDIR	United Nations Institute for Disarmament Research
US	United States
WIPO	World Intellectual Property Organisation

Table 7 Acronyms & Abbreviations

8.4. Who We Are

The Deloitte's European Policy Centre (EUPC) makes Deloitte's insights and research on public policy issues and legislation available to key policy makers and clients, building relationship between professionals, business leaders, and decision-makers.

EUPC TEAM

Pablo Zalba

Managing Director EU Policy | Partner

Deloitte EU Policy Centre

pzalba@deloitte.es

+34 914381908

Edoardo Giglio

EU Cyber Policy Leader | Partner

Deloitte EU Policy Centre

egiglio@deloitte.it

+39 33712761

Mosche Orth

EU Policy Centre | Senior Manager

Digital Economy & Cyberspace

moorth@deloitte.de

+49 151580711859

EUPC SUPPORT TEAM

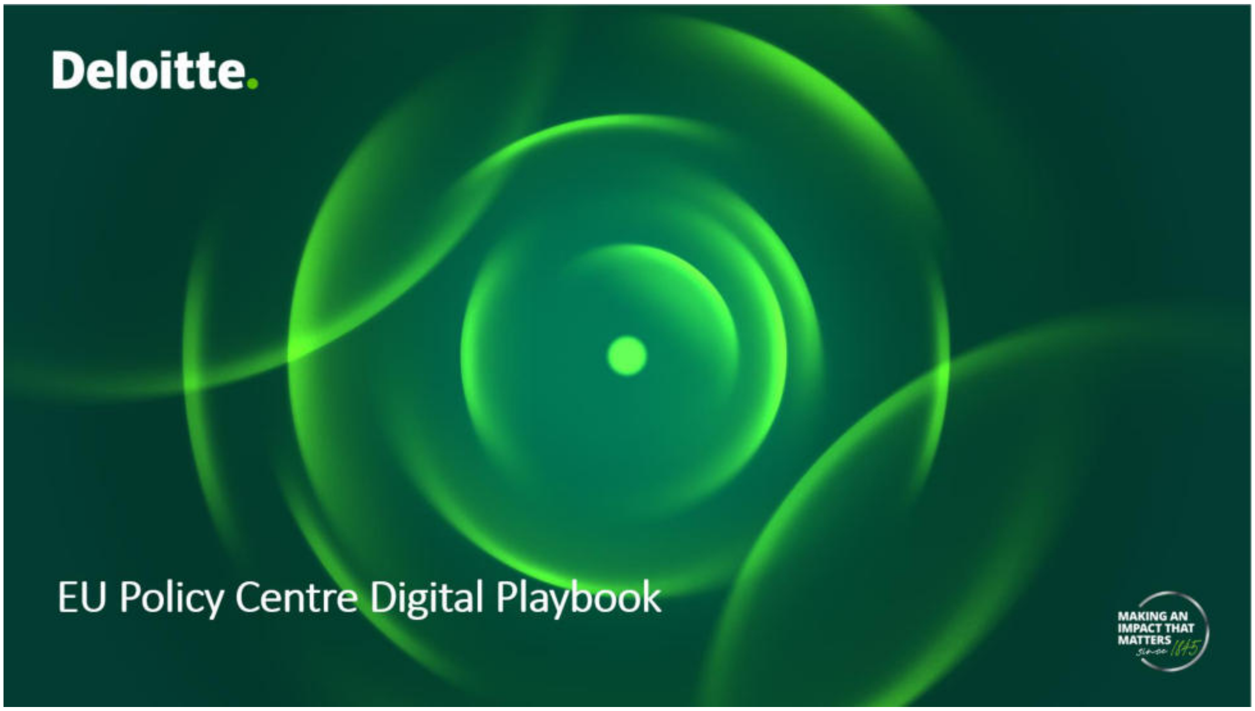
Biagio Salerno (Director, Deloitte Italy)

Alessia Sposini (Analyst, Deloitte Italy)

Nicolò Benussi (Analyst, Deloitte Italy)

8.5. Deloitte's EUPC Digital Playbook. Navigating the EU's Cyber Legislative Landscape

In light of the increasing complexity of the EU digital and cyber legislative landscape, as extensively outlined in the beginning of this paragraph, there is a compelling need to explore the new market opportunities opened by EU legislation. In this regard, the Deloitte's EUPC has published the Digital Playbook[241], looking across the plethora of digital and cyber legislation from the European Commissions´ last term. The **EUPC Digital Playbook** is a living document that aims to spread awareness on the existing Union's digital and cyber legislative framework and unveil intersections and synergies among their requirements.



Deloitte.
EU Policy Centre Digital Playbook
MAKING AN IMPACT THAT MATTERS Since 1845

[241] Deloitte. (2025, January 17). EUPC Digital Playbook. https://www.deloitte.com/content/dam/assets-zone2/be/en/docs/about/2024/eupc-digital-playbook.pdfhttps://www.deloitte.com/mt/en/services/consulting-risk/analysis/digital-playbook-summary.html