CyberHubs

Cybersecurity skills strategy Greece.

Final version.

Co-funded by
the European Union

About CyberHubs

The European Network of Cybersecurity Skills Hubs (CyberHubs) is a 3-year project aiming to enhance the cybersecurity skills ecosystem in Europe. It will establish a network of seven Cybersecurity Skills Hubs in Belgium, Estonia, Greece, Hungary, Lithuania, Slovenia, and Spain, which will promote the development of digital skills in cybersecurity and support the development of a skilled cybersecurity workforce.

Expected results of the project include the establishment of a sustainable European Network of Cybersecurity Skills Hubs, the development of national cybersecurity skills strategies, the creation of innovative cybersecurity solutions through the Hackathon and the establishment of long-term partnerships and collaboration with the wider cybersecurity ecosystem.

info@cyberhubs.eu | cyberhubs.eu

Project consortium

The CyberHubs consortium brings together 21 full partners spanning 11 European Member States and 3 associated partners.

Full partners

DIGITALEUROPE | ADECCO FORMAZIONE SRL | AGORIA | AMETIC | Athens University of Economics and Business | Breyer Publico SL | Cyber Ireland | EIT Digital | GZS/CCIS | HOWEST | INFOBALT | ITL Estonia | IVSZ | Kaunas University of Technology | NUMEUM | SEPE | Solvay Brussels School of Economics and Management | Tallinn University of Technology | Universidad Internacional de La Rioja (UNIR) | Ludovika University of Public Service (NKE) | UNIVERZA V MARIBORU

Associated partners

Association of Applied Research in IT (AAVIT) | Digital Technology Skills (DTSL) | IT Ukraine

Legal Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by
the European Union

Cybersecurity skills strategy Greece, 2025, Final version.

Deliverable D.2.3 “Country-specific cybersecurity skills strategies”

Authors: Anna **Matsouka** (SEPE), George **Iakovakis** (AUEB), **S. Katsaganis** (SEPE)

Editors/Reviewers: Yota **Paparidou** (SEPE), Dimitris **Gritzalis** (AUEB) / Luis Alejandro **Velásquez** Hurtado (UNIR)

Revision History			
Version	**Date**	**Modified by**	**Version**
0.7	02/01/2025	**A. Matsouka** (SEPE), **G. Iakovakis** (AUEB), **S. Katsaganis** (SEPE)	Draft version
0.8	03/01/2025	**Luis Alejandro Velásquez Hurtado** (UNIR)	Review and feedback
1.1	04/01/2025	**D. Gritzalis** (AUEB)	Updated draft version
1.2	10/01/2025	**G. Iakovakis** (AUEB)	Revised draft version
2.0	23/01/2025	**A. Matsouka** (SEPE), **G. Iakovakis** (AUEB), **S. Katsaganis** (SEPE), **D. Gritzalis** (AUEB)	Final version

Table of contents

List of Tables

List of Figures

1 Executive Summary

Introduction

This document outlines Greece's Cybersecurity Skills Strategy, designed to address the pressing need for a skilled workforce capable of combating evolving digital threats. It emphasises the importance of aligning education, training, and industry collaboration to close the skills gap, enhance national resilience, and meet the demands of a rapidly digitizing economy.

By fostering partnerships among academia, government, and the private sector, the strategy aims to build a sustainable and adaptable cybersecurity ecosystem that safeguards the country's critical infrastructure and supports its digital transformation.

Objective

The aim of this document is to present a comprehensive strategy for developing Greece's cybersecurity workforce to address current and future challenges in the digital landscape. It targets a wide range of groups, including, professionals in the public and private sectors, students at all educational levels and citizens who interact with digital technologies.

Key areas of focus include professional development programmes to upskill and reskill the workforce, the integration of cybersecurity into educational curricula, and public awareness campaigns to promote a culture of cybersecurity. By addressing these areas, the strategy seeks to build a resilient, skilled, and informed society capable of navigating and mitigating digital risks effectively.

Approach

The development of this document employed a multi-faceted approach, combining quantitative and qualitative methods to ensure a comprehensive understanding of Greece's cybersecurity skills landscape. Additionally, insights from the Cybersecurity Skills Needs Analysis were integrated to identify skill gaps, market demands, and educational opportunities.

This strategy aligns closely with key European and national cybersecurity initiatives, such as the EU Cybersecurity Strategy, the NIS2 Directive, and the European Cybersecurity Skills Framework (ECSF) of ENISA. By adhering to these frameworks, the document ensures Greece's compliance with EU standards while addressing unique national needs. For example, it incorporates the NIS2 Directive's emphasis on workforce development and operational resilience and supports the categorisation of ECSF.

Moreover, the strategy connects directly with the broader objectives of the CyberHubs project by leveraging deliverables and activities from other participating countries and hubs. This includes shared methodologies, cross-border partnerships, and collective learning to enhance the cybersecurity workforce ecosystem across Europe. By situating Greece's efforts within this larger collaborative framework, the strategy not only addresses domestic challenges but also contributes to the overarching goals of strengthening cybersecurity capacities across the EU.

Results

The document highlights the critical findings from the analysis of Greece's cybersecurity skills ecosystem, revealing a significant mismatch between the supply of skilled professionals and market demand. It presents data on workforce gaps, showing a projected annual shortfall of professionals in cybersecurity roles, alongside insights into the educational landscape, which lacks comprehensive undergraduate programmes in cybersecurity.

The results emphasise the pressing need for targeted initiatives, such as advanced training programs, public-private partnerships, and awareness campaigns, to close these gaps. By addressing these findings, the strategy outlines actionable solutions to build a resilient and capable cybersecurity workforce.

Conclusions

The analysis underscores the urgent need to address the cybersecurity skills gap in Greece, with a clear demand for skilled professionals far exceeding current supply.

Key takeaways include the necessity of integrating cybersecurity education at all levels, from foundational learning to specialised postgraduate programmes, and enhancing accessibility to professional certifications. Strengthening public-private partnerships is essential to align training with industry needs and foster innovation. Additionally, raising public awareness of cybersecurity and embedding it into societal norms are critical for resilience.

The strategy provides a roadmap for achieving these goals, ensuring Greece is prepared to meet evolving cyber threats while supporting economic growth and digital transformation.

2 Introduction

2.1 Cybersecurity in Greece

Cyber threats are evolving rapidly and organisations across various sectors are striving to enhance their cybersecurity capabilities to protect data and maintain the integrity of their operations. During Q1/2024, the cybersecurity sector continued to face challenges that emerged in 2023, with a notable increase in cyber-attacks across various sectors and regions. Specifically, there was a 28% increase in global cyber-attacks compared to the last quarter of 2023, and a 5% increase from 2022. This indicates a troubling trend of rapidly escalating threats in cyberspace.

It is vital to understand the cybersecurity situation to develop effective strategies and policies. With regards to mid-term demand forecasts, ENISA[1] updated (2024) its Cybersecurity forecast. The analysis of emerging threats projected for 2030 (see Table 1) includes two significant threats (ranked 2nd and 3rd in the list of top 10) related to the **shortage of trained cybersecurity workforce**.

Specifically, the **second position** in the table refers to the **skills shortage** in cybersecurity. The study notes that organisations intend to incorporate personnel with appropriate knowledge and skills into their workforce and bridge the educational gap that remains a serious problem in cybersecurity. This is linked to the third threat concerning **outdated systems** (exploitation of unpatched and out-of-date systems within the overwhelmed cross-sector technological ecosystem). The connection between these two major threats highlights that the skills shortage hampers **workforce familiarity with the available tools** used to update outdated information systems, resulting in these systems progressively becoming more vulnerable to cyberattacks (ENISA, 2024).

#	Threat	Impact * Likelihood	Impact	Likelihood
1	Supply Chain Compromise of Software Dependencies	17,71	4,21	4,21
2	**Skills Shortage**	**17,20**	**4,10**	**4,20**
3	**Human Error and Exploited Legacy Systems within Cyber-Physical Ecosystems**	**16,69**	**3,96**	**4,22**
4	Exploitation of Unpatched and Out-of-date Systems within the Overwhelmed Cross-sector Tech Ecosystem [Optional]	16,21	4,05	4,00
5	Rise of Digital Surveillance Authoritarianism/Loss of Privacy	15,34	3,96	3,88
6	Cross-border ICT Service Providers as Single Point of Failure	15,12	4,14	3,65
7	Advanced Disinformation/Influence Operations (IO) Campaigns	14,38	3,42	4,21
8	Rise of Advanced Hybrid Threats	14,03	3,68	3,81
9	Abuse of AI	13,22	3,43	3,86
10	Physical Impact of Natural/Environmental Disruptions on Critical Digital Infrastructure [Optional]	12,99	3,68	3,53

***Table 1:** Ranking of projected new threats (2030)*

[1] ENISA, *Foresight Cybersecurity Threats for 2030* (update), March 2024, https://www.enisa.europa.eu/ news/skills-shortage-and-unpatched-systems-soar-to-high-ranking-2030-cyber-threats

According to ENISA, the European job market **must ensure an adequate number** of skilled professionals in all areas of Cybersecurity, who should be properly trained to support and lead solutions to the emerging industrial, scientific, social, and political challenges in the field of Cybersecurity.

The survey[2] (SEPE - Deloitte, 2024) by the Federation of Hellenic ICT Enterprises (SEPE) assessing the adequacy of specialised ICT skills in Greece, confirmed that most businesses have vacant positions for ICT specialists. A significant increase in demand for these specialties is expected in the near future. The estimated demand-supply gap for the period 2023-2030 is between 7,000 and 7,500 individuals annually. The study found that **cybersecurity is one of the top three specialisations with the highest demand in the whole ICT sector.**

In a market valued globally in the hundreds of billions of euros, Greek technology entrepreneurs are vying for the largest possible market share, often partnering with powerful investors. The Greek market continues to invest in cybersecurity. Greek technology conglomerates in this sector are growing in both quantitative and qualitative terms and investors are supporting related ventures.

2.2 Global and regional trends in cybersecurity

As the 2024 **Fortinet State of Operational Technology and Cybersecurity Report** shows (Fortinet, 2024), there are positive signs that OT security is maturing in many organisations. However, at the same time, some of the gains seen in the previous year slipped in the current survey cycle, with organisations experiencing more intrusions and OT becoming less of a factor in determining risk score. To reverse these trends, there must be renewed evangelism for protecting sensitive OT systems and allocating resources for an effective, purpose-built security architecture.

Survey respondents were from different locations around the world, including Australia, New Zealand, Argentina, Brazil, Canada, Mainland China, France, Germany, Hong Kong, India, Japan, Mexico, Norway, South Africa, South Korea, Spain, Taiwan, Thailand, United Kingdom, and the United States, among others.

The main key takeaways are that nearly one-third (31%) of respondents reported 6+ intrusions, compared to only 11% last year. Organisations with advanced maturity levels reported high intrusions for this cycle. All intrusion types increased compared to the previous year, except for a decline seen in malware. Phishing and compromised business email intrusions were the most common types, while the most common techniques used were mobile security breaches and web compromise (see Graph 1).

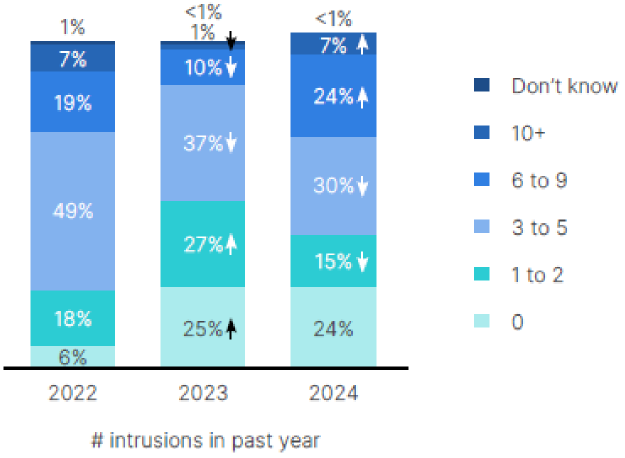

Figure 1: *Number of intrusions in past year (Fortinet, 2024)*

[2] SEPE – Deloitte Survey, *Evaluation of the proficiency of ICT Specialists in Greece*, https://www.sepe.gr/research-studies/21142064/m3eleti-sepe-deloitte-apotimisis-eparkeias-eidikon-tpe-stin-ellada/

Another clear sign of increasing maturity comes from steady growth in organisations that have already rolled OT security under a CISO, from only 10% in 2022 to 17% in 2023 to 27% this year. At the same time, we saw a reversal of last year's trend with organisations that were not planning to move OT security under the CISO in the next 12 months, which went from 11% in 2022 down to 4% last year, but back up to 12% in 2024.

During 2024, the **Cybersecurity Workforce Study** (ISC^2) surveyed (ISC2 cybersecurity workforce study, 2024) a record of 15,852 international practitioners and decision-makers responsible for cybersecurity in workplaces across North America to Asia, Latin America, Europe, the Middle East and Africa. ISC^2 estimates the cybersecurity global workforce to be 5,468,173 employees. This is a 0.1% increase from 2023. This change resulted from growth in the Middle East and Africa (7.4%), and Asia-Pacific (3.8%). This growth was countered by reductions across **Europe (-0.7%),** North America (-2.7%) and Latin America (-0.9%) cybersecurity workforces (see Graph 2).

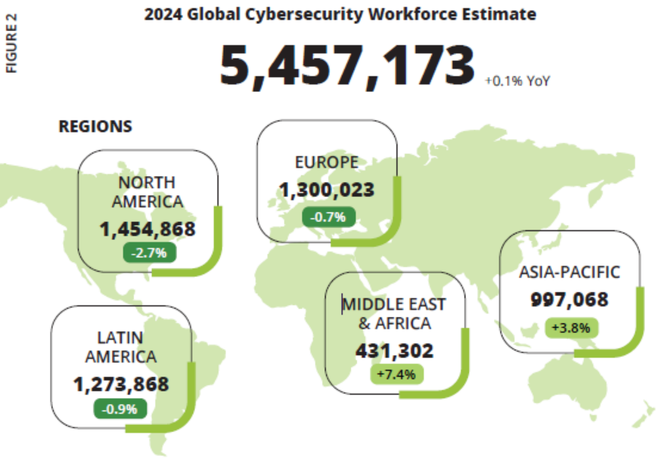

Figure 2: Global Cybersecurity Workforce (2024) (ISC2, 2024)

The workforce gap estimate methodology considers the security team shortages, as reported by study participants, and the staff needed to adequately keep their organisations secure. It also incorporates the workforce size estimate previously mentioned and other primary and secondary data sources. This year, the workforce gap was 4,763,963 people. This is a **19.1% increase from 2023,** with the greatest rise in Asia-Pacific (+26,4%) and **Europe (+12,8%)** (see Graph 3).

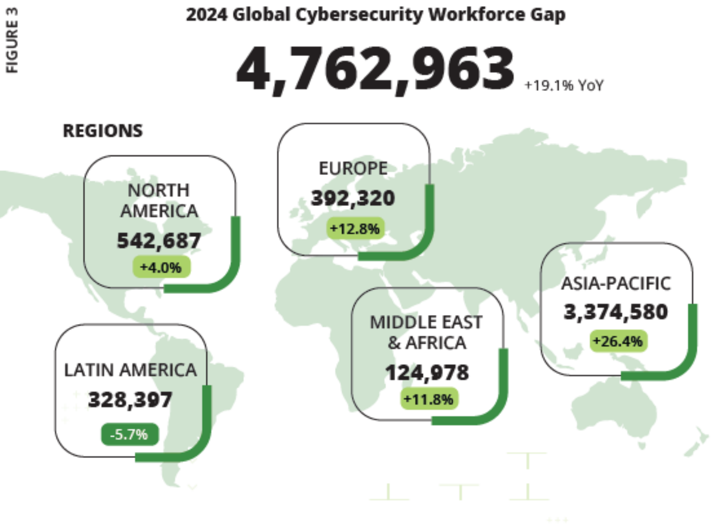

Figure 3: Global Cybersecurity Workforce Gap (2024) (ISC2, 2024)

Skills shortages make it difficult to secure the organisation. 64% of respondents believe that skills gaps can have a more significant negative impact than a staffing shortage. Cybersecurity professionals are feeling this pressure, as 90% of respondents have one or more skills gaps on their cybersecurity teams (see Graph 4). AI was the second most desired technical skill among non-hiring managers. Hiring managers are focused on skills that can provide immediate benefits and see AI as a future benefit. This may explain why skills like security engineering and risk assessment analysis rank above AI.

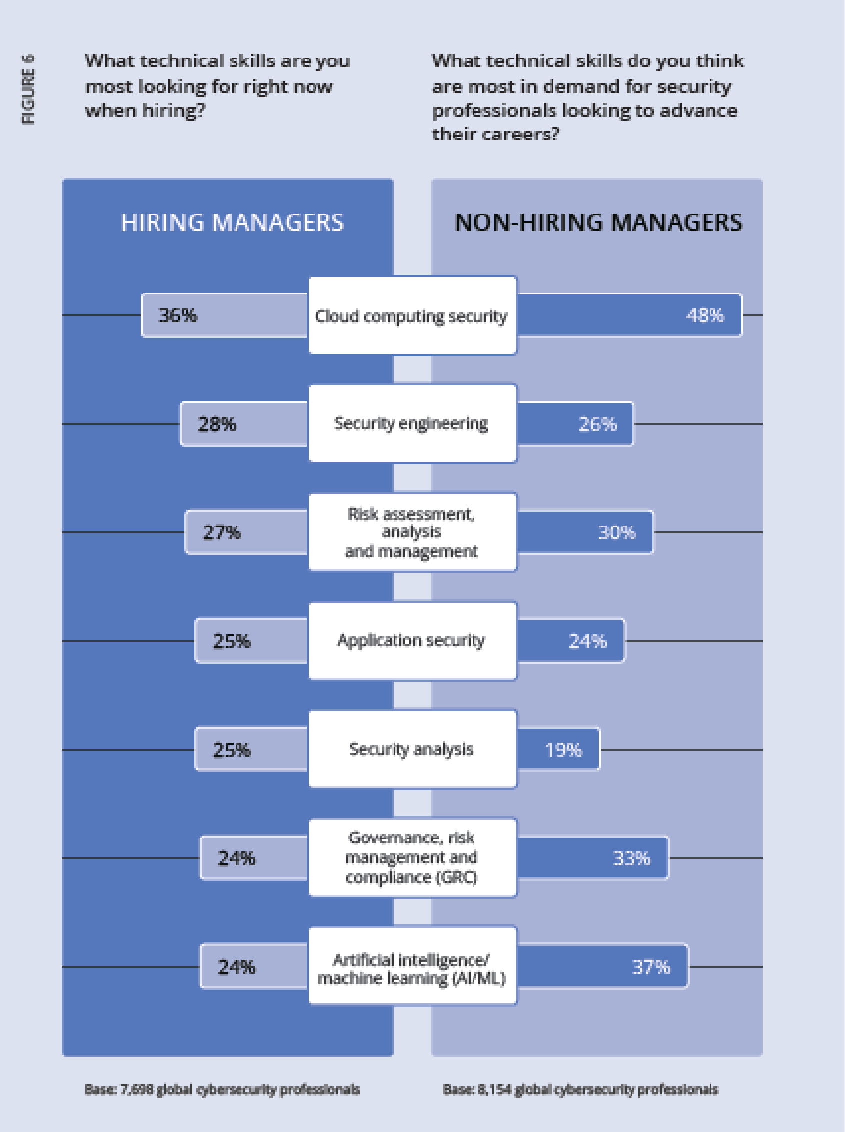

***Figure 4:** Cybersecurity Technical Skills (2024) (ISC2, 2024)*

Recognising the challenges facing European businesses, the European Union has adopted the Digital Operational Resilience Act (DORA) and the Network and Information Security 2 (NIS2) Directive, with the aim of shielding the operations of financial entities and companies providing critical infrastructure-related services, respectively.

Directive NIS2

Recent years have been active for legislators all over the world when it comes to cybersecurity and privacy regulation. The first EU cybersecurity rules introduced in 2016 (Directive 2016/1148/EU, known as NIS1) and updated by the NIS2 Directive (Directive (EU) 2022/2555) that came into force in 2023 with a transposition to Member States national legislation deadline, the 17th of October 2024. The NIS2 Directive (NIS2 Directive, 2023) is the EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU. It modernised the existing legal framework to keep up with increased digitisation and an evolving cybersecurity threat landscape. By expanding the scope of the cybersecurity rules to new sectors and entities, it further improves the resilience and incident response capacities of public and private entities, competent authorities and the EU.

The Directive on measures for a high common level of cybersecurity across the Union provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:

- Member States' preparedness, by requiring them to be appropriately equipped. For example, with a Computer Security Incident Response Team (CSIRT) and a competent national network and information systems (NIS) authority,
- cooperation among all the Member States, by setting up a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States.
- a culture of security across sectors that are vital for our economy and society and that rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.

Businesses identified by the Member States as operators of essential services in the above sectors will have to take appropriate security measures and notify relevant national authorities of serious incidents. Key digital service providers, such as search engines, cloud computing services and online marketplaces, will have to comply with the security and notification requirements under the Directive.

A recent ENISA study (ENISA - NIS 2, 2024) on the impact of NIS2 and other related regulations on cybersecurity investment and business maturity found that:

- **Information security now represents 9% of EU IT investments, a significant increase of 1.9% from 2022,** marking the second consecutive year of growth in cybersecurity investment post-pandemic.
- In 2023, **median IT spending for organisations rose to EUR 15 million, with information security spending doubling** from EUR 0.7 million to EUR 1.4 million.
- For the fourth consecutive year, **the percentage of IT Full Time Equivalents (FTE) dedicated to information security has declined, from 11.9% to 11.1%.** This decrease may reflect recruitment challenges, with 32% of organisations—and 59% of SMEs—struggling to fill cybersecurity roles, particularly those requiring technical expertise. This trend is especially notable given that **89% of organisations expect to need additional cybersecurity staff to comply with NIS2.**
- **New NIS2 sectors are comparable in cybersecurity spending to existing NIS Directive entities, with their investments largely focused on developing and maintaining baseline cybersecurity capabilities.** Emerging areas, such as post-quantum cryptography, receive limited attention with only 4% of surveyed entities investing and 14% planning future investments.
- **The majority of organisations anticipate a one-off or permanent increase in their cybersecurity budgets for compliance with NIS 2.** Notably, a substantial number of entities will not be able to ask for the required additional budget, a percentage that is especially high for SMEs (34%).
- **90% of entities expect an increase in cyberattacks next year, in terms of volume, costliness or both.** Despite that, 74% focus their cybersecurity preparedness efforts internally, with much lower participation in national or EU-level initiatives. This gap underscores a critical area for improvement, as effective cross-border cooperation in managing large-scale incidents can only be achieved at these higher levels.
- **Overall awareness among in-scope entities is encouraging, with 92% being aware of the general scope or specific provisions of the NIS 2 Directive.** However, a notable percentage of entities in certain new NIS 2 sectors remain unaware of the Directive, suggesting a potential need for increased awareness campaigns by the national competent authorities.

- **Entities in sectors already covered by NIS outperform those newly included under NIS 2 across various cybersecurity governance, risk, and compliance metrics**. Similarly, entities in new NIS 2 sectors show lower engagement and higher non-participation rates **in cybersecurity preparedness activities**. This highlights the positive impact the NIS Directive has had on the sectors already in scope; and creates anticipation for the impact NIS 2 will have on the new sectors.

DORA

DORA regulation (DORA, 2024) comes into force in January 2025 and aims to ensure the smooth operation of companies offering financial services by addressing cyberthreats that may affect critical business processes.

DORA and NIS2 require the implementation of integrated management systems through which it is possible to identify and effectively address Information Security risks in a timely manner. The adaptation of companies to the new regulatory framework is a difficult gamble, which companies must win, either on their own or with the help of specialist consultants.

GREECE – Cybersecurity legislative environment

By recognising the fundamental importance of Cybersecurity, Greece has undertaken significant initiatives to meet international and EU requirements, create a secure environment for digital technologies and increase the trust of citizens and businesses in digital applications and services. These efforts aim to benefit both the economy and society. In this context, Greece's initial initiatives included:

(a) **Law 4577/2018**[3] (Ministry of Digital Governance, 2018) on the "Incorporation into Greek legislation of Directive 2016/ 1148/EU of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems throughout the EU and other provisions."

(b) **Ministerial Decision** 1027/2019[4] (Ministry of Digital Governance, 2019) based on which the framework of obligations was defined for the Operators of Essential Services (OES) and for the Providers of Digital Services (PDS), including the security requirements they must comply with, etc.

(c) **Law 5160/2024** (National Printing House, 2024) on the "Transposition of Directive (EU) 2022/2555 of the European Parliament and of the Council, of 14 December 2022, on measures for a high common level of cyber security throughout the Union, amending the Regulation (EU) 910/2014 and Directive (EU) 2018/1972, and the repeal of Directive (EU) 2016/1148 (NIS 2 Directive) and other provisions.

2.3 Vision

2.3.1 Cybersecurity professionals for ECSF roles

The Greek CyberHub presents a cybersecurity skills strategy to defend Greece from cyberattacks by connecting highly skilled cybersecurity professionals with industry. Through dynamic collaboration with academia, employers, industry and government, the Greek CyberHub is developing comprehensive strategies and innovative solutions to meet the evolving cybersecurity workforce needs across the country.

The statement provides a strong vision for the Greek CyberHub's cybersecurity skills strategy. It emphasises collaboration between key stakeholders - government, education, industry, and the broader community - and highlights the need for a highly skilled, adaptable cybersecurity workforce that can address Greece's evolving cyber threats. By outlining the collaborative and strategic approach of the CyberHub, this statement provides an inspiring foundation for the following core objectives:

[3] https://mindigital.gr/wp-content/uploads/2019/09/N.4577_2018.pdf

[4] https://mindigital.gr/wp-content/uploads/2020/01/3739B-19-1.pdf

- **Foster workforce development partnerships:** Establish ongoing partnerships among academia, industry, and government to align cybersecurity education with current and anticipated needs. This includes creating apprenticeship programmes, internships, and collaborative projects that prepare students and professionals to address real-world security challenges.
- **Develop specialised training and certification programmes**: Develop targeted training and certification programmes that reflect both the basic and specialised skills needed in the Greek cybersecurity sector. These programmes can range from introductory courses to advanced skill building in niche areas such as incident response, ethical hacking, and security management.
- **Promote cybersecurity awareness and culture:** Integrate awareness initiatives that reach diverse groups-from government employees and industry leaders to the general public. By fostering a culture that values cybersecurity, the Greek CyberHub can strengthen the resilience of organisations and individuals against cyber threats.
- **Foster innovation in cybersecurity solutions:** Support innovation by creating opportunities for cybersecurity professionals to work on complex challenges through research, hackathons, and collaborations with tech startups. This will ensure that Greece's cybersecurity landscape evolves in line with new technologies and threat landscapes.
- **Establish benchmarks for skills and progress:** Implement a framework to measure workforce competency and growth in cybersecurity skills across Greece. Regular assessments will help identify gaps, track progress, and ensure that ongoing development aligns with industry and national security needs.

This holistic approach not only addresses Greece's immediate cybersecurity needs, but also positions the country to proactively manage future risks through a highly skilled, resilient, and continuously evolving cybersecurity workforce.

3 Current situation and strategic objectives

The Cybersecurity Skills Needs Analysis identified the mismatch between supply and demand in cybersecurity skills in Greece and provided an accurate picture of Greece's cybersecurity skills ecosystem maturity, opportunities, and peculiarities.

A multi-method approach (quantitative and qualitative) was followed, including: (a) desk research, (b) survey in Greek, (c) job vacancies scrapping powered by the EIT Digital Skills Academy Platform (SAP), and (d) expert focus groups. With respect to expert panels, two of them were established. One staffed by experienced cybersecurity professionals from both the private and the public sector, and the second by academics specialising in cybersecurity or a closely related field.

The mapping of skills and roles followed the European Cybersecurity Skills Framework (ECSF) of ENISA. The responses were also categorised based on the corresponding high-criticality taxonomy according to the Directive on measures for a high common level of cybersecurity (NIS2).

Critical market needs in terms of Cybersecurity skills, and professional roles demand, as well as the training and education programme gaps, were thus uncovered.

On the **supply** side, there is no undergraduate academic programme on Cybersecurity skills in the country, however some colleges offer undergraduate study programmes in Cybersecurity in cooperation with foreign universities.

While there is a good number of postgraduate cyber programmes available (both in Greek public universities and in some colleges), several student places remain unfilled.

Additionally, (a) Greek universities may grant doctoral degrees to students with dissertation topic related to cybersecurity (b) relevant professional certifications are provided by international professional associations, (such as, ICS2 και ISACA) appear to play a visibly supportive role.

On the **demand** side, there was no systematic and reliable study that address and assess cybersecurity skills demand, short or long-term, prior to the Cybersecurity Skills Needs Analysis of the Greek CyberHub.

3.1 Key Actors in Cybersecurity Area

The main entities in the field of cybersecurity skills in the Greece are:

- National Cybersecurity Authority (NCSA)
- Ministry of Digital Governance (MoDG)
- Ministry of Education, Religious Affairs and Sports (MoE)
- Academic & Research Institutions
- ICT enterprises (mainly in NTAs’ network, not exclusively)
- ENISA
- ISACA and ISC2 (Hellenic Chapter)

Representatives of the aforementioned entities participated in the expert panels that contributed to the Cybersecurity Skills Needs Analysis and the Skills Strategy. Greek CyberHub acted as an orchestrator. The entities and the CyberHub have established a considerable level of collaboration that will enable the implementation of the strategy and the fulfillment of the short-term (next 2 years), medium-term (3-5 years), and long-term (>5 years) objectives that will be presented in this document.

3.2 ECSF common language for cybersecurity professional workforce development

Cybersecurity professional competences performance play a vital role for the European economy and society as a whole, and dedicated European reference frameworks that can be used by all key stakeholders of the digital professional eco-system are essential.

The European Cybersecurity Skills Framework (ECSF) published by ENISA in 2022[5] (ENISA - ECSF, 2022), being the result of joint work between ENISA and a dedicated AdHoc Work Group composed of Cybersecurity Professionals from many European countries, provides the needed common language and reference point for all parties to act upon, giving a common basis for specific and combined action for cybersecurity professional workforce development at all levels and across Europe in the short, mid and long-term.

The key objectives of the ECSF are:

- Establishing a common understanding of the most typical cybersecurity professional roles, missions and tasks required in the cyber secure organisation, together with their competences, skills and knowledge requirements, that can be used by and for individuals, organisations, learning providers, policy makers and cyber enthusiasts in all EU Member States, in order to effectively address the cybersecurity skills shortage.
- Contributing to further facilitate the recognition of cybersecurity professional-related skills and competences, the design of market needs oriented learning programmes, the cybersecurity workforce development in the organisation, and career guidance to individuals.

The 12 Cybersecurity Professional Role Profiles provided by the ECSF are ensuring the common language for the CyberHubs consortium across all work stages, and they are implemented from multiple viewpoints on European and national levels in workplace, learning, legal and policy making context. Adopting the ECSF as a high-level taken strategic decision significantly accelerates collaboration processes in the country and EU-level connected and from the start, enabling all cybersecurity ecosystem key stakeholders to:

- Get a **common understanding** of the necessary professional roles, competences, skills and knowledge,
- Support **cybersecurity workforce roles and skills needs identification, planning and development,** e.g. to prepare for organisational compliance with the new coming NIS2 Directive[6],
- Facilitate **cybersecurity skills recognition,**
- Support the **design of** cybersecurity related **training programmes,**
- Help **shape content of applications** for **funding programmes** on national and European levels,

In this context, it is crucial to understand the ECSF (ENISA - ECSF, 2024) as a flexible offer and as a tool that is provided for flexible usage. The framework seeks to enable wherever helpful and never to restrict. This can be easily achieved by selecting the components that are most suitable in context and further customising where needed.[7]

[5] ECSF Part 1: 12 Cybersecurity Professional Role Profiles, ENISA 2022.

[6] See ENISA Report “Preparing for NIS2 Compliance — NIS2 Mapping with ECSF Role Profiles” expected for 2025, reference to be added when available.

[7] See ECSF Part 2: User Manual, ENISA, 2022.

3.3 EU and member-state regulations

At both the European Union and national levels, robust regulatory frameworks have been put in place to secure critical infrastructure, protect data, and improve cybersecurity resilience across member states. The European Union has implemented several directives and regulations that set minimum standards for cybersecurity, requiring member states to take measures to protect their digital environments and ensure rapid, coordinated responses to cyber threats. In Greece, national laws and policies complement these EU regulations, adapting them to the local context and addressing specific national security concerns.

Key EU Cybersecurity Regulations

1. **NIS Directive (Directive on the Security of Network and Information Systems):** A cornerstone of the EU's cybersecurity strategy, the NIS Directive requires member states to improve national cybersecurity capabilities, increase cooperation, and mandate that operators of essential services and digital service providers implement robust security measures. A new iteration, NIS2, expands the scope and mandates more stringent security measures and oversight mechanisms.
2. **Cybersecurity Act:** This law establishes the European Cybersecurity Certification Framework, which provides certifications for ICT products, services and processes. It aims to build trust in digital solutions and create a common standard for cybersecurity practices across the EU, supporting a common cybersecurity market.
3. **General Data Protection Regulation** (GDPR): While GDPR focuses on data protection, it has significant implications for cybersecurity. GDPR requires organisations to implement appropriate security measures to protect personal data and report breaches, which aligns with broader cybersecurity goals.
4. **Digital Operational Resilience Act** (DORA): Of particular relevance to financial institutions, DORA establishes comprehensive requirements to ensure that financial institutions can withstand and recover from cyber incidents. It mandates risk management, incident reporting, and resilience testing in the financial sector.

Key Greek National Cybersecurity Regulations and Frameworks

In alignment with EU directives, Greece has developed national policies and legal frameworks to address cybersecurity, including:

1. **Greek National Cybersecurity Strategy**: This strategy outlines Greece’s cybersecurity vision, including objectives for protecting critical infrastructure, enhancing public-private partnerships, and establishing cybersecurity training programmes. It highlights Greece’s commitment to meeting EU cybersecurity requirements while addressing the unique threats faced domestically.
2. **Law on Data Protection and Cybersecurity (Law 4624/2019)**: Complementing GDPR, this law further defines personal data protection requirements specific to Greece, including the establishment of a national data protection authority responsible for enforcing cybersecurity regulations for personal data.
3. **Critical Infrastructure Protection Legislation**: Greece has specific laws that address the protection of critical infrastructure, with mandates for cybersecurity preparedness, risk assessment, and incident reporting, particularly for sectors such as energy, transportation, and telecommunications.

3.4 Industry/Country needs

The top cybersecurity roles, according to the ENISA Framework and to the current needs of the organisations, as considered by the respondents, appear in Table 2.

GREECE - People working today in ENISA Cybersecurity Roles (ECSF)		
Less than needed	**As many as needed**	**More than needed**
Penetration Tester	Cybersecurity Educator/Trainer	Cybersecurity Researcher
Cyber Threat Intelligence Specialist	Cyber Legal, Policy & Compliance Officer	Cybersecurity Risk Manager
Digital Forensics Investigator	Chief Information Security Officer (CISO)	Cybersecurity Architect
Cybersecurity Implementer		Cyber Incident Responder
Cybersecurity Auditor		

Table 2: *GREECE - People working today in ENISA Cybersecurity Roles (ECSF)*

Today, most people work as Cyber Incident Responders and this trend is expected to continue in the next 5 years. In the near future (2-5 years), the greater need will be for Cyber Incident Responders and Cybersecurity Implementers. Additionally, the roles expected to see the greatest increase in cybersecurity experts are Digital Forensics Investigator, Cybersecurity Auditor and Cyber Threat Intelligence Specialist.

During the expert panels discussions, the role of Cyber Legal, Policy & Compliance Officer was considered equivalent/similar to this of a Data Protection Officer (DPO), according to ENISA's European Cybersecurity Skills Framework (ECSF). Rather surprisingly, several respondents reported that no Cybersecurity, Legal, Policy & Compliance Officers are currently working in this role, or that there is no need for such officers at present.

The top cybersecurity skills needed now, according to the respondents, appear in Table 3.

GREECE – IT security skills needed in the organisation (top-down)		
No need	**Substantial need**	**Lot of need**
Supply Chain Security	Cloud Security	Data Privacy
	DevSecOps	Information Systems & Network Security / Cyber Resiliency
Some need	Communications Security	Access Controls / Identity Management
AI Security	Operating Systems (OS) Security	Threat Analysis
Physical Device Security	Data Security & Cryptography	
Intelligence Analysis	Incident Management	
Digital Forensics	Access Controls / Identity Management	
Operational Technology Security	Threat Analysis	
	Operational Technology Security	

Table 3: *GREECE – IT security skills needed in the organisation (top-down)*

The fact that several respondents stated that there is no need for Supply Chain Security skills was discussed at the expert panel meetings. The panels concluded that this perception likely stems from the practice of outsourcing procurement, which places the responsibility for supply chain security to the supplier.

The expert panels also discussed the limited need expressed by respondents for AI Security and Intelligence Analysis skills. They attributed this to the fact that most local organisations purchase products and solutions developed in other countries. Additionally, the expert panels noted that while AI can be a highly beneficial tool in cybersecurity, most local organisations have not yet fully recognised the adequate maturity of this new technology.

The expert panels said it is imperative to shield critical infrastructures to deal promptly and effectively with security breaches. It was also noted that Data Privacy skill scores very high due to GDPR requirements.

The Role of Advanced Technologies in Cybersecurity: The role of emerging technologies such as artificial intelligence, machine learning, and blockchain has become a key factor in improving cybersecurity practices. Analysis reveals that organisations using AI and ML for threat detection report a notable improvement in their ability to identify and respond to potential breaches in real time. The AI instruments have enabled these organisations to analyse large data sets, determining unusual models that may indicate the attack.

Since organisations are subject to a digital transformation, they face increased cybersecurity problems. The proliferation of digital technologies has expanded the attack surface, exposing organisations to a range of cyber threats including data breaches, ransomware attacks, and insider threats. Training and awareness programmes are essential for equipping employees with the knowledge and skills needed to recognise and respond to cyber threats effectively. The demand for skilled cybersecurity professionals will continue to grow as organisations face the increasing complexity of cyber threats. Tomorrow's workforce will need a diverse set of skills, including technical expertise, analytical thinking, and a deep understanding of new technologies.

Organisations must invest in ongoing training and development programmes to equip their employees with the knowledge and skills they need to keep up with the evolving cybersecurity landscape. Collaboration between educational institutions and industry players is essential to close the skills gap and develop a new generation of cybersecurity talent.

The Cybersecurity skills forecasting model (D2.2) will be used for a yearly update of the Cybersecurity skills needs in our country. This model provides information on which cybersecurity roles and skills are gaining importance and for which the needs are declining. This is done by combining quantitative data from job vacancies which are refined by other data and qualitative data from experts that analyse and interpret the quantitative data. This yearly update can lead to changes in priorities depending on the outcomes.

3.5 Educational landscape

As presented in the Cybersecurity Skills Needs Analysis, in the formal educational system of Greece, education in Cybersecurity or related areas is provided by **Postgraduate Programmes** (EQF 7) offering Master's Degrees of Specialisation (**M.Sc**.), as well as by **Doctoral Programmes** (EQF 8) offering Doctoral Degrees (**Ph.D**.). Such specialisation is not provided by **Undergraduate Programmes** (EQF 6) thus no corresponding degree title (**B.Sc**.) is awarded.

In non-formal education, such specialisations are offered by **colleges**, at both the **undergraduate** level (**B.Sc**.) and **postgraduate** level (**M.Sc**.). Additionally, relevant training certifications are provided by the **Centres of Training and Lifelong Learning** (KEDIVIM), which operate mainly, but not exclusively, within the framework of universities. Finally, a series of relevant **professional certifications**, widely accepted by the domestic market but not by the Greek Public Administration, are provided by collective professional bodies/associations with broad international presence (ISC2, ISACA).

Table 4 reports the overall quantitative data of the workforce in Greece that obtained academic degrees and professional certifications in Cybersecurity (**EQF levels 4 to 8** of the European Qualifications Framework) during the triennium **2021-23**.

CyberHub Greece	2021-23		
	M	W	M+W
FORMAL EDUCATION SYSTEM			
UNIVERSITIES	**456** (78%)	**128** (22%)	**584** (44%)
Undergraduate Programmes (**EQF 6**)	**0** (0%)	**0** (0%)	**0** (0%)
Graduate Programmes (M.Sc.) (**EQF 7**)	**432** (78%)	**121** (22%)	**553** (95%)
Doctoral Theses (Ph.D.) (**EQF 8**)	**24** (77%)	**7** (23%)	**31** (5%)
NON FORMAL EDUCATION AND TRAINING			
COLLEGES[8]	**89** (80%)	**21** (20%)	**110** (8%)
Undergraduate Programmes (**EQF 6**)	**39** (93%)	**3** (7%)	**42** (38%)
Graduate Programmes (M.Sc.) (**EQF 7**)	**50** (74%)	**18** (26%)	**68** (62%)
Training and Life-long Learning Centres (ΚΕΔΙΒΙΜ)	**93** (57%)	**69** (43%)	**162** (12%)
TOTAL (Education, Training)	**638** (74%)	**218** (26%)	**856** (64%)
PROFESSIONAL CERTIFICATIONS	*No gender-related data stored*		**480** (36%)
TOTAL (Education, Training, Certification)			**1.336**

***Table 4**: GREECE – Cybersecurity: Degrees/Certifications awarded (totals, 2021-23)*

Table 5 presents the corresponding quantitative data.

[8] In Greece, "college" graduates hold a degree recognised by the State as equivalent to those graduated by universities but do not have equivalent professional rights.

CyberHub Greece	2021			2022			2023			2021-23		
	M	W	M+W	M	W	M+W	M	W	M+W	M	W	M+W
FORMAL EDUCATION SYSTEM												
UNIVERSITIES	**157**	**41**	**198**	**143**	**43**	**186**	**156**	**44**	**200**	**456**	**128**	**584**
Undergraduate Programmes (**EQF 6**)	-	-	-	-	-	-	-	-	-	**0**	**0**	**0**
Postgraduate Programmes (**EQF 7**)	149	38	187	138	42	180	145	41	186	**432**	**121**	**553**
Ph.Ds (**EQF 8**)	8	3	11	5	1	6	11	3	14	**24**	**7**	**31**
NON-FORMAL EDUCATIONAL SYSTEM & TRAINING												
COLLEGES[9]	**19**	**6**	**25**	**27**	**9**	**36**	**43**	**6**	**49**	**89**	**21**	**110**
Undergraduate Programmes (**EQF 6**)	6	0	6	9	2	11	24	1	25	**39**	**3**	**42**
Postgraduate Programmes (**EQF 7**)	13	6	19	18	7	25	19	5	24	**50**	**18**	**68**
Training and Lifelong Learning Centres (ΚΕΔΙΒΙΜ)	**16**	**17**	**33**	**25**	**22**	**47**	**52**	**30**	**82**	**93**	**69**	**162**
TOTAL (Education, Training)	**173**	**58**	**231**	**171**	**65**	**236**	**218**	**74**	**292**	**638**	**218**	**856**
PROFESSIONAL CERTIFICATIONS	**ISC^2**: 290 and **ISACA**: 190 (02/2024)									No gender-related data kept		**480**
TOTAL (Education, Training, Certification)												**1.336**

***Table 5**: GREECE – Cybersecurity: Degrees/Certifications awarded (annually, 2021-23)*

[9] College graduates hold an undergraduate degree (B.Sc.) or postgraduate degree (M.Sc.) that are recognised by the Greek State as equivalent to those of universities. However, the recipients are not granted with equivalent professional rights.

From Table 5 the following key conclusions emerge:

1. At **EQF levels 4 and 5** in Greece (Junior Highschool, Highschool, Vocational Schools, Apprenticeship Schools, Institutes of Vocational Training), **certified knowledge** in Cybersecurity or related fields is **not provided**.

2. There is **no university** in Greece that offers a **basic degree** (**EQF level 6**, title: "Ptychio," **B.Sc**). However, there are **Colleges** (4) that have provided such degree titles (**42, B.Sc**).

3. **The majority (553, 65%)** of individuals trained/in training in Cybersecurity in Greece come from **Postgraduate Programmes (M.Sc.)** of Universities (**EQF level 7**, title: "Master's degree of Specialisation," **M.Sc**.) (5 Universities, 6 Programmes).

4. Colleges in Greece that offer specialisation, at **both undergraduate and postgraduate levels**, in Cybersecurity or related fields are **sufficient (14)** (6 Colleges, 8 Programmes), but the number of their graduates is **very limited (107, 13%).**

5. **KEDIVIM** Centres providing **training** in Cybersecurity or related fields in Greece are few (7), mainly operating within the framework of universities, lacking clear integration into the EQF, and have trained a **limited** number of participants (**162, 19%**).

6. Some international and reputable **professional organisations** (ISC2, ISACA) provide a **considerable number of certifications** (480) in various fields of Cybersecurity and related knowledge areas in Greece, following examination.

7. Graduates of programmes/seminars in Cybersecurity or related knowledge areas in Greece are **predominantly male, with no significant trend towards balancing or reversing** this during the period of 2021-23.

8. In Greece, the quota against women (24-28%) in Cybersecurity or related knowledge areas applies regardless of academic study programmes. In **KEDIVIM** seminars, there was a **temporarily high** representation (43%), mainly due to a **legal** training seminar (KEDIVIM). During the period of 2021-23, the following trends were observed:

   (a) a **stable number of graduates** from Master's programmes per year (205-210),

   (b) **a significant decrease in the percentage of female graduates from KEDIVIM programmes** (from **51.5%** to **36.5%**),

   (c) a **limited percentage (23%) of female doctoral graduates**,

   (d) **consistently limited representation (21-24%) of female** graduates from postgraduate study programmes, and

   (e) a **minimal** percentage (7%) of **female** graduates from undergraduate study programmes.

3.6 Cybersecurity Skills Gap Assessment

Based on the analysis in Report D2.1, several discrepancies were identified between EU cybersecurity directives and their implementation in Greece. These include:

- **Inconsistent implementation of the NIS Directive:** Greece has made progress in implementing the NIS Directive, but challenges remain in establishing standardised security measures across all critical sectors. Some sectors are lagging in meeting the Directive's requirements, particularly with regard to incident response and risk assessment.
- **Limited scope of cybersecurity certification:** While the EU Cybersecurity Law promotes a comprehensive certification framework, the uptake of certifications in Greece remains limited. This has led to gaps in the standardisation of cybersecurity practices across industries, potentially impacting the security and trustworthiness of products and services.

- **Inadequate awareness and training programmes:** EU directives emphasise workforce training, but Greece faces challenges in implementing consistent training and awareness programmes across sectors, especially for SMEs and public sector organisations.
- **Fragmented incident reporting mechanisms**: Although required by EU regulations, the coordination and efficiency of incident reporting mechanisms in Greece need to be improved. Fragmented reporting and analysis hinder rapid response and sector-wide awareness of cyber incidents.

The survey conducted under Cybersecurity Skills Needs Analysis recorded the demand for the ENISA Framework Cybersecurity roles, appear on Table 6. The rows of the table represent the roles. The columns represent the employees for four instances (working now, needed now, needed in 2 years, needed after 5 years).

GREECE	Demand for specific cybersecurity roles[10]			
Cybersecurity Roles	Number of people working in this role now	Number of people need-ed in this role now, including the people working in it now	Expected number of people needed in this role in 2 years, including the people working in it now	Expected number of people needed in this role in the long run (>5 years), including the people working in it now
Cybersecurity Risk Manager	141	121	168	196
Cyber Legal, Policy & Compliance Officer	102	102	134	146
Cybersecurity Architect	105	98	144	175
Cyber Threat Intelligence Specialist	60	76	111	149
Cybersecurity Auditor	68	76	123	169
Cybersecurity Educator/Trainer	91	90	129	168
Cybersecurity Researcher	130	93	137	187
Digital Forensics Investigator	41	54	77	109
Penetration Tester	90	119	157	197
Chief Information Security Officer (CISO)	79	80	105	126
Cybersecurity Implementer	165	173	236	261
Cyber Incident Responder	168	162	219	267

***Table 6**: Demand for cybersecurity roles*

The above results were verified by the expert groups and complemented by the job vacancies provided by EIT Digital.

The Cybersecurity Skills Needs Analysis reached the following conclusions.

3.6.1 ENISA Cybersecurity roles

- **Cyber Incident Responders**: currently most people work in this role and this trend is expected to continue in the next 5 years, mainly in medium and large size organisations.
- **Cybersecurity Implementers**: great need in the near future (2-5 years), mainly in medium and large size organisations.

[10] Green color indicates high values and yellow low ones.

Digital Forensics Investigator, Cybersecurity Auditor and Cyber Threat Intelligence Specialist: are expected to see the greatest increase. Specifically, in the next 5 years:

- **Cyber Threat Intelligence Specialist**: major increase at micro size (300%) and medium (350%) organisations.
- **Digital Forensics Investigators**: major increase, at small organisations (900%).
- **Cybersecurity Auditors**: major increase in large organisations (119%).

Surprisingly, several respondents reported that no Cyber Legal, Policy & Compliance Officers are currently working in this role, or that there is no need for such officers at present.

Furthermore, in the top 3 NIS2 sectors, the need for ENISA Cybersecurity Roles is:

- In the **Research & Academia** sector, the greater need is for Cybersecurity Researchers while the greater increase is for Auditors (600%).
- In the **Digital Infrastructure** sector, the greater need is for Cybersecurity Implementers while the greater increase is for Penetration Testers (68%).
- In the **ICT Service Management** sector, the greater need is for Cyber Incident Responders and Cybersecurity Implementers, while the greater increase is for Cybersecurity Researchers (220%).

It is worth noting that in the ICT Service Management sector there is an increase in all ENISA roles, which is not the case in the Digital Infrastructure sector.

3.6.2 Skills for cybersecurity professionals

The skills for cybersecurity professionals, divided in 4 categories (**Cybersecurity, IT related, Organisational, Soft**), that are mostly needed (**a lot or substantial need**) are presented at the table 7 below:

Cybersecurity skills	IT related skills	Organisational skills	Soft skills
Data Privacy	**Operating Systems**	**Risk Management**	**Analytical thinking**
Information Systems & Network Security / Cyber Resiliency	**Network Management**	**Education & Training**	**Creative thinking**
Incident Management	**Data Analysis**	Process Control	Act responsibly
Access Controls / Identity Management	Enterprise Architecture & Infrastructure Design	Business Continuity	**Problem solving**
Threat Analysis	System Administration & Integration	Strategic Planning	Planning and organizing

***Table 7**: Categories for cybersecurity Skills*

Job vacancy analysis (June 2024) has been shown that companies in Greece seek Cybersecurity personnel with skills across all categories. According to the same analysis, the skills marked in red above, are among the **most wanted** skills.

Several responders stated that there is no need for Supply Chain Security skills, leadership is considered the comparatively least needed skill, and expert panels consider that the lack of personality skills lead to reckless business behaviour which is unacceptable in cybersecurity roles.

3.6.3 Education and training of cybersecurity professionals

It has been demonstrated that personnel should be trained, as new (technological) developments require new skills. However, that fact that cybersecurity experts don't have time for training, and that training is too expensive, leads to no backlog in personnel training.

In order to have cybersecurity experts with the right skills, companies prefer to upskill their own ICT personnel, hire people with already the right skills, or train them on-the-job. Hiring people with the right skills is considered very difficult and therefore upskilling is preferred. However, when hiring people in cybersecurity roles, formal professional education relevant for the role and formal certification relevant for the role are the most preferred qualifications.

Hiring qualifications
Formal certification relevant for the role
Formal professional education relevant for the role
Bachelor/Master's degree relevant for the role
Certificates relevant for the role
Formal professional education in any field

***Table 8**: Hiring qualifications*

3.7 Strategic Goals

The Greek Cybersecurity Skills Strategy is built on a foundation of addressing workforce shortages, enhancing education, and fostering collaboration to create a resilient cybersecurity landscape. It envisions the development of a skilled workforce that is equipped to meet the demands of an evolving cyber threat environment while also supporting the nation's digital transformation and economic growth. The strategic goals will be achieved through a series of initiatives, each with varying timeframes (2 years, 2-3 years, 2-5 years, and 5+ years). The completion of these goals is outlined in the following action plan.

3.7.1 Develop a Skilled Cybersecurity Workforce

- Create a robust pipeline of cybersecurity talent by aligning education and training programmes with current and emerging industry needs.
- Foster advanced skill development through specialised certifications, postgraduate programmes, and hands-on experience.
- Promote lifelong learning to upskill existing professionals and adapt to evolving cyber threats.

3.7.2 Strengthen Public-Private Collaboration

- Build partnerships among academia, government, and the private sector to enhance training opportunities, promote innovation, and share resources.
- Encourage private-sector investment in employee training and development to increase workforce capacity and expertise.

3.7.3 Enhance National Cybersecurity Awareness and Culture

- Cultivate a culture of cybersecurity awareness through targeted public education campaigns and training programmes.
- Promote cybersecurity best practices across all sectors of society to reduce vulnerability to cyber threats.

3.7.4 Establish a Sustainable Cybersecurity Ecosystem

- Develop a framework for continuous monitoring and evaluation of cybersecurity skills needs, ensuring alignment with industry demands and regulatory requirements.
- Create centres of excellence and observatories to support long-term workforce planning and innovation in cybersecurity solutions.

By achieving these strategic goals, Greece will be positioned as a leader in cybersecurity, equipped to tackle the challenges of a rapidly evolving digital landscape while fostering economic growth and societal resilience.

3.8 Conclusions

By aligning strategic goals with identified challenges, the CyberHub's strategy aims to create a resilient, skilled, and inclusive cybersecurity workforce.

Through education, accessible training, public awareness, and cross-sector collaboration, Greece can close the cybersecurity skills gap, enhance its defense capabilities, and build a sustainable framework for addressing future cybersecurity needs.

4 Action Plan

The action plan is crucial for translating the cybersecurity skills strategy into concrete steps that drive progress toward the overall vision and strategic goals. It ensures alignment with the CyberHub's vision of fostering a skilled, resilient, and adaptable cybersecurity workforce. By outlining high-level initiatives and key activities, the action plan provides a clear framework for advancing each strategic objective. Each initiative directly supports one or more strategic objectives, with defined activities, timelines, and responsible parties guiding implementation.

The action plan is organised according to the strategic objectives defined in the previous section, with each initiative structured at a high level. This approach maintains alignment with the strategy's overarching goals, with more specific details to be expanded upon in the WP3 report. The following table 8 briefly presents an overview of the proposed initiatives.

Initiative No.	Initiative Name	Objective	Focus Area
1	Public Cybersecurity projects	Strengthen Greece's cybersecurity framework by addressing existing challenges, creating new job opportunities in the cybersecurity domain, and supporting the country's digital transformation.	Public Sector
2	Cooperation with other countries	Cooperation with third countries will help us to exchange ideas, views, technologies so that we can integrate practices and adopt strategies that will help us	Collaboration
3	Development of a Standardised Cybersecurity Curriculum	Identify core skills and industry requirements to develop a baseline curriculum. Establish a cohesive cyber-security curriculum across all levels of education to ensure foundational and advanced cybersecurity knowledge.	Education and Training
4	Cybersecurity Awareness and Public Education Campaign	Enhance cyber literacy among the general population and non-IT professionals to build a baseline of cyber-security awareness.	
5	Expansion of Flexible Learning and Certification Programmes	Increase accessibility to cybersecurity education through online courses, modular certifications, and flexible learning options. Provide scholarships (covering tuition fees or offering job guarantees) to postgraduate and doctoral students from the private sector, with a commitment to employment upon graduation.	
6	Public-Private Internship and Apprenticeship Programme	Bridge the skills gap by providing practical cybersecurity experience through collaborative internship pro-grams.	Industry Partnerships
7	Targeted Research & Development funding	Targeted EU and public funding on research and technological development.	Research and Development
8	National Cybersecurity Threat Intelligence Platform	Establish a centralized threat intelligence-sharing platform to enable real-time collaboration between public and private sectors.	

***Table 9:** Action plan's proposed initiatives*

Initiative I: Public Cybersecurity projects

In general, the public sector has an almost exclusive role in supply (as highlighted by the D2.1 survey) but also in demand. Public projects in cybersecurity need to be targeted, i.e. to provide a solution to existing problems and at the same time create a demand for jobs for people with specialised knowledge and experience in this area. Greece is building strong defenses against cyber threats as the public sector is running its digital transformation, adding new services that facilitate citizen-state relations, with the Ministry of Digital Governance moving ahead immediately with the digital projects the country needs. In addition to the digital transformation of critical sectors such as Health and Justice, the Ministry of Digital Governance has put cybersecurity at the centre of its focus as it moves into the second phase of digitisation of its services. At the same time, the implementation of the single CRM of the public sector is also starting. The single digital infrastructure that will be created will integrate and host all digital services, existing, new and redesigned, so that citizens and businesses can carry out a significant part of their transactions with the Public Administration electronically.

Initiative II: Cooperation with other countries

Cooperation with third countries will help us to exchange ideas, views, technologies so that we can integrate practices and adopt strategies that will help us:

- Finding the right people in roles that are in high demand in the labour market.
- Acquiring skills to meet the challenges ahead (cutting-edge technologies such as fifth generation networks (5G), Artificial Intelligence (AI) and the Internet of Things (IoT)). Due to the above challenges and threats, Greece, as a member of the European Union, must actively participate in the processes of building a common and high level of cybersecurity capabilities.

Other actions in the wider cybersecurity ecosystem

1. Contribution to the establishment of the European CyberSec Skills Academy.

   The Commission has launched a Cybersecurity Skills Academy to help increase the number of skilled cybersecurity professionals in the EU. The Cybersecurity Skills Academy aims to:

   - Increase the number of cybersecurity professionals, including the share of women in the field
   - Reduce the gap between the offer and demand of cybersecurity skills on the labour market
   - Provide the skills needed to meet cybersecurity legal and policy requirements at EU or national level
   - Improve comparability, quality assurance, and certification of cybersecurity skills
   - Improve the visibility and synergies between public and private initiatives on cybersecurity skills
   - Equip citizens with in-demand cybersecurity skills

2. Increase starting salary and competitive pay package for public sector salaries in cybersecurity responsibility positions - security and damage prevention pay off. Salaries to reach a level that attracts young scientists (give incentives) to join and staff start-ups such as the National Cyber Security Authority.

3. Better use of digital technologies such as cloud, digital signatures, software solutions etc.

4.1 Education and Training

This subsection sets out the objectives and proposed initiatives and activities to be undertaken in the field of education and training. In the following text we will briefly and concisely present these initiatives with their specific activities.

Initiative III: Development of a Standardised Cybersecurity Curriculum

Objective: Identify core skills and industry requirements to develop a baseline curriculum. Establish a cohesive cybersecurity curriculum across all levels of education to ensure foundational and advanced cybersecurity knowledge.

Activity 1 (Duration: 2 - 5 years)

Activity 1.1: The survey conducted in 2024 under deliverable D2.2 "Cybersecurity Skills Needs Analysis" to identify current and emerging skills needs, using a questionnaire distributed to organisations with cybersecurity skills needs, will be repeated. The goal is to update the roles and skills needed. The updated data will be used to better design the actions to reduce the gap.

Activity 1.2: Throughout the project's duration, various actions will facilitate the establishment of an observatory. This observatory will monitor and analyse market changes, ensuring the ability to track trends over time. The insights and findings from these surveys will be regularly shared with the hub to inform and guide decision-making.

Activity 2 (Duration: 2 - 5 years)

Activity 2.1: The findings from the deliverable D2.2 "Cybersecurity Skills Needs Analysis" and the update from the new survey will be discussed with representatives from the Ministry of Education, Religious Affairs and Sports. CyberHub's proposals for the establishment of MSc Cybersecurity and BSc Cybersecurity degrees will be discussed and needed actions will be scheduled.

Activity 2.2: Collaborate with educational institutions to integrate cybersecurity content into secondary, vocational, and university programmes.

Activity 3 (Duration: 5+ years)

Activity 3.1: Establish MSc and BSc Cybersecurity degree programmes that aim to expand the pool of cybersecurity specialists, helping to address the growing demand and better balance the supply in the market.

Activity 3.2: Periodically review and update curriculum content to reflect technological advancements and evolving threats.

Responsible Parties: Ministry of Education, academic institutions, industry representatives, curriculum development experts

Resources Required: Funding for curriculum development, academic partnerships, industry consultants

Initiative IV: Cybersecurity Awareness and Public Education Campaign

Objective: Enhance cyber literacy among the general population and non-IT professionals to build a baseline of cybersecurity awareness.

Activity 1: Launch a public awareness campaign on cybersecurity best practices, targeting various demographics.

Activity 2: Organize community workshops and information sessions to promote basic cybersecurity knowledge.

Activity 3: Develop online resources, such as videos and articles, to be distributed through media channels.

Timeline: 2 years

Responsible Parties: Ministry of Education, public relations firms, cybersecurity experts, community organisations

Resources Required: Media partnerships, digital content production, public relations staff

Initiative V: Expansion of Flexible Learning and Certification Programmes

Objective: Increase accessibility to cybersecurity education through online courses, modular certifications, and flexible learning options. Provide scholarships (covering tuition fees or offering job guarantees) to postgraduate and doctoral students from the private sector, with a commitment to employment upon graduation.

Activity 1: Establish partnerships with SEPE member companies to encourage and financially support employees in attending part-time postgraduate courses or pursuing corporate cybersecurity certifications. Companies will cover tuition fees or sponsor certification programmes.

Activity 2: Collaborate with online learning platforms and industry organisations to offer a variety of cybersecurity certification courses tailored to different skill levels. Offer part-time postgraduate courses sponsored by companies, where employees receive corporate cybersecurity certifications (e.g., ISACA, ISC2, Cisco, Fortinet, Microsoft), enhancing their qualifications while continuing to work.

Activity 3: Develop micro-credential programmes to enable students and professionals to upskill in specific cybersecurity domains.

Activity 4: Promote certification and learning programmes to employers for continuous employee training.

Timeline: 2 years

Responsible Parties: Academic institutions, online education providers, industry partners, Ministry of Education

Resources Required: Online learning platforms, instructional design resources, industry sponsorships

4.2 Industry Partnerships

This subsection sets out the objectives and proposed initiatives and activities to be undertaken in the field of industry partnerships. In the following text we will briefly and concisely present these initiatives with their specific activities.

Initiative VI: Public-Private Internship and Apprenticeship Programme

Objective: Bridge the skills gap by providing practical cybersecurity experience through collaborative internship programmes.

Activity 1: Establish partnerships with industry to define internship requirements and scope. EU funding and supply from business but also from SoC and ENISA - priority for postgraduate students and 4-year undergraduates (senior undergraduates)

Activity 2: Establish a working group withing the CyberHub to plan internships. All shareholders will offer internship opportunities. In addition, barriers will be identified, and solutions will be proposed. Develop an internship placement programme in collaboration with academic institutions, allowing students to earn credit.

Activity 3: Monitor and evaluate the internship programme to ensure alignment with industry needs and update as necessary through the established observatory.

Timeline: 2-3 years

Responsible Parties: Industry partners, Ministry of Education, academic institutions, internship coordinators

Resources Required: Funding for internship stipends, programme coordinators, industry mentors

4.3 Research and Development

This subsection sets out the objectives and proposed initiatives and activities to be undertaken in the field of research and development. In the following text we will briefly and concisely present these initiatives with their specific activities.

Initiative VII: Targeted Research & Development funding

Targeted EU and public funding on research and technological development. It is through research that innovation is born and especially in the field of cybersecurity this is particularly important. R&D policy should be a multi-annual framework programme setting out the set of objectives, priorities and financial support. Innovation is playing an increasingly important role in our economy. As well as benefiting EU consumers and workers, it is essential for creating better jobs, building a greener society and improving our quality of life. It is also crucial to maintaining the EU's competitiveness in global markets.

Initiative VIII: National Cybersecurity Threat Intelligence Platform

Objective: Establish a centralised threat intelligence-sharing platform to enable real-time collaboration between public and private sectors.

Activity 1: Design and launch a secure platform for sharing threat intelligence and incident data.

Activity 2: Create guidelines and protocols to ensure data privacy and security in threat-sharing practices.

Activity 3: Promote platform usage among critical infrastructure operators and industry partners.

Timeline: 5+ years

Responsible Parties: National cybersecurity agencies, private sector IT security teams, regulatory bodies

Resources Required: Platform development funding, cybersecurity infrastructure, data privacy legal consultants

4.4 Conclusions

These high-level initiatives provide a structured roadmap for implementing the cybersecurity skills strategy, ensuring that efforts remain aligned with the broader vision. Each initiative directly supports strategic objectives, creating a cohesive approach to addressing current cybersecurity workforce challenges.

5 Evaluation and Monitoring

Effective monitoring and evaluation are essential to ensure that planned initiatives and activities achieve the goals of the Cybersecurity Skills Strategy. Oversight will be provided by a designated CyberHub Monitoring Committee, which includes representatives from government, industry partners, academic institutions, and relevant stakeholders. This committee will monitor progress, review data, and make recommendations to ensure alignment with the broader strategic goals.

5.1 Metrics and Monitoring

The achievement of each objective will be evaluated using **Key Performance Indicators (KPIs)** specific to each initiative, which may include metrics such as participation rates, curriculum adoption rates, internship completion rates, and levels of public engagement in awareness programmes. The CyberHub Monitoring Committee will compile periodic reports to assess progress against these KPIs, allowing for timely adjustments as necessary.

Key Performance Indicators (KPI)

Initiative III: Development of a Standardised Cybersecurity Curriculum

KPI-III-1: Number of educational institutions adopting the curriculum

KPI-III-2: Curriculum completion rates and student enrolment in cybersecurity courses

KPI-III-3: Feedback from industry and educational institutions on curriculum relevance

Initiative IV: Cybersecurity Awareness and Public Education Campaign

KPI-IV-1: Engagement levels across different demographic groups

KPI-IV-2: Public awareness metrics, such as survey-based cybersecurity knowledge assessments

KPI-IV-3: Feedback from participants in workshops and online campaigns

Initiative V: Expansion of Flexible Learning and Certification Programmes

KPI-V-1: Enrollment in online and certification programmes

KPI-V-2: Completion and certification rates

KPI-V-3: Participant feedback on programme accessibility and relevance

Initiative VI: Public-Private Internship and Apprenticeship Programme

KPI-VI-1: Number of internships/apprenticeships offered and completed

KPI-VI-2: Placement rates for interns within cybersecurity roles

KPI-VI-3: Employer satisfaction with intern performance and skills

Initiative VIII: National Cybersecurity Threat Intelligence Platform

KPI-VII-1: Number of organisations actively participating on the platform

KPI-VII-2: Response times to cyber incidents, as measured by data from the platform

KPI-VII-3: Frequency and relevance of actionable intelligence generated from shared data

The **CyberHub Monitoring Committee** will regularly review these KPIs to assess the success and impact of each initiative and activity, identifying areas for improvement as necessary.

5.2 Continuous Improvement

The cybersecurity landscape is rapidly evolving, and CyberHub's initiatives must adapt to changes in technology, industry requirements, and emerging threats. To respond to these changes, the CyberHub Oversight Committee will conduct annual reviews to assess the continued relevance of the Action Plan's activities and KPIs.

In response to significant changes - such as shifts in cyber threat types, new technological advances, or regulatory updates - both initiatives and KPIs may be revised to reflect the new context.

If an initiative or activity fails to meet its KPIs for two consecutive review periods, the committee will initiate an evaluation to determine whether adjustments are needed. This may include refining programme content, reallocating resources, or changing timelines to improve effectiveness. Feedback from participants and stakeholders will play a critical role in guiding these adjustments.

5.3 Conclusions

The Action Plan provides a structured, adaptive approach to building a resilient cybersecurity workforce in Greece. Through close monitoring and targeted KPIs, the CyberHub Monitoring Committee will ensure that each initiative meets its objectives and contributes to the overall strategy. Continuous improvement mechanisms allow for flexibility to adapt to emerging cybersecurity trends, ensuring the strategy remains effective and relevant over time.

Key takeaways include:

- A clear, measurable roadmap for closing the cybersecurity skills gap.
- Strong collaboration among the public and private sectors, academia, and government to ensure an aligned and relevant strategy.
- An adaptable framework that allows for adjustments based on continuous feedback and evolving threats.

The successful implementation of this action plan will enable Greece to build a robust, skilled cybersecurity workforce that can effectively protect the country's digital infrastructure.

6 Conclusions

The Greek Cybersecurity Skills Strategy represents a transformative approach to address the nation's urgent cybersecurity challenges. Grounded in a detailed analysis of the existing skills landscape and market demands, this strategy offers a cohesive framework for building a skilled workforce, fostering collaboration, and strengthening the country's overall resilience against cyber threats. The vision is clear: to align education, training, and innovation with national and European objectives, ensuring Greece's cybersecurity capabilities evolve in tandem with the rapidly changing digital environment.

At the heart of this strategy lies the commitment to workforce development. By bridging the gap between the supply and demand of cybersecurity professionals, the strategy emphasises both short-term and long-term solutions. Initiatives such as integrating cybersecurity into all levels of education, expanding flexible learning opportunities, and developing advanced training and certification programmes reflect a focus on adaptability and inclusivity. These efforts are designed to empower students, professionals, and organisations with the tools they need to thrive in a digital-first world.

Collaboration across public and private sectors is another cornerstone of the strategy. By fostering partnerships among academia, government, and industry, Greece is creating an ecosystem where innovation and resource-sharing drive progress. Programmes like public-private internships, research initiatives, and the establishment of a cybersecurity center of excellence will help sustain and expand these efforts. Private sector engagement, including financial support for training and certifications, ensures that these partnerships are mutually beneficial and sustainable.

Public awareness and education also play a critical role in the strategy's success. Cybersecurity is no longer the sole responsibility of IT professionals—it is a societal challenge that requires broad engagement. Through targeted campaigns and community-driven initiatives, the strategy aims to foster a culture of cyber awareness that extends to every level of society, reducing vulnerabilities and strengthening national defense.

The implementation of this strategy is guided by a robust action plan, with initiatives categorised into short-term, medium-term, and long-term goals. This phased approach ensures that progress is measurable and responsive to changing needs. Continuous monitoring and evaluation, supported by clear Key Performance Indicators (KPIs), provide a feedback loop to refine and optimise efforts over time. This adaptability ensures that Greece remains prepared for both current and emerging cybersecurity threats.

Ultimately, the Greek Cybersecurity Skills Strategy is not just about addressing immediate needs—it is a forward-looking blueprint for national resilience and growth. By investing in skills, education, and partnerships, Greece is positioning itself as a leader in the European cybersecurity landscape. The success of this strategy will not only safeguard critical infrastructure and digital assets but also contribute to economic growth, societal trust in digital systems, and the nation's global competitiveness.

With a strong foundation, clear objectives, and a commitment to collaboration, Greece is well-equipped to meet the challenges of an increasingly interconnected and complex digital future. This strategy reflects a collective vision for a secure, innovative, and resilient nation, ensuring that Greece remains at the forefront of global efforts to combat cyber threats.

References

1. ENISA. (2024). Foresight Cybersecurity Threats for 2030 (update), https://www.enisa.europa.eu/ news/skills-shortage-and-unpatched-systems-soar-to-high-ranking-2030-cyber-threats

2. SEPE - Deloitte. (2024). Evaluation of the Proficiency of ICT Specialists in Greece. https://www.sepe.gr/research-studies/21142064/meleti-sepe-deloitte-apotimisis-eparkeias-eidikon-tpe-stin-ellada/

3. Fortinet. (2024). State of Operational Technology and Cybersecurity Report, https://www.fortinet.com/re-sources/reports/state-of-ot-cybersecurity

4. ISC2. (2024). Cybersecurity Workforce Study, https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

5. NIS2. (2024). Directive. https://nis2directive.eu/

6. ENISA. (2024). Navigating cybersecurity investments in the time of NIS 2, https://www.enisa.eu-ropa.eu/news/navigating-cybersecurity-investments-in-the-time-of-nis-2

7. DORA. (2023). Digital Operational Resilience Act, https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

8. Ministry of Digital Governance.(2018). LAW NUMBER, 4577/2018., https://mindigital.gr/wp-content/up-loads/2019/09/N.4577_2018.pdf

9. Ministry of Digital Governance.(2019). Ministerial Decision 1027/2019, https://mindigital.gr/wp-content/up-loads/2020/01/3739B-19-1.pdf

10. Law 5160/2024. (2024). National Printing House, https://search.et.gr/el/fek/?fekId=774154

11. ENISA. (2022). ECSF Part 1: 12 Cybersecurity Professional Role Profiles, https://www.enisa.europa.eu/publica-tions/european-cybersecurity-skills-framework-role-profiles

12. ENISA. (2022). European Cybersecurity Skills Framework (ECSF) - User Manual, https://www.enisa.eu-ropa.eu/publications/european-cybersecurity-skills-framework-ecsf

13. CyberHubs. (2024). Cybersecurity Skills Needs Analysis report Greece, https://cyberhubs.eu/wp-content/up-loads/2024/10/Greece_Cybersecurity-Skills-Needs-Analysis-Report.pdf

CyberHubs

European Network of Cybersecurity Skills Hubs

info@cyberhubs.eu | cyberhubs.eu

Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.