

TALLINN UNIVERSITY OF TECHNOLOGY  
School of Information Technologies

Csaba Virág

# **Building Competitive Cyber Capacity for Europe: A Strategic Framework for Digital Readiness**

Master's thesis

Supervisor: Rain Ottis  
PhD

Tallinn 2025

TALLINNA TEHNIKAÜLIKOOL  
Infotehnoloogia teaduskond

Csaba Virág

**Konkurentsivõimelise kübervõimekuse loomine  
Euroopas: digitaalse valmisoleku strateegiline  
raamistik**

Magistritöö

Juhendaja: Rain Ottis  
PhD

Tallinn 2025

## **Author's declaration of originality**

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Csaba Virág

18.05.2025

## **Abstract**

The European Union's digital transformation strategy recognises the cyber domain as a fundamental enabler of economic competitiveness, institutional and societal resilience, and digital sovereignty. Yet despite the adoption of various advanced frameworks like the NIS2 directive, the Cyber Resilience Act, or the Digital Decade Policy Programme, the cyber skills gap continues to grow. This thesis examines and addresses the possible shortfalls in the EU's cyber capacity-building efforts to close the skills gap: the persistent misalignment between strategic intent and the operational environment of human-centric cyber competencies.

The study assesses and evaluates the coherence, implementation and effectiveness of EU-level cybersecurity strategies and their implementation on selected Member States, specifically focusing on the balance between technical and non-technical skills development. Through literature review, policy analysis and structured synthesis of the competitive environment and workforce trends, the research identifies 10 systematic gaps – ranging from fragmented implementation and quantitative-based KPIs to low adoption of existing instruments such as the European Cybersecurity Skills Framework.

In response, this thesis introduces the Next-Generation EU Cyber Capacity Framework as a structured modular model designed to enhance EU cyber workforce development efforts. The framework integrates nine components: strategic skills intelligence, curriculum architecture, credential governance, institutional accreditation, incentive infrastructure, future readiness, KPI alignment, inclusion protocols, and continuous policy feedback - each aimed at enabling scalable, harmonised, and outcome-oriented talent development.

This thesis is written in English and is 134 pages long, including 6 chapters, 4 figures and 13 tables.

## **Annotatsioon**

Euroopa Liidu digitaalülemineku strateegias tunnustatakse kübervaldkonda kui majandusliku konkurentsivõime, institutsionaalse ja ühiskondliku vastupanuvõime ning digitaalse suveräänsuse põhitegurit. Kuid vaatamata erinevate kõrgetasemeliste raamistike, nagu NIS2 direktiiv, kübervastupidavuse seadus või digitaalse aastakümne poliitikaprogramm, vastuvõtmisele, kasvab küberoskuste puudujääk jätkuvalt. Käesolevas väitekirjas uuritakse ja käsitletakse võimalikke puudujääke ELi kübervõimekuse suurendamise jõupingutustes, et kõrvaldada oskuste puudujäägid: püsiv ebakõla strateegiliste kavatsuste ja inimkeskse küberpädevuse operatiivkeskkonna vahel.

Uuringus hinnatakse ELi tasandi küberturvalisuse strateegiate sidusust, rakendamist ja tõhusust ning nende rakendamist valitud liikmesriikides, keskendudes eelkõige tehniliste ja mittetehniliste oskuste arendamise vahelisele tasakaalule. Kirjanduse läbivaatamise, poliitika analüüsi ning konkurentsikeskkonna ja tööjõu suundumuste struktureeritud sünteesi abil tuvastatakse uuringus 10 süstemaatilist puudujääki - alates killustatud rakendamisest ja kvantitatiivsetel andmetel põhinevast küberturvalisuse infosüsteemist kuni olemasolevate vahendite, näiteks Euroopa küberturvalisuse oskuste raamistiku vähese kasutuselevõtmiseni.

Vastusena sellele probleemile tutvustatakse käesolevas töös ELi järgmise põlvkonna kübervõimekuse raamistikku kui struktureeritud moodulimudelit, mis on kavandatud ELi kübertööjõu arendamise jõupingutuste tõhustamiseks. Raamistik hõlmab endas üheksat komponenti: strateegilised oskused, õppekavade ülesehitus, kvalifikatsioonide haldus, institutsionaalne akrediteerimine, stiimulite infrastruktuur, tulevikuvalmidus, tulemusnäitajate (KPI) ühtlustamine, kaasamisprotokollid ja pidev poliitika tagasisidestamine. Kõigi nimetatud komponentide eesmärk on toetada skaleeritavat, ühtlustatud ning tulemustele orienteeritud talentide arendust.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 134 leheküljel, 6 peatükki, 4 joonist, 13 tabelit

## List of abbreviations and terms

AI	Artificial Intelligence
CCAF	Cybersecurity Culture Assessment Framework
CGI	Cyber Governance Instruments
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
CSF	Cybersecurity Skills Framework
Cyber Capacity Building	Developing skills, institutions, and frameworks to improve national or organisational cyber resilience.
Cyber Hygiene	Practices and steps that users take to maintain system health and improve cybersecurity.
Cyber Ranges	Simulated environments for training and testing cyber capabilities and incident response.
Cyber Skills Gap	Mismatch between cybersecurity skills required by employers and those available in the workforce.
Cyber Solidarity Act	Proposed EU act to enhance collective response capabilities to large-scale cyber incidents.
CyberHEAD	Cybersecurity Higher Education Database
Cybersecurity Certification Framework	EU framework providing certification schemes for trusted cybersecurity products and services.
Cybersecurity Literacy	Basic understanding of cyber risks, safe behaviours, and security practices.
DDPP	Digital Decade Policy Programme
DEP	Digital Europe Programme
DESI	Digital Economy and Society Index
Digital Europe Programme	EU programme funding digital transformation initiatives, including cybersecurity training and infrastructure.
Digital Sovereignty	The capacity of a state or region to control its own digital infrastructure, data, and cybersecurity capabilities.
EC	European Commission
ECCC	European Cybersecurity Competence Centre
ECSA	European Cybersecurity Skills Academy
ECSF	European Cybersecurity Skills Framework
ENISA	European Union Agency for Cybersecurity
ESCO	European Classification of Skills
EU-CyCLONe	EU Cyber Crisis Liaison Organisation Network
GCI	Global Cybersecurity Ind
Human-Centric Cybersecurity	Approach that prioritises behavioural, educational, and organisational factors in cyber defence.
ICT	Information and Communication Technology
ITU	International Telecommunications Union

KPI	Key Performance Indicator
Microcredentials	Short, focused educational qualifications certifying specific skills, often in cybersecurity.
NCSI	National Cyber Security Index
NIS2	Network and Information Security Directive 2
PPP	Public-Private Partnership
PQC	Post-Quantum Cryptography
SCYWF	Skills Framework for Cybersecurity
SME	Small and Medium-sized Enterprise
SOC	Security Operations Center
STEM	Science, Technology, Engineering, and Mathematics
VET	Vocational Education and Training

## Table of contents

1 Introduction .....	15
1.1 Problem Statement.....	16
1.2 Research Questions.....	18
1.3 Study Aim and Objectives .....	18
1.4 Outline of Dissertation.....	19
2 Literature and Policy Landscape .....	21
2.1 Sources and Methodological Approach.....	21
2.2 The Strategic Relevance of Cybersecurity in the EU .....	25
2.3 Future Readiness as a Strategic Imperative .....	28
2.4 EU Cyber Governance Instruments and the Human Capital Agenda .....	30
2.4.1 ENISA and the European Cybersecurity Skills Framework .....	30
2.4.2 The Cybersecurity Skills Academy .....	31
2.4.3 Legal and Regulatory Instruments: NIS2, CRA, CSA .....	33
2.4.4 Funding Mechanisms and Policy Alignment .....	35
2.4.5 Supporting Instruments and Strategic Enablers .....	36
2.5 Performance Measurement and Capacity Indicators .....	37
2.5.1 Measuring Effectiveness: Metrics and Methodological Challenges .....	38
2.6 Impact of Cybersecurity Skills Gaps on EU Competitiveness and Economic Security .....	42
3 Methodology.....	45
3.1 Research Design .....	45
3.2 Case Selections .....	45
3.3 Data Analysis Procedures .....	47
3.4 Research Limitations .....	47
4 Discussion: Towards an Adaptive EU-National Capacity Framework .....	48
4.1 Introduction and Strategic Context.....	48
4.2 Strategic Benchmarking: Global Models and EU Positioning .....	48
4.2.1 Introduction .....	49
4.2.2 Strategic Framing: Defensive versus Offensive Workforce Development ...	49



4.2.3 USA .....	50
4.2.4 China.....	50
4.2.5 Russian Federation .....	51
4.2.6 Singapore .....	53
4.2.7 South Korea .....	54
4.2.8 Strategic Patterns and Lessons for the EU .....	54
4.3 Comparative EU Member State Insights .....	55
4.3.1 Estonia .....	56
4.3.2 Finland.....	57
4.3.3 France .....	58
4.3.4 Poland.....	59
4.3.5 Czech Republic.....	60
4.3.6 Translating EU Ambitions into National Practice.....	60
4.4 Gap Analysis.....	61
4.4.1 Strategic Gaps.....	62
4.4.2 Systematic Gaps .....	66
4.4.3 Operational Gaps .....	69
4.4.4 Measurement and Governance Gaps .....	72
4.4.5 The EU’s Implementation Dilemma .....	74
4.4.6 Conclusion.....	75
5 From Insight to Action: Designing a Next-Generation EU Cyber Capacity Framework (NG-EUCCF).....	77
5.1 Strategic Implications of the Cybersecurity Skills Gap.....	77
5.1.1 Identification and Clarification of Key Gaps .....	78
5.2 Conceptual Framework Overview .....	80
5.3 Framework Components and Implementation Design .....	82
5.3.1 Strategic Cyber Skills Intelligence Core .....	82
5.3.2 EU Cyber Capacity KPI Hub .....	83
5.3.3 Dual-Tier Curriculum Architecture (HEIs + ECCTPs).....	84
5.3.4 Credential Lifecycle and Recognition System .....	85
5.3.5 HEI Accreditation Scheme for Cybersecurity Excellence .....	87
5.3.6 Incentive Infrastructure.....	88
5.3.7 Future Readiness and Foresight Layer .....	90
5.3.8 Cyber Inclusion and Retention Protocol.....	91

5.3.9 Policy Feedback and Refinement Loop.....	93
5.4 Structure of the NG-EUCCF .....	95
5.5 Summary.....	96
5.6 Validation of NG-EUCCF .....	97
5.7 Key Findings of the Validation .....	97
6 Conclusion and Future Directions .....	102
6.1 Summary of Findings .....	102
6.1.1 Response to Main Research Question: How can EU cybersecurity capacity- building be improved to effectively and sustainably close the skills gap?.....	102
6.1.2 Responses to the Sub-Research Questions .....	103
6.2 Scientific and Practical Contributions .....	104
6.3 Limitations.....	105
6.4 Future Research Directions .....	105
6.5 Final Reflection .....	107
References .....	108
Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis .....	118
Appendix 2 - Tools Used.....	119
Appendix 3 – Digital Competence Test Samples.....	120
Appendix 4 – Validation Survey Questions & Responses .....	125

## **List of figures**

Figure 1 – Evolution of the cybersecurity skills gap [9] .....	17
Figure 2 The four strategic pillars of DDPP [20] .....	26
Figure 3 ENISA’s EU legislative landscape [45] .....	34
Figure 4 CyberHubs comparison of ICT Workforce and Cybersecurity Professionals by country[65] .....	40

## **List of tables**

Table 1 Research Keyword Matrix used during the literature review.....	25
Table 2 Gap-to-Framework Mapping Table.....	80
Table 3 Summary for Strategic Cyber Skills Intelligence Core .....	83
Table 4 Summary for EU Cyber Capacity KPI Hub .....	84
Table 5 Summary of the Dual-Tier Cyber Curriculum Model.....	85
Table 6 Summary of the Credential Lifecycle and Recognition Framework.....	87
Table 7 Summary of the HEI Cybersecurity Excellence Accreditation .....	88
Table 8 Summary of the EU Cyber Incentive Infrastructure.....	90
Table 9 Summary of the Future Readiness and Strategic Foresight Layer .....	91
Table 10 Summary of Diversity and Retention Measures.....	92
Table 11 Summary of Cyber Policy Feedback and Refinement .....	94
Table 12 NG-EUCCF Strategic Pillar View.....	94
Table 13 Functional Roles of NG-EUCCF Components .....	96

# DEDICATION

To my family, who believed me when I said this would be an easy ride and stood by me even when it wasn't.

To the colleagues, mentors, and partners who have shaped my professional journey through their trust, challenges, and examples.

To all those out there holding the line in one of the most underappreciated roles, quietly securing the digital future of the European Union.

To those building capacity, not just defences, you are the architects of a future in which technology serves freedom, not fear. Your quiet efforts may decide whether we inhabit a resilient, competitive, and humane Europe or one that relinquishes its future to fragility, fragmentation, or control. You draw us closer to a better version of tomorrow in every line of code, every training programme, and every act of foresight.

Finally, thank you for taking the time to read it.

# ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my supervisor, Dr. Rain Ottis, for his patience, insightful guidance, constructive feedback, and unwavering support throughout this research project. I would not have been able to finish this without you.

I also thank the faculty and staff of the School of Information Technologies at Tallinn University of Technology, whose input and encouragement helped shape the final thesis.

Finally, I appreciate the valuable discussions and perspectives shared by colleagues, policy experts, and practitioners, which helped sharpen the policy relevance of this work.

# 1 Introduction

The European Union acknowledges that cybersecurity skills are crucial for maintaining its competitiveness, technological independence, and digital resilience [1]. Key EU initiatives, including the NIS2 Directive[2], the Cyber Resilience Act [3] , and the Digital Decade Policy Programme [4] establish the cybersecurity workforce as a vital element in protecting digital infrastructure, fostering innovation, driving economic growth, and ensuring sustainable digital transformation across various sectors.

Nonetheless, despite this strategic framing, a significant gap remains between the goals of these policies and their actual implementation. Much of the existing literature focuses on cybersecurity workforce development primarily through the lens of technical training, addressing cyber skills. It tends to neglect the EU's view of cybersecurity competence as a more comprehensive capacity that enables secure digital ecosystems, facilitates cross-sectoral transformation, and supports democratic and economic stability.

This thesis reveals a critical flaw: while EU strategies emphasise the importance of cyber talent, the vague mechanisms and fragmented approaches hinder the practical implementation of coherent, outcome-oriented capacity-building across Member State. Frameworks like the European Cybersecurity Skills Framework and programs like the European Cybersecurity Skills Academy exist. However, their adoption is inconsistent, KPIS typically focus on outputs, and national implementations lack a unified efficiency tracking mechanism.

A thorough analysis of strategies implemented across the EU, including specific actions by Member States and the larger geopolitical and technological factors shaping the evolution of cyber capabilities, reveals 14 key shortcomings in the current cybersecurity capacity-building framework. These include insufficient strategic workforce intelligence, a disproportionate focus on compliance over capability development, the absence of standardised, outcome-oriented KPIs, weak integration of cybersecurity in non-cyber technical domains, and a lack of institutional incentives and accountability mechanisms.

This thesis proposes the Next-Generation EU Cyber Capacity Framework, a conceptual modular framework designed to align strategy with operational delivery. It introduces nine interconnected components: strategic skills intelligence, curriculum architecture,

credential governance, institutional accreditation, incentive infrastructure, future readiness, KPI alignment, inclusion protocols, and continuous policy feedback.

The conceptual framework is not a new policy instrument, but a structuring mechanism designed to support the coherent, scalable, and evidence-based delivery of cybersecurity capacity across the EU. It seeks to help EU institutions and Member States synchronise their initiatives, bridge the skills gap, and view cyber human capital not merely as an afterthought, but as a critical asset that enhances Europe's long-term competitiveness and resilience.

## **1.1 Problem Statement**

Despite the consistent emphasis on workforce development in EU cybersecurity strategies and vehicles such as the NIS2 Directive[2], the Cyber Resilience Act [3], or the EU Cybersecurity Strategy [5] a clear gap remains between political ambitions and implementation outcomes. While global economic instability and geopolitical conflicts grow, the worldwide spending on digital transformation is rising, which is expected to reach nearly \$4 trillion by 2027, according to the International Data Corporation [6]. Some even argue that the coming decade may deliver as much technological change as the previous century[7].

This exponential expansion of the digital landscape intensifies dependence on a skilled cyber workforce; however, talent availability remains a global challenge. Organisational and national success increasingly relies on adapting cutting-edge technology and the availability of human talent to operate it. In practice, the human factor consistently lags behind technical priorities. However, it is precisely this human layer – the skills, behaviours, and institutional readiness – that determines whether digital investments translate into long-term resilience and innovative capacity [8].

As illustrated in Figure 1 below, the cybersecurity skills gap, though widely acknowledged, continues to grow. The emergence of more complex and interdependent digital systems has made the capacity-building challenge both structural and urgent.



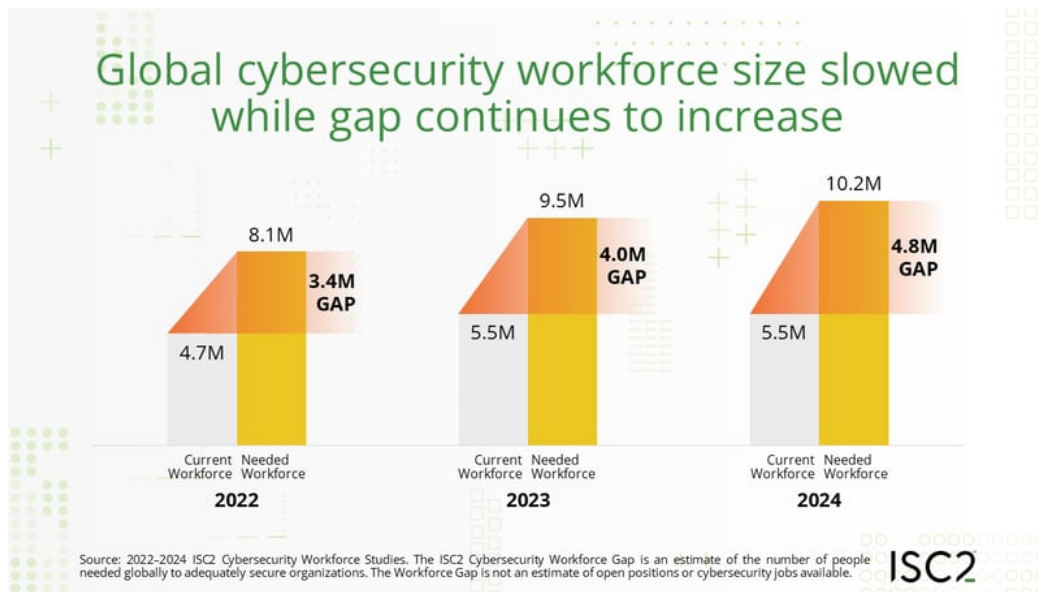


Figure 1 – Evolution of the cybersecurity skills gap [9]

Official policy documents frame cybersecurity as a technical discipline focused on networks and data protection. Consequently, less attention is given to its non-technical aspects essential for sustainable resilience, such as cyber-aware decision-making, behavioural resilience and critical cybersecurity literacy in non-technical roles [10]. In practice, cybersecurity should be a foundational skill, and it should be approached as a broader domain[11]. Even where broader human-factor elements are recognised, EU-level strategies often lack actionable implementation mechanisms, aligned incentives and consistent national uptake [12].

This gap in the approach risks compromising the EU's ability to leverage emerging technologies fully, capitalise on the digital single market and transition to a resilient digital economy. Bridging this requires shifting how necessary cyber skills are framed and developed, moving from a technology compliance-centric, siloed model to one that treats cyber capability as a strategic enabler embedded across the digital ecosystem.

This research investigates the extent to which existing EU cybersecurity strategies and related policies comprehensively address this broader cyber skills gap. It explores how policies are being implemented across Member States, covering both technical and non-technical competencies required to support and progress Europe's cyber-digital transformation.

The ENISA State of Cybersecurity in the EU report [12] reinforces the timeliness of this research. It calls for coordinated effort through the Cybersecurity Skills Academy, including standardised training, identification of emerging skills, stakeholder engagement and a European attestation framework for cybersecurity competencies.

## **1.2 Research Questions**

This research is guided by one main research question and five supporting sub-questions. It aims to explore and address potential gaps between EU cybersecurity strategies and actual capacity-building outcomes.

**MRQ: How can EU cybersecurity capacity-building be improved to effectively and sustainably close the skills gap?**

RQ1: How do existing EU cybersecurity strategies and policies prioritise human-factor cybersecurity competencies?

RQ2: How are these strategies being implemented by selected Member States?

RQ3: Do current EU cybersecurity policy frameworks primarily treat cybersecurity as a technical discipline or an enabling domain for broader digital readiness?

RQ4: What are the implications of these gaps for the EU's digital competitiveness and broader economic security?

RQ5: What practical strategic measures or incentives could the EU adopt to integrate and scale human-centric cybersecurity competencies effectively and sustainably to enhance long-term competitiveness?

## **1.3 Study Aim and Objectives**

This research aims to enhance the EU's cyber workforce development by examining the disparity between strategic goals and their execution, and proposing a structured framework for future capacity-building initiatives. The analysis focuses on identifying ongoing initiatives and evaluating their alignment with broader EU strategic goals, as well as understanding how current efforts contribute to the EU's long-term digital resilience

and competitiveness ambitions. In doing so, the research contributes to academic and policy discussions on EU cybersecurity capacity-building by:

- Examining the gap between strategic intentions at the EU level and their execution by Member States;
- Pinpointing systemic deficiencies in present cyber governance tools, especially the oversight of non-technical cyber abilities;
- Suggesting the Next-Generation EU Cyber Capacity Framework (NG-EUCCF) to facilitate scalable, skills-oriented growth;
- Providing actionable policy suggestions for unified, results-focused cybersecurity capacity enhancement throughout the EU.

## 1.4 Outline of Dissertation

This thesis is structured into six chapters, each contributing to analysing and resolving the EU cybersecurity skills gap by designing a strategic, future-ready capacity-building framework.

It starts with **Chapter 1 – Introduction**, which frames the strategic issue, clarifies the research objectives and questions. This chapter sets the context for the entire thesis, highlighting the importance of cybersecurity as a foundational element for EU competitiveness and resilience.

**Chapter 2 – Literature and Policy Landscape** synthesises academic and EU policy resources to examine the divide between theoretical goals and practical implementation in the context of cybersecurity workforce development. It reveals the gap between the EU's high-level ambitions and the actual measures taken to address the critical shortage of skilled cybersecurity professionals. This chapter also discusses the challenges associated with aligning strategic intent with practical workforce development at the Member State level.

**Chapter 3 – Methodology** outlines the research design, data sources, and analysis methods employed to assess EU and Member State practices. Additionally, it clarifies the criteria for spotting systemic gaps and suggests possible limitations.

#### **Chapter 4 – Discussion: Towards an Adaptive EU-National Capacity Framework**

presents the findings from the gap analysis, focusing on the structural and functional discrepancies between EU and national cybersecurity strategies. This chapter examines the challenges of translating strategic intent into practical implementation, particularly about human-centric competencies.

#### **Chapter 5 – From Insight to Action: Designing a Next-Generation EU Cyber Capacity Framework (NG-EUCCF)**

introduces the conceptual Next-Generation EU Cyber Capacity Framework, detailing its components and how it addresses challenges related to implementation fragmentation, scalability, and strategic misalignment. This framework is proposed as a structured solution to align policy ambitions with measurable outcomes.

#### **Chapter 6 – Conclusion and Recommendations**

summarises key insights, offers policy recommendations for the EU and Member States, and outlines future research priorities to advance a cohesive, outcome-driven cybersecurity workforce agenda. It reflects the implications of the findings for EU competitiveness and resilience, providing a roadmap for future capacity-building efforts.

## **2 Literature and Policy Landscape**

Chapter 2 establishes the analytical groundwork for this research by exploring the treatment of cybersecurity workforce development in both EU strategic frameworks and academic literature. While academic discussions mainly emphasise technical skills and workforce pathways, EU policy increasingly regards cybersecurity and cyber competence as vital for achieving digital sovereignty, promoting economic growth, and fostering cross-sector innovation [13].

This chapter highlights a significant misalignment: despite a shared concern about the skills gap, there is a lack of clarity, both conceptually and operationally, on how to develop sustainable, measurable, and human-centric cyber capabilities on a large scale. The conclusions drawn from this chapter inform the subsequent gap analysis in Chapter 4 and ultimately shape the framework design in Chapter 5.

### **2.1 Sources and Methodological Approach**

This section outlines the sources and methodological approach to review the literature and policy material. The review draws from two interdependent perspectives:

1. Analysing EU strategic and regulatory instruments, or as they are collectively referred to in this research, Cyber Governance Instruments (CGIs), to understand the EU's formal vision, priorities and implementation mechanisms regarding cyber skills development.
2. Academic research, to understand empirical findings and theoretical debates on the effectiveness of current policy and its implementation.

This combined method systematically evaluates strategic alignment and operational efficacy, establishing a foundation for assessing the consistency between policy goals and actual results.

#### **Sources used:**

Institutional (Policy and Strategy):

- European Commission

- ENISA publications
- EUR-Lex
- European Cybersecurity Skills Academy
- OECD policy briefings
- Selected Member States and international national strategy and policy sources

#### Academic:

- IEEE Xplore
- Scopus
- ScienceDirect
- JSTOR
- ProQuest
- Taylor & Francis Online

The search utilised thematic clusters corresponding to the research questions, incorporating term combinations like: "cybersecurity skills gap", "European Cybersecurity Skills Framework", "cyber capacity building", "human factors in cybersecurity", "NIS2 implementation", "digital competitiveness", and "cyber resilience KPIs".

Furthermore, citation tracking or "snowballing" was used on key articles and policy reports to identify additional relevant resources. Where applicable, grey materials like news articles and video reports were sourced.

#### **Inclusion and Exclusion Criteria**

To ensure the reviewed literature is directly relevant and of sufficient quality, the following inclusion and exclusion criteria are applied:

#### **Inclusion Criteria:**

- EU-level strategies, directives, frameworks, or official publications addressing cybersecurity capacity building, skills development, or policy implementation.
- Academic research discussing cybersecurity skills in Europe, including technical and non-technical competencies, policy analysis, and implementation studies.
- Documents published mainly 2020 onward, with select foundational works included when highly cited or referenced in official EU frameworks.
- Materials published in English or reliably translated.
- Policy and research documents on global competitiveness and skills development in the digital age.
- In some cases, pre-2020 documents are used if no recent document is available.

#### **Exclusion Criteria:**

- Publications lacking clear relevance to the research context or without transferability to EU-level policy, capacity-building structures or global competitiveness in the digital age.
- Outdated frameworks or policy drafts superseded by current legislation.
- Technical cybersecurity research without workforce development, education, or policy implications.

#### **Research and Selection Protocol**

- Keyword-driven database queries were executed using thematic filters (e.g., "human-centric cyber skills", "EU cybersecurity strategy", "workforce readiness").
- Titles and abstracts were screened against defined criteria, and materials that did not align with the research focus were discarded.
- A full-text review of eligible sources ensured depth and conceptual alignment.

- Snowballing was used to identify additional key publications from the references of both academic articles and EU documents.
- A keyword matrix was used to track search terms and database outputs.

### Methodological Considerations and Limitations

- The review may exclude non-English policy documents and research papers that are unavailable through official EU portals or reliable translations.
- In some instances, AI-assisted translation was employed when no reliable alternative solution could be found.
- Some implementation data at the Member State level remains restricted or unpublished, restricting cross-national comparison.
- The scope and timeframe of the thesis may limit the depth of research on specific topics.

Table 1 below presents the research keyword matrix used during the literature review.

Prompt	JSTOR	OECD	ProQuest	Scopus	Science Direct	IEEE
"EU cybersecurity skills strategy" AND labor market	0/0	0/0	0/0	0/0	0/0	0/0
"European Cybersecurity Skills Framework" AND implementation	0/0	0/0	0/2	0/2	3/4	0/0
"ENISA" AND cybersecurity education	0/69	0/3	0/328	4/18	15/181	2/5
"Digital Decade 2030" AND cybersecurity workforce	0/0	0/0	0/0	0	1/1	0/0
"Digital Decade 2030"	1/1		1/1	0/6	0/4	0/0
"EU Skills gap"	0/0	0/0	0/0	0/0	0/0	0/0
"EU Skills Agenda"	1/1	v	1/1	3/1	0/0	0/0
"Cybersecurity policy" AND "European Union" AND skills AND gap	4/13	1/1	6/102	0	6/51	0/0
national AND future AND readiness	0/0	0/0	0/1	0/541	0/23755	0/150
"national future readiness"	0/0	0/0	0/0	0/0	0/0	0/0



future readiness	0/295	0/3	0/411	0/0	0/0	0/0
------------------	-------	-----	-------	-----	-----	-----

Table 1 Research Keyword Matrix used during the literature review

While the systematic research in the selected databases provided limited academic results, using snowballing method from these and the EU level strategies, policies and documentations provided enough results for the research. Altogether 150 references have been used for the research.

Examining the policy documents and academic literature reveals several recurring themes that significantly impact the cyber skills gap in the EU. These themes reflect perceptions of the issue and outline how capacity building is prioritised, implemented, and assessed. The synthesis below identifies and analyses the primary patterns crucial for understanding the strategic gap between the EU's objectives and the actions of Member States. These themes act as an analytical bridge between the policy landscape and the forthcoming gap analysis in Chapter 4.

## 2.2 The Strategic Relevance of Cybersecurity in the EU

Since the early 2010s, cybersecurity and its capacity-building aspects have gained strategic importance within the European Union. This shift is driven by the accelerating digital transformation and increasingly complex cyber threats, which directly affect national competitiveness and future preparedness [14], [15], [16]. Although technical frameworks and standards support EU cybersecurity policy, the integration of human-centric factors varies significantly across Member States [14].

The EU's policy framework ecosystem comprises an expanding collection of strategies, directives, and regulations, collectively termed Cyber Governance Instruments (CGIs) in this study. Tools like the NIS2 Directive [17], Cybersecurity Act (CSA) [18], Cyber Resilience Act (CRA) [2], and the 2020 EU Cybersecurity Strategy [5] highlight the need for regulatory harmonisation to enhance cyber resilience. However, the effectiveness of these frameworks often falters due to their inadequate addressing of human factors—behavioural risks, educational alignment, and true workforce competency gaps [14].

The EU Cybersecurity Strategy 2020 [5] covers a wide array of topics, from technical capabilities, through cyber resilience capability development to diplomacy matters. For the human capital development in the cyber domain, the Strategy refers to the Digital

Education Action Plan (2021-2027) [19] to raise cybersecurity awareness among individuals and encourage women's participation in STEM education. The Action Plan outlines 13 priority actions to build a “high-performing digital education ecosystem” and enhance digital skills across EU society.

This emphasis continues through the Digital Decade Policy Programme 2030 (DDPP) [4], which formalised key targets for EU digital transformation as shown in Figure 3. The first strategic pillar is establishing a digitally skilled population and highly skilled digital professionals, including at least 20 million ICT specialists by 2030. These targets are tracked by the Digital Economy and Society Index (DESI) [20], which uses metrics such as the proportion of individuals with basic or advanced skills.

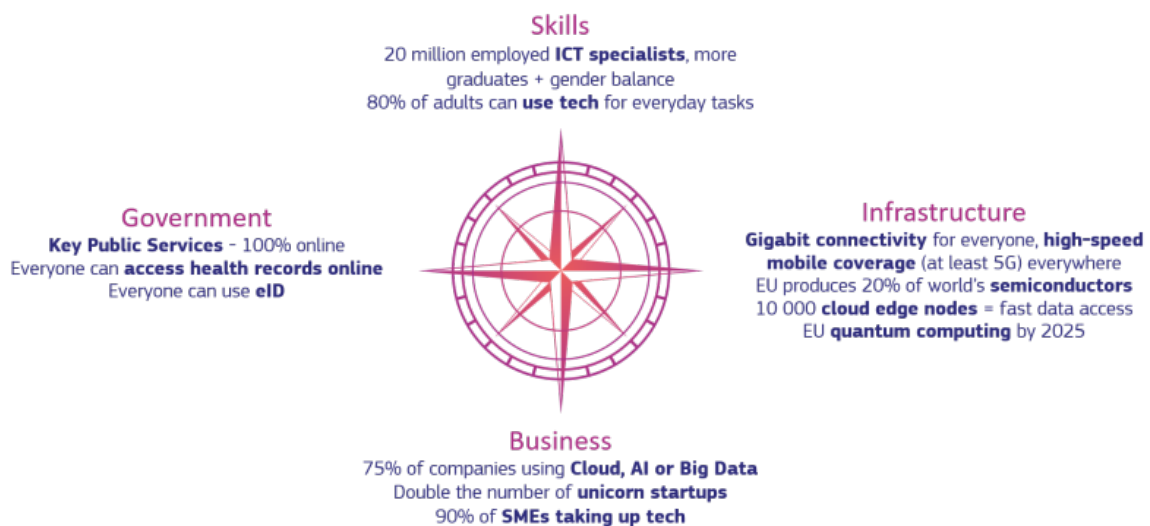


Figure 2 The four strategic pillars of DDPP [20]

While DESI indirectly includes indicators relevant to cybersecurity, it focuses primarily on general digital readiness. Metrics such as the number of ICT specialists or gender representation in tech reflect the digital workforce rather than specialised cybersecurity capacity or workforce that is cyber enabled. Also, it is a quantitative rather than a qualitative metric, showing a gap for better situational awareness on the actual skills and competencies of the talents accounted for.

Complementary frameworks such as the European Skills Agenda [21] also highlight cybersecurity, while advocating for transversal skills like critical thinking, collaboration, and problem-solving, as essential to digital transformation. It introduces individual skills accounts, which could incentivise lifelong learning and upskilling in cyber-related

domains. As a financing mechanism, the Digital Europe Programme [22] aims to expand specialised cybersecurity training and academic offerings across the EU. The growing challenge of lacking skilled cyber talent supporting cybersecurity and also innovation capability is discussed as a compounding urgent priority by ENISA [12].

Despite progress, the current cyber talent pipeline remains insufficient. Data from the Cybersecurity Higher Education Database (Cyberhead)[20] shows that in 2023 only 3,400 cybersecurity graduates entered the European workforce, a 44% increase over four years, but still far below the estimated 300,000 specialists required. Consequently, re-skilling and upskilling initiatives are urgent.

The United Nations Open-Ended Working Group defines cyber capacity-building as enhancing digital resilience, requiring sustainability, evidence-based practice, and alignment with national priorities [23]. In addition to bridging digital divides, capacity-building strengthens critical infrastructure protection, enhances legal and policy coordination, and facilitates international engagement in cyber diplomacy.

Beyond bridging the digital divide, cyber capacity-building enhances ICT resilience, protects critical infrastructure, and fosters coordination between technical and policy capacities. It also fosters expertise in legal, policy, and diplomatic domains, enabling states to engage in international processes and address systemic cybersecurity risks [23].

However, within the EU, institutional barriers persist. Member States continue to treat cybersecurity as a sovereign issue, often resisting deeper integration or shared mechanisms for workforce development [5]. Moreover, the EU Cybersecurity Strategy focuses heavily on state-level resilience and threat-based logic, deprioritising human-centric and individual-level capacity-building initiatives or the broader impact of the cyber domain. This fragmented approach limits the effectiveness of EU-wide strategies and also complicates the implementation across Member States.

This institutional fragmentation extends beyond the EU. For example, the widely adopted NIST NICE framework underrepresents human factors, reducing behavioural aspects to secondary prioritisation [24]. However, understanding human cognition and behaviour is as crucial as analysing malicious code in mitigating vulnerabilities [25].

The EU Cybersecurity Strategy mentions numerous ambitious projects supported by the EC and implemented; however, the document does not align the human capacity-building requirements to support these ambitions. The only mentions are the importance of the skilled workforce, the need for cyber hygiene, a proposed development of EU curricula, and a reference to the Revised Digital Education Action Plan [26] to raise awareness. But it doesn't discuss or mandate the actual skills needed to support the overall strategic ambitions.

The EU Cyberskills Report further reveals that the majority of the 12916 respondents of businesses interviewed have not heard about the European Cyber Security Skills Framework (ECSF)[27]. The low uptake and awareness for the ECSF is also reflected in the validation survey done during the current research. Other research [26] on digital skills certifications found no actual demand for such certifications, which might not be true for cybersecurity job postings, as the majority of the job advertisements still demand cybersecurity certifications and experience [28], [29].

## **2.3 Future Readiness as a Strategic Imperative**

The concept of future readiness often appears in policy and economic discussions; however, its definition remains vague, especially regarding national strategic planning. Academic literature offers limited clarity, and its main emphasis is limited to specific sectors like education. An analysis of scholarly databases shows that although many papers mention "future readiness," there is no uniform framework for national assessment [34, 35].

In broad terms, future readiness refers to the ability of societies, economies, or institutions to anticipate, adapt to, and thrive amidst disruption. The IMD World Digital Competitiveness Ranking conceptualises it through indicators such as adaptive attitudes, business agility, and IT integration [33]. However, as stated above, no standardised indicators exist at the national level.

In the EU context, the term often appears alongside the Twin Transitions [33] – the digital and the green, and is closely linked to the labour market's adaptability. A future-ready workforce is characterised by its ability to leverage emerging technologies, innovate within dynamic digital environments, and adapt to continuous change [34].

The EU's focus on future readiness is reflected in initiatives such as the European Year of Skills 2023 [35] and the Digital Decade targets for 2030 [1]. European leaders link future readiness with widespread digital literacy, a solid foundation of ICT specialists, and a culture of lifelong learning [34].

Cybersecurity is recognised as an enabling factor for future readiness [11]. It is defined as “an essential element of the new digitally driven society”, as stated in a report by the Joint Research Centre [16]. A digitally advanced society cannot be considered “future-ready” if its infrastructure and workforce remain vulnerable. EU officials have emphasised that enhancing cybersecurity skills is “the best way to tackle the evolving cybersecurity threat landscape and respond to emerging threats”, advocating for reskilling and upskilling across all sectors to achieve a higher level of cyber preparedness [32]. Cybersecurity competence ensures Europe can adopt advanced and emerging technologies (such as cloud, AI, and quantum), and it has the expertise to secure these systems against new threats while taking advantage of the benefits [12], [16]. This capability is essential for resilience and a core component of technological sovereignty [1].

The World Economic Forum advocates that a “future-ready workforce” is inclusive, digitally skilled, and empowered to handle technologies like AI responsibly [15]. One of the most recent comprehensive reports on EU competitiveness, The Future of European Competitiveness Report [36], emphasises the importance of equipping citizens with the skills necessary to thrive in an era of rapid technological change. It also highlights that the EU's competitiveness now relies more on the knowledge and skills of its workforce, than on traditional labour cost advantages. The report also describes the EU's structural limitations in rapidly designing and coordinating effective industrial policy measures, especially when compared to the US or China.

The three main coordination challenges defined by the Competitiveness report are (1) poor alignment between Member States, leading to duplicated efforts and unequal state support within the Single Market; (2) fragmented financing mechanisms, which prevent the pooling of capital and introduce complexity for private sector actors; and (3) disjointed policy frameworks, where industrial, fiscal, trade, and foreign economic policies remain siloed rather than integrated. Based on the report, the EU's current

governance structure and slow policymaking processes hinder the development of coherent, large-scale responses required for global competitiveness.

In summary, future readiness in the EU context is both a strategic goal and a measurement challenge. It requires forward-looking alignment of skills development with anticipated technological and geopolitical trends. Cybersecurity skills occupy a dual role: they present both a specialised domain and a foundational enabler of sustainable digital transformation. While the EU's strength lies in its diversity as a political and economic union, the same diversity can also hinder unified action on talent shortages and competitiveness compared to more centralised actors like the US, China or Russia.

## **2.4 EU Cyber Governance Instruments and the Human Capital**

### **Agenda**

As the cyber domain grew, so did investment in EU institutional and regulatory frameworks to enhance cybersecurity capacity. Previously viewed as a secondary matter, human capital development is now central to EU cybersecurity policy, supported by directives, funding initiatives, and collaborative platforms. This section examines the key Cyber Governance Instruments (CGIs), their focus on human elements, and the strategic objectives to develop a skilled cybersecurity workforce.

#### **2.4.1 ENISA and the European Cybersecurity Skills Framework**

The EU's cybersecurity agency, ENISA, drives capacity building and skills development with the EU as mandated by the Cybersecurity Act[18]. In 2022, ENISA released the European Cybersecurity Skills Framework (ECSF) [37], a practical tool to harmonise role profiles, competencies, skills, and knowledge areas for cybersecurity professionals across Europe. The ECSF identifies 12 typical cybersecurity roles, including security analyst, incident responder, security architect, and cybersecurity auditor, along with the required competencies and skills and links them to standardised knowledge, skills and competencies.

The harmonised taxonomy supports governments, employers, and educators in identifying skill requirements and developing targeted training programmes. For example, an organisation can utilise the ECSF to conduct a skills gap analysis and plan training for specific roles (e.g. identifying the need for a cybersecurity legal officer vs. a

cryptography expert). The ECSF also facilitates cross-border recognition of skills and certifications to support the free movement of talent.

ENISA also coordinates cybersecurity training and exercise programs (such as Cyber Europe cyber crisis exercises and “train-the-trainer” initiatives) [38]. This operationalises ECSF’s competences through experiential environments for national authorities, critical infrastructure operators and incident response teams.

While ECSF is aimed to be an essential strategic instrument, its adoption is limited. As mentioned earlier, the State of the Cybersecurity Report [12] found that most European employers and education institutions are still either unaware of the framework or have not yet adapted it. Without a broad uptake, the ECSF cannot fulfil its function as unifying standard across EU’s cyber talent ecosystem [39].

Moreover, the EU faces a critical shortage of cybersecurity professionals, jeopardising the security of businesses, institutions, and critical infrastructure [40]. The lack of qualified personnel hampers the ability to detect and respond to cyber incidents promptly and also limits EU’s ability for sustainable digital innovation and a resilient digital society [1], [16], [41].

ECSF aims to be a fundamental denominator addressing the joint understanding of cyber skills and competences. As its integration into national education and workforce development strategies is limited, its success depends on institutional commitment to implementation and employer recognition. The challenges with these are explored in the following sections.

#### **2.4.2 The Cybersecurity Skills Academy**

To close the cybersecurity talent gap and boost the EU’s competitiveness, growth and resilience, the EU has established the European Cybersecurity Skills Academy (ECSA) [40]. The Academy was established in response to Europe's growing cybersecurity skills gap. The initiative arose from an urgent need to enhance digital resilience amid rising cyber threats and increasingly stringent EU cybersecurity regulations.

Hosted on the Digital Skills and Jobs Platform [42], the Academy is a hub for mapping training initiatives, showcasing best practices, and facilitating a structured engagement. The Academy builds around four pillars: (1) Knowledge & Training – establishing a

common EU approach to cybersecurity curricula; (2) Funding & Projects – aligning funding and maximising impact of skills initiatives; (3) Industry-Academia Network & Pledges – mobilising companies and universities to increase training (with a focus on diversity and inclusion); and (4) Measuring Progress – developing metrics to monitor the workforce gap and track improvements.

The Academy has already garnered support from industry and academia through pledges. For example, professional bodies have committed to training and certifying thousands of Europeans, and companies expressed their willingness to train 100,000 European learners. This reflects a public-private alliance approach to expanding the talent base.

The Academy aims to address the low uptake in standardised cybersecurity job profiles and improve coordination among key stakeholders. Additionally, it seeks to address the challenges of assessing the quality and relevance of cybersecurity training. It states that without a well-trained workforce, EU policies and regulatory frameworks - including the NIS2 Directive, Cyber Resilience Act, and Cyber Solidarity Act - risk falling short of their intended impact [43].

The Academy establishes itself as the EU's premier resource for cybersecurity training, offering customised learning opportunities for students, professionals, small and medium-sized enterprises (SMES), and public administrations. Its implementation is also expected to strengthen cooperation between higher education institutions and vocational training centres, supporting joint degree programs, micro-credentials, and practical learning experiences such as apprenticeships, simulation-based training, and immersion weeks. By integrating cybersecurity into broader education and workforce development programs, the initiative aims to equip the EU with the skilled workforce necessary to sustain its digital sovereignty, economic competitiveness, and cyber resilience in an increasingly interconnected world.

The Report on the State of Cybersecurity [9] reinforces the Academy's importance, and goes even further in recommendations: To address the cybersecurity workforce gap, ENISA and the European Commission (EC) are encouraged to conduct an advanced skills gap analysis using the European Cybersecurity Skills Framework [37], identifying misalignments between industry demand and workforce supply. The findings recommend that Member States collaborate with the EC and ENISA to develop a monitoring



framework for workforce trends and integrate a cybersecurity workforce strategy into their national cybersecurity strategies, in line with NIS2 Directive requirements.

The report also recommends specific actions to attract and retain cybersecurity specialists, enhance cyber hygiene, and promote mentorship programs to address gender imbalances. Additionally, it emphasises the importance of reskilling professionals from other disciplines and providing cybersecurity training for public sector employees in response to increasing cyber threats targeting public administration.

Despite its strategic promise, the Academy's success depends on the broad adaptation, alignment with stakeholders and national strategies. Its voluntary nature and uneven awareness across MSs limits its potential impact. As a coordination instrument and mechanism, ECSA represents an important evolution in EU cyber capacity governance. Still, its ability to scale depends on closing the structural gaps in standardisation and institutional uptake, as further discussed in the following sections.

#### **2.4.3 Legal and Regulatory Instruments: NIS2, CRA, CSA**

The European Union has developed a broad cybersecurity and digital resilience framework to address the growing cyber threat landscape [44]. Key legislative initiatives aim to secure critical infrastructure, enhance incident response, and improve cybersecurity governance. Figure 4 below visualises the legislative landscape.

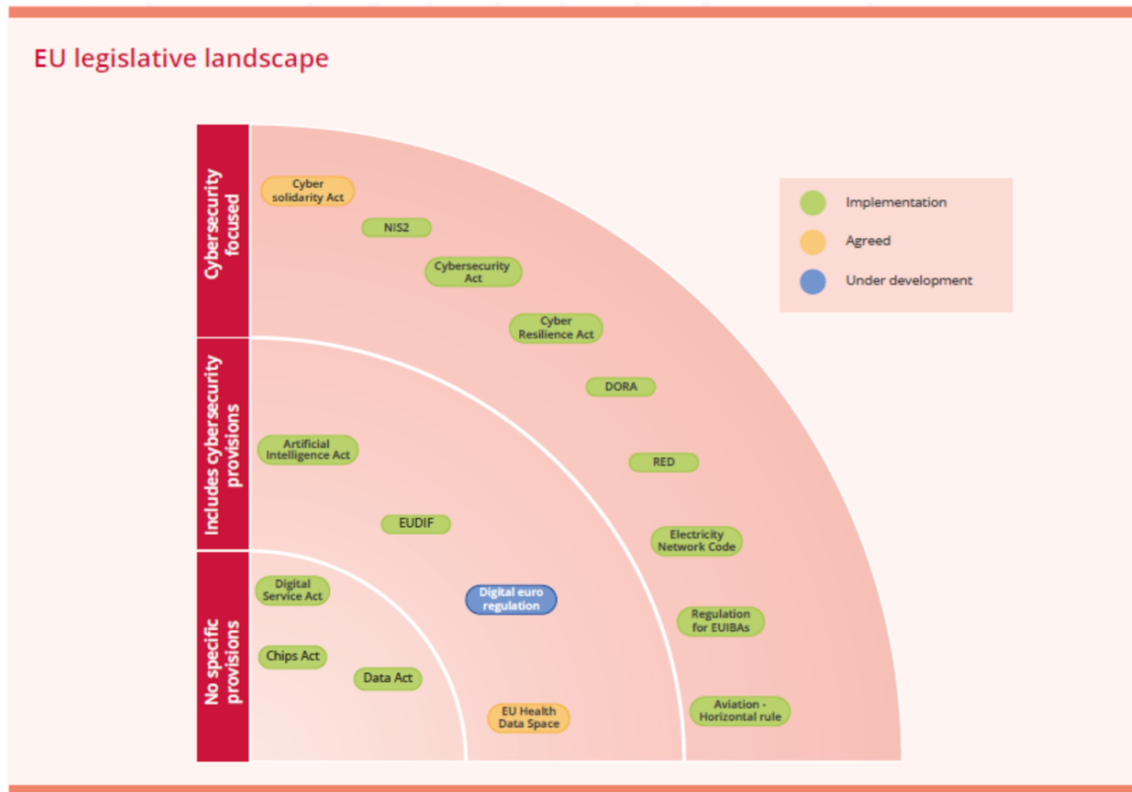


Figure 3 ENISA's EU legislative landscape [45]

The Cybersecurity Act (CSA) [46] established ENISA as a permanent body, formalising its role in capacity-building, strategic coordination, and skills development across Member States. It also introduced the Cybersecurity Certification Framework, which sets a mechanism to establish trust in digital services and products, and as well as competencies.

The strategic shift in the evolving regulatory framework is also reflected in the revised Directive on Security of Network and Information Systems (NIS2) [47] that entered into force in 2023, broadening the range of sectors subject to EU cybersecurity requirements and elevating the importance of workforce skills.

Article 21 of the NIS2 directive explicitly requires Member States promoting cybersecurity education, exercises, and skills-building across public and private entities, and Article 22 obliges executives of essential services to undergo training in cybersecurity risks [47]. These NIS2 provisions affirm that robust cyber resilience depends on the availability of skilled and adequately trained professionals, reinforcing the role of workforce development in EU cybersecurity policy.

NIS2 requires national authorities to ensure that the supervisory tasks over essential entities are conducted by trained professionals with the necessary skills for on-site inspections, off-site supervision, and identifying vulnerabilities in critical cybersecurity infrastructure. It also mandates that MSs adopt policies promoting cybersecurity education, training, skills development, awareness initiatives, research, and good cyber hygiene practices for citizens and organisations as part of their national cybersecurity strategies.

The Cooperation Group under NIS2 has been established to facilitate strategic cooperation, information exchange, and the building of trust. It supports capacity building, cybersecurity exercises, standardisation efforts, and the sharing of best practices among MSs. This collaboration is structured through biennial work programs, guiding implementation efforts such as threat intelligence, incident response, and workforce development under the directive.

Complementing the NIS2 directive, the Cyber Resilience Act (CRA) [46] sets the requirements for security-by-design for products and services, reinforcing the need for skilled and cyber-informed developers, compliance professionals, lifecycle managers, and an overall cyber-competent workforce in the digital space.

Together, CSA, NIS2, and CRA showcase the evolution of the regulatory approach: from guidance to enforcement and also making cybersecurity a responsibility. Human capital is no longer a side objective, but a legal and operational pillar of cybersecurity governance. As discussed in the following section, these instruments form the basis for policy alignment and funding coordination.

#### **2.4.4 Funding Mechanisms and Policy Alignment**

The practical implementation of any policy depends on regulatory mandates, sustained funding, and strategic coherence. The EU is constantly embedding human capital development into its broader digital investment agenda, with a focus on aligning skills initiatives with strategic goals for resilience, competitiveness, and digital sovereignty.

The Digital Europe Programme (2021–2027) (DEP) allocates a significant portion of its €7.5 billion overall budget, approximately € 1.9 billion, to cybersecurity and the development of advanced digital skills. Under Specific Objective 3 (“Cybersecurity and

Trust”) [48], DEP explicitly aims to “support closing the cybersecurity skills gap” by aligning training programs with sector needs and improving access to specialised cybersecurity training. Likewise, Specific Objective 4 targets Advanced Digital Skills for the current and future workforce, offering on-the-job training, courses, and short-term professional training in key technologies, including cybersecurity. However, the exact cybersecurity skills gap to be addressed is defined in broad terms.

A European Data Space for Skills is under development to support evidence-based planning. This initiative aims to provide real-time visibility into supply and demand for skills based on stakeholders’ needs. However, the latest news from them was posted in 2023 [49].

In parallel, the European Skills Agenda (2020) [50] functions as an overarching EU policy roadmap for future workforce development. It highlights that accelerated digitalization creates urgent demand for experts, citing a gap of nearly 291,000 cybersecurity professionals in Europe as of 2019. The Skills Agenda frames cybersecurity skills as part of ensuring Europe’s workforce is “future-proof” and resilient. Notably, the Agenda links cybersecurity preparedness to broader resilience: “Challenges to IT infrastructure and e-systems have revealed the need to improve our human capacity for cybersecurity preparedness and response.”

Collectively, these instruments represent the resourcing mechanisms supporting the EU’s policy ambitions. However, challenges remain. Despite growing investment and focus, fragmentation persists between EU-level programs and their implementation. Limited interoperability between workforce data and the lack of standardised indicators weaken the feedback loop between funding, performance and long-term capacity outcomes. These issues are examined in the following sections and Chapter 4.

## **2.4.5 Supporting Instruments and Strategic Enablers**

Alongside the regulatory and funding instruments previously discussed, several other notable EU initiatives and CGIs contribute to a broader strategic and institutional environment conducive to capacity-building. These initiatives create structural incentives, set capability baselines, and set the operational environment for a cyber-informed workforce and society in the EU.

The **Cyber Solidarity Act** [51] establishes a European Cybersecurity Alert System to coordinate incident detection and response across the EU. While the scope is operational, it increases the need for skilled cyber operators and cross-border coordination capability.

The **EU Cybersecurity Certification Framework** [52] established under the Cybersecurity Act, it creates a foundation for trusted digital services and products through certification schemes such as the EU Common Criteria and cloud security standards. While primarily product-focused, these schemes help define competence expectations for design, assessment, and compliance practitioners.

The **Cybersecurity Risk Management for EU Institutions** [53] establishes institutional governance and control mechanisms for EU bodies, by strengthening the role of CERT-EU. Similarly, the **EU Cyber Defence Policy** [54] strengthens cooperation between civilian cybersecurity efforts and military defence systems, creating a comprehensive cyber deterrence strategy.

The **European Cybersecurity Competence Centre and Network** [55] promotes joint investments in cybersecurity innovation and capability-building efforts to enhance the EU's technological sovereignty. The **Economic Security Strategy** [54] conducts cybersecurity risk assessments for emerging technologies, including AI, semiconductors, and quantum computing, domains that require specialised cyber expertise.

Finally, the **EU Cyber Liaison Officers Network (EU-CyCLONe)** [56] strengthens crisis management and coordination between Member States during cyber incidents, reinforcing standardised protocols and the value of joint training and preparedness.

Collectively, these instruments serve as strategic enablers within the broader EU policy domains for human capital development, encompassing certifications and defence, technology leadership, and institutional resilience.

## **2.5 Performance Measurement and Capacity Indicators**

Measuring performance effectively is essential for providing situational awareness on tracking the progression of converting strategic goals into real results. EU cybersecurity strategies typically define Key Performance Indicators and metrics to monitor progress; however, the actual contribution of these measures to the strategic objectives set varies

significantly. This section examines the various metrics established within Cyber Governance Instruments. It evaluates their alignment with the strategic objectives outlined in EU policy, assessing whether these indicators accurately reflect the desired outcomes.

### **2.5.1 Measuring Effectiveness: Metrics and Methodological Challenges**

Several quantitative KPIs are being set to assess cybersecurity skills development, while future or digital readiness is mainly covered as a qualitative indicator across the various strategies and literature.

Measuring capacity-building performance is a challenging and underdeveloped aspect of the EU's strategic agenda. While ambitions and key targets have been established and the Digital Decade Policy Program [57] is tracking KPIs, many existing indicators are too general and offer limited granularity to assess specific progress made.

According to the OECD [58] a key challenge lies in defining what to measure and how. Different sources gather and present cybersecurity data using varied methodologies influenced by the respective incentives, regulatory requirements and operational context. Official bodies rely on surveys mandated by law or administrative registers, offering systematic but often delayed data. At the same time, the private actors typically use non-sample surveys and expert assessments shaped by commercial motives, resulting in inconsistent quality and scope.

As of 2022, the shortage of cybersecurity professionals in the EU was estimated to be between 260,000 and 500,000, while the total workforce required was approximately 883,000 [59]. Additionally, only about 19% of ICT specialists and ~20% of cybersecurity graduates in Europe are women, so improving gender balance is a priority [1]. In 2024 the estimated skills gap is 299.000 showing a growing gap even though more specialists have been trained [40]. The European Commission has explicitly warned that Europe's "most valuable resource: its people" are urgently needed in cybersecurity roles to protect the economy [40].

The EU's Cybersecurity Strategy and Digital Decade program [60] both emphasise the development of "highly skilled digital professionals" (which includes cybersecurity

experts) as vital for Europe's digital sovereignty [5]. The EU relies on a set of KPIs to measure progress on these priorities, though some are broad in scope.

The headline KPIs are the Digital Decade's twin targets for skills: percentage of the population with at least basic digital skills (target 80%) and number of ICT specialists employed (target 20 million)[4]. These are tracked annually through reports like the Digital Economy and Society Index (DESI) [61] and Eurostat [57] data. For example, according to Eurostat, by 2023, 56% of EU citizens had basic digital skills (up from 54% in 2019), while ICT specialists were about 9 million (just over 4% of the workforce) – indicating significant ground to cover. The share of female ICT specialists is another KPI (with the aim of “gender convergence”), as is the share of recent ICT graduates.

As described by ISC2 [9], findings show that the skills gap is significant and is constantly rising across the globe, although the number of available specialists is increasing. Rapid digitalisation is happening faster than the skilling of the workforce can keep pace with it. As a KPI, several strategies set targets for training outputs, like the number of ICT or cybersecurity specialists trained, certified or educated[12], [40], [62], [63].

At EU level, various KPIs are monitored alongside broader digital benchmarks, with some explicitly focusing on cybersecurity. DESI is the leading indicator for tracking cybersecurity skills, evaluating Member States' digital performance. Relevant KPIs within DESI include the percentage of individuals with at least basic digital skills, the number of ICT specialists in the workforce, and gender representation among ICT specialists. These metrics serve as an overall measure of the talent pool. For example, by 2030, the EU aims to increase the number of employed ICT specialists to 20 million, up from approximately 9 million in 2020, while fostering a more balanced gender[1].

Not every ICT specialist is a cybersecurity expert, yet this KPI serves as a proxy. As the number of ICT specialists increases, so does the expectation for more cybersecurity professionals. The EU Cybersecurity Strategy and its subsequent initiatives highlight metrics such as the cybersecurity workforce gap, which is monitored over time as a key indicator of success.

European Cybersecurity Skills Academy is also focused on monitoring efforts: one of its four main action areas is “Measuring progress,” which is developing a methodology to track changes in the cybersecurity job market and efforts to bridge the skills gap. Specific

indicators being created under this initiative include the number of people achieving cybersecurity certifications or completing recognised training programs throughout the EU, the number of companies committing to provide cyber training pledges, and possibly qualitative measures, like employer satisfaction with new graduates.

Additional KPIs can be found under ENISA CyberHEAD[64] database tracking how many nations have integrated the European Cybersecurity Skills Framework into their national frameworks or how many cybersecurity courses are available Europe-wide. Under the NIS2 Directive’s reporting mechanisms, the Commission will likely track compliance-related stats, such as the proportion of essential entities whose management has undergone cybersecurity training.

The CyberHubs[65] project, a three-year initiative aimed at enhancing the cybersecurity skills ecosystem in Europe, assessed the 7 CyberHubs countries, revealing an interesting proportional relationship between the ICT workforce and the cyber workforce presented in Figure 5.

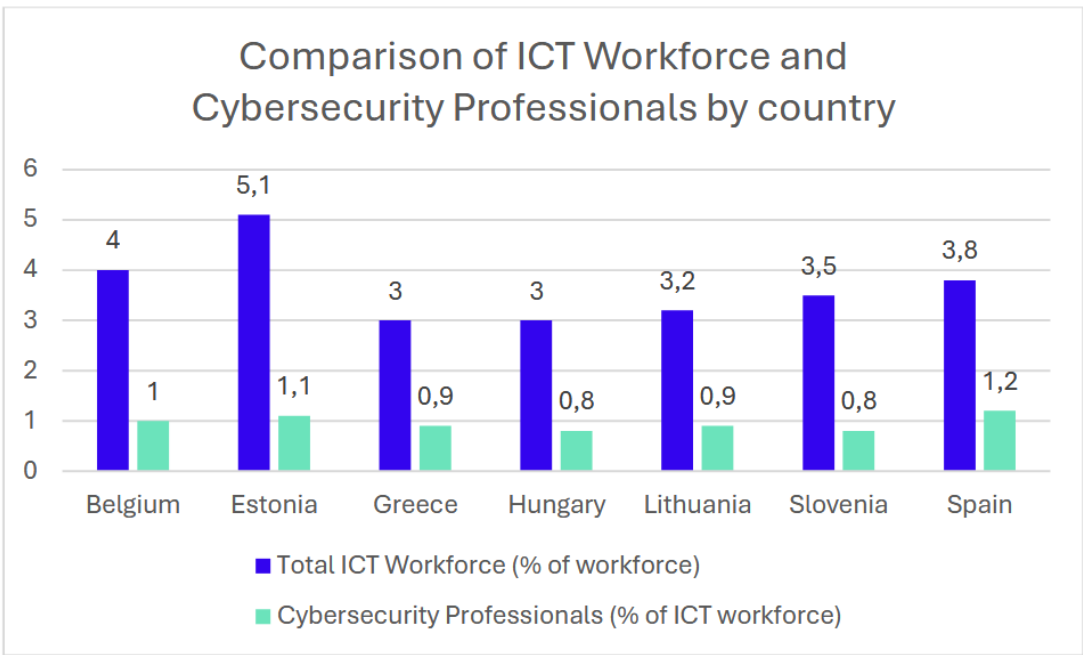


Figure 4 CyberHubs comparison of ICT Workforce and Cybersecurity Professionals by country[65]

EU KPIs are strongest in quantitative measures – e.g., the number of specialists and training uptake – which are crucial for goal-setting. However, these numbers alone don’t



capture quality and impact. For instance, designating a person as a “cybersecurity specialist” doesn’t necessarily indicate their skill level or practical proficiency. Also, the assessment itself might vary in methodology and depth. Some sample screenshots are provided in Appendix 2 from the EU Digital Skills Assessment Tool [66] showcasing the limitations of the assessment method applied. Also, as it is captured in the screenshots, the recommendations for more proficient people were irrelevant after the evaluation was completed.

ITU’s Global Cybersecurity Index (GCI)[67], the National Cyber Security Index (NCSI)[68] by e-Governance Academy or ENISA’s self-assessment tools [69] for national education maturity, provide ratings incorporating expert judgment on the effectiveness of education and training from a qualitative perspective. Still, a gap remains in EU-level KPIs.

There is currently no standardised EU-wide measure of the quality of cybersecurity curricula or the industry readiness of graduates. The current KPIs only track the directly defined cybersecurity skills and competencies and not the broader “cyber-relevant but undermeasured” skill areas like SecDevOps/DevOps, Secure Software Development, AI Engineering, and OT engineering. EU CGIs and decision-making tend to rely on indirect indicators.

National strategies typically set their targets, often with greater granularity [70],[71],[72], that can be grouped into several categories: educational output, workforce development, awareness, and capacity-building measures. For example, educational output KPIs might include the number of graduates in cybersecurity programs annually or the number of teachers trained to deliver cybersecurity content.

One notable attempt at qualitative measurement is ENISA’s Cybersecurity Education Maturity Assessment [73], which can be used to self-evaluate the level on a scale (basic, intermediate, advanced) regarding cybersecurity education in primary and secondary schools. It presents a more nuanced picture than simply counting classes – it examines curriculum integration, teacher skills, and other factors.

Another interesting initiative is the Skills Forecast project by the European Centre for the Development of Vocational Training (CEDEFOP)[74], which aims to provide comprehensive information on future labour market trends as an “early warning”

mechanism. The results and applicability of what influences the results will mean to policymakers are yet to be seen, but the data harmonisation and decision-making support are already progressing.

Other performance indicators remain fragmented. The EU's education targets include a KPI that by 2030, fewer than 15% of students aged 13-14 should be "low performers" in computer and information literacy as measured by ICILS [75]. The data from ICILS shows that this figure is around 43% on average, revealing a gap in digital competency among youth that must be addressed for future cybersecurity readiness.

Cybersecurity-specific data from a 2024 Eurobarometer study [76] show only 25% of companies in the EU had provided cybersecurity training or awareness to employees in the past year, while 45% reported difficulty finding qualified cyber candidates for open positions. These kinds of survey-based KPIS help identify weaknesses in organisational capacity building and can highlight focus areas for improvement.

While there is effort to provide more data-driven visibility on the progress closing the cyber skills gap, there is currently no official EU-wide KPI for the number of cybersecurity professionals trained, retained, or reskilled. Available workforce estimates are typically subsets of larger quantitative KPIs like "number of ICT professionals trained" and originate primarily from educational databases or industry analysis and one-off studies, with no formal mechanism established to track annual progression.

In summary, the EU strategy has established important targets and initiated progress measurement, but most KPIs continue to focus on general digital skills. To bridge the cyber skills gap, future indicators must extend beyond mere headcounts and consider the quality, distribution, and integration of cyber competencies. Without precise, cyber-specific KPIs, the EU's capacity to measure, forecast, and scale its workforce will remain limited.

## **2.6 Impact of Cybersecurity Skills Gaps on EU Competitiveness and Economic Security**

The cybersecurity talent shortage has a significant impact on the European Union's digital competitiveness, innovation capacity, and broader economic security. Multiple studies

and strategic reports highlight the systematic risks posed by the growing human capital gap across sectors.

To begin with, the cybersecurity talent gap significantly hampers economic growth and technological progress. The shortage of qualified cybersecurity experts represents a prime obstacle hindering growth and innovation within Europe's digital industries [77], [78]. Proficiency in cybersecurity is vital for the secure implementation of innovations such as fintech solutions, Industry 4.0, Artificial Intelligence, and the Internet of Things. Without skilled professionals, European businesses may hinder their digital capabilities, jeopardising their competitive edge against global players [36].

Second, the shortage of cybersecurity skills is associated with a rise in both the frequency and severity of security incidents, resulting in significant economic losses. Recent statistics[79] reveal that almost 90% of organisations in 2023 cited inadequate cybersecurity skills as a contributing factor to security breaches, while 70% directly linked the skills gap to heightened cyber risks. The financial ramifications of these breaches are also substantial, with reports indicating that more than half of the affected organisations experienced losses of over \$1 million per incident.

Third, the EU's Digital Economy and Society Index (DESI) [80] also consistently indicates that a shortage of digital skills remains a significant challenge to Europe's digital performance. The struggle to recruit ICT specialists, particularly in cybersecurity, continues to hinder digital transformation [36]. European cybersecurity startups are facing slower growth due to challenges in attracting qualified professionals, which hinders the EU's ambition of developing a robust cybersecurity sector. This talent shortage undermines Europe's strategic objective of digital sovereignty, a point highlighted by European Commission President Ursula von der Leyen [81].

Fourth, cybersecurity capacity is closely linked to overall economic security. A significant shortage of cybersecurity experts in essential sectors, such as energy, finance, healthcare, and transportation, increases the risk of systemic cyberattack disruptions. These disruptions often have ripple effects on other sectors, potentially resulting in widespread outages and financial turmoil. Europe is facing an estimated deficit of around 299,000 cybersecurity professionals, contributing to a global gap of 4.8 million[9], [42]. Both law enforcement and cybersecurity agencies warn that this shortfall in human

resources hampers overall cyber preparedness, leaving Europe's digital infrastructure vulnerable to ever-evolving threats [83].

Finally, Europe's cybersecurity talent shortage worsens concerns about talent drain, as global competition - particularly from North America and Asia - draws European cybersecurity professionals away [84]. This trend may result in increased reliance on external cybersecurity services and technologies, heightening security and supply-chain vulnerabilities and compromising Europe's goal for cybersecurity autonomy [36].

Academic and policy research support these observations. The OECD's 2024 report "Building a Skilled Cyber Security Workforce in Europe" [83] noted that multiple policies have been implemented to reduce the gap, and that industry involvement is crucial, implying that if the gap persists, it could weaken Europe's industrial base and resilience.

In summary, the cybersecurity skills gap is no longer a peripheral issue - it has become a structural constraint on Europe's ability to compete, innovate, and safeguard its digital infrastructure. The shortage of skilled professionals affects not only incident response and system resilience, but also the EU's capacity to lead in critical technology areas. As the demand for cybersecurity talent grows globally, Europe's ability to nurture and retain its expertise remains a pivotal factor in determining whether it can achieve digital sovereignty or remain reliant on external capabilities. Bridging this gap is not merely a matter of numbers; it is about ensuring that cybersecurity becomes integral to the EU's broader vision for economic and strategic resilience.

### **3 Methodology**

This study investigates how the European Union conceptualises, governs, and implements cyber competence as a strategic enabler for digital transformation, economic competitiveness, and future readiness. Rather than narrowing the focus to purely technical cybersecurity skills, the research adopts a broader perspective on cyber competence as a foundational capability that supports the EU's digital agenda. The methodology is designed to assess the alignment between the vision and ambition articulated in EU CGIs and their actual implementation, monitoring and performance tracking.

#### **3.1 Research Design**

The research employs a multi-method qualitative approach, combining various non-quantitative methods to investigate a complex and multi-layered policy environment. The study utilises diverse techniques to triangulate findings and enhance analytical depth. This includes structured document analysis of EU CGIs, comparative analysis of case studies examining Member States' implementation, and selective use of published EU and global data to support and contextualise observations. Additionally, a targeted validation survey, further detailed in section 5.6, is used to gather stakeholder perspectives, providing insights and feedback on the relevance and practicality of the framework. This design enables exploration of the policy-practice gaps, strategic misalignments, and the institutional embedding of cyber competence, where systematic interpretation is more important than quantitative measurements.

#### **3.2 Case Selections**

The research investigates five Member States' implementation practices and analyses five global actors for external comparison. While it would have been beneficiary to investigate more international use-cases, the format and the scope of the study limits these options.

##### **EU Member States:**

Five countries were selected for comparative analysis based on maturity, strategic role, and geographic diversity. The selection was based on a combination of size and complexity challenge of digital transformation, the Member States' weight in the EU and

their positioning on indices like the Belfer Center's National Cyber Power Index [85] , the ITU's Global Cybersecurity Index [86] , and the e-Governance Academy's National Cybersecurity Index [68].

The final selection includes:

- Estonia, recognised internationally for its digital innovation and governance leadership;
- Finland, acknowledged globally for its education and skills development model;
- France, as a key EU policymaker with a large population, complex digital infrastructure, and global strategic posture;
- Poland represents a fast-growing economy with a large population and an evolving digital landscape; and
- Czech Republic, selected for its Central European context, smaller size, and consistently high performance in international cybersecurity rankings.

This selection represents varied institutional models and levels of cyber maturity within the EU.

### **Global Outlook:**

For international benchmarking, three strategic competitors – the United States, China and Russia - were selected on their relevance to the EU's framing of digital competition and strategic autonomy. These countries are considered economic and geopolitical challengers, and their approaches to cyber competence development offer reference points for understanding what the EU and its Member States are competing against in the digital age.

In addition, two “neutral” innovation leaders, Singapore and South Korea, have been selected as comparative cases. Both are recognised for their effective cyber talent pipeline development and policy agility, as well as their ability to build resilient societies in the face of complex geopolitical environments.

### **3.3 Data Analysis Procedures**

Thematic analysis extracted and organised key patterns across EU CGIs and selected MS implementation cases. The study employed a structured reading of documents, utilising predefined categories such as skills, strategies, performance indicators, future readiness, cyber competence, and institutional roles. Based on patterns emerging during the reading process, some analysis structures were developed inductively, for example, identifying recurring gaps in monitoring or inconsistencies in how policies were interpreted across national contexts.

### **3.4 Research Limitations**

As noted in section 2.1, the study had several limitations. First, it relied exclusively on publicly available and predominantly English-language materials. While EU-level documents were accessible and consistent, national-level strategies and reports varied significantly in quality, depth, and availability. In some cases, particularly for international comparisons such as those with China, only partial translations or summaries were available, and online translation tools were used when necessary. This introduces a risk of overlooking details or nuances.

Secondly, no primary data was collected for this study except for the framework validation. All findings are drawn from secondary sources, including academic papers, strategic documents, and datasets. While this approach was sufficient for the research's scope and aims, it does limit the ability to investigate internal decision-making processes or to capture first-hand insights from practitioners.

## **4 Discussion: Towards an Adaptive EU-National Capacity Framework**

### **4.1 Introduction and Strategic Context**

This chapter synthesises the reviewed literature, CGIs, and comparative Member State analysis to identify the potential gaps in the EU's cybersecurity capacity-building efforts. While EU CGIs articulate strong ambitions around digital resilience, cyber competence, and strategic autonomy, tracking implementation efficiency across Member States remains uneven, and the actual context of what skills and competencies are needed remains unclear.

The chapter examines how institutional, operational, and strategic misalignments hinder the EU's ambitions to translate policy into measurable outcomes and enable an agile feedback loop between outcomes and policymaking.

Rather than treating cyber capacity-building as a standalone technical function and skill, this chapter analyses it as a strategic enabler of resilience, competitiveness and future readiness. The aim is to highlight where the EU's cyber competence ambitions, as articulated in the CGIs, are not matching policy implementation, institutional commitment or systematic incentives.

### **4.2 Strategic Benchmarking: Global Models and EU Positioning**

As discussed in Chapter 3.2, three strategic competitors – the United States, China and Russia, and two “neutral” innovation leaders, Singapore and South Korea, have been selected as comparative cases. To contextualise the EU's effort in cyber workforce development and strategic talent development, this section will examine these five global reference cases. The models analysed offer diverse and somewhat contrasting approaches to institutional coordination, strategic investment, and skill development. The outcomes can provide strategic insights into the activities and capabilities the EU should cultivate to maintain a competitive edge.



#### **4.2.1 Introduction**

The EU CGIs are addressing what the EU should look like to meet future goals, including competitiveness, innovation capability, and social and economic aspects. The Competitiveness Report [36], describes how “Europe’s competitiveness is being squeezed from two sides: by a widening innovation and productivity gap with the United States, and by rising industrial and technological competition from China.” Not detailed in this report, the EU faces a different kind of competition from Russia as well as from the rest of the world, as digital transformation accelerates.

#### **4.2.2 Strategic Framing: Defensive versus Offensive Workforce Development**

Cybersecurity education programs worldwide generally prioritise defensive skills – protecting systems, detecting intrusions, and mitigating vulnerabilities – as these are essential for all sectors[87], [88], [39]. However, the degree to which offensive techniques (such as ethical hacking, exploit development, and offensive cyber operations) are taught varies by nation and is often influenced by government or military involvement.

Most civilian cybersecurity education and certifications in the U.S. and EU focus on defence. University curricula train students to be defenders by securing networks, implementing encryption, and responding to incidents[89]. Offensive training is often referred to as “ethical hacking” or penetration testing courses. For example, many U.S. programmes include courses where students learn to think like attackers to improve their defence strategies, covering techniques such as SQL injection, malware, and red-team/blue-team exercises [90].

In Europe, a similar trend is evident: several universities maintain laboratories where students engage in practical challenges, yet the emphasis remains on a defensive approach [91], [92], [93]. European initiatives prioritise “cyber defence” over “offence” due to legal and ethical issues. Even within military training in Western countries, although offensive cyber techniques are taught for specific roles, this component is concealed chiefly and separated from civilian educational programs. The goal is to develop security professionals capable of performing authorised penetration tests or vulnerability assessments [94].

Nonetheless, Western nations recognize the necessity for some offensive skills. In the U.S., the NSA’s Center of Academic Excellence in Cyber Operations (CAE-CO) [95]

designation is for universities that provide in-depth offensive training (such as low-level programming and reverse engineering). The limited number of institutions awarded this designation suggests that offensive cyber education is somewhat isolated.

Generally, the West's open teaching of offensive tactics is tempered by concerns of misuse and legal restrictions. These concerns, and the lack of addressing them on an EU level might become a strategic disadvantage if actors considered to be contesting the EU are building such capacity.

#### **4.2.3 USA**

The U.S. has long recognised cybersecurity human capital as a cornerstone of national cyber strategy. The 2023 National Cybersecurity Strategy[96] states, "Cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy... and our national defence." It emphasises the expansion of the cyber workforce through education, training, and public-private partnerships. The National Initiative for Cybersecurity Education (NICE)[97] framework provides a foundation by defining work roles and skills. It guides curricula nationwide and is regarded as a global benchmark.

While there are multiple federal programs supporting workforce development in the U.S., the cyber talent gap remains significant – about 225.000 [98]– reflecting an ongoing challenge to keep up with demand. The U.S. strategy increasingly stresses diversity and inclusion in cyber jobs, recognising untapped talent pools and the need for skilled defenders and cyber innovators to safeguard economic and national security.

The US model illustrates how a long-term workforce strategy supported by national frameworks, public-private collaboration, and defence sector collaboration can scale effectively, even in a fragmented political, geographical, and maturity landscape. For the EU, which faces similar fragmentation, the harmonisation of the skills taxonomies, stakeholder coordination could serve as an example of delivering impact on scale.

#### **4.2.4 China**

There is limited independent English documentation on China's cybersecurity capacity-building efforts, yet some insights can be gleaned. In 2022, China's Ministry of Education published a "White Paper on the Real-World Capabilities of Cybersecurity Talent,"

[99]revealing that 34 universities in the country now offer programs in cyberspace security. However, projections for 2027 indicate a shortfall of 3.27 million cybersecurity professionals, while the annual number of graduates in this field is expected only to reach 30,000.

China's approach to cybersecurity blends robust talent development initiatives with a focus on technological self-sufficiency. The government prioritised enhancing the talent pipeline in its 2016 National Cyberspace Security Strategy ("solidifying the cybersecurity base")[100], which resulted in the establishment of World-Class Cybersecurity Schools (WCCS) in 2017[101]. Under this program, 11 top Chinese universities were certified as WCCS, standardising high-quality cyber curricula. Notably, Chinese cybersecurity degree programs tend to integrate emerging technologies – 8 of 11 WCCS universities include courses on AI and machine learning in cybersecurity, a far higher integration than comparable U.S. or EU programs.

This suggests that China is enhancing the AI competencies of its cyber workforce to gain a competitive edge in AI-driven security technologies. Chinese authorities are enhancing educational capacity in colleges and specialised institutes to address the skills gap challenge, including military-linked programs and nationwide competitions to scout talent. It is worth noting that China's strategy combines both defensive and offensive capability development [102]. This dual-purpose approach – preparing cyber operators who can launch attacks and defend against them – is a unique aspect of China's strategy linked to its ambition for cyber power and digital sovereignty.

China's capacity to align its cybersecurity workforce strategy with national innovation and security agendas offers a competitive model of systemic integration. For the EU, this prompts strategic questions about maintaining democratic openness while addressing coordination gaps and preparing for capability shifts driven by AI and dual-use technologies.

#### **4.2.5 Russian Federation**

Russia's public cybersecurity strategy is closely tied to its information security doctrine [103] and the "sovereign internet" [104] policy. While less is published about civilian cyber workforce initiatives, the country has heavily invested in elite technical training and military instruction to staff its cyber units[105]. The Information Space Activities

Concept (2011) [106] and later military doctrines guide the training of information security specialists in military academies, indicating a strong emphasis on cultivating skilled cyber operators for military and intelligence roles through state institutions.

In Russia, there has historically been a substantial emphasis on offensive cyber capabilities [107], spearheaded mainly by state security and military programs. As noted, Russia's military and intelligence agencies have taken the lead in cultivating hackers [108]. The Federal Security Service (FSB) and military intelligence (GRU) recruit from top technical universities and also train their cadres. The military's establishment of a cadet cybersecurity program in 2015 [109] signalled an effort to educate young officers in cyber-operations formally. Case studies demonstrate that Russia's approach effectively blurs the lines between state-trained hackers and independent hackers – for example, some researchers have noted that talent from university programming competitions can be co-opted into state-sponsored offensive operations. Research shows that Russia has published multiple versions of its Information Security Doctrine, emphasising both civilian and military talent development in computing and security. Informatics, taught in middle school, sees around 60,000 students annually registered for advanced computer science exams, contributing to an overall pool of more than 600,000 trained specialists. [111].

On the civilian front, Russia's Digital Economy program (2017–2030) aims to increase the number of ICT security professionals [112], with some universities offering specialised programs. However, the approach remains centrally controlled [113]. The 2021 National Security Strategy [114] underscores the importance of safeguarding Russia's "cultural sovereignty" and shielding its cyberspace from foreign interference. This priority translates to a focus on skills for controlling and monitoring information, such as content censorship and securing Russian networks, as well as developing offensive cyber capabilities for strategic leverage [115]. Although Russia benefits from a historically robust STEM education and success in international hacking contests, it faces challenges in retaining talent, as many cyber experts either join government roles or seek prospects abroad due to limited opportunities in the private sector. While less transparent, Russia's cybersecurity skills strategy is aligned with national security goals, often emphasising offensive and espionage capabilities. It aims to sustain a sovereign internet rather than mobilise a broad cyber workforce in the private economy [114], [116].

In summary, Russia strongly emphasises offensive training for those in its cyber ranks, viewing cyber as a tool of national power. It also has a baseline of defensive training for conventional IT security roles. While not a governance model the EU would emulate, Russia highlights the risks of strategic asymmetry if Europe underinvests in institutional readiness, especially within critical sectors.

#### **4.2.6 Singapore**

Singapore distinguishes itself with its proactive and comprehensive cybersecurity strategy, emphasising a strong cyber workforce essential for security and economic growth [117]. The Singapore Cybersecurity Strategy 2021 [118] identifies workforce development as one of its four strategic pillars, designed to meet security and economic expectations. Compared to the 2016 [119] plan, this updated strategy prioritises workforce and ecosystem development as vital enablers.

Singapore's government collaborates with educational institutions and industries: cybersecurity topics are integrated into school curricula; Institutes of Higher Learning [120] work with the Cyber Security Agency (CSA) to align their courses with competency frameworks; and initiatives like Skills Future scholarships [121] or Cyber Youth [122], professional conversion programs, and the CSA Academy aim to enhance workforce skills.

To mitigate the skills gap, Singapore invests in local talent through cybersecurity innovation and R&D labs, while utilising immigration to bring in foreign specialists for immediate requirements [123]. The strategy emphasises cybersecurity as a "critical enabler" of the Smart Nation's digital transformation. It aims to stimulate a dynamic cybersecurity industry by encouraging the development of "Made-in-Singapore" security products through startup initiatives. Singapore consistently ranks among the leading countries in global cybersecurity indices, highlighting its capacity-building and governance strengths.

Singapore's approach to cyber talent development demonstrates how a smaller nation can effectively address the skills gap through robust government coordination. However, due to the nation's size, the expansion of the talent pool remains an ongoing challenge. For the EU, this can show the value of national-level alignment mechanisms that link cybersecurity workforce goals to education, innovation, and economic competitiveness.

#### **4.2.7 South Korea**

South Korea's National Cybersecurity Initiatives [124] emphasise human capital, shaped by economic objectives and a critical threat landscape, including ongoing cyberattacks from North Korea. The ROK Cybersecurity Strategy (2019) [125] and its updated 2023/24 version [124] outline goals to enhance specialised educational programs that prepare professionals for cybersecurity roles in public and private sectors, fostering collaboration with industry and academia.

This plan includes expanding university cyber defence programs, establishing cyber labs and competitions and promoting certifications. The focus remains on workforce development, while also indicating a shift in approach: it aligns with the U.S. doctrine of "defend forward." It prepares for more proactive cyber operations against adversaries, specifically naming North Korea. This shift involves training a group for proactive cyber defence and retaliation, likely through the National Intelligence Service and military cyber units [126].

South Korea's advantages are its strong technical education and effective government-industry collaboration (for instance, the strategy advocates mobilising private-sector cyber responders during national crises). Nevertheless, a significant challenge remains in retaining talent within the public sector and fostering innovation.[126]

In summary, South Korea adopts a resilience-centred strategy, focusing on strengthening critical infrastructure and raising public awareness, while developing talent capable of defending against and, if necessary, counterattacking in cyberspace, reflecting its security posture and geopolitical context. For the EU, it highlights the need to tailor workforce development to address skills shortages and evolving risk environments, as well as geopolitical dependencies.

#### **4.2.8 Strategic Patterns and Lessons for the EU**

The analysed national strategies show both contrasting governance models and shared success factors in cyber workforce development. The United States adopts a federated, competency-based model supported by partnerships between the public and private sectors alongside inclusive workforce policies. In contrast, China and Russia opt for a centrally managed, state-led model that tightly integrates cyber education with national

innovation and military goals, prioritising sovereignty, technological self-sufficiency and offensive capabilities.

Singapore and South Korea demonstrate how smaller states can build high-performing cyber capacity through whole-of-government strategies, agile coordination across government, academia, and industry, as well as early talent identification. Both nations view cybersecurity as a crucial driver of national growth, with Singapore utilising its compact size for enhanced integration and efficiency, and South Korea seeking to balance resilience with proactive deterrence.

In these use cases, three common elements emerge: ongoing public investment, well-defined strategic objectives, and cohesive delivery systems. Although the geopolitical context influences priorities, every country views cyber competence as a vital national strategic asset. In contrast, despite its sophisticated policy frameworks and regulatory aspirations, the EU continues to encounter implementation fragmentation, weak enforcement of common standards, and a lack of coherent incentives to convert strategy into workforce outcomes.

To ensure the EU remains competitive and digitally sovereign, it needs to address the execution gap, not by copying existing models, but by capitalising on its advantages in institutional collaboration, governance based on shared values, and cross-border integration. In the following section, an analysis of how certain Member States implement EU-level strategies will be explored, identifying areas where increased coordination, incentives, and alignment of performance could be improved.

### **4.3 Comparative EU Member State Insights**

While the EU-level strategies identify the cybersecurity skills gap as a shared challenge, implementation varies significantly across Member States. Five countries were selected for comparative analysis based on maturity, strategic role, and geographic diversity. The selection was based on a combination of size and complexity challenges of digital transformation, the Member States' weight in the EU and their positioning on indices such as the Belfer Center's National Cyber Power Index [85] , the ITU's Global Cybersecurity Index [86] , and the e-Governance Academy's National Cybersecurity Index [68].

This section explores how Member States understand and apply the EU's cyber workforce goals. It highlights the alignment of national strategies, metrics for skills development, public–private collaboration, and the degree to which Member States utilize or modify EU frameworks like the NIS2 Directive or the ECSF.

#### **4.3.1 Estonia**

Estonia is often considered a forerunner in digital transformation and is frequently cited as a reference model with the EU for e-governance and e-service delivery. Nevertheless, the country is struggling with the widening skills gap as significant talent shortages have been identified under the Cyberhubs report [65]. According to the report, Estonia produces approximately 735 IT graduates annually, far short of the estimated 2600 needed to meet demand. According to another report, by 2023, the Estonian cybersecurity sector will require an additional 270-870 specialists, with other sectoral needs going unaccounted for in existing research [66].

This shortage spans across sectors and job roles, primarily affecting small and medium enterprises, which often rely on one IT staff member handling multiple roles, including cybersecurity as well. This later mirrors the EU-wide concern that several cyber duties rely on non-cyber personnel [12]. Estonia recognises that growing domestic talent is crucial, and it is constantly assessed and addressed via various methods [67]: training, camps, cyber competitions, university education, and vocational training.

The Estonian National Cybersecurity Strategy 2024-2030 [68] puts cybersecurity “as a horizontal cornerstone in the digitalisation, management and development of services.” Beyond the necessity of technical capabilities, the strategy emphasises human capacity building through societal resilience, active community participation, and targeted cybersecurity education across various societal segments.

Estonia’s cybersecurity strategy closely aligns with EU goals, positioning cyber competence as a key component of digital transformation. However, ongoing workforce shortages, particularly in SMEs and non-technical fields, highlight challenges in maintaining adequate staffing, even in digitally advanced Member States. While Estonia’s decentralised, community-oriented approach offers valuable lessons in adaptability and engagement, it also emphasises the need for scalable, skills-based forecasting and coordination at the EU level to address the implementation gap.



#### **4.3.2 Finland**

Finland represents a leading model in framing cybersecurity as a shared civic responsibility and a strategic enabler of innovation and resilience. Its National Cybersecurity Strategy 2024-2035 [69] places human competence at the center of its vision with the first core pillar - Competence, Technology, and RDI - stating the importance of making cybersecurity a shared responsibility. It also defines the aim to “harness the benefits of emerging and disruptive technologies and requires integrated security in devices, software, and services.”

The strategy envisions a cybersecurity ecosystem that fosters a competent, innovative, and resilient digital society by integrating cybersecurity comprehensively across all educational levels, societal sectors, and workplaces. It aims to establish cybersecurity as a civic responsibility, enhancing critical media literacy, cyber risk awareness and routine information security practices. It also recognises the importance of emerging and disruptive technologies and advocates for integrating cybersecurity principles in technology design, standardisation and certification.

To achieve these goals, the strategy calls for self-sufficiency in critical technologies and strengthening domestic research and innovation, along with collaboration between the public and private sectors. It aims for sustainable economic development, employment creation, and societal resilience. Continuous competence development through education, training, and lifelong learning opportunities shall further reinforce the necessary cybersecurity expertise.

Finland explicitly ties its national goals to European efforts. The strategy notes alignment with NIS2 requirements and aims to leverage EU, NATO, and other programmes to boost R&D and training activities. Finland also has robust cyber reserve training under its military, complementing the EU’s ambition to create additional channels for skilled personnel development.

Finland’s cybersecurity strategy presents a well-developed, unified approach closely aligned with EU goals. By considering cyber capabilities as essential to society and a driver of innovation, Finland sets a standard for Member States aiming to link national resilience ambitions with EU regulatory frameworks and long-term competitive advantage. Its strategic incorporation of EU regulatory alignment and funding

mechanisms with national aims offers a replicable framework for harmonizing national interests with EU objectives.

### **4.3.3 France**

France put cybersecurity as a foundational component of national strategy [68] - embedding it within economic development, digital governance, and international cooperation. France positions cybersecurity as a sovereign strategic domain, akin to national defence. Instead of viewing cybersecurity solely as a technical task, it is positioned as a driver of societal trust, business continuity, and national resilience. This strategy advocates for cybersecurity-by-design in various sectors and emphasises the need for regulatory consistency, while also incorporating social policy objectives like gender equity, public access, and sustainability.

France further institutionalises cybersecurity as a persistent and evolving threat environment (much like US approaches [70]), requiring long-term investment, regular national planning, and coordinated sector-specific resilience mechanisms. The strategy is strongly aligned with EU cybersecurity regulations and mechanisms. Although it does not explicitly define metrics for closing the skills gap, it aligns with EU-wide initiatives like the Digital Education Action Plan and the Cybersecurity Skills Academy, fostering convergence around workforce mobility, training standardisation, and decentralised resilience.

Human capacity building is at the centre of the strategy and is backed with a significant investment. A €1 billion public funding package aims to double the cybersecurity workforce to 75,000 by 2025, develop three domestic cybersecurity “unicorns,” and strengthen exports [127].

Training initiatives target initial education and professional retraining, particularly expanding cybersecurity awareness among SMEs, public servants, and the general public. The Cyber Campus [71] initiative represents a national platform model, consolidating training, research, and operational functions to strengthen public-private synergies and regional capacity. Over 160 ecosystem players are engaged, illustrating a coordinated approach to workforce development and continuous learning within the ecosystem.

France's national strategy demonstrates how cybersecurity is a vital enabler of digital sovereignty, an enhancer of industrial competitiveness, and a catalyst for European unity. Its significant investments, coordinated ecosystem approach, and active engagement in EU governance frameworks establish France as a key contributor to the Union's collective capacity-building initiatives. To optimise impact, France - and by extension the EU - needs to develop strong, outcomes-focused metrics to assess implementation impacts with greater specificity and responsiveness to policymakers.

#### **4.3.4 Poland**

The current Polish National Cybersecurity Strategy [72] "The New Strategy for 2019–2024" presents a structured approach strengthening national digital resilience. It is framed around five strategic objectives, evaluating how Poland conceptualises cybersecurity in the digital transformation era, aligning with EU strategies, and setting human capital development as a cornerstone of national cybersecurity.

The strategy frames cybersecurity as a cross-cutting enabler of societal and economic well-being. It explicitly links the integrity of digital systems to national prosperity and institutional trust. To future-proof infrastructure and services, the strategy promotes the principles of security-by-design and privacy-by-design, particularly in emerging domains such as IoT, AI, 5G, and innovative city development.

Poland's policies closely follow EU regulations. It pledges to enact the EU Cybersecurity Act, which includes adopting European certification schemes, and has set up a national certification authority that aligns with ENISA standards [73]. To enhance cybersecurity education and awareness, initiatives include integrating cyber topics into school curricula, developing national awareness platforms, and fostering university–industry collaborations for cybersecurity training and research.

While the strategy does not define specific KPIs for closing the skills gap, it outlines qualitative indicators such as education output, institutional preparedness, and public awareness, acting as proxies for capacity development. A national action plan complements the strategy, creating a foundation for future monitoring and policy adaptation.

Poland aligns strongly with EU cybersecurity objectives and embeds cyber resilience as a fundamental aspect of its national development. Its focus on certification, education, and legal alignment aids the EU's goal to harmonise capacity-building efforts among Member States. Nonetheless, the lack of quantitative performance indicators hinders the ability to benchmark progress or evaluate cross-border interoperability. The Polish experience highlights the need to convert EU-level frameworks into practical, measurable national tools that consistently and sustainably bridge the skills gap.

#### **4.3.5 Czech Republic**

The Czech Republic's National Cybersecurity Strategy (2021–2025) [74] frames cybersecurity as a strategic, cross-sectoral priority rooted in national sovereignty, democratic stability, and long-term digital development. It articulates education, workforce, and collaboration, addressing the vision of a “Resilient Society 4.0.” Despite the strategic emphasis on digital resilience, a substantial and persistent gap remains between the demand for cybersecurity professionals and their supply, especially in the public sector, which has also been highlighted by academic literature [75]. The labour market analysis by Drmola et al. [128] reveals that the severe undervaluation of cybersecurity professionals in public service, the systemic bureaucratic constraints, and a mismatch between educational outputs and market needs undermine strategic ambitions.

The strategy is well-aligned with EU cybersecurity governance. While there are initiatives in the Czech Republic for a local qualifications framework, it explicitly aims to be compatible with EU-wide frameworks[76].

The Czech Republic's thoughtful and principled national cybersecurity strategy aligns closely with EU goals. Its difficulties are not rooted in vision but in implementation, particularly in synchronising education systems, public-sector incentives, and workforce retention strategies. The Czech example reflects a broader EU challenge: transforming strategy into sustainable talent pipelines, especially in public institutions where market dynamics impact competitiveness. Tackling this challenge is crucial for the EU to develop resilient and fair cyber capabilities among its Member States.

#### **4.3.6 Translating EU Ambitions into National Practice**

The Member State cases examined in this section reveal a collective effort to address the cybersecurity workforce gap while highlighting differences in interpretation,

prioritisation, and implementation of EU-level objectives. Countries like Finland and France showcase integrated models that closely align with EU frameworks. However, other nations encounter structural challenges, including bottlenecks in the skills pipeline and insufficient metrics alongside institutional fragmentation. Despite the evident strategic intent across all cases, which mirrors shared values, executing these strategies is inconsistent. This inconsistency is particularly noticeable in how national strategies implement EU instruments like the NIS2 Directive and the European Cybersecurity Skills Framework.

These differences extend beyond administrative challenges; they reveal a systemic shortfall in capacity planning, incentive frameworks, and performance oversight. Even in digitally advanced Member States, obstacles remain in attracting, keeping, and coordinating cyber talent across public, private, and critical infrastructure sectors. This analysis confirms that, while the EU provides strategic guidance and common tools, execution among Member States is disjointed, lacking sufficient mechanisms to ensure consistency or widespread impact. Additionally, the lack of standardised KPIs limits the MS level feedback loop's efficiency at the EU level, hindering the definition of corrective actions or the development of new approaches.

The following section synthesises the research findings to date into a structured gap analysis, highlighting areas where policy ambition falls short of implementation. It will also identify the critical barriers that must be addressed to enable scalable, outcome-oriented capacity building across the Union.

## **4.4 Gap Analysis**

The EU and its Member States have made significant progress in articulating a shared vision for the digital domain. Yet, the implementations reveal a persistent disconnect between strategic ambitions and operational reality. The gaps stem from technical or financial ambitions and indicate a systematic flow in governance design, institutional incentives, measurement frameworks, and strategic coherence. After analysing national strategies, policy instruments, and implementation patterns, this section identifies and categorises the most urgent obstacles to closing the EU cyber skills gap sustainably.

The gaps are grouped into four thematic areas: strategic misalignment, systemic barriers, operational shortfalls, and measurement and governance limitations. Each category reflects a different layer of the implementation challenge, and together, they outline the core structural deficiencies that must be addressed if the EU is to scale, harmonise, and future-proof its cyber capacity-building agenda.

#### **4.4.1 Strategic Gaps**

Strategic gaps highlight the disconnect between the EU's elevated policy objectives and the practicalities of their implementation. These gaps often arise from misaligned aspirations, with EU-level strategies establishing common KPIs that may not adequately represent national security interests, economic priorities, or distinct digital ecosystems. While Member States may adopt strategies aligned with EU goals, they often lack the relevant metrics necessary for consistent measurement and evaluation at the EU level. This section explores the underlying causes of these disparities, including fragmented governance, inconsistent emphasis on human-centric skills, and the lack of coherent, outcome-focused performance indicators.

##### **4.4.1.1 Cybersecurity as a National Enabler vs. Technical Compliance Focus**

Several EU and national documents describe cybersecurity as a strategic enabler for economic and societal advancement; however, the focus appears to remain primarily on compliance and technical KPIs.

Cybersecurity capacity-building metrics primarily consist of a collection of risk-mitigation tasks characterised by technical KPIs, such as the number of trainings conducted, security measures implemented, professionals trained, or incident response times reduced. While these metrics are important, they fail to fully encompass the role of cybersecurity as a strategic asset essential for economic competitiveness, innovation ecosystems, and societal digital growth.

This contrast creates a strategic gap: if cybersecurity is not recognised as an enabler, the workforce development initiatives may miss the mark, resulting in narrowly focused technical profiles rather than versatile professionals capable of enabling digital transformation. Cybersecurity or broader cyber competence must be integrated and addressed as a horizontal capability, influencing national R&D agendas, SME digitalisation, education reform, and public sector innovation.

To bridge this gap, national strategies must focus on KPIs that link cybersecurity with digital innovation, economic growth, and human capital development. These KPIs should measure the extent to which cybersecurity is integrated into national research and development strategies, the delivery of public services, and the digital transformation of SMEs. Cyber resilience should be a key priority across economic, labour and education policies, and not limited to security or IT policies.

#### **4.4.1.2 Adapting Strategic Thinking to a Contesting and Unpredictable Environment**

The European Union's cybersecurity strategies have made considerable progress in regulatory harmonisation and resilience-building, especially with instruments like NIS2, CSA or the CRA. However, a systematic gap persists in strategic anticipation: existing frameworks are insufficiently addressing the realities of a continuously contested, hyperconnected digital environment. The operating context is no longer defined by episodic cyber incidents but by a sustained competitive dynamic, driven by adversaries - both state and non-state - who pursue incremental strategic gains across cognitive, technical, and operational layers of cyberspace [129].

This contest is increasingly asymmetric. Although the EU's cybersecurity stance is mainly defensive, adversarial actors leverage various cyber tools. They employ influence operations, supply chain disruption, data manipulation, and infrastructure targeting, often below the conflict threshold and frequently at the MS level [130]. The EU, constrained by a defensive policy orientation and subsidiarity in offensive cyber capabilities, lacks a unified conceptual approach to contestability in cyberspace. This leads to a structural delay in translating strategic priorities into actionable capabilities.

Additionally, the institutional separation of cyber defence and cybersecurity remains unaddressed. Current EU instruments often address these domains separately; cyber defence is perceived as a military competence, while cybersecurity is seen as a civilian concern. However, the battlefield is shared. Without convergence in doctrine, situational awareness, and human capital development, the EU risks lacking the agility required to act impactfully in an environment where interconnectedness is both a strategic asset and a vulnerability multiplier.

The exponential pace of technological integration, particularly in AI, IoT, and cloud-enabled infrastructure, introduces uncertainty that traditional KPI frameworks and strategic plans struggle to accommodate. There is no coherent methodology for embedding adaptive foresight or resilience against contestation into metrics for building cybersecurity capacity. This represents a missed opportunity.

The EU must adjust its implementation tools to bridge this gap, transforming broad strategic goals into effective, sustainable capabilities. This transition moves from a compliance-oriented resilience to a capability-focused, contestation-conscious strategic stance that requires:

- Embedding contestability and persistent engagement logic into the operational layer of EU and national cybersecurity strategies, including doctrinal updates;
- Integrating foresight and strategic intelligence tools with performance management frameworks, ensuring KPIs capture adaptability and system-wide readiness;
- Establishing a baseline for adaptive cyber capacity across the Union to guide funding, programme design, and accountability mechanisms;
- Advance civil-military convergence, acknowledging adversaries exploit blurred boundaries while the EU response remains compartmentalised.

Without these adjustments, the EU risks strategic irrelevance in a domain that increasingly underpins geopolitical power, technological sovereignty, and economic security[12] [131] [36] [1].

#### **4.4.1.3 Future Skills and Emerging Technologies**

Cybersecurity skill requirements continually evolve in response to rapid technological advancements, such as artificial intelligence, quantum computing, and autonomous IoT. Strategies are beginning to address this: China's head start in fusing AI with cyber education is one example; the U.S. and EU are also investing in AI for cybersecurity and training analysts to manage AI-driven security tools. Countries plan to update their curricula continuously, as the long-term vision is a workforce that not only reacts to



current threats but also anticipates future ones (skills in areas such as securing AI, bio-cybersecurity, and space cybersecurity for satellites, among others).

Several EU strategies acknowledge this trajectory, and national plans (e.g. France, Finland, and Poland) include language on "future-proofing" curricula and training systems. However, current capacity-building mechanisms are still largely reactive, and often fail to anticipate the speed and depth of skill turnover required to remain competitive. For example, AI-integrated security operations require cross-disciplinary teams fluent in cybersecurity and machine learning. Yet such hybrid roles are rarely supported by academic programmes or funding incentives. Similarly, while China's national WCCS university initiative integrates AI into core cybersecurity curricula, no equivalent EU-wide programme exists.

This also highlights an essential aspect of the cyber domain: it has a short shelf life. Technical and hands-on skills fade quickly unless regularly updated, and a professional trained today might need entirely new skills in five years due to emerging technologies and the complexity of the systems. A lifelong learning ecosystem shall be in place to support such needs with incentives and planned time for such activities.

To future-proof the EU cyber workforce, Member States and EU institutions should:

- Establish agile curriculum update cycles that reflect market demand and threat evolution;
- Infuse cyber competence into all digital skills programmes, including in general education and non-technical professions;
- Invest in instructor training and educator retention, as many high-skilled professionals opt out of teaching roles;
- Build a Union-wide culture of lifelong cyber learning, supported by portable credentials and employment-linked incentives.

Without this shift, the EU's long-term cyber resilience and innovation capacity will remain vulnerable to disruption by faster-moving, more adaptive actors [1] [12] [65] [36] [132] [133].

#### **4.4.2 Systematic Gaps**

Systematic gaps expose weaknesses in EU cybersecurity strategies among Member States. They arise from fragmented regulations, inconsistent adoption of frameworks like the ECSF, and inadequate workforce development approaches. This section explores root causes such as misaligned priorities, limited collaboration, and a lack of cohesive skills development mechanisms.

##### **4.4.2.1 Workforce supply vs Demand**

The most evident gap is quantitative, referring to the number of cybersecurity professionals not keeping up with the market demand. As stated in its policies, the EU aims to address the cybersecurity workforce deficit primarily. However, workforce estimates reveal a constantly growing shortage of hundreds of thousands of European experts. Regardless of their maturity levels, all five Member States profiled experienced challenges in filling cybersecurity positions, which is common in the reports on the EU level. This indicates that implementation has not yet reached the expected scale or speed.

Numerous factors contribute to this issue. Educational systems need time to produce graduates, especially as many programs have recently been introduced or expanded, necessitating significant time to develop new curricula. Furthermore, there is a global shortage of experienced professionals beyond the reach of EU or national authorities.

Despite ramped-up educational efforts, the shortfall in skilled professionals remains significant. The EU has estimated a cybersecurity workforce gap of around 299,000 [42], and experts in Poland suggest the gap could grow to millions if future demand is included [134]. National outputs of graduates are increasing, but not at a fast enough rate. For example, France's plan to add ~9,000 specialists [83] over five years is ambitious, yet the global cyber job market is growing faster; attracting foreign talent is also highly competitive.

A strategic gap here is that no coordinated EU mechanism exists to track and manage the supply of cyber labour. Member States often lack detailed data on cyber-skilled employment and needs. Only a few have conducted comprehensive labour with varying methodologies, and this inconsistency makes it difficult to measure progress across the EU. Without consistent metrics, bridging the gap remains a guesswork. Furthermore,

some countries still rely on poaching talent from one another or shifting talent from the private sector to the public sector, which merely redistributes shortages.

Member State actions will remain reactive, fragmented, and ultimately insufficient without a centralised EU capacity to forecast, track, and incentivise cybersecurity labour development. Additionally, innovative solutions should be enhanced to support the steady progress made through traditional academic pathways.

#### **4.4.2.2 Long-term Sustainability and Funding**

The EU strategy is forward-looking (targeted 2030), but many national plans operate on shorter political and budgetary cycles. For instance, Poland's current strategy is valid until 2024, France's strategy targets 2025, and the Czech Republic's roadmap ends in 2025, all pending revision.

This temporal misalignment poses a risk to continuity. Many national initiatives are funded as pilots or multi-year programmes without renewal guarantees. For example, it remains unclear whether France's current funding for cybersecurity education - over €1 billion - will persist post-2025, or whether Estonia's digital training pilots will scale into permanent mechanisms [135].

Moreover, EU funding is often disbursed in tranches tied to deliverables, but lacks sustained institutional anchoring beyond the project lifecycle. Member States risk backsliding or uneven follow-through without accountability mechanisms to ensure long-term commitment once headline targets are met.

The biannual State of the Digital Decade Report aims to track long-term digital progress, but its integration into national performance incentives remains limited.

In summary, strategic vision without funding continuity or multi-cycle monitoring can lead to volatility. Digital society strategies envision long-term transitional needs; however, the same long-term commitment to cyber capacity development appears to be lacking. However, it requires the same institutional permanence, not just project-based momentum.

#### **4.4.2.3 Alignment and Recognition of Qualifications**

The ECSF and similar competence frameworks are meant to harmonise skills definitions, but implementation gaps exist in their adoption. Many Member States have not formally integrated the ECSF into national qualification or job classification schemes. As of 2024, awareness of the ECSF among employers and academia is limited, as mentioned in EU reports [12] and also in the survey conducted for this research. A typical HR department or university department in Poland or Finland might not use it to design job profiles or curricula. The European Classification of Skills (ESCO) [136] includes cybersecurity roles, and ECSF maps to it, but national labour taxonomies may also lag in updating these categories.

The lack of standardisation has tangible consequences:

- Hinders cross-border mobility, as roles like “cybersecurity analyst” might vary by country,
- Credential portability is low, complicating cross-border hiring and talent mobility,
- Even employers struggle to articulate their needs, preventing the alignment between graduate output and industry needs.

Some Member States, like the Czech Republic (CyQUAL) [137], are adopting localised standard mappings, but these efforts remain isolated.

Without widespread adoption of ECSF-aligned frameworks, the EU cannot realise a seamless cyber labour market. The result is inefficiency, reduced mobility, and persistent skills mismatches.

#### **4.4.2.4 Interdisciplinary Integration Gap**

The cyber domain's defining characteristic is its interconnectedness, and digital transformation is characterised by exponentiality [7]. However, most capacity-building efforts are often limited to technical professions in a linear, siloed manner. The EU emphasises the necessity for interdisciplinary cyber competence across various sectors, yet implementation remains inconsistent and culturally isolated.

For example, numerous MBA or public administration programs provide little to no cybersecurity education, meaning prospective managers or civil servants may lack essential knowledge about managing cyber risks, falling short of what is expected of future-ready professionals.

Training remains inconsistent even in sectors where “cybersecurity culture” is formally promoted, such as healthcare and education. Too often, cybersecurity is viewed as an IT issue rather than a collective responsibility, whereas EU-level instruments call for inclusive cybersecurity responsibility. Shifting this perspective requires time and a strong focus on leadership.

Although the NIS2 directive mandates cyber awareness and training across essential entities and calls for decision-makers' responsibility, delays in compliance, cultural transformation, and diverse implementation across different Member States may still occur.

To summarise, without mainstreaming cybersecurity across disciplines and institutions, the EU will continually fall short of achieving its vision for cyber-aware societies and digitally resilient economies.

#### **4.4.3 Operational Gaps**

Operational gaps arise from the disconnect between strategic intentions and the realities of execution. They often involve inconsistent cyber skills development and a lack of scalable, outcome-driven capacity building. This section explores the root causes, including resource constraints, varying institutional capabilities, and the absence of standardised operational frameworks across Member States.

##### **4.4.3.1 Training and Awareness Gap – Policy vs. Practice**

While EU cybersecurity strategies - including the NIS2 Directive and Digital Education Action Plan - emphasise the importance of widespread awareness and training, implementation remains inconsistent across Member States. According to the Eurobarometer on Cyberskills (2023), 74% of EU companies did not provide any cybersecurity training to their employees [63].

The report highlights further trends: SMEs and local governments often lack regular training programmes even in countries with robust strategies. For instance, while Poland and Estonia run national awareness campaigns, many small businesses still underestimate the need, as evidenced by the 68% of EU-wide companies that believe no training is necessary for their staff.

This signals an operational gap: recognition of importance is not translating into action. Possible reasons include budget constraints (noted by approximately 16% of companies) and limited access to training resources, particularly in smaller markets. To address this, nations may need to incentivise training (e.g., tax breaks or integrating cyber modules into all professional development curricula) and better enforce standards (for instance, through sector regulators under NIS2).

Member States risk leaving large segments of the workforce unprepared without bridging the gap between awareness and practice, which undermines joint competitiveness and resilience efforts.

#### **4.4.3.2 Depth and Quality of Skills**

Beyond mere statistics, a persistent qualitative gap persists. The EU aims to increase the number of cyber professionals, develop highly skilled individuals across various specialities, and foster a cyber-aware public. However, the practical reality of training reveals significant variability in quality and outcomes. Not everyone who completes “cybersecurity training” leaves with the adequate skills required for their position. An academic cybersecurity degree in one country can mean a different background than in another.

For example, some accelerated training programs may produce junior analysts; hence, companies often need additional on-the-job training. Similarly, while integrating cybersecurity into school curricula appears promising, its effectiveness is hindered if teachers lack confidence in the subject matter. Contributing factors include pedagogical and curricular challenges: the rapidly changing nature of cybersecurity makes it difficult for many educational institutions to keep their content relevant and hands-on. A common issue is the lag between current teaching and industry needs, leading to a skills mismatch [138] [139].

The shortage of trainers exacerbates the situation; seasoned cybersecurity professionals often prefer lucrative roles in the industry over teaching positions, making it hard for universities and vocational programs to attract instructors with up-to-date practical knowledge. This shortage can result in a gap in educational quality.

Expanding training volumes may produce inflated numbers without corresponding capability gains, without ensuring content relevance, pedagogical quality, and trainer capacity.

#### **4.4.3.3 SMEs and Sectoral Disparities**

The EU's vision for cyber resilience includes the principle of “no sector left behind,” but operational reality falls short, as national implementations often struggle to reach smaller enterprises. Most national strategies do not define KPIs for SME cybersecurity capacity, nor systematically track training uptake [140], which is notable, as SMEs represent 99% of all businesses in the EU [141].

The Estonian Cyberhubs analysis [135] noted SMEs have acute workforce issues, with IT generalists stretched thin to cover security. Many SMEs across the EU cannot afford a full-time cybersecurity expert and rely on external contractors or “accidental admins”. The shadow workforce in SMEs – employees handling security informally – is enormous, yet training and support for them is patchy.

This represents a strategic gap: the EU and states have not fully resolved how to provide scalable cybersecurity services or shared personnel for SMEs (though concepts like “cybersecurity as a service” or regional cybersecurity centres are being explored). The SME cybersecurity gap amplifies a systemic weakness throughout the EU. Until Member States implement targeted actions addressing these challenges, this sector will continue to limit the Union's broader cyber resilience objectives.

#### **4.4.3.4 Gender and Diversity**

Despite recognising the gender gap in strategies and at the EU level, progress in female participation in cybersecurity roles remains slow. The gap is evident: only ~19% of ICT specialists in Europe are women [142], and in cybersecurity it's often estimated around 10–20%. The Eurobarometer's [63] found that 56% of companies have no women in cyber roles.

Most national strategies recognise the importance of diversity, but concrete measures or targets for enhancing gender balance are scarce. For example, none of the five countries studied has a specific percentage target for women in cybersecurity by a particular date.

This is an operational gap in implementation: general statements of support have not translated into structured programs (aside from voluntary initiatives like Women4Cyber [143] chapters or ad-hoc scholarships). The result is that half the population remains underutilised in addressing the skills shortage.

The EU's call for "gender convergence" by 2030 [1] appears off-track in light of current trends. Overcoming this requires more than encouragement; it likely needs funded programs (e.g. grants for women in cyber training or company incentives for diverse hiring) and tackling cultural biases. The EU cannot afford to leave half its potential workforce underrepresented. Without concrete mechanisms, diversity efforts will remain aspirational rather than operational.

#### **4.4.4 Measurement and Governance Gaps**

Measurement and governance gaps arise from inconsistent, outcome-oriented metrics and insufficient oversight. These issues impede effective progress tracking, evaluation of capacity-building initiatives, and alignment with EU strategic objectives. This section explores the structural challenges in defining, collecting, and analysing relevant data, emphasising the need for unified measurement frameworks to ensure accountability improvement.

##### **4.4.4.1 KPI Maturity: From Counting to Competence**

As discussed in Chapter 2.5, KPIs related to cyber competence and capacity prioritise quantitative outputs over qualitative ones. Also, capacity KPIs overlap with skills, such as the number of operational Security Operations Centres (SOCs) in the country or the number of cybersecurity startups created, which indirectly reflect the available human capital and its utilisation [144], [145]. These figures are essential for political visibility and basic accountability, but fall short in measuring impact, readiness, and competence.

A recurring theme in evaluating national-level KPIs is that quantitative targets are more frequently stated. For example, a national strategy might specify "train 500 cybersecurity experts for public administration by 2025" which are straightforward to report, yet



whether those 500 experts significantly improved security or contributed to digital competitiveness is more challenging to measure. Qualitative evaluation often comes later in the form of audits or incident analysis.

For instance, the fact that “500,000 Europeans have received free cybersecurity training via various initiatives” [146] is a positive quantitative outcome of EU programs. However, simple counts do not capture the qualitative dimensions, like how skilled those trainees are, how well they apply knowledge, and whether organisations are more secure, though harder to assess.

Yet, as seen in some cybersecurity strategies and approaches [70], [71], [72], qualitative assessments are required. These typically require prolonged observation and ongoing feedback loops; however, metrics can involve methods such as certification exams and skills competitions to measure them. For the increase in individuals passing recognised certification exams to be a relevant indicator, there must be a common standard ensuring exams accurately reflect skill and link quantity with quality.

Furthermore, cybersecurity exercises can serve as indirect KPIs; for instance, if a nation’s teams repeatedly excel in EU cybersecurity exercises or international cyber competitions [147] over the years, it reflects a rise in skill levels that raw numbers cannot reveal.

In summary, while quantitative KPIs remain essential for accountability and political visibility, they should be augmented by more impact-oriented, skills-proficiency-aligned indicators. Indicators that extend beyond the narrowly defined cybersecurity competence and begin to track cyber competence availability in a broader sense. The complexity of the cyber domain renders standardised qualitative metrics difficult to apply universally; however, mixed approaches, such as merging certifications, feedback loops, and applied performance, could offer a more precise assessment of workforce capability and availability. A shift toward outcome-based, proficiency-aligned KPIs is essential for evaluating the actual return on cyber investment and to steer funding where it is most effective.

#### **4.4.4.2 Monitoring and Evaluation Gap**

Even where strategies exist, measurement systems are underdeveloped. Many Member States do not track the number of certified professionals, nor do they track the distribution of skills across sectors.

Basic inquiries, such as the number of cybersecurity experts available and the sectors with the most significant skill shortages, remain unanswered with precision in various states, complicating progress measurement. This issue arises primarily because measurement systems are still evolving. Until recently, few countries recognised the “cybersecurity workforce” as a distinct category in labour statistics or maintained registries of certified professionals.

The ECSF and ENISA’s evolving roles in benchmarking are promising, but tools remain fragmented, and uptake is slow. Moreover, cybersecurity is rarely distinguished from broader ICT categories in national labour statistics, delaying meaningful analysis.

This creates a critical feedback gap: without timely, comparable data, Member States and the EU cannot identify what works, scale good practices, or course-correct misaligned efforts. This results in policies outpacing measurement. Until evaluation catches up, the EU’s ability to track progress and optimise investments will remain constrained.

#### **4.4.5 The EU’s Implementation Dilemma**

The EU’s greatest strengths - diversity and respecting national values - is its greatest implementation challenge. While the Union provides vision, funding instruments, and regulatory direction, implementation is left to Member States. The result is an asymmetric progress, with some countries leading in integration, while others lag due to bureaucratic inertia, resource limitations, or policy fragmentation. The multilingual, multicultural training needs complicate the implementation of one-size-fits-all solutions; curricula and awareness programmes must be localised, and there is still no alignment on an EU-wide scale what cybersecurity trainings and education materials should cover. This is entirely driven by local market and academic requirements or ambitions, and not through policies or EU certifications.

Additionally, the EU focuses primarily on defensive and civilian-oriented cyber capabilities, while some Member States are building their offensive capability as part of

their military doctrine [148], [149]. This lack of an offensive dimension creates a gap in the EU's ability to attract and retain high-end cyber talent, many of whom are drawn to more comprehensive military cyber operations [150]. Meanwhile, adversarial states are actively advancing their offensive cyber capabilities.

This strategic imbalance highlights the need for the EU to establish a robust, Union-wide retention and development system that can maintain essential expertise, enhance operational readiness, and bolster long-term resilience in the changing cyber landscape. The standard capacity framework must be paired with shared accountability, better coordination mechanisms, and a stronger Union-level steering function.

#### **4.4.6 Conclusion**

The review of implementations in Member States and EU frameworks shows a strong agreement on the strategic importance of cybersecurity skills, yet there remains a noticeable gap in execution. Several structural, economic, institutional, and cultural factors contribute to this gap.

Structural inertia, particularly within the educational system, slows the responsiveness of curricula and certification mechanisms. Economic disparities drive brain drain within the EU, weakening national capacity despite EU investment. Coordination challenges, both horizontal (across sectors) and vertical (between EU and Member States), result in fragmented delivery: duplicative initiatives coexist with critical capability gaps. For example, EU-funded programmes may train individuals without follow-on integration or permanent institutional support.

Cultural aspects also contribute to the issue. In many organisations and administrations, cybersecurity remains undervalued, regarded as a peripheral IT matter rather than a strategic competency. This “it won't happen to us” mindset hinders the adoption of EU recommendations, such as regular staff training and risk-aware governance practices.

The gap analysis confirms that while policy alignment has improved, implementation remains uneven, under-measured, and often reactive. Data limitations, unclear accountability, and limited convergence on quality standards further hinder progress and situational awareness.

That said, EU is not standing still. Initiatives like EU's Cyber Skills Academy aims to address coordination and utilisation issues by establishing a centralised effort to fill these gaps. This agenda requires ongoing political commitment, flexible investments, and a governance model that actively integrates feedback to ensure success.

The following section translates this diagnostic insight into a series of targeted recommendations, addressing the structural, systemic, and strategic misalignments that currently inhibit the full realisation of the EU's cybersecurity capacity-building vision.

## **5 From Insight to Action: Designing a Next-Generation EU Cyber Capacity Framework (NG-EUCCF)**

The previous analysis reveals that, while the European Union has effectively articulated a detailed vision for developing cyber competence and tries to close the skills gap, its implementation remains uneven, reactive, and inconsistent among Member States. This gap does not stem from a lack of policy but rather from issues in operational alignment, systemic coherence, and measurable impact.

Providing a lasting solution requires a systematic and harmonised approach that turns high-level ambitions into scalable, sustainable, and outcome-oriented capacity-building processes. This chapter presents the Next-Generation EU Cyber Capacity Framework (NG-EUCCF): a modular, evidence-based conceptual model to facilitate the integration, optimisation, and monitoring of current EU instruments and national strategies. By directly linking identified strategic gaps to actionable design principles, the framework empowers the EU and its Member States to cultivate future-ready cyber talent pipelines on a large scale, defined by shared standards, adaptable structures, and measurable results.

### **5.1 Strategic Implications of the Cybersecurity Skills Gap**

Bridging the gap between EU strategic ambitions and implementation realities requires a systematic realignment of how the development of the cyber skills pipeline is conceptualised, delivered, and measured. This study's evidence shows that while Member States share broad goals, the tools and governance mechanisms used to achieve them remain fragmented, misaligned, or underpowered.

This section introduces a structured integration framework designed to operationalise existing EU mechanisms by improving alignment, scale, and outcome orientation. It builds on instruments such as the European Cybersecurity Skills Framework, the Cyber Skills Academy, the Digital Decade Policy Programme, and ENISA-supported initiatives. The intent is to translate policy into practice, ensuring that strategic intent matches measurable, sustainable, and forward-looking results.

The model is grounded in three core assumptions:

1. Cyber capacity-building is not just a technical or regulatory endeavour; it is a strategy for human capital that necessitates educational reform, market incentives, and alignment across sectors.
2. Fragmentation in qualification systems, measurement, and governance remains a key limiting factor throughout the EU.
3. Scalability, standardisation, and adaptability are vital for managing rapid technological change and rising contestation in the cyber domain.

The forthcoming sections clarify the gap typology derived from the preceding analysis and introduce a targeted model to guide policymakers in recalibrating their approach.

### **5.1.1 Identification and Clarification of Key Gaps**

Drawing from the diagnostic analysis in Chapter 4, this section consolidates the most critical systemic and structural gaps discussed. As introduced above, several gaps have been identified across EU-level strategies and their national implementations. These gaps reflect a structural limitation or a misalignment between policy goals and operational realities. The aim is to address them systematically, enabling coherent, scalable, and future-ready talent development across the EU.

The gaps identified and to be addressed:

- Workforce Supply vs. Demand
- Future Skills and Emerging Technologies
- Adapting Strategic Thinking to a Contesting and Unpredictable Environment
- Alignment and Recognition of Qualifications
- Interdisciplinary Integration Gap
- Depth and Quality of Skills
- SMEs and Sectoral Disparities
- Gender and Diversity

- Long-term Sustainability and Funding
- Cybersecurity as a National Enabler vs. Technical Compliance Focus
- Monitoring and Evaluation Gap
- Structural Fragmentation and Strategic Coherence Gap

To support clarity and traceability between findings and proposed solutions, Table 2 below maps each identified strategic or operational gap (as outlined in Chapter 4.4) to its analytical origin and the specific NG-EUCCF framework components designed to address it. This mapping has three objectives: first, it shows that the framework is based on the identified shortcomings of existing EU and Member State practices; second, it demonstrates the framework's internal coherence; and third, it confirms that each intervention area is linked to a specific problem statement.

While specific gaps were analysed independently in their own subsections, others were addressed in a more integrated way; the table consolidates these relationships and guides the reader through the rationale for each design choice in Section 5.3. The structured approach should also support future implementation efforts, assisting stakeholders align problem domains with the corresponding institutional policy and operational levers proposed in this framework.

Gap Identified	Discussed in	Addressed by Framework Component
Workforce Supply vs. Demand	4.4.2.1	5.3.1 Strategic Cyber Skills Intelligence Core
		5.3.3 Dual-Tier Curriculum Architecture
		5.3.6 Incentive Infrastructure
Future Skills and Emerging Technologies	4.4.1.3	5.3.3 Dual-Tier Curriculum Architecture
		5.3.7 Future Readiness and Foresight Layer
Adapting Strategic Thinking to a	4.4.1.2	5.3.7 Future Readiness and Foresight Layer

Contesting and Unpredictable Environment		5.3.1 Strategic Cyber Skills Intelligence Core
Alignment and Recognition of Qualifications	4.4.2.3	5.3.4 Credential Lifecycle and Recognition System
		5.3.5 HEI Accreditation Scheme
Interdisciplinary Integration Gap	4.4.2.4	5.3.3 Dual-Tier Curriculum Architecture
		5.3.6 Incentive Infrastructure
Depth and Quality of Skills	4.4.3.2	5.3.2 EU Cyber Capacity KPI Hub
		5.3.4 Credential Lifecycle and Recognition System
SMEs and Sectoral Disparities	4.4.3.3	5.3.6 Incentive Infrastructure
		5.3.9 Policy Feedback and Refinement Loop
Gender and Diversity	4.4.3.4	5.3.8 Cyber Inclusion and Retention Protocol
Long-term Sustainability and Funding	4.4.2.2	5.3.6 Incentive Infrastructure
		5.3.9 Policy Feedback and Refinement Loop
Cybersecurity as a National Enabler vs. Technical Compliance Focus	4.4.1.1	5.3.7 Future Readiness and Foresight Layer

Table 2 Gap-to-Framework Mapping Table

## 5.2 Conceptual Framework Overview

This section introduces the conceptual Next-Generation EU Cyber Capacity Framework (NG-EUCCF), proposing a solution to the systemic gaps identified in the previous section. The framework's objective is to provide a coherent, actionable and operationally viable model that supports the development of a skilled, agile, and strategically aligned cybersecurity workforce across the European Union. Rather than proposing new institutions or policies, the NG-EUCCF builds upon and integrates existing EU initiatives such as the European Cybersecurity Skills Framework (ECSF), the European



Cybersecurity Skills Academy (ECSA), and the Digital Decade Policy Programme (DDPP).

The framework comprises nine interdependent components designed to be modular, interoperable, and policy-relevant. These components align with EU-level strategic objectives and national implementation needs, supporting vertical (EU-to-national) and horizontal (inter-sectoral) coordination. Each component addresses a specific subset of the observed gaps while collectively functioning as a coherent model for EU-wide application.

The framework rests on six core principles:

- Outcome orientation – prioritising measurable improvements in cyber resilience over procedural activity metrics.
- Scalability and inclusion – ensuring EU-wide accessibility through modular, digital-first delivery.
- Standards alignment – ensuring consistency in curricula, credentialing, and institutional quality using ECSF as a unifying baseline.
- Strategic foresight – embedding anticipatory planning into curriculum cycles and capacity development.
- Sustainability – leveraging multi-source funding and structural incentives to ensure long-term uptake and viability.
- Human-centric integration – embedding diversity, well-being, and retention as critical enablers of capacity, not peripheral considerations.

As mentioned above, the framework is not intended to replace existing initiatives, but to operationalise and extend them into a unified and implementable architecture for EU-wide application. These components are designed to operate in synergy, enabling dynamic feedback, continuous improvement, and implementation across diverse national contexts.

5.3 Framework Components and Implementation Design

The NG-EUCCF comprises nine interdependent components that collectively deliver a harmonised, future-proof, and metrics-driven model for cybersecurity workforce development in the EU.

5.3.1 Strategic Cyber Skills Intelligence Core

**Addresses:** Fragmented labour market intelligence, lack of real-time alignment between threat landscape and workforce needs, absence of predictive insights for capacity planning.

**Description:** This component establishes a permanent EU-level intelligence mechanism to monitor, analyse, and forecast cybersecurity workforce demand and supply. Operated jointly by ENISA, Eurostat, and the EU Cybersecurity Skills Academy, it consolidates data on labour trends, threat evolution, educational output, and certification uptake.

The core function is to produce continuous, actionable insights. These include threat-skills correlation analyses, labour market dashboards, and predictive reports to guide national workforce planning and EU funding strategies. This ensures that cyber workforce development is proactive, strategic, and informed by the actual evolution of systemic risks.

Value delivered:

- Enables evidence-based curriculum and capacity planning.
- Aligns workforce investment with threat evolution and digitalisation demands.
- Supports early warning for skill shortages and regional market failures.
- Anchors EU policy in real-time, cross-domain workforce intelligence.

Component Summary Table

Aspect	Detail
Primary Function	Continuous data integration and threat–skills correlation
Operated By	ENISA, Eurostat, and Cyber Skills Academy

<b>Key Outputs</b>	Skills outlook reports, dashboards, early-warning forecasts
<b>Dependencies</b>	KPI Hub (5.3.2), Foresight Layer (5.3.7)
<b>Linked Gaps</b>	4.4.1.2, 4.4.2.1, 4.4.4.1, 4.4.4.2
<b>Target Stakeholders</b>	EU and national policymakers, education planners, private sector consortia

Table 3 Summary for Strategic Cyber Skills Intelligence Core

### 5.3.2 EU Cyber Capacity KPI Hub

**Addresses:** Output-centric measurement, lack of shared EU-wide qualitative indicators for cyber competence, and fragmented national reporting with slow feedback loops.

**Description:** This component introduces a unified measurement framework to standardise, track, and interpret cyber capacity-building progress across the Union. Operated as a function within the EU Cybersecurity Skills Academy and aligned with DESI, ECSF, and the Digital Decade Policy Programme, it defines multi-tier indicators for input, output, outcome, and impact. It also supports benchmarking tools, allowing countries to track their trajectory against regional averages, strategic goals, and sectoral targets.

The KPIs include technical quantitative details such as mean time to detect or respond, ECSF role penetration rates, SME and supply chain coverage, training effectiveness, diversity metrics, and cyber workforce retention. It also qualitatively demonstrates alignment with other CGIs, such as NIS2 and the AI Act, highlighting cohesion with priorities set out in various policies. Implementation can be supported by automated dashboards that feed into the Digital Decade monitoring cycle and Member State data pipelines supported by ENISA technical templates.

#### **Value delivered:**

- Moves the EU from volume-based to value-based measurement,
- Enables adaptive programme design by linking performance to policy,
- Improves accountability and cross-border comparability,

- Helps justify investment through tangible, long-term outcome tracking.

### Component Summary Table

Aspect	Detail
<b>Primary Function</b>	Common KPI framework for EU-wide cyber skills measurement
<b>Operated By</b>	EU Cyber Skills Academy in collaboration with ENISA and Eurostat
<b>Key Outputs</b>	Standardised KPI sets, benchmarking tools, performance dashboards
<b>Dependencies</b>	Strategic Intelligence Core (5.3.1), Credential Lifecycle (5.3.4)
<b>Linked Gaps</b>	4.4.3.2, 4.4.5, 4.4.2.2
<b>Target Stakeholders</b>	National authorities, education providers, EU programme evaluators

Table 4 Summary for EU Cyber Capacity KPI Hub

### 5.3.3 Dual-Tier Curriculum Architecture (HEIs + ECCTPs)

**Addresses:** Slow curriculum cycles; shortage of qualified instructors and training capacity; and inconsistent skill provisioning.

**Description:** Integrates key academic pathways (HEIs) with modular, ECSF-aligned practical training from EU Certified Cyber Training Providers (ECCTPs). Features the EU Virtual Cyber Campus for multilingual, remote access, along with a Train-the-Trainer program to enhance instructor capacity in Member States. It builds on existing education systems but introduces modularity, scalability, and specialisation through a stackable design. The curriculum is divided into foundational and transversal cyber competencies (targeting broad digital professionals) and specialised technical and non-technical domains (AI, OT, forensics, quantum, etc.), stackable and ECSF aligned micro-credentials.

**Value delivered:**

- Accelerates the availability of critical skills while preserving academic legitimacy;
- Harmonises quality across Member States, while respecting national autonomy;
- Facilitates career progression through flexible, stackable modules;
- Reduces regional disparities by enabling virtual access and scalable content delivery.

**Component Summary Table**

Aspect	Detail
<b>Primary Function</b>	Modular dual-tier curriculum integrating HEIs and ECCTPs
<b>Operated By</b>	EU Virtual Cyber Campus in partnership with HEIs and certified providers
<b>Key Outputs</b>	ECSF-aligned micro-credentials, Train-the-Trainer, AI/OT/cloud specialisms
<b>Dependencies</b>	KPI Hub (5.3.2), Credential System (5.3.4), Foresight Layer (5.3.7)
<b>Linked Gaps</b>	4.4.2.1, 4.4.1.3, 4.4.2.4, 4.4.3.2
<b>Target Stakeholders</b>	Universities, training providers, employers, ministries of education

Table 5 Summary of the Dual-Tier Cyber Curriculum Model

**5.3.4 Credential Lifecycle and Recognition System**

**Addresses:** Lack of credential interoperability; employer distrust regarding training quality and relevance; overreliance on non-EU certifications and fragmented national qualification systems; and absence of dynamic updating mechanisms for fast-evolving cyber competences.

**Description:** Implements a standardised EU credentialing framework linked to ECSF (and any other EU-recognised taxonomies) roles. It defines common structures for

credential issuance, renewal, versioning, and expiry, ensuring that qualifications remain valid, up-to-date, and trustworthy over time.

To operationalise this, the framework establishes a Digital Credential Registry, maintained at the EU level and accessible to employers, education providers, and regulators. The registry is a clearinghouse for validating credentials, monitoring lifecycle status, and mapping qualifications to ECSF roles. The system supports integration with micro-credentials, certification pathways, and stackable learning tracks delivered under the Dual-Tier Curriculum (5.3.3). The system ensures cyber qualifications reflect real-world relevance and competence through embedding dynamic update mechanisms: e.g. aligning credentials with emerging domains like AI or PQC.

#### **Value delivered:**

- Establishes a trusted and transparent EU-wide certification ecosystem;
- Enables labour mobility and credential portability across Member States;
- Reduces reliance on proprietary or non-EU certifications, advancing digital sovereignty;
- Facilitates employer validation and curriculum alignment with ECSF standards;
- Future-proofs credential systems through structured version control.

#### **Component Summary Table**

<b>Aspect</b>	<b>Detail</b>
<b>Primary Function</b>	Harmonised credential lifecycle management and validation registry
<b>Operated By</b>	EU Cyber Skills Academy + National Qualification Authorities + EU Level Industry Association like ECSO
<b>Key Outputs</b>	Expiry/renewal logic, versioning, EU-recognised digital credential ledger
<b>Dependencies</b>	Curriculum Architecture (5.3.3), KPI Hub (5.3.2), Accreditation (5.3.5)
<b>Linked Gaps</b>	4.4.2.3, 4.4.3.2, 4.4.4.2

<b>Target Stakeholders</b>	Employers, certification bodies, universities, and regulators
----------------------------	---

Table 6 Summary of the Credential Lifecycle and Recognition Framework

### 5.3.5 HEI Accreditation Scheme for Cybersecurity Excellence

**Addresses:** Inconsistent education quality across Member States, a lack of recognition mechanisms for high-performing institutions, and limited incentives for universities to align with emerging EU priorities or deliver applied cyber outcomes.

**Description:** This component establishes a formal EU-level accreditation scheme for Higher Education Institutions that demonstrate cybersecurity excellence across key strategic domains. Institutions would be evaluated based on ECSF curriculum alignment, the relevance of applied research, modern laboratory infrastructure, collaboration with industry, and practices for inclusion and retention, particularly concerning underrepresented groups.

The scheme operates through an annual evaluation cycle, coordinated by ENISA in collaboration with DG CNECT (or other relevant DG) and national education quality assurance bodies. Accredited institutions will be included in a publicly accessible EU Cyber Excellence Directory, which can be utilised for visibility, benchmarking, and eligibility for targeted EU funding calls. Evaluation criteria would be tiered and include forward-looking capabilities such as AI integration, offensive/defensive lab infrastructure, research capacity, etc. The process will incentivise HEIs to compete on quality and strategic contribution, rather than volume alone.

Awards EU-wide recognition to institutions that demonstrate excellence across key domains: ECSF alignment, applied research output, cyber lab infrastructure, inclusion and retention practices, and strategic relevance.

#### **Implementation:**

Annual evaluation cycle managed by ENISA and selected DGs like DG CNECT with public directory publication.

**Value delivered:**

- Elevates standards in cyber education through structured competition and peer benchmarking;
- Strengthens EU-wide curriculum coherence and innovation capacity;
- Encourages institutional specialisation in strategically relevant subdomains (e.g., OT, AI, PQC);
- Facilitates strategic investment, public-private partnerships, and cross-border collaboration.

**Component Summary Table**

Aspect	Detail
<b>Primary Function</b>	EU-level recognition for high-quality cybersecurity education institutions
<b>Operated By</b>	ENISA + DG CNECT, in partnership with national QA authorities, HEI stakeholders
<b>Key Outputs</b>	Multi-tier evaluation, public EU directory, eligibility for funding boosts
<b>Dependencies</b>	Curriculum Architecture (5.3.3), Credential Registry (5.3.4)
<b>Linked Gaps</b>	4.4.3.2, 4.4.2.4, 4.4.2.3
<b>Target Stakeholders</b>	Universities, quality assurance agencies, and education ministries

Table 7 Summary of the HEI Cybersecurity Excellence Accreditation

**5.3.6 Incentive Infrastructure**

**Addresses:** Limited private sector and SME engagement in cyber workforce development; the lack of scalable, sustainable funding mechanisms; and the absence of economic levers linking capacity-building with EU policy objectives.

**Description:** This component establishes a structured incentive model designed to enhance uptake and investment in cybersecurity training, particularly for SMEs,



underrepresented sectors, and private industry. It combines financial and non-financial instruments to encourage market participation and strengthen strategic alignment.

Key mechanisms include:

- Individual learning accounts and SME vouchers (financial incentives, reimbursement, etc) subsidised through EU and national programmes to support access to ECSF-aligned training;
- Tax relief schemes or similar benefits for companies that hire ECSF-certified professionals or invest in recognised training programmes;
- Procurement incentives giving preferential scores to organisations that demonstrate compliance with EU-recognised cyber workforce development standards;
- A tri-tier funding ladder, combining: (1) baseline EU grants, (2) matched private sector co-funding, and (3) scalable national financial contributions (e.g. tax credits, wage subsidies, or innovation grants).

The system is designed to integrate with existing EU frameworks (e.g., Digital Europe Programme, Horizon Europe, ESF+), while giving Member States flexibility to localise delivery.

#### **Value delivered:**

- Mobilises co-investment from industry, reducing reliance on public-only funding;
- Increases SME participation by lowering upfront training costs;
- Creates strong economic motivation to accelerate ECSF certification uptake;
- Reinforces cyber capacity-building as a lever of competitive advantage, not just compliance.

#### **Component Summary Table**

Aspect	Detail
<b>Primary Function</b>	Align economic incentives with cyber skills development
<b>Operated By</b>	European Commission + National Governments + Private Sector Consortia

<b>Key Outputs</b>	Tax relief, SME vouchers, EU grants, procurement incentives
<b>Dependencies</b>	Credential System (5.3.4), KPI Hub (5.3.2), Strategic Intelligence (5.3.1)
<b>Linked Gaps</b>	4.4.3.3, 4.4.2.2, 4.4.2.1, 4.4.3.4
<b>Target Stakeholders</b>	SMEs, large enterprises, training providers, and ministries of finance

Table 8 Summary of the EU Cyber Incentive Infrastructure

### 5.3.7 Future Readiness and Foresight Layer

**Addresses:** Outdated and static curricula that lag behind technological advancement; weak alignment between cyber skills development and emerging technologies; and absence of anticipatory mechanisms in education and workforce strategy.

**Description:**

This component incorporates strategic foresight into the cybersecurity skills development lifecycle by creating a systematic approach for updating curricula and integrating emerging domains. The foundation of this process is the biennial Cyber Skills Foresight Report, crafted by ENISA in partnership with the EU Cyber Skills Academy, JRC, Eurostat and select Member State agencies.

The foresight cycle identifies new threat areas and technology shifts, such as AI red-teaming, cognitive security, quantum resilience, and digital convergence. Findings from this report inform a regular refresh cycle for ECSF-aligned modules and are also disseminated to HEIs, ECCTPs, and accreditation bodies for curriculum adjustment.

**Value delivered:**

- Future-proofs EU cyber workforce development against technological disruption;
- Builds a responsive education ecosystem linked to strategic foresight outputs;
- Facilitates integration of new disciplines;
- Enhances EU strategic autonomy by preparing human capital for next-gen risks.

## Component Summary Table

Aspect	Detail
<b>Primary Function</b>	Embed foresight into curriculum and capacity planning
<b>Operated By</b>	ENISA, ECSA, foresight labs, strategic intelligence centres
<b>Key Outputs</b>	Biennial foresight report, structured curriculum refresh cycle
<b>Dependencies</b>	Curriculum Architecture (5.3.3), Intelligence Core (5.3.1), KPI Hub (5.3.2)
<b>Linked Gaps</b>	4.4.1.2, 4.4.1.3, 4.4.2.1, 4.4.3.2, 4.4.1.1
<b>Target Stakeholders</b>	Education ministries, training providers, standards bodies, ECSF stewards

Table 9 Summary of the Future Readiness and Strategic Foresight Layer

### 5.3.8 Cyber Inclusion and Retention Protocol

**Addresses:** High burnout among cybersecurity professionals; gender imbalance and underrepresentation in cybersecurity roles, and the lack of institutional accountability for diversity and workforce sustainability.

**Description:** This component creates a structured protocol for inclusion and retention to provide equal access to cybersecurity careers and minimise workforce attrition. It requires participating institutions: HEIs, Employment and Career Training Providers, and government-associated employers, to adopt and report on inclusive talent development practices as a prerequisite for EU accreditation or funding.

Core requirements include:

- Mentorship schemes and support networks targeting underrepresented groups;
- Transparent diversity reporting, using standardised metrics disaggregated by gender and demographic profile;

- Inclusion audits for publicly funded programmes and ECSF-aligned training initiatives;
- Incentives for returnship programmes (e.g. after parental leave), inclusive internships, and hybrid remote roles to support retention.

The protocol is directly tied to Digital Decade 2030 diversity benchmarks and monitored through the KPI Hub (5.3.2), enabling cross-EU visibility into progress.

#### **Value delivered:**

- Expands and diversifies the cybersecurity talent pool;
- Reduces dropout and burnout by improving workplace inclusion and support structures;
- Strengthens the legitimacy of public investment in skills initiatives;
- Aligns EU workforce strategies with gender equality and digital inclusion goals.

#### **Component Summary Table**

<b>Aspect</b>	<b>Detail</b>
<b>Primary Function</b>	Institutionalise diversity, inclusion, and retention across cyber workforce
<b>Operated By</b>	National labour ministries + EU Cyber Skills Academy
<b>Key Outputs</b>	Diversity reporting, mentorship, returnships, funding-linked compliance
<b>Dependencies</b>	Accreditation (5.3.5), KPI Hub (5.3.2), Curriculum (5.3.3)
<b>Linked Gaps</b>	4.4.3.4, 4.4.2.1, 4.4.3.2
<b>Target Stakeholders</b>	Training and education providers, public agencies, employers, EU grant recipients

Table 10 Summary of Diversity and Retention Measures

### 5.3.9 Policy Feedback and Refinement Loop

**Addresses:** Policy inertia and strategic misalignment over time; weak integration between outcome data and decision-making processes; delays in adapting to threat evolution or skill market imbalances.

**Description:** This component closes the data collection, implementation, and policy refinement loop. It seamlessly connects all NG-EUCCF components - the KPI Hub, Foresight Layer, and Credential Lifecycle - into a dynamic, iterative governance cycle. The loop enables continuous calibration of EU cyber capacity-building policies in response to measurable changes in labour markets, threat environments, and stakeholder performance.

Outputs such as revisions to ECSF roles, updated funding priorities, refreshed curricula, or modified accreditation criteria can be activated proactively rather than reactively. This guarantees strategic agility at both the EU and Member State levels, relying on evidence rather than solely on political momentum.

The loop's governance is anchored within the EU Cyber Skills Academy and supported by annual synthesis reports, biennial foresight updates, and structured consultations with Member States.

#### **Value delivered:**

- Embeds institutional learning and adaptive governance into EU cybersecurity policy;
- Maintains alignment between capacity investments and emerging digital risks;
- Enables timely recalibration of funding, education, and certification priorities;
- Supports transparent, data-informed leadership across the EU cyber ecosystem.

#### **Component Summary Table**

Aspect	Detail
Primary Function	Data-driven strategic refinement of EU cyber workforce policy
Operated By	EU Cyber Skills Academy, with support from ENISA, and relevant stakeholders, CSIRT coordination groups

<b>Key Outputs</b>	Synthesis reports, ECSF updates, policy recalibration triggers
<b>Dependencies</b>	All other framework components (esp. 5.3.1, 5.3.2, 5.3.7)
<b>Linked Gaps</b>	4.4.3.3, 4.4.4.2, 4.4.5, 4.4.2.2
<b>Target Stakeholders</b>	EU institutions, national governments, ECSF stewards, and education bodies

Table 11 Summary of Cyber Policy Feedback and Refinement

The NG-EUCCF repositions cybersecurity workforce development as a strategic enabler of European competitiveness and resilience. Integrating intelligence, incentives, inclusivity, and implementation into a cohesive model enables Member States to tailor their cybersecurity capacity building to their specific maturity levels and societal context while staying aligned with a unified European vision. NG-EUCCF embeds adaptability through foresight, feedback, and interactive improvement mechanisms, ensuring that Europe’s capacity-building effort remains fit for purpose in a dynamic threat and technology environment.

The framework components are visualised in Table 13 below, aligning with the four strategic pillars.

<b>Pillar</b>	<b>Framework Components</b>
<b>Insight &amp; Alignment</b>	1. Strategic Cyber Skills Intelligence Core
	2. EU Cyber Capacity KPI Hub
<b>Execution &amp; Delivery</b>	3. Dual-Tier Curriculum Architecture
	4. Credential Lifecycle System
<b>Enablement &amp; Quality</b>	5. HEI Accreditation Scheme
	6. Incentive Infrastructure
<b>Adaptation &amp; Inclusion</b>	7. Future Readiness Layer
	8. Inclusion & Retention Protocol
	9. Policy Feedback Loop

Table 12 NG-EUCCF Strategic Pillar View

## 5.4 Structure of the NG-EUCCF

In Table 13 below, the nine components of the NG-EUCCF are summarised.

Component	Primary Function	Gaps Addressed	Proposed Stakeholders	Lead
<b>Strategic Cyber Skills Intelligence Core</b>	Aggregates labour data, threat trends, and policy foresight	Workforce supply-demand mismatch, foresight integration, and misaligned KPIs	ENISA, Eurostat, national observatories	
<b>EU Cyber Capacity KPI Hub</b>	Defines standardised metrics and benchmarks for cyber capacity	Lack of outcome-based indicators, fragmented monitoring	EU Cyber Skills Academy, Eurostat, DESI contributors	
<b>Dual-Tier Curriculum Architecture (HEI + ECCTP)</b>	Delivers role-based training through HEIs and certified providers	Curriculum obsolescence, SME access, depth/quality of instructor skills	HEIs, ECCTPs, EU Virtual Cyber Campus	
<b>Credential Lifecycle and Recognition System</b>	Implements EU-wide credentialing with expiry and validation mechanisms	Credential trust, workforce mobility, quality assurance, non-EU dependency	EU Cyber Skills Academy, national certification bodies	
<b>HEI Accreditation Scheme for Cyber Excellence</b>	Recognises and incentivises HEIs with advanced training and research capabilities	Visibility of excellence, teaching quality, research-policy integration, inconsistent education quality, lack of competitiveness	ENISA, DG CNECT, national QA bodies, HEI stakeholders	
<b>Incentive Infrastructure</b>	Stimulates training investment through tax reliefs, grants, and procurement rules	Low SME uptake, funding gaps, underinvestment	European Commission, Member States, SMEs, and local associations	

<b>Future Readiness and Foresight Layer</b>	Embeds future skills and technology trends into workforce development	Reactive strategy posture, lack of skills for emerging domains, curriculum stagnation, delayed adaptation	ECSA, ENISA foresight labs, strategic intelligence centres
<b>Cyber Inclusion and Retention Protocol</b>	Institutionalises workforce well-being, diversity, and long-term retention	Burnout, gender imbalance, attrition, and underutilised talent pools	HEIs, HR policy bodies, EC diversity units, Labour ministries
<b>Policy Feedback and Refinement Loop</b>	Enables adaptive policy design through data-driven recalibration.	Strategic rigidity, disconnect between implementation and intent	ENISA, ECSA, CSIRT coordination groups, ECSF governance bodies

Table 13 Functional Roles of NG-EUCCF Components

## 5.5 Summary

The NG-EUCCF provides a structured and actionable model to assist the European Union develop a resilient, skilled, and strategically aligned cyber workforce and closing the skills gap. Through nine interlinked components, it addresses the full range of identified gaps in current EU and selected national strategies.

The framework combines workforce intelligence, curriculum development, credentialing, foresight, inclusion, and feedback mechanisms into a unified structure that promotes scalability and contextualization among Member States. It redefines cybersecurity capacity building as not just a compliance task or technical skill offering but as a fundamental component of Europe’s digital sovereignty, economic competitiveness, and social wellbeing resilience.

This chapter presents an innovative conceptual model that converts wide-ranging strategic goals into actionable constructs. It serves as a guideline for policymakers and institutional stakeholders, enabling them to align capacity-building efforts with quantifiable results and the necessary readiness for the future.



## **5.6 Validation of NG-EUCCF**

To validate whether the proposed Next-Generation EU Cyber Capacity Framework aligns with the practical needs and strategic priorities of the European cybersecurity ecosystem, a structured validation survey was conducted among a targeted group of stakeholders. This group comprised members of the ENISA Advisory Group, CISOs from European multinational corporations, academic leaders, policymakers from the European Commission, and representatives from key EU agencies. The survey specifically focused on high-profile professionals with extensive expertise in cybersecurity, digital resilience, and capacity building, to ensure that the results reflect well-informed perspectives from those directly influencing European cybersecurity policy and practice.

This approach aimed to capture insights from experienced professionals in cybersecurity capacity building, maintaining quality and relevance in feedback. The survey was conducted through direct invitations, avoiding mass distribution on platforms like LinkedIn for targeted expert responses input.

The survey collected both quantitative ratings and qualitative insights across the following dimensions:

- Familiarity with EU cybersecurity strategies (e.g., NIS2, Cyber Resilience Act, ECSF)
- Perceptions of NG-EUCCF components, including strategic alignment and scalability
- Identification of gaps and challenges in current capacity-building efforts
- Recommendations for enhancing EU cybersecurity resilience

A total of 31 respondents contributed, creating a solid basis for the analysis in this section. The survey questions and the response details can be found in Appendix 4.

## **5.7 Key Findings of the Validation**

Nearly all respondents identified technical skills, governance, risk management, compliance, cybersecurity leadership, and critical thinking in cyber contexts as the most essential gaps. Notably, 48% agreed that current EU and national initiatives are

insufficiently addressing non-technical cybersecurity competencies, highlighting a significant gap in leadership, decision-making, and cross-functional coordination. All respondents concurred that cybersecurity competence should be systematically integrated and assessed across non-cyber domains, such as education, law, and public administration, to ensure national future-readiness and cross-sectoral resilience.

In a quest to identify priority investment areas aimed at bridging the cybersecurity skills gap, 27 respondents highlighted upskilling and reskilling programs for mid-career professionals as the top priority. This was closely followed by incentives for collaboration between industry and education (14) and initiatives focused on public awareness and behavioural change (13). Numerous respondents also emphasised the necessity of sustainable, long-term financial backing for these initiatives, advocating for structural integration and reliable funding mechanisms to maintain continuity as the digital landscape progresses.

In response to prioritising investment areas to address the cybersecurity skills gap, 27 respondents highlighted upskilling and reskilling programs for mid-career professionals as the top priority. This was followed by incentives for collaboration between industry and education (14) and initiatives aimed at raising public awareness and promoting behavioural change (13). This highlights the importance of continuous professional development as digital transformation accelerates and dependence on technology grows.

A notable result from the survey shows ongoing fragmentation between EU and national cybersecurity capacity-building strategies. Twenty-one respondents identified this issue as a key barrier to practical implementation, with low prioritisation by leadership (18) and ongoing skills gaps in realising strategic objectives (17) following closely behind. To mitigate these challenges, respondents suggested adopting harmonised metrics, common KPIs, and unified performance tracking systems to enhance coordination and consistency in national efforts.

A key takeaway from the survey is the ongoing division between EU and national strategies for enhancing cybersecurity capacity. Twenty-one respondents pointed this out as a major obstacle to effective execution, with low prioritisation by leadership (18) and ongoing skills deficiencies in achieving strategic goals (17) coming in next.

While standardised frameworks are crucial, only one participant indicated that their organisation actively employs the ECSF. The remaining respondents either knew about the ECSF but did not use it (15) or were completely unaware of it (8). This discrepancy highlights the need for better dissemination, operational support, effective communication and proper incentives regarding the benefits for organisations, such as structured training programs and alignment with industry needs.

Most respondents expressed concerns about the coordination between EU institutions and national authorities in developing cybersecurity skills. Only six respondents felt confident that existing EU policies, such as NIS2, the Digital Decade, and ECSF, would effectively bridge the cybersecurity skills gap by 2030. In contrast, 12 respondents remained neutral, and 14 expressed a lack of confidence, suggesting a possible disconnect between the policy framework and its practical effects. Respondents emphasised the importance of strong strategic leadership to enhance coordination, simplify decision-making, and ensure alignment between EU and national initiatives.

The majority of respondents expressed worries regarding the collaboration between EU institutions and national authorities in enhancing cybersecurity skills. Merely six individuals indicated confidence that current EU policy instruments, including NIS2, the Digital Decade, and ECSF, will significantly reduce the cybersecurity skills gap by 2030. In contrast, 12 respondents were neutral, and 14 lacked confidence, indicating a potential disconnect between policy development and its practical implications.

The survey also explored the perceived relevance of the NG-EUCCF components. The highest-ranked components included:

- Inclusion of non-cyber domains (e.g., law, public administration, executive leadership)
- Governance and coordination mechanisms to clarify responsibilities between EU institutions and Member States
- Accreditation schemes for HEIs focused on cybersecurity excellence

Integrating threat and labour market intelligence for cyber workforce planning and ECSF training was deemed less relevant, revealing ongoing challenges in aligning strategic foresight with workforce development.

The survey featured three open-ended forms that allowed respondents to share their thoughts. In response to the first question about what key action they believe the EU or member states should take to address the skills gap, participants emphasised the need for a standardised, EU-wide cybersecurity curriculum that meets actual industry demands and facilitates cross-border cooperation. They also stressed the importance of practical training and public-private partnerships in bridging the gap between academia and industry, ensuring that graduates possess the essential skills required for real-world cybersecurity jobs. Many answers emphasised the importance of long-term, adaptable programs that predict emerging technologies and market trends, backed by structural incentives such as competitive apprenticeships, retraining opportunities, and targeted assistance for SMEs. Additionally, many participants emphasised the importance of support from senior leadership, strategic prioritisation, and stable funding mechanisms to foster ongoing workforce development and alignment with broader EU digital objectives.

In response to the inquiry regarding the blind spots hindering the effectiveness of current cybersecurity capacity-building programs, several key gaps were identified. These include inadequate incorporation of cybersecurity within broader educational frameworks, a deficiency in cross-skilling and reskilling opportunities for mid-career professionals, and a disconnect between theoretical training and the practical, hands-on skills necessary to handle live cyber incidents. Many participants emphasised the excessive focus on technical skills, neglecting the human and operational challenges faced by cybersecurity teams, as well as the cultural and sector-specific variations among Member States. Additionally, respondents indicated that a lack of awareness among decision-makers, resource limitations, and minimal collaboration among the public, academic, and private sectors present significant obstacles to effective capacity-building.

In general, respondents showed support for the initiative, recognising its potential for essential standardisation and alignment among Member States. However, many emphasised the necessity of flexibility to respond to rapidly changing threats, the value of practical validation via pilot programs, and the difficulty of ensuring local relevance while upholding a standardised EU-wide approach. Additionally, numerous respondents

emphasised the importance of collaboration between the public and private sectors to facilitate scalability and generate tangible outcomes, particularly for small and medium-sized enterprises. Some feedback indicated concerns that the framework could become overly theoretical without robust implementation mechanisms and clear pathways tailored to various learning environments.

Overall, the survey findings support the need for improved EU-wide coordination. Respondents widely supported the NG-EUCCF components, especially valuing explicit role definitions and measurable KPIs in cyber capacity building. This is in line with the main objectives of the NG-EUCCF, which seeks to connect the strategic divide between policy aspirations and practical implementation, thereby guaranteeing Europe's enduring digital resilience and competitiveness.

## 6 Conclusion and Future Directions

This chapter summarises the main findings of the thesis, considering the gaps identified in EU cybersecurity capacity building and how the proposed NG-EUCCF framework can address these issues. It evaluates the broader implications for EU digital resilience, competitiveness, and long-term strategic positioning. Furthermore, the chapter suggests potential future research avenues, emphasising the need for ongoing adaptation as the digital landscape evolves and new strategic priorities emerge.

### 6.1 Summary of Findings

This thesis examines the structural and operational challenges in existing EU cybersecurity capacity-building strategies, with a particular emphasis on human-centric skills. Comparing EU-level policies with those of Member States uncovered fourteen specific gaps hindering the effective development of a skilled and resilient cyber workforce. These issues include workforce shortages, training inconsistencies, inadequate foresight, misconfigured KPIs, weak cross-sector collaboration, and a lack of incentive mechanisms.

The research introduced the Next-Generation EU Cyber Capacity Framework (NG-EUCCF), a conceptual structure for transforming strategic goals into operational capabilities. This framework comprises nine interlinked components. It consolidates and extends current instruments such as the European Cybersecurity Skills Framework, the Cybersecurity Skills Academy, and the Digital Decade Policy Programme. It is designed to be modular and scalable, enabling national adaptation while supporting EU-wide strategic cohesion.

#### **6.1.1 Response to Main Research Question: How can EU cybersecurity capacity-building be improved to effectively and sustainably close the skills gap?**

This research demonstrates that the EU's ambitious cyber capacity-building agenda remains fragmented, overly focused on compliance and technology, and insufficiently aligned with workforce sustainability and competitiveness goals. The proposed NG-EUCCF responds by offering a governance-aware, future-oriented framework that translates strategic ambition into measurable outcomes. Specifically, the thesis proposes

the Next-Generation EU Cyber Capacity Framework as a structural solution for operationalising human-centric capacity building at scale.

The framework enhances the EU's capacity-building efforts in cybersecurity by:

- Embedding outcome orientation via a common KPI architecture to track resilience impacts, workforce retention, and diversity;
- Aligning delivery systems through dual-tier curriculum infrastructure, micro-credentialing, and a credential lifecycle system mapped to ECSF roles;
- Closing implementation gaps by supporting scalable, remote-ready training ecosystems, instructor pipeline growth, and SME inclusion;
- Creating structural incentives through co-financing models, learning accounts, and procurement-linked benefits;
- Integrating strategic foresight and adaptability by linking curriculum cycles to threat intelligence and emerging technology domains;
- Institutionalising continuous improvement through an EU-wide policy feedback loop that informs strategic recalibration.

### 6.1.2 Responses to the Sub-Research Questions

- **RQ1: How do existing EU cybersecurity strategies and related policies prioritise human-factor cybersecurity competencies (both technical and non-technical)?**

Existing EU cybersecurity strategies formally recognise human-centric competencies, yet implementation disproportionately emphasises technical roles. Non-technical skills, including behavioural, legal, and organisational expertise, remain underdeveloped and are often sidelined in operational KPIs and national policy instruments.

- **RQ2: How are these strategies being implemented by selected Member States?**

National implementation is uneven. Some Member States have built ECSF-aligned systems and support structures, while others lag in workforce planning, monitoring, or inter-institutional collaboration, contributing to fragmentation across the Union. There is no coordinated approach to assessing national progress

or aligning implementation with EU-level strategic goals, especially regarding shared KPI level tracking.

- **RQ3: Do current EU cybersecurity policy frameworks primarily treat cybersecurity as a technical discipline or an enabling domain for broader digital readiness?**

Despite recognising cybersecurity as a digital enabler, EU frameworks still primarily view it as a risk mitigation function. Consequently, the potential of cybersecurity to foster innovation, trust, and competitiveness remains unrealised.

- **RQ4: What are the implications of these gaps for the EU's digital competitiveness and broader economic security?**

These misalignments pose significant risks to the EU's digital sovereignty and competitiveness. Without a coordinated, future-oriented approach to talent development, the Union will continue to rely on external expertise and remain vulnerable to technological challenges and shocks.

**RQ5: What practical strategic measures or incentives could the EU adopt to effectively integrate and sustainably scale human-centric cybersecurity competencies to enhance long-term competitiveness?**

The NG-EUCCF addresses these challenges by offering interdependent solutions—including a KPI intelligence core, curriculum infrastructure, credentialing system, incentive framework, foresight mechanism, inclusion protocol, and real-time feedback loops.

## 6.2 Scientific and Practical Contributions

This thesis contributes to both theory and practice by:

- Translating policy fragmentation into an integrated, modular solution;
- Demonstrating how multi-level governance can be aligned through shared incentives and standardised instruments;
- Filling a previously unaddressed gap by analysing the misalignment between EU-level strategic goals and the mechanisms used to monitor and implement them;
- Providing a conceptual and practical bridge between EU strategic documents (e.g. ECSF, DDPP, ECSA) and Member State implementation efforts;



- Embedding governance-aware design principles that allow for contextual flexibility and policy learning;
- Developing a conceptual framework that integrates institutional instruments into a governance-aware model with embedded performance tracking, real-time feedback, and cross-sector adaptability;
- Offering a replicable methodology for developing capacity frameworks across adjacent domains (e.g. AI, digital innovation, critical infrastructure).

In addition, the NG-EUCCF can serve as a policy experimentation framework, supporting pilot initiatives, comparative performance assessments, and continuous recalibration through data-driven feedback mechanisms. Its modular design and governance-aware structure make it suitable for longitudinal workforce tracking and dynamic benchmarking across sectors and states.

### **6.3 Limitations**

As discussed in Chapter 3.4, this research is limited by its reliance on secondary data sources and the absence of direct empirical validation. Several Member State documents and international comparators were inaccessible or only partially available in English. Moreover, the lack of a unified EU-wide metric system for cybersecurity workforce development constrained the depth of benchmarking. These limitations do not undermine the framework's value but highlight the need for its empirical extension and institutional co-creation—areas further addressed under future research directions.

### **6.4 Future Research Directions**

The NG-EUCCF provides a strategic foundation, but its refinement and operationalisation require empirical expansion. Three future research tracks are proposed:

#### **1. Operationalisation and Pilot Validation**

To test the framework's implementation feasibility across diverse contexts, future research should:

- Conduct Member State pilots to assess component-level integration, policy alignment, and institutional readiness;
- Engage stakeholders from ECSO, ENISA, national agencies, training providers, and higher education institutions to co-develop operational roadmaps;
- Analyse variation in adoption pathways, particularly for SMEs, public administration, and critical infrastructure sectors.

These efforts would support calibration of the framework based on governance maturity, resource availability, and local constraints.

## **2. Data-Driven Governance and KPI Intelligence**

A significant contribution of this thesis is the identification of outcome-KPI misalignment and the absence of systemic performance tracking. To address this, future research should:

- Develop AI-enabled data analytics models to extract labour market insights, predict skills demand, and support real-time curriculum adaptation;
- Construct a multi-layered KPI framework combining quantitative indicators (e.g., role density, time-to-fill, retention rates) and qualitative signals (e.g., training impact, behavioural change);
- Design feedback loop mechanisms that link policy interventions to measured outcomes, allowing the EU to course-correct in near real time;
- Evaluate cross-sectoral feedback maturity in critical infrastructure, defence, and public sector cybersecurity domains.

Embedding AI-powered monitoring and continuous feedback into EU workforce policy would represent a step-change in governance agility.

## **3. Strategic Depth and Cyber Posture Extension**

Cyber capacity building is a resilience measure and a competitive and strategic imperative. Further research should explore:

- How human-centric capacity intersects with the EU's offensive cyber posture and strategic autonomy ambitions, especially in contesting persistent engagements below the threshold of war;

- The integration of cyber readiness into hybrid threat response, military-civil coordination, and crisis management systems at the EU level;
- The role of cyber competence in digital diplomacy and foreign policy, including support for third countries through capacity export models;
- Convergence with other EU digital agendas, such as artificial intelligence, data spaces, and quantum ecosystems—exploring how a cyber-skilled workforce becomes a foundational enabler across these domains.

## **6.5 Final Reflection**

Human capacity has become a strategic currency as Europe navigates a rapidly evolving and contested digital environment. Cybersecurity can no longer be addressed in isolation from economic strategy, innovation policy, or geopolitical posture.

The NG-EUCCF offers a roadmap for moving beyond fragmented initiatives toward a coordinated, outcome-driven, and future-resilient system of capacity building. Its success will depend on institutional alignment and sustained political will, cross-sector collaboration, and a collective commitment to resilience, inclusion, and leadership in the digital age.

This thesis offers one pathway forward.

## References

- [1] European Commission, Ed., *2030 Digital Decade: report on the state of the Digital Decade 2024*. Brussels: European Commission, 2024. doi: 10.2759/122170.
- [2] “Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).”
- [3] “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) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance).”
- [4] “Digital Decade - Policy programme | Shaping Europe’s digital future.” Accessed: Mar. 16, 2025. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/digital-decade-policy-programme>
- [5] W. Ramses A, “The EU’s Cybersecurity Strategy for the Digital Decade,” in *Oxford Encyclopedia of EU Law*, Oxford University Press, 2022. doi: 10.1093/law-oeul/e66.013.66.
- [6] “Worldwide Spending on Digital Transformation is Forecast to Reach Almost \$4 Trillion by 2027, According to New IDC Spending Guide,” IDC: The premier global market intelligence company. Accessed: Mar. 09, 2025. [Online]. Available: <https://www.idc.com/getdoc.jsp?containerId=prUS52305724>
- [7] P. H. Diamandis, *The Future Is Faster Than You Think: How Converging Technologies Are Transforming Business, Industries, and Our Lives*. in Exponential Technology Ser. New York: Simon & Schuster, 2020.
- [8] A. Carbonaro, J. Moss Breen, and F. Piccinini, “A new digital divide threatening resilience: exploring the need for educational, firm-based, and societal investments in ICT human capital,” *J. E-Learn. Knowl. Soc.*, pp. 66-73 Pages, Dec. 2022, doi: 10.20368/1971-8829/1135567.
- [9] “Employers Must Act as Cybersecurity Workforce Growth Stalls and Skills Gaps Widen.” Accessed: Mar. 09, 2025. [Online]. Available: <https://www.isc2.org/Insights/2024/09/Employers-Must-Act-Cybersecurity-Workforce-Growth-Stalls-as-Skills-Gaps-Widen>
- [10] B. Jerman Blažič, “Cybersecurity Skills in EU: New Educational Concept for Closing the Missing Workforce Gap,” in *Cybersecurity Threats with New Perspectives*, M. Sarfraz, Ed., IntechOpen, 2021. doi: 10.5772/intechopen.97094.
- [11] B. J. Blažič, “Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?,” *Educ. Inf. Technol.*, vol. 27, no. 3, pp. 3011–3036, Apr. 2022, doi: 10.1007/s10639-021-10704-y.
- [12] European Union Agency for Cybersecurity., *2024 report on the state of cybersecurity in the Union*. LU: Publications Office, 2024. Accessed: Mar. 12, 2025. [Online]. Available: <https://data.europa.eu/doi/10.2824/0401593>
- [13] “European Union Agency for Cybersecurity, A Trusted and Cyber Secure Europe: ENISA Strategy, Oct. 2024. [Online]. Available: <https://www.enisa.europa.eu>.”

- [14] “European Union Agency for Cybersecurity. 2024 Report on the State of Cybersecurity in the Union. Publications Office of the European Union, 2024. [Online]. Available: <https://data.europa.eu/doi/10.2824/0401593>.”
- [15] “World Economic Forum, Strategic Cybersecurity Talent Framework, White Paper, April 2024. Available: <https://www.weforum.org>.”
- [16] Europäische Kommission, Ed., *Cybersecurity: our digital anchor: a European perspective*. in EUR, no. 30276. Luxembourg: Publications Office of the European Union, 2020. doi: 10.2760/352218.
- [17] N. Vandezande, “Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor,” *Comput. Law Secur. Rev.*, vol. 52, p. 105890, Apr. 2024, doi: 10.1016/j.clsr.2023.105890.
- [18] “Regulation (EU) 2019/ 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)”.
- [19] “Digital Education Action Plan (2021-2027) - European Education Area.” Accessed: Mar. 16, 2025. [Online]. Available: <https://education.ec.europa.eu/focus-topics/digital-education/action-plan>
- [20] “Digital Decade DESI visualisation tool.” Accessed: Mar. 16, 2025. [Online]. Available: <https://digital-decade-desi.digital-strategy.ec.europa.eu/>
- [21] “European Commission, European Skills Agenda for Sustainable Competitiveness, Social Fairness and Resilience, Publications Office of the European Union, 2020.”
- [22] “Annexes to COM(2018)434 - Digital Europe programme for the period 2021-2027 - EU monitor.” Accessed: Apr. 06, 2025. [Online]. Available: [https://www.eumonitor.eu/9353000/1/j4nvirkkkr58fyw\\_j9vvik7m1c3gyxp/vkp1fqrgymox](https://www.eumonitor.eu/9353000/1/j4nvirkkkr58fyw_j9vvik7m1c3gyxp/vkp1fqrgymox)
- [23] “United Nations, Final Substantive Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, A/AC.290/2021/CRP.2.”
- [24] “NIST - NICE Framework Current Versions.” Accessed: Apr. 19, 2025. [Online]. Available: <https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-current-versions>
- [25] Z. M. King, D. S. Henshel, L. Flora, M. G. Cains, B. Hoffman, and C. Sample, “Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment,” *Front. Psychol.*, vol. 9, p. 39, Feb. 2018, doi: 10.3389/fpsyg.2018.00039.
- [26] “Digital Education Action Plan (2021-2027) - European Education Area.” Accessed: Apr. 19, 2025. [Online]. Available: <https://education.ec.europa.eu/focus-topics/digital-education/action-plan>
- [27] “European Commission, Flash Eurobarometer 547 – Cyberskills – Eurobarometer Data Annex April-May 2024, Directorate-General for Communications Networks, Content and Technology, Apr.–May 2024. Available: <https://ec.europa.eu>.”
- [28] “Your roadmap for finding the right cybersecurity job,” Cybersecurity Guide. Accessed: Apr. 19, 2025. [Online]. Available: <https://cybersecurityguide.org/resources/cybersecurity-jobs/>
- [29] “C. Osborne and S. Morgan, 2023 Cybersecurity Jobs Report. Northport, NY: Cybersecurity Ventures, 2023. [Online]. Available: <https://cybersecurityventures.com>.”

- [30] Ch, “MD Institute for Management Development, IMD World Digital Competitiveness Ranking 2024, IMD World Competitiveness Center, Nov. 2024. Available: <https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/>.”
- [31] “I. Khan, Whitepaper: The Future Readiness Score™ (FRS), Futuracy LLC, New York, Aug. 2019. Available: <https://www.iankhan.com/wp-content/uploads/2019/08/The-Future-Readiness-Score-Whitepaper.pdf>.”
- [32] G. Clark, “FUTURE READY: The Path to Growth”.
- [33] S. Muench, E. Stoermer, K. Jensen, T. Asikainen, M. Salvi, and F. Scapoo, *Towards a green & digital future: key requirements for successful twin transitions in the European Union*. in EUR, no. 31075. Luxembourg: Publications Office of the European Union, 2022. doi: 10.2760/977331.
- [34] “EU decade of skills: Building a future-ready labor market,” POLITICO. Accessed: Apr. 06, 2025. [Online]. Available: <https://www.politico.eu/sponsored-content/eu-decade-of-skills-building-a-future-ready-labor-market/>
- [35] “European Year of Skills.” Accessed: Apr. 06, 2025. [Online]. Available: [https://year-of-skills.europa.eu/index\\_en](https://year-of-skills.europa.eu/index_en)
- [36] “European Commission, The Future of European Competitiveness: A Competitiveness Strategy for Europe, European Commission, Brussels, 2024.”
- [37] European Union Agency for Cybersecurity., *ECSF, European cybersecurity skills framework*. LU: Publications Office, 2022. Accessed: Mar. 17, 2025. [Online]. Available: <https://data.europa.eu/doi/10.2824/859537>
- [38] European Union Agency for Cybersecurity, Ed., *Cyber Europe 2024: after action report*. Luxembourg: Publications Office, 2024. doi: 10.2824/3428659.
- [39] P. Rathod, N. Polemi, M. Lehto, K. Kioskli, J. Wessels, and R. Lugo, “Leveraging the European Cybersecurity Skills Framework(ECSF) in EU Innovation Projects: Workforce Development Through Skilling, Upskilling, and Reskilling,” in *2024 IEEE Global Engineering Education Conference (EDUCON)*, Kos Island, Greece: IEEE, May 2024, pp. 1–9. doi: 10.1109/EDUCON60312.2024.10578846.
- [40] European, “The Cybersecurity Skills Academy.” doi: 10.1163/2210-7975\_HRD-4679-0058.
- [41] S. Autolitano, “A Europe Fit for the Digital Age: The Quest for Cybersecurity Unpacked,” IAI Istituto Affari Internazionali. Accessed: Mar. 11, 2025. [Online]. Available: <https://www.iai.it/en/pubblicazioni/c05/europe-fit-digital-age-quest-cybersecurity-unpacked>
- [42] “Cyber Skills Academy | Digital Skills and Jobs Platform.” Accessed: Apr. 19, 2025. [Online]. Available: <https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy>
- [43] DigitalEU, *European Skills Agenda*, (Apr. 18, 2023). Accessed: Apr. 19, 2025. [Online Video]. Available: [https://www.youtube.com/watch?v=inx\\_RocApgU](https://www.youtube.com/watch?v=inx_RocApgU)
- [44] “Seventh Progress Report on the implementation of the EU Security Union Strategy.” Accessed: Mar. 08, 2025. [Online]. Available: [https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52024DC0198\(01\)&qid=1741456295606](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52024DC0198(01)&qid=1741456295606)
- [45] “Cybersecurity policies | ENISA.” Accessed: Apr. 09, 2025. [Online]. Available: <https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies>
- [46] “communication-from-the-commission-to-the-european-parliament-and-the-council.” doi: 10.1163/2210-7975\_HRD-4679-0058.

- [47] “NIS2 Directive: new rules on cybersecurity of network and information systems | Shaping Europe’s digital future.” Accessed: Apr. 19, 2025. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>
- [48] “Annexes to COM(2018)434 - Digital Europe programme for the period 2021-2027 - EU monitor.” Accessed: Apr. 06, 2025. [Online]. Available: [https://www.eumonitor.eu/9353000/1/j4nvirkkkkr58fyw\\_j9vvik7m1c3gyxp/vkp1fqrqymox](https://www.eumonitor.eu/9353000/1/j4nvirkkkkr58fyw_j9vvik7m1c3gyxp/vkp1fqrqymox)
- [49] “DS4Skills - Data Space For Skills,” DS4Skills. Accessed: Apr. 19, 2025. [Online]. Available: <https://www.skillsdataspace.eu/>
- [50] “European Commission, European Skills Agenda for Sustainable Competitiveness, Social Fairness and Resilience, Publications Office of the European Union, 2020.”
- [51] “The EU Cyber Solidarity Act | Shaping Europe’s digital future.” Accessed: Apr. 19, 2025. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity>
- [52] “The EU Cybersecurity Certification Framework | Shaping Europe’s digital future.” Accessed: Apr. 19, 2025. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework>
- [53] “Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union”.
- [54] “Cyber Defence: EU boosts action against cyber threats,” European Commission - European Commission. Accessed: Apr. 19, 2025. [Online]. Available: [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_22\\_6642](https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6642)
- [55] “European Cybersecurity Competence Centre and Network.” Accessed: Apr. 19, 2025. [Online]. Available: [https://cybersecurity-centre.europa.eu/index\\_en](https://cybersecurity-centre.europa.eu/index_en)
- [56] “EU CyCLONe | ENISA.” Accessed: Apr. 19, 2025. [Online]. Available: <https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/eu-cyclone>
- [57] “Towards Digital Decade targets for Europe.” Accessed: Apr. 19, 2025. [Online]. Available: [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Towards\\_Digital\\_Decade\\_targets\\_for\\_Europe](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Towards_Digital_Decade_targets_for_Europe)
- [58] “New perspectives on measuring cybersecurity,” OECD Digital Economy Papers 366, Jun. 2024. doi: 10.1787/b1e31997-en.
- [59] “A-Eurelectric-snapshot-of-Cybersecurity-2024-11-18-FINAL.pdf.” Accessed: May 18, 2025. [Online]. Available: <https://www.eurelectric.org/wp-content/uploads/2024/11/A-Eurelectric-snapshot-of-Cybersecurity-2024-11-18-FINAL.pdf>
- [60] “Europe’s digital decade: 2030 targets | European Commission.” Accessed: Apr. 20, 2025. [Online]. Available: [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en)
- [61] “The Digital Economy and Society Index (DESI) | Shaping Europe’s digital future.” Accessed: Apr. 19, 2025. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/desi>
- [62] European Union Agency for Cybersecurity., *Addressing the EU cybersecurity skills shortage and gap through higher education*. LU: Publications Office, 2021. Accessed: Nov. 03, 2024. [Online]. Available: <https://data.europa.eu/doi/10.2824/033355>

- [63] European Commission. Directorate General for Communications Networks, Content and Technology. and Ipsos European Public Affairs., *Cyberskills: Eurobarometer report*. LU: Publications Office, 2024. Accessed: Apr. 13, 2025. [Online]. Available: <https://data.europa.eu/doi/10.2759/221137>
- [64] E. ENISA, “ENISA CyberHEAD,” Accessed: Apr. 03, 2025. [Online]. Available: <https://videos.enisa.europa.eu/w/nAGdWjVKXNQ8sMFpZbGeni>
- [65] “Summary-report\_Cybersecurity-Skills-Needs-Analysis-1.”
- [66] “Digital Skills Assessment Tool.” Accessed: Apr. 06, 2025. [Online]. Available: <https://europa.eu/europass/digitalskills/screen/questionnaire/generic>
- [67] “International Telecommunication Union, Global Cybersecurity Index 2024, ITU Publications, Geneva, 2024”.
- [68] “NCSI :: Ranking.” Accessed: Apr. 06, 2025. [Online]. Available: <https://ncsi.ega.ee/ncsi-index/>
- [69] European Network and Information Security Agency., *National capabilities assessment framework*. LU: Publications Office, 2020. Accessed: Apr. 06, 2025. [Online]. Available: <https://data.europa.eu/doi/10.2824/590072>
- [70] “Ministry of Economic Affairs and Communications and Estonian Information System Authority, Cybersecurity Strategy 2024–2030: Cyber-Conscious Estonia, Tallinn, Estonia, 2024”.
- [71] “Finland’s Cyber Security Strategy 2024–2035, Publications of the Prime Minister’s Office 2024”.
- [72] “Agence nationale de la sécurité des systèmes d’information (ANSSI), Stratégie nationale pour la sécurité du numérique – Dossier de presse, ANSSI, Paris, France, 18 Feb. 2021.”
- [73] European Union Agency for Cybersecurity., *Cybersecurity education maturity assessment*. LU: Publications Office, 2024. Accessed: Mar. 23, 2025. [Online]. Available: <https://data.europa.eu/doi/10.2824/3832>
- [74] “Skills forecast | CEDEFOP.” Accessed: Apr. 14, 2025. [Online]. Available: <https://www.cedefop.europa.eu/en/projects/skills-forecast>
- [75] J. Fraillon, “J. Fraillon, ‘An International Perspective on Digital Literacy,’ International Association for the Evaluation of Educational Achievement (IEA), 2024”.
- [76] European Commission. Directorate General for Communications Networks, Content and Technology. and Ipsos European Public Affairs., *Cyberskills: Eurobarometer report*. LU: Publications Office, 2024. Accessed: Mar. 24, 2025. [Online]. Available: <https://data.europa.eu/doi/10.2759/221137>
- [77] B. J. Blažič, “The cybersecurity labour shortage in Europe: Moving to a new concept for education and training,” *Technol. Soc.*, vol. 67, p. 101769, Nov. 2021, doi: 10.1016/j.techsoc.2021.101769.
- [78] “2024-cybersecurity-skills-gap-report.pdf.” Accessed: May 18, 2025. [Online]. Available: <https://www.fortinet.com/content/dam/fortinet/assets/reports/2024-cybersecurity-skills-gap-report.pdf>.”
- [79] “2024-cybersecurity-skills-gap-report.pdf.” Accessed: May 18, 2025. [Online]. Available: <https://www.fortinet.com/content/dam/fortinet/assets/reports/2024-cybersecurity-skills-gap-report.pdf>
- [80] “European Commission, Digital Economy and Society Index (DESI) 2022 – Human Capital Thematic Chapters, Publications Office of the European Union, 2022.”
- [81] “European Commission, Political Guidelines for the Next Commission (2019–2024), European Commission, Brussels, 2019.”



- [82] European Union Agency for Cybersecurity., *ENISA threat landscape 2024: July 2023 to June 2024*. LU: Publications Office, 2024. Accessed: Apr. 14, 2025. [Online]. Available: <https://data.europa.eu/doi/10.2824/0710888>
- [83] OECD, *Building a Skilled Cyber Security Workforce in Europe: Insights from France, Germany and Poland*. in OECD Skills Studies. OECD, 2024. doi: 10.1787/3673cd60-en.
- [84] B. J. Blažič, “The cybersecurity labour shortage in Europe: Moving to a new concept for education and training,” *Technol. Soc.*, vol. 67, p. 101769, Nov. 2021, doi: 10.1016/j.techsoc.2021.101769.
- [85] “National Cyber Power Index 2022 | The Belfer Center for Science and International Affairs.” Accessed: Apr. 20, 2025. [Online]. Available: <https://www.belfercenter.org/publication/national-cyber-power-index-2022>
- [86] “Global Cybersecurity Index,” ITU. Accessed: Apr. 20, 2025. [Online]. Available: <https://www.itu.int:443/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx>
- [87] J. Hajny, S. Ricci, E. Piesarskas, O. Levillain, L. Galletta, and R. De Nicola, “Framework, Tools and Good Practices for Cybersecurity Curricula,” *IEEE Access*, vol. 9, pp. 94723–94747, 2021, doi: 10.1109/ACCESS.2021.3093952.
- [88] G. Austin, Ed., *Cyber Security Education: Principles and Policies*, 1st ed. Names: Austin, Greg, 1951- editor. Title: Cyber-security education : principles and policies / edited by Greg Austin. Description: London ; New York : Routledge/Taylor & Francis Group, 2021. | Series: Routledge studies in conflict, security and technology: Routledge, 2020. doi: 10.4324/9780367822576.
- [89] P. Rathod *et al.*, “P. Rathod et al., ‘Cybersecurity Practical Skills Gaps in Europe: Market Demand and Analyse,’ CyberSecPro Project Deliverable D2.1, Version 1.0, May 2023. [Online]. Available: <https://www.cybersecpro.eu/>”.
- [90] M. Ismail *et al.*, “Cybersecurity activities for education and curriculum design: A survey,” *Comput. Hum. Behav. Rep.*, vol. 16, p. 100501, Dec. 2024, doi: 10.1016/j.chbr.2024.100501.
- [91] B. J. Blažič, “Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?,” *Educ. Inf. Technol.*, vol. 27, no. 3, pp. 3011–3036, Apr. 2022, doi: 10.1007/s10639-021-10704-y.
- [92] S. Ricci *et al.*, “PESTLE Analysis of Cybersecurity Education,” in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, Vienna Austria: ACM, Aug. 2021, pp. 1–8. doi: 10.1145/3465481.3469184.
- [93] E. W. Ecsó, “European Cybersecurity Education & Professional Training: Minimum Reference Curriculum”.
- [94] S. S. Costigan, “Shifting the Boundaries: Conceptual and Practical Challenges of Cybersecurity Education, Definitions and Expectations”.
- [95] “National Security Agency/Central Security Service > Academics > Centers of Academic Excellence > Cyber Operations.” Accessed: Apr. 13, 2025. [Online]. Available: <https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/Cyber-Operations/>
- [96] “The White House, National Cybersecurity Strategy, The White House, Washington, DC, Mar. 2023.”
- [97] “NICE Workforce Framework for Cybersecurity (NICE Framework) | NICCS.” Accessed: Apr. 13, 2025. [Online]. Available: <https://niccs.cisa.gov/workforce-development/nice-framework>

- [98] Lightcast, “The Cybersecurity Gap — White House Report,” Lightcast. Accessed: Apr. 13, 2025. [Online]. Available: <https://lightcast.io/resources/research/quarterly-cybersecurity-talent-report-june-24>
- [99] “China’s shortfall in cybersecurity talent will exceed 3 million by 2027: report,” South China Morning Post. Accessed: Apr. 13, 2025. [Online]. Available: <https://www.scmp.com/tech/tech-trends/article/3191781/chinas-demand-cybersecurity-talent-will-exceed-supply-over-3>
- [100] “M. Raud, National Cyber Security Organisation in China, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Tallinn, Estonia, 2016.”
- [101] “D. Cary, China’s CyberAI Talent Pipeline, Center for Security and Emerging Technology (CSET), Washington, DC, July 2021.”
- [102] M. M. Kolton, “Interpreting China’s Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence”.
- [103] K. Pynnöniemi and M. J. Kari, “Russia’s New Information Security Doctrine: Guarding a besieged cyber fortress”.
- [104] “Deciphering Russia’s ‘Sovereign Internet Law’ | DGAP.” Accessed: Apr. 20, 2025. [Online]. Available: <https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law>
- [105] U. Drazdovich, “A Thesis in the Field of International Relations”.
- [106] “Russian Government, Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space (2011), 2011 | National Security Archive.” Accessed: Apr. 20, 2025. [Online]. Available: <https://nsarchive.gwu.edu/document/17098-russian-government-conceptual-views-regarding>
- [107] A. Greenberg, “Gamaredon: The Turncoat Spies Relentlessly Hacking Ukraine,” *Wired*. Accessed: Apr. 20, 2025. [Online]. Available: <https://www.wired.com/story/gamaredon-turncoat-spies-hacking-ukraine/>
- [108] A. S. Borogan Irina, “Russian Cyberwarfare: Unpacking the Kremlin’s Capabilities,” CEPA. Accessed: Apr. 20, 2025. [Online]. Available: <https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/>
- [109] M. Bodner, “Russian Military Launches Cybertraining Program for Youth,” *The Moscow Times*. Accessed: Apr. 13, 2025. [Online]. Available: <https://www.themoscowtimes.com/2015/09/01/russian-military-launches-cybertraining-program-for-youth-a49276>
- [110] *Russia’s Strategy in Cyberspace*. Riga [Latvia]: NATO Strategic Communications Centre of Excellence, 2021.
- [111] B. Murphy, “2022 White Paper on the Live-Fire Capabilities of Cybersecurity Talents: Attack and Defense Live-Fire Capability Edition”.
- [112] A. Lowry, “Russia’s Digital Economy Program: An Effective Strategy for Digital Transformation?,” in *The Palgrave Handbook of Digital Russia Studies*, D. Gritsenko, M. Wijermars, and M. Kopotev, Eds., Cham: Springer International Publishing, 2021, pp. 53–75. doi: 10.1007/978-3-030-42855-6\_4.
- [113] D. Gritsenko, M. Wijermars, and M. Kopotev, Eds., *The Palgrave Handbook of Digital Russia Studies*. Cham: Springer International Publishing, 2021. doi: 10.1007/978-3-030-42855-6.
- [114] “Russia’s National Security Strategy 2021: the Era of ‘Information Confrontation,’” Institut Montaigne. Accessed: Apr. 20, 2025. [Online]. Available: <https://www.institutmontaigne.org/en/expressions/russias-national-security-strategy-2021-era-information-confrontation>

- [115] G. Wilde and J. Sherman, “No Water’s Edge: Russia’s Information War and Regime Security”.
- [116] J. Hakala and J. Melnychuk, *Russia’s Strategy in Cyberspace. NATO Strategic Communications Centre of Excellence, Riga, Latvia, Jun. 2021. ISBN: 978-9934-564-90-1. [Online]. Available: <https://stratcomcoe.org>*. Riga [Latvia]: NATO Strategic Communications Centre of Excellence, 2021.
- [117] K. Teh, V. Suhendra, S. C. Lim, and A. Roychoudhury, “Singapore’s cybersecurity ecosystem,” *Commun. ACM*, vol. 63, no. 4, pp. 55–57, Mar. 2020, doi: 10.1145/3378552.
- [118] Cyber Security Agency of Singapore, *The Singapore Cybersecurity Strategy 2021, Singapore: Cyber Security Agency of Singapore, 2021*. 2021.
- [119] “Singapore’s Cybersecurity Strategy 2016,” Cyber Security Agency of Singapore. Accessed: Apr. 20, 2025. [Online]. Available: <https://www.csa.gov.sg/resources/publications/singapore-s-cybersecurity-strategy-2016/>
- [120] “Special educational needs support at Institutes of Higher Learning | MOE.” Accessed: Apr. 20, 2025. [Online]. Available: <https://www.moe.gov.sg/special-educational-needs/school-support/ihl>
- [121] “SkillsFuture Singapore | Homepage.” Accessed: Apr. 20, 2025. [Online]. Available: <https://www.skillsfuture.gov.sg/>
- [122] “SG Cyber Youth,” Cyber Security Agency of Singapore. Accessed: Apr. 20, 2025. [Online]. Available: <https://www.csa.gov.sg/our-programmes/talent-and-skills-development/sg-cyber-talent/sg-cyber-youth/>
- [123] “CSA Establishes CyberSG R&D Programme Office with Four Year Funding of S\$62 Million to Drive Research and Development to Build Up Cybersecurity Capabilities in Singapore,” Cyber Security Agency of Singapore. Accessed: Apr. 20, 2025. [Online]. Available: <https://www.csa.gov.sg/news-events/press-releases/csa-establishes-cybersg-r-d-programme-office-with-four-year-funding-of-62-million-to-drive-research-and-development-to-build-up-cybersecurity-capabilities-in-singapore/>
- [124] “South Korea’s 2024 Cyber Strategy: A Primer | Strategic Technologies Blog | CSIS.” Accessed: Apr. 13, 2025. [Online]. Available: <https://www.csis.org/blogs/strategic-technologies-blog/south-koreas-2024-cyber-strategy-primer>
- [125] “National Security Office, National Cybersecurity Strategy, Republic of Korea, Apr. 2019. [Online]. Available: [https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National\\_Strategies\\_Repository/National%20Cybersecurity%20Strategy\\_South%20Korea.pdf](https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf).”
- [126] S. J. Kim, “ROK’s New National Cybersecurity Strategy and Its Implications”.
- [127] “‘France 2030’ Investment Plan – Policies,” IEA. Accessed: Apr. 20, 2025. [Online]. Available: <https://www.iea.org/policies/14279-france-2030-investment-plan>
- [128] J. Drmola, F. Kasl, P. Loutocký, M. Mareš, T. Pitner, and J. Vostoupal, “The Matter of Cybersecurity Expert Workforce Scarcity in the Czech Republic and Its Alleviation Through the Proposed Qualifications Framework,” in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, Vienna Austria: ACM, Aug. 2021, pp. 1–6. doi: 10.1145/3465481.3469186.
- [129] M. P. Fischerkeller and R. J. Harknett, “Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics and Escalation”.

- [130] European Union Agency for Cybersecurity., *Foresight cybersecurity threats for 2030: update : extended report*. LU: Publications Office, 2024. Accessed: Mar. 23, 2025. [Online]. Available: <https://data.europa.eu/doi/10.2824/349493>
- [131] “Long-term competitiveness of the EU: looking beyond 2030.”
- [132] “Cybersecurity Skills Needs Analysis Summary Report,” CyberHubs. Accessed: Apr. 20, 2025. [Online]. Available: <https://cyberhubs.eu/resource/cybersecurity-skills-needs-analysis-summary-report/>
- [133] “Blueprint,” REWIRE. Accessed: Apr. 20, 2025. [Online]. Available: <https://rewireproject.eu/blueprint/>
- [134] “Kościuszko Institute, Skills and Cyber Hygiene: Support and Development of Digital Competences – Policy Brief, Ministry of Digital Affairs, Kraków, Poland, 2024.”
- [135] “B. Lorenz et al., Cybersecurity Skills Needs Analysis Report – Estonia. CyberHubs Project, Deliverable D2.1, Version 1.0, Oct. 2024. [Online]. Available: <https://cyberhubs.eu/resource/cybersecurity-skills-needs-analysis-in-estonia/>.”
- [136] “ENISA, Crosswalk Between ESCO and ECSF, ENISA, Sept. 2024. Available: <https://www.enisa.europa.eu/>.”
- [137] M. University, “PUBLICATIONS,” CyQUAL Czech National Qualifications Framework in Cybersecurity. Accessed: Apr. 13, 2025. [Online]. Available: <https://www.cyqual.cz/publications>
- [138] “Why closing the cyber skills gap requires a collaborative approach,” World Economic Forum. Accessed: Mar. 26, 2025. [Online]. Available: <https://www.weforum.org/stories/2024/07/why-closing-the-cyber-skills-gap-requires-a-collaborative-approach/>
- [139] “World Economic Forum, Strategic Cybersecurity Talent Framework, White Paper, April 2024. Available: <https://www.weforum.org/>.”
- [140] “Cybersecurity for SMEs - Challenges and Recommendations | ENISA.” Accessed: Apr. 20, 2025. [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes>
- [141] “SME definition - European Commission.” Accessed: Apr. 20, 2025. [Online]. Available: [https://single-market-economy.ec.europa.eu/smes/sme-fundamentals/sme-definition\\_en](https://single-market-economy.ec.europa.eu/smes/sme-fundamentals/sme-definition_en)
- [142] “Growing focus on digital skills,” Epthinktank. Accessed: Apr. 13, 2025. [Online]. Available: <https://epthinktank.eu/2025/03/04/growing-focus-on-digital-skills/>
- [143] “Home - Women4Cyber.” Accessed: Apr. 20, 2025. [Online]. Available: <https://women4cyber.eu/>
- [144] European Union Agency for Network and Information Security., *Cybersecurity skills development in the EU: the certification of cybersecurity degrees and ENISA’s Higher Education Database*. LU: Publications Office, 2019. Accessed: Mar. 26, 2025. [Online]. Available: <https://data.europa.eu/doi/10.2824/525144>
- [145] “Special report 05/2022: Cybersecurity of EU institutions, bodies and agencies : Level of preparedness overall not commensurate with the threats,” European Court of Auditors. Accessed: Apr. 20, 2025. [Online]. Available: [http://www.eca.europa.eu/en/publications/sr22\\_05](http://www.eca.europa.eu/en/publications/sr22_05)
- [146] “European Cybersecurity Skills Academy, Cyber Skills Academy – Digital Skills and Jobs Platform, ECSA, 2024.”
- [147] “T. De Zan, Mitigating the Cyber Security Skills Shortage: The Influence of National Skills Competitions on Cyber Security Interest, Ph.D. dissertation, Univ. of Oxford, Oxford, U.K., 2021.”

- [148] C. E. Aanonsen, “Digital Borders, Global Ties: The EU’s Dual Quest for Cybersecurity and Digital Sovereignty”.
- [149] “Upping the Ante on EU Cyber Defence: What Should we Expect from our Capitals? :: EU Cyber Direct,” Horizon. Accessed: Apr. 20, 2025. [Online]. Available: <https://eucyberdirect.eu/blog/upping-the-ante-on-eu-cyber-defence-what-should-we-expect-from-our-capitals>
- [150] “A language of power? | European Union Institute for Security Studies.” Accessed: Apr. 20, 2025. [Online]. Available: <https://www.iss.europa.eu/publications/chaillot-papers/language-power>

## **Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis<sup>1</sup>**

I Csaba Virág

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Closing the Cyber Skills Gap: A Framework for Strengthening EU Competitiveness and Digital Resilience”, supervised by Rain Ottis
  - 1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
  - 1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

20.04.2025

---

<sup>1</sup> The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

## Appendix 2 - Tools Used

The following digital tools have been used to support the writing and editing process of this thesis:

- Grammarly Premium for grammar, punctuation and clarity
- ChatGPT, Gemini, Copilot, Perplexity for guidance on structure, coherence and ideation.
- Litmaps, Elicit, Research Rabbit for researching literature
- Zotero for citation management
- Google Translate, DeepL for translation
- Microsoft Word for drafting and formatting.

These tools were used in a supportive capacity only. No content was generated by AI without author validation. All academic arguments, interpretations, and contributions are my own.


## Appendix 3 – Digital Competence Test Samples

The following screenshots showcase the depth and quality of the digital skills assessment proposed to assess ICT proficiency. As is visible, the questions vary in depth of digital literacy and user-level knowledge, and their usefulness in tracking EU level digital competencies and skills are questionable.

The screenshot shows a web browser window with the URL `europa.eu/europass/digitalskills/screen/questionnaire/generic`. The page header includes the European Union flag and the text "europa.eu/europass/digitalskills/screen/questionnaire/generic". Below the header, there is a logo for "europass" and the text "Test your digital skills". A progress bar is visible, showing a green segment followed by a grey segment. A "Help" button is located on the right side of the progress bar. The main content area contains a question: "Which of the following is a program to delete and clean the computer?" with the instruction "Choose one answer only". The question is followed by four radio button options: "SnapChat", "Keylogger", "CCleaner", and "Dashlane". A timer in the top right corner shows "0 : 57" with "mins" and "secs" labels. At the bottom of the question area, there is a button labeled "I don't know" with a right-pointing arrow. To the right of the question area, there is a "Next" button with a right-pointing arrow. At the bottom left of the page, there is a link labeled "Exit" with a small "x" icon.

europa.eu/europass/digitalskills/screen/questionnaire/generic

bsite of the European Union How do you know? ▾

 **europass**  
Test your digital skills

0 : 57  
mins secs

Help

Which of the following is a program to delete and clean the computer?  
Choose one answer only

☐ SnapChat

☐ Keylogger

☐ CCleaner

☐ Dashlane

I don't know ►►


Next ►

✕ [Exit](#)



europa.eu/europass/digitalskills/screen/questionnaire/generic

ite of the European Union How do you know? ▾

 **europass**  
Test your digital skills

Help

**In WhatsApp, how will the text be displayed when writing '\_text\_'?**  
Choose one answer only

0 : 37  
mins secs

☐ In italics  
☐ In bold  
☐ Strikethrough  
☒ Unchanged


I don't know ►►

Next >

× [Exit](#)

europa.eu/europass/digitalskills/screen/questionnaire/generic

of the European Union How do you know? ▾

 **europass**  
Test your digital skills

Help

**The main advantages of dynamic and interactive presentations are:**  
Choose one answer only

1 : 02  
mins secs

☐ They allow the use of various audiovisual high-impact resources (images, gifs, audios, videos, etc.) which maintain expectation and arouse emotions and feelings in the spectator.  
☐ The incorporation of attractive images, even if they are not related to the text.  
☐ They can help the presenter to come across as professional.  
☐ All of the above options are correct.

I don't know ►►

Next >

× [Exit](#)



## europass

### Test your digital skills

Help

SMS communication is unsafe by default.

0 : 49  
mins secs

- ☐ True
- ☐ False

I don't know ►►

All changes have been saved

Next >

× [Exit](#)

Which of the following statements concerning the digital divide is correct?

Choose one or more answers

1 : 20  
mins secs

- ☐ There is no digital divide between sexes.
- ☐ It is not possible to accurately measure the size of the digital divide.
- ☐ It is associated with low purchasing power, and with a lack of economic development.
- ☐ One of its consequences is digital illiteracy.

I don't know ►►

Next >

[< Back](#)

Exit

# Learning roadmap

## Learning goals

Select a learning goal to see the corresponding learning roadmap. You can always go back and check out another one!



### Working Remotely

Working remotely requires a set of digital skills for regular tasks on your computer. One needs to be familiar with a range of software and applications in order to work successfully away from the physical work place.

You are a master!



### Participating and engaging with society online

Participating and engaging with society in the digital era include interacting with other people through online communities and social networks. Active participation also requires a range of skills for using digital services, from e-banking, to online shopping and voting.

You are a master!



## Why test your digital skills?

Digital skills are important for working, studying, accessing services and buying products, or keeping in touch with friends and family. Take this test to learn more about your digital skills, discover what your level is and take the next step to improve them.

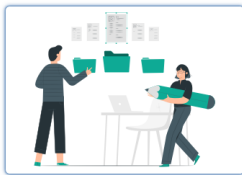


## Which competence areas will be tested?

### Information and data literacy

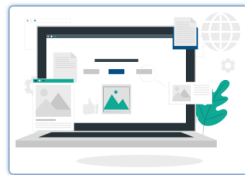
< You will be tested on the set of skills needed to search for, access and navigate between different types of digital content (files, websites, etc.). This also includes being able to compare different sources of information and understand which ones are reliable. The ability to store, manage, and organise folders and various types of files is part of this competence area as well. >

## What else can you do ?



Record your digital skills

After completing the test, you will be able to add your digital skills to an online profile or a CV. Don't miss the chance to highlight your digital skills!



Receive course suggestions

Get matching suggestions of courses and learning opportunities based on your test results and take your digital skills to the next level! (Available soon)



Discover your learning roadmap

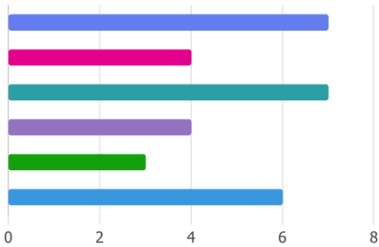
Explore learning paths that help you understand which digital skills you should focus on and guide you on how to improve them to reach your goal.

# Appendix 4 – Validation Survey Questions & Responses

1. What is your primary role?

[More details](#)

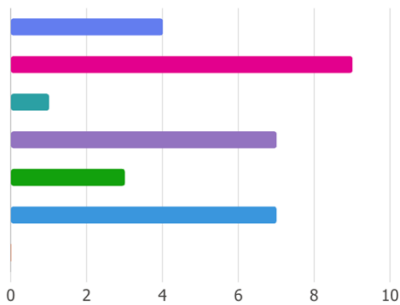
Policy-maker	7
CERT/SOC Lead	4
C-level Exec	7
Academic	4
Industry member	3
Other	6



2. Organisation type

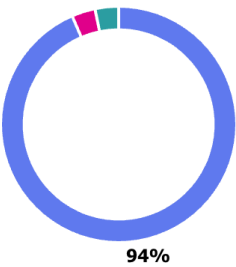
[More details](#)

Public	4
Private sector (Large enterprise)	9
Private sector (SME)	1
Civil Society/NGO	7
Academia	3
EU Institution or Agency	7
Other	0



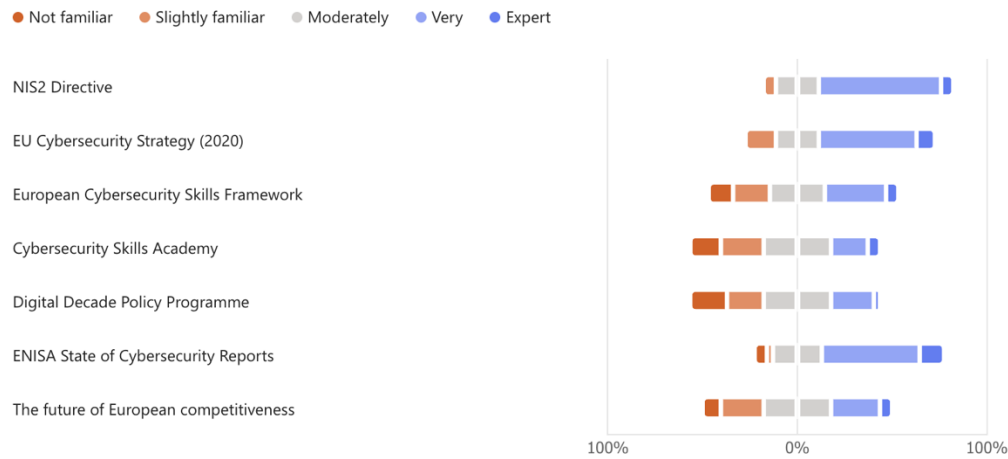
3. Where is your organisation headquartered?

EU	29
Europe (but not EU)	1
International	1
Other	0



4. How familiar are you with the following EU initiatives?

[More details](#)



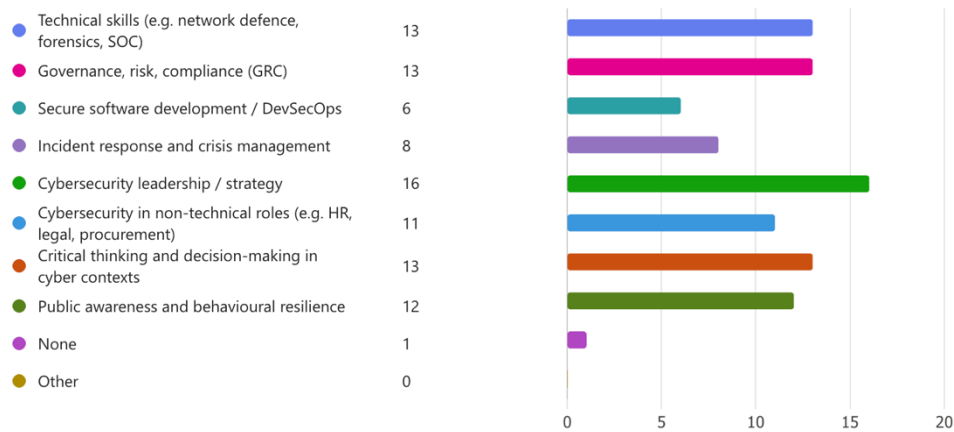
5. How many years of professional experience do you have in the field of cybersecurity or digital policy?

[More details](#)



6. In your experience, where do you observe the most significant skills shortages in cybersecurity?  
(Select up to 3)

[More details](#)



7. Do you believe current EU and national initiatives address non-technical cybersecurity competencies (e.g. behaviour, policy, leadership) adequately? [More details](#)

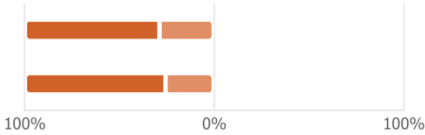


8. To what extent do you agree with the following statement: [More details](#)

Strongly agree Agree Disagree Strongly disagree Neutral

Cybersecurity competence should be systematically embedded and measured across non-cyber domains—such as education,...

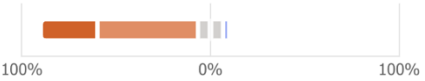
A nation or institution cannot be considered future-ready without a resilient, cross-sectoral foundation of cybersecurity competence.



9. How strongly do you agree with this statement: Current cybersecurity education and training initiatives are overly concentrated on technical roles and do not sufficiently support other vital sectors and professions essential for resilience? [More details](#)

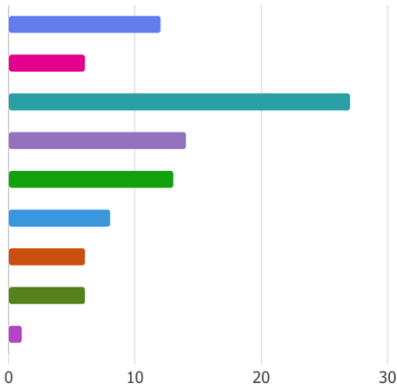
Strongly agree Agree Neutral Disagree Strongly disagree

Option

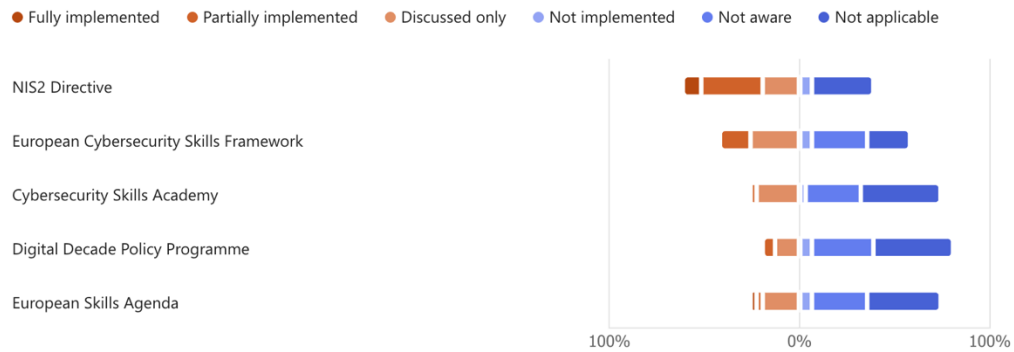


10. In your view, what are the most critical areas for investment to close the cybersecurity skills gap in the EU? (Rank the following, or select top 3) [More details](#)

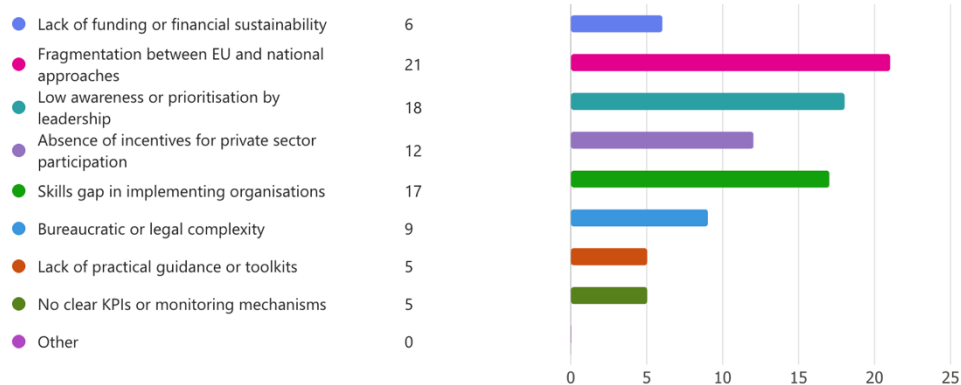
University and VET curriculum development	12
Synthetic and practical environments (Digital twins, cyber ranges, etc)	6
Upskilling/reskilling initiatives for mid-career professionals	27
Incentives for industry–education collaboration	14
Public awareness and behavioural programmes	13
Leadership training for cyber crisis management	8
EU certification and standardisation of skills	6
Incentives for EU cyber initiatives	6
Other	1



11. To what extent are the following EU-level cybersecurity strategies, frameworks, or initiatives reflected in your organisation or country's activities? [More details](#)



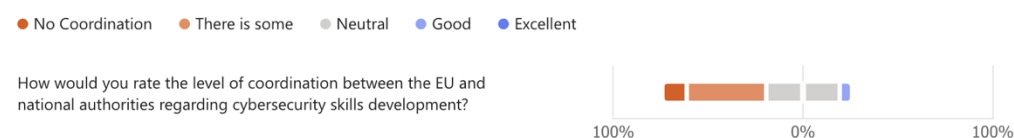
12. What are the main challenges preventing effective implementation of EU-level cybersecurity capacity-building strategies in your context? (Select up to 3) [More details](#)



13. How is the European Cybersecurity Skills Framework (ECSF) used in your organisation or sector? [More details](#)



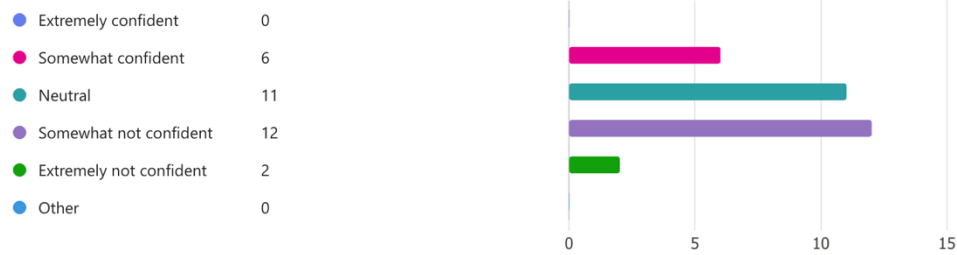
14. 3.4 Feedback on Coordination [More details](#)





15. How confident are you that current EU policy instruments (NIS2, Digital Decade, ECSF, etc.) will significantly reduce the cybersecurity skills gap by 2030?

[More details](#)

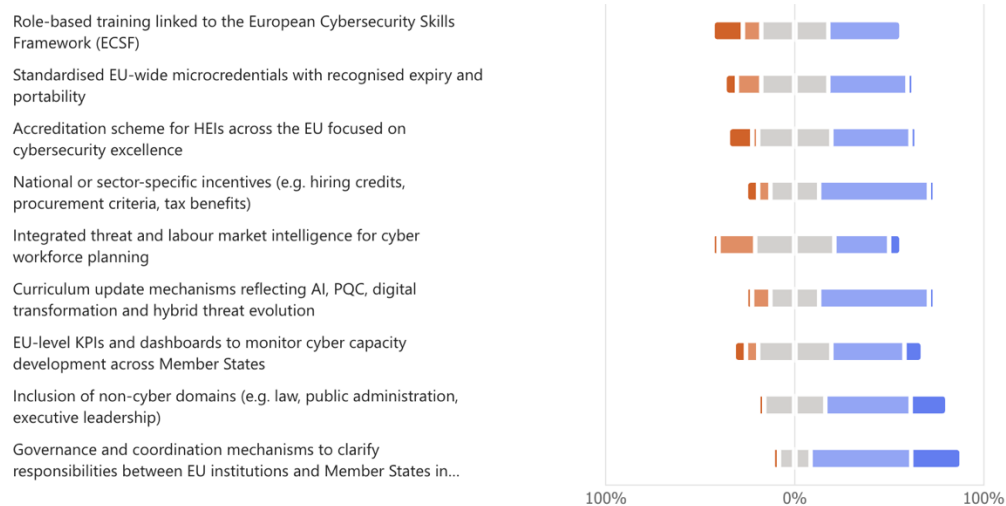


16. Based on the short description above, how relevant are the following proposed components of the NG-EUCCF to your organisation or context?

[More details](#)

(Rate each: Not Relevant / Somewhat Relevant / Relevant / Highly Relevant / Critically Important)

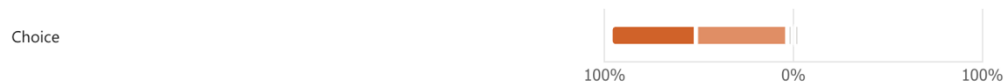
● Not Relevant ● Low Relevance ● Moderate Relevance ● High Relevance ● Critically Important



17. To what extent do you agree: Improved EU-wide coordination and clearly defined roles between national and EU actors would accelerate progress in building cyber capacity.

[More details](#)

● Strongly agree ● Agree ● Neutral ● Disagree ● Strongly disagree



18. How valuable is having EU-level standardised cybersecurity role profiles and competence models?

[More details](#)

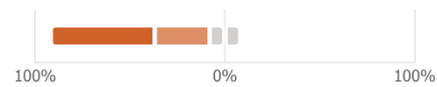
● Extremely important ● Somewhat important ● Neutral ● Somewhat not important ● Not Important



19. To what extent do you agree: A harmonised EU cybersecurity certification system (voluntary or mandatory) would increase trust in qualifications across Member States. [More details](#)

Strongly agree Agree Neutral Disagree Strongly disagree

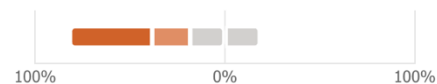
Choice



20. How important is it to implement measurable KPIs and progress-tracking systems for cyber capacity-building across Member States? [More details](#)

Very important Extremely important Somewhat important Not so important Somewhat not important

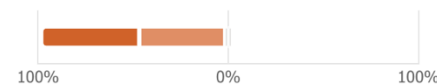
Choice



21. To what extent do you agree: *Effective cyber capacity-building requires stronger and better-incentivised collaboration between government, industry, academia, and civil society.* [More details](#)

Strongly agree Agree Neutral Disagree Strongly disagree

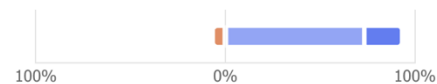
Choice



22. How important is it to establish sustainable, long-term funding mechanisms (e.g. public-private, structural funds) for national and EU-level cyber skills development? [More details](#)

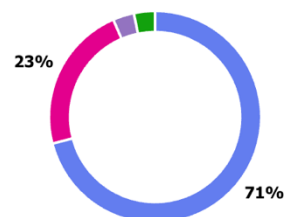
Not so important Somewhat important Very important Extremely important

Choice



23. In your view, does the EU need a more structured, unified approach to cybersecurity human capacity-building? [More details](#)

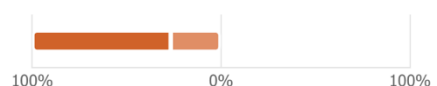
Yes, urgently	22
Yes, in the medium term	7
No	0
Not sure	1
Other	1



24. To what extent do you agree: *Cybersecurity should be treated as a cross-cutting enabler across all digital transformation strategies, not just as a standalone field.* [More details](#)

Strongly agree Rather Agree Neutral Strongly disagree Disagree

Choice



25. How valuable is an EU-wide mechanism for forecasting cybersecurity workforce needs? [More details](#)



26. To what extent do you agree with the following statement: *"A nation or institution cannot be considered future-ready without a resilient, cross-sectoral foundation of cybersecurity competence."* [More details](#)



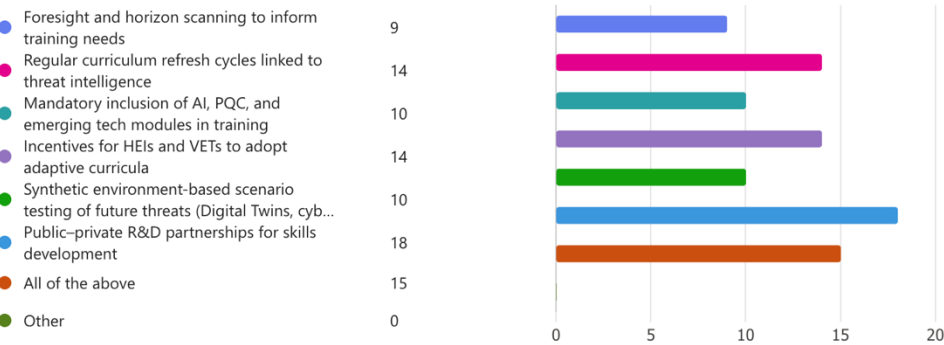
27. Cybersecurity competence should be systematically embedded and measured across non-cyber domains—such as education, healthcare, law, defence, and public administration—as a prerequisite for digital transformation and strategic resilience. [More details](#)



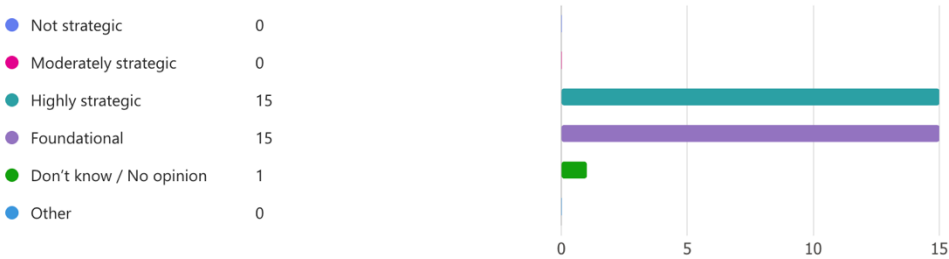
28. How confident are you that current cybersecurity training frameworks (e.g. ECSF, national strategies) can adapt to emerging domains such as AI, quantum computing, and hybrid threats? [More details](#)



29. Which of the following mechanisms would best support future-readiness in EU cybersecurity skills development? [More details](#)



30. In your view, how strategic is cyber competence for ensuring national competitiveness in the next decade? [More details](#)



31. What is the most important action the EU or Member States should take to close the cybersecurity skills gap in the next 5 years?

23

Responses

Latest Responses

"to make sure academic programs are more aligned with i... "

"support for the SMEs as they make up 99% of the enterpr..."

...



32. In your view, what blind spots or overlooked areas are limiting the effectiveness of current cybersecurity capacity-building strategies?

23

Responses

Latest Responses

"to resolve the imbalance between academic output speed..."

"too much focus on academia and theoretical knowledge ... "

...



33. Do you have any comments, concerns, or suggestions regarding the idea of a more structured, EU-wide framework like the NG-EUCCF?

17

Responses

Latest Responses

"would be great to see how it could work on EU level"

...

