



CyberSecPro

CYBERSECURITY PRACTICAL SKILLS GAPS IN EUROPE REPORT

x



IMPORTANT NOTE

This is a pre-publication of the report and has not been reviewed by the European Commission yet.



Co-funded by
the European Union



D2.1

Cybersecurity Practical Skills Gaps in Europe: Market Demand and Analyse

Document Identification	
Due date	30 April 2023
Submission date	02 May 2023
Version	1.0

Related WP	WP2	Dissemination Level	PU - Public
Lead Participant	LAU, GUF, IMT, TALTECH	Lead Author	Paresh Rathod Paulinus Ofem Nineta Polemi Timo Hynninen Ricardo Gregorio Lugo Cristina Alcaraz Kitty Kioskli Kai Rannenberg
Contributing Participants	LAU, GUF, IMT, TALTECH, TUBS, TUC, TRUSTILIO, UCY, UMA, AIT, CNR, COFAC, SINTEF, UNI, UPRC, ACEEU, APIRO, FP, ITML, MAG, SLC, FCT	Related Deliverables	D2.2 – Blended CyberSecPro technological training interactive technologies and academic practice D2.3 – CyberSecPro Programme Specifications



Abstract: The CyberSecPro Deliverable D2.1 report investigates the cybersecurity practical skills gaps in Europe and analyses the market demand for these skills. The report acknowledges that a complete list of cybersecurity practical skills can be complex and interpreted differently by EU nations and organisations. For that reason, the report combines them into a list of cybersecurity practical knowledge areas and highly essential practical skills. The deliverable also aims at the market driven and practitioner's approach, therefore, adopted development methodology combines the practical and applied research, including an integrated research model. This deliverable captures the cybersecurity skill sets needed by the markets, the practical skills offered in the EU academic programmes and the gaps between demand and supply of practical skills. Special attention will be given to the three industrial sectors: health, energy and maritime. The deliverable reflects the outcomes of tasks T2.1 and T2.2.



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 Health and Digital Executive Agency (HADEA). Neither the European Union nor the European Health and Digital Executive Agency (HADEA) can be held responsible for them.

This document is issued within the CyberSecPro project. This project has received funding from the European Union's DIGITAL-2021-SKILLS-01 Programme under grant agreement no. 101083594. This document and its content are the property of the CyberSecPro Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license to the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the CyberSecPro Consortium and are not to be disclosed externally without prior written consent from the CyberSecPro Partners. Each CyberSecPro Partner may use this document in conformity with the CyberSecPro Consortium Grant Agreement provisions and the Consortium Agreement.

The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.



Executive Summary

The Cybersecurity Deliverable D2.1 report presents the cybersecurity skills gaps in Europe. The report provides valuable Analyses, insights, market needs and potential solutions by identifying the market-demanded cybersecurity knowledge areas and skills. It further provides insights on the potential solutions to consolidate European cybersecurity workforce capacity-building efforts. The report acknowledges that a comprehensive list of cybersecurity skills can be complex and interpreted differently by EU nations and organisations. Besides, European Cybersecurity Skills Framework (ECSF) provides the key European cybersecurity skills list. Therefore, the report combines them into a list of cybersecurity knowledge areas and essential skills to provide valuable insights and outcomes. The outcome is represented as the cybersecurity practical skills gap in Europe.

Development work and methodology: In order to achieve Deliverable D2.1, the project adopted practical and applied research methodologies, including quantitative and qualitative research methods. The integration and implementation of these methods enabled to:

- Conduct desk research that majorly followed a general and systematic literature review strategy—for instance, analyses of cybersecurity frameworks, knowledge areas and skills offered by European academic programmes.
- Conduct a cybersecurity market demand survey with industry professionals as respondents.
- Collect and analyse data from workshops and seminars from experts including industry participants.

This development work was conducted under tasks ‘T2.1: Cybersecurity Market Skills and Competencies Analysis’ and ‘T2.2: Practical cybersecurity skills offered in EU Academic Programs’ of CyberSecPro. One of the primary goals of both tasks is to analyse the current state of the art of European cybersecurity workforce skills demands and supply ecosystem, including existing cybersecurity tools. Therefore, the project identifies cybersecurity market demand skills and skills offered by EU academic programmes.

Findings and outcomes: Based on a mapping between skills demand and supply, this development work found a significant cybersecurity skills gap in Europe. The study also identified knowledge areas and highly essential skills in demand for the health, energy, and maritime sectors. The analysis of existing cybersecurity tools is beyond this deliverable. The main work and findings from this deliverable are as follows.

- Identified more than 25 essential practical knowledge areas for the health, energy, maritime, ICT and other sectors.
- More than 25 top practical skills in demand were identified for the health, energy, maritime, ICT and other sectors.
- Analyses of European cybersecurity higher education programmes (supply side); and
- Report on the cybersecurity practical skills gaps in Europe - listing of the essential cybersecurity practical skills needed in Europe.

The practical cybersecurity skills offered in EU academic programmes analysis confirmed that the demand for skilled professionals outpaces the supply of cybersecurity professionals. The results also suggest a significant gap in essential cybersecurity skills. Based on the results, the following recommendations are proffered to address the cybersecurity skills gap.

- Boost the transformation of higher education programmes to address market demand and increase investment in cybersecurity education and training.
- Encourage effective dissemination and implementation of the European Cybersecurity Skills Framework (ECSF) and consolidate the cybersecurity workforce training programme.



- Encourage collaboration between educators and industry experts for cybersecurity skilling, upskilling and reskilling of educators/trainers and professionals; and
- Promote collaboration between academia, industry, government, and other stakeholder in developing cybersecurity talent and workforce.

Conclusion: This CyberSecPro deliverable D2.1 report provides valuable insights into the current state of cybersecurity skills in Europe. This deliverable captures the cybersecurity skill sets needed by the markets, the practical skills offered in the EU academic programmes and the gaps between demand and supply of practical skills. Special attention will be given to the three industrial sectors: health, energy and maritime. The deliverable reflects the outcomes of tasks T2.1 and T2.2.



Document information

Contributors

Name	Partner
Paresh Rathod, Paulinus Ofem, Nineta Polemi, Timo Hynninen, Ricardo Gregorio Lugo, Kitty Kioskli, Theodoros Karvounidis, Antonis Spatharos, Kai Rannenberg, Christos Douligieris, Cristina Alcaraz, Luís Miguel Campos, Nikos Nikolaou, Per Håkon Meland, Ricardo Lugo, Ahad Niknia, Ann-Kristin Lieberknecht, Spiros Borotis, Jyri Rajamäki, Pasi Kämppi, Jari Räsänen, Jari Savolainen, Rauno Pirinen, Ilkka Tikanmäki, Harri Ruoslahti, Veli Sulkava, Eveliina Hytönen, Javier Lopez, Rubén Ríos del Pozo, Carmen Fernández, Nikos Nikolaou, Elias Athanasopoulos, Narges Arastouei, Frederic Tronnier, Fabio Martinelli, Nuno Mateus-Coelho, Gregor Langner, Stella Markopoulou, Bruno BENDER	LAU, GUF, IMT, TALTECH, TUBS, TUC, TRUSTILIO, UCY, UMA, AIT, CNR, COFAC, SINTEF, UNI, UPRC, ACEEU, APIRO, FP, ITML, MAG, SLC, FCT

Reviewers

Name	Partner
Christos Douligieris	UPRC (Technical Manager)

History

Version	Date	Authors	Comment
0.01	2023-02-20	Paresh Rathod, Nineta Polemi, Paulinus Ofem, Timo Hynninen, Ricardo Gregorio Lugo, Nikos Nikolaou	1st Draft of ToC
0.02	2023-02-28	Nineta Polemi, Chatzopoulou Argyro, Cristina Alcaraz, Luís Miguel Campos, Nikos Nikolaou, Per Håkon Meland, Ricardo Gregorio Lugo, Ahad Niknia, Ann-Kristin Lieberknecht, Spiros Borotis, Kai Rannenberg, Theodoros Karvounidis, Christos Douligieris, Antonis Spatharos	High-level review and comments on ToC
0.03	2023-03-15	Paresh Rathod, Paulinus Ofem, Timo Hynninen, Ricardo Gregorio Lugo	Consolidated ToC
0.04	2023-03-20	Paulinus Ofem, Timo Hynninen, Nineta Polemi, Paresh Rathod, Ricardo Lugo, Theodoros Karvounidis, Ann-Kristin Lieberknecht	Review of the structure and consolidation between D2.1, D2.2 and D2.3.
0.05	2023-04-03	Paulinus Ofem, Timo Hynninen, Cristina Alcaraz, Nineta Polemi, Paresh Rathod, Ricardo Lugo, Theodoros Karvounidis, Ann-Kristin Lieberknecht, Kitty Kioskli, Chatzopoulou Argyro, Herve Debar, Antoni Spatharos, T. Karvounidis, C. Douligieris	Early Draft



0.06	2023-04-20	Same as the contributors listed above	Draft review (partners) and consolidation
0.07	2023-04-21	Paresh Rathod, Paulinus Ofem, Nineta Polemi, Timo Hynninen, Ricardo Gregorio Lugo, Cristina Alcaraz	Editorial and images updates
0.08	2023-04-25	Paresh Rathod, Paulinus Ofem, Nineta Polemi, Timo Hynninen	Editorial improvements
0.09	2023-04-26	Narges Arastouei, Atiyeh Sadeghi	Check and preliminary preparation for submission
0.10	2023-04-30	Paresh Rathod	Improvements after discussion at WP 2 meeting on 2023-04-28/29
0.11	2023-05-01	Kai Rannenberg	Further improvements (Section 2.3.9) after discussion at WP 2 meeting on 2023-04-28/29
0.12	2023-05-01	Paresh Rathod	Final improvements with survey images and chapter 4.
1.0	2023-05-02	Ahad Niknia	Final check, layout correction and refinement and submission process



Table of Contents

Document information	v
1 Introduction	1
1.1 Background	1
1.2 Scope	2
1.2.1 Relationship with Other Work Packages	2
1.2.2 Purpose and Objective.....	2
1.3 Methodology and Development Process	3
1.3.1 Research Methodology:	3
1.3.2 Development Process	4
1.3.3 Desk Research, Literature Review and Expert Inputs	4
1.3.4 Market Demand Survey: Practitioner’s Approach.....	5
1.4 Structure of the Report	5
2 Cybersecurity Skills Framework and Relevant Initiatives	6
2.1 International and Non-EU Cybersecurity Skills Frameworks	6
2.1.1 National Initiative for Cybersecurity Education (NICE) Framework.....	6
2.1.2 ACM, IEEE, AIS SIGSEC, IFIP Cybersecurity Curricula Guidelines (CSEC2017)	8
2.1.3 Singaporean Cybersecurity Skills Framework.....	10
2.1.4 Australian Cybersecurity Skills Framework	10
2.1.5 Canadian Cybersecurity Skills Framework.....	12
2.1.6 Saudi Arabian Cybersecurity Skills Framework.....	16
2.1.7 Indian Cybersecurity Skills Framework.....	18
2.2 EU-Based Cybersecurity Skills Frameworks and Development Work	21
2.2.1 ENISA European Cybersecurity Skills Framework (ECSF)	21
2.2.2 JRC European Cybersecurity Centres of Expertise Map	23
2.2.3 Cybersecurity Body of Knowledge (CyBOK)	24
2.2.4 European e-Competence Framework (e-CF)	25
2.2.5 European Skills, Competencies, Qualifications and Occupations (ESCO)	26
2.2.6 European Cybersecurity Organisation Working Group (ECISO)	27
2.2.7 ECHO Cybersecurity Skills Framework (ECHO-CSF).....	28
2.2.8 Cybersecurity cOmpeteNce fOr Research and InnovAtion (CONCORDIA).....	30
2.2.9 Cybersec4Europe	32
2.2.10 Strategic Programmes for Advanced Research and Technology in Europe (SPARTA).....	33
2.2.11 REWIRE Cybersecurity Skills Framework	34



2.3	EU and Member States: Notable Cybersecurity Strategies, Guidelines and Directives	38
2.3.1	EU Member State Initiatives: Austria	38
2.3.2	EU Member State Initiatives: Belgium	40
2.3.3	EU Member State Initiatives: Cyprus	44
2.3.4	EU Member State Initiatives: Czech Republic	47
2.3.5	EU Member State Initiatives: Denmark.....	49
2.3.6	EU Member State Initiatives: Estonia.....	51
2.3.7	EU Member State Initiatives: Finland.....	54
2.3.8	EU Member State Initiatives: France.....	58
2.3.9	EU Member State Initiatives: Germany.....	59
2.3.10	EU Member State Initiatives: Greece	61
2.3.11	EU Member State Initiatives: Italy	63
2.3.12	EU Member State Initiatives: Netherlands	64
2.3.13	EU Member State Initiatives: Norway.....	66
2.3.14	EU Member State Initiatives: Spain.....	70
2.3.15	Summary- European National Cybersecurity Initiatives	73
2.4	Private Sector Cybersecurity Workforce Development Initiatives	74
2.4.1	SANS Institute	74
2.4.2	ISACA.....	75
2.4.3	Information Systems Security Certification Consortium (ISC) ²	76
2.4.4	Summary- Private Sector Cybersecurity Skills Initiatives	78
3	Cybersecurity Workforce Analyses: Market Demands.....	79
3.1	Goal of the Market Analysis Survey.....	79
3.2	Methodology	79
3.3	Structure and Lifecycle CSP Survey	80
3.4	Cybersecurity Market Survey Results	81
3.4.1	Respondents and data.....	81
3.4.2	Cybersecurity job roles	82
3.4.3	Knowledge areas	83
3.4.4	Hands-on skills.....	84
3.5	Discussion.....	86
3.5.1	Cybersecurity Skills Required in the Health, Energy, and Maritime Sectors	86
3.5.2	Cybersecurity Skills for the Health Sector.....	87
3.5.3	Cybersecurity Skills for the Energy Sector.....	87
3.5.4	Cybersecurity Skills for the Maritime Sector.....	88
4	Cybersecurity Practical Skills Gaps in Europe: Analyses and Prioritisation	89



4.1	The Market Demand Side: Essential Cybersecurity Practical Skills.....	89
4.1.1	Cybersecurity Skills Demand Prioritisation Criteria:	89
4.1.2	The Sectoral Specific Cybersecurity Knowledge Area Prioritisation: Health, Energy, Maritime, ICT and Others	91
4.1.3	The Sectoral Specific Cybersecurity Hands-on Skills Prioritisation: Health, Energy, Maritime, ICT and Other.....	93
4.2	The Market Supply Side: Analyses of Practical Cybersecurity Skills Offered in EU Academic Programmes.....	94
4.2.1	ENISA/CyberHEAD: Analyses of the European Cybersecurity Education Roadmap..	94
4.2.2	Cybersec4Europe: Analyses of the European Academic Offering	96
4.2.3	CONCORDIA: Analyses of the European Academic Offering	97
4.2.4	JRC Atlas: Analyses of Cybersecurity Knowledge Areas	102
4.2.5	Mapping of Market Demand Skills with Knowledge Areas in Mandatory HEIs Courses	104
4.3	Cybersecurity Practical Skills Gaps in Europe: Main findings.....	109
4.3.1	Progress Beyond the State of The Art (BSOTA).....	109
4.3.2	European Cybersecurity Framework Workforce Roles: Sectoral Specific Mapping ..	109
4.3.3	Final Outcomes and Result: Cybersecurity Practical Skills Gap in Europe	111
4.3.4	Summary	115
5	Recommendation and Pointers for CyberSecPro Programme Specification	116
5.1	Cybersecurity Practical Skills: Market Demand and Recommendation.....	116
5.2	Cybersecurity Higher Education Programmes and Recommendations	118
5.3	Conclusion of the CyberSecPro D2.1 report.....	120
	References	121
	Annex A: Market analysis survey.....	132
	Annex B: Analyses work.....	141



List of Figures

Figure 1: CyberSecPro D2.1 Development Methodology [40]	3
Figure 2: CyberSecPro Practical Skills Gaps in Europe: Development Work Process	4
Figure 3: NICE Framework	7
Figure 4: Cybersecurity Career Paths [21].....	11
Figure 5: Saudi Arabia- SCyWF Cybersecurity Taxonomy [26].....	15
Figure 6: DSCI Cybersecurity Career Map [27].....	19
Figure 7: European Cybersecurity Skills Framework Principles [29]	21
Figure 8: European Cybersecurity Skills Framework: Job Profiles [29]	22
Figure 9: JRC Cybersecurity Taxonomy.....	23
Figure 10: European Cybersecurity Body of Knowledge (CyBOK) Clusters [35]	25
Figure 11: ECSO Market Demanded Cybersecurity Domains [40]	27
Figure 12: ECHO Cybersecurity Framework	29
Figure 13: Austria- Operative Coordination Structure.....	39
Figure 14: Cybersecurity Defence-in-depth approach of Greece	62
Figure 15: SANS Cybersecurity Roadmap Summary [125].....	74
Figure 16: CyberSecPro Market analysis survey	80
Figure 17: Respondent’s Types of the Organisation.....	82
Figure 18: ENISA CyberHEAD: European Cybersecurity Higher Education Programme Summary ..	95
Figure 19: CONCORDIA’s Five Pillars of Education Roadmap	97
Figure 20: CyberSecPro: Cybersecurity Skills Gaps in Europe.....	115



List of Tables

Table 1 : Summary of NICE Framework Classification.....	7
Table 2 : ASD-CSF Disciplines and Roles	12
Table 3 : ASD-CSF Disciplines and Roles	13
Table 4: Core C-CSF Roles and Competencies.....	14
Table 5: Summary of SCyWF.....	16
Table 6: Summary of DSCI cybersecurity framework	19
Table 7: ESCO Cybersecurity Occupations.....	26
Table 8: Sample Knowledge and Skills for Identity Module.....	30
Table 9: CONCORDIA’s Reports on Key Deliverables.....	31
Table 10: CyberSec4Europe Work Package 6 Deliverables.....	32
Table 11: Knowledge Adaptation of NICE CSF to EU Legal Landscape	34
Table 12: Cybersecurity Roles Adaptation of NICE CSF to EU Legal Framework	35
Table 13: REWIRE Cybersecurity Skills Recommended Changes.....	36
Table 14: REWIRE Cybersecurity Knowledge and Competencies Recommended Changes	37
Table 15 : Summary of CNQFC Work Role Categories and Specialisations.....	48
Table 16 : Summary of CNQFC Investigations Work Role Category and Work Roles.....	48
Table 17: ISACA Key Certification Areas	75
Table 18: Cybersecurity Job Roles Needed in the Industry (Distinguished in the Survey).....	82
Table 19: Cybersecurity Knowledge Areas in Demand.....	83
Table 20: Cybersecurity Hands-on Skills in Demand.....	85
Table 21: Cybersecurity Knowledge Areas and Hands-on Skills in Demand (Combined List from the Survey Results)	90
Table 22: Knowledge Area Prioritisation for All Sectors.....	92
Table 23: Hands-on Skills Prioritisation for All Sectors	93
Table 24: Summary of Cybersecurity Academic Offerings Based on Job Roles	95
Table 25: Summary of CONCORDIA Analysed Academic Offerings	98
Table 26: Summary of Knowledge Areas from EU Academic Programmes	102
Table 27: Mapping of Market Skills with HEI Skills for Mandatory Cybersecurity Courses.....	104
Table 28: Mapping ECSF Job Role with Academic Offerings in Each Sector	110
Table 29: Comprehension of Cybersecurity Practical Skills Names	111
Table 30: Cybersecurity Practical Skills Gaps in Europe	114



List of Acronyms

A	ACM	Association for Computing Machinery
	AI	Artificial Intelligence
	AIA	Artificial Intelligence Act
	API	Application Programming Interface
	APT	Advanced Persistent Threat
	ATO	Account Take Over
B	BCMS	Business Continuity Management System
	BYOD	Bring Your Own Device
C	CA	Contract Agent
	CC	Computing Curricula
	CCN	Competence Centers Network, Cyber Competence Network
	CCPA	California Consumer Privacy Act
	CDO	Chief Data Officer
	CE	Computer Engineering
	CERT	Computer Emergency Response Team
	CI	Critical Infrastructures
	CISO	Chief Information Security Officer
	CISSP	Certified Information Systems Security Professional
	CMMC	Cybersecurity Maturity Model Certification
	CNI	Critical National Infrastructure
	COTS	Commercial Off-the-shelf
	CR	Cyber Range
	CS	Compute Science
	CSCL	Computer-Supported Collaborative Learning
	CSIRT	Computer Security Incident Response Team
	CSO	Chief Security Officer
	CSP	Cloud Service Provider
	CSR	Corporate Social Responsibility
	CWA	Common Weakness Enumeration
	CyPR	Cybersecurity Professional Register
D	DDoS	Distributed Denial of Service
	DigCompEdu	European Framework for the Digital Competence of Educators
	DPA	Data Protection Act, Data Protection Authority
	DPI	Deep Packet Inspection
	DPO	Data Protection Officer
	DRaaS	Disaster Recovery as a Service



E	ECHO-CSF	ECHO Cybersecurity Skills Framework
	ECSF	European Cybersecurity Skills Framework
	EDR	Endpoint Detection and Response
	E-MAF	ECHO Multi-Sector Assessment Framework (previously E-MSAF)
	EMEA	Europe, Middle East, and Africa
	ENISA	European Union Agency for Cybersecurity
	E2EE	End-to-end encryption
F	FNC	Foro Nacional de Ciberseguridad
G	GA	Grant Agreement
	GDPR	General Data Protection Regulation
	GRC	Governance, Risk, and Compliance
H	HIPAA	Health Insurance Portability and Accountability Act
I	IaaS	Infrastructure as a Service
	ICT	Information and communications technology
	IEC	International Electrotechnical Commission
	IEEE	Institute of Electrical and Electronics Engineers
	IIoT	Industrial Internet of Things
	INCIBE	Instituto Nacional de Ciberseguridad
	IoT	Internet of Things
	IPS	Intrusion Prevention System
	ISO	International Organization for Standardization
J	JTF	Joint Task Force
	JRC	Joint Research Committee
K	KA	Knowledge Area
	KPI	Key Performance Indicator
	KSA	Knowledge, Skills, Abilities
	KU	Knowledge Unit
L	LEA	Law Enforcement Agency
	LGPD	Lei Geral de Proteção de Dados (General Data Protection Law)
M	MITRE	The MITRE Corporation
	MOOC	Massive Open Online Course
	MRCDD	Marco de Referencia de la Competencia Digital Docente
	MSSP	Managed Security Service Provider
	M2M	Machine to Machine
N	NAC	Network Access Control



	NCSC	National Cybersecurity Center
	NIS	Network and Information Security
	NIST	National Institute of Standards and Technology
	NIS2	Network and Information Security Directive
	NLP	Natural Language Processing
O	OEM	Open Educational Material
	OER	Open Educational Resource
	ONTSI	Observatorio Nacional de Tecnología y Sociedad
	OT	Operational Technology
P	PaaS	Platform as a Service
	PII	Personally Identifiable Information
	PKI	Public Key Infrastructure
	PoC	Proof of Concept
R	RAT	Remote Access Trojan
	RD	Real Decreto
	RDP	Remote Desktop Protocol
S	SaaS	Software as a Service
	SIEM	SIEM: Security Information and Event Management
	SOAR	Security Orchestration, Automation and Response
	SOC	SOC: Security Operations Center
	SQL injection	a type of injection attack that exploits vulnerabilities in SQL databases
	SSL/TLS	Secure Sockets Layer/Transport Layer Security
	SSO	Single Sign-On
	STIX	Structured Threat Information eXpression
T	TLS	Transport Layer Security
	TPM	Trusted Platform Module
	TTP	Tactic, Technique, and Procedure
	TTX	Tabletop Exercise
U	UEBA	User and Entity Behaviour Analytics
V	VPN	Virtual Private Network
W	WAF	Web Application Firewall
	WEP	Wired Equivalent Privacy
	WPA	Wi-Fi Protected Access
X	XSS	Cross-site Scripting



Glossary of terms: Generic and CSPro specific

A Generic Glossary of terms based on JRC, Taxonomy and glossary for Cybersecurity by European Commission

Link: <https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf>

C CSP training programme

will consist of training modules that can be offered individually or as a package; it will not lead to any certification or degree or career paths; it will be used to enhance existing training offers to close the gaps between academic training supply and marketing professional demands.

CSP training modules

comprises courses, mini-courses, lectures, cyber hands-on exercises, cyber hackathons, cyber mornings & events, cybersecurity games, red/blue team exercises, summer schools, workshops, ad-hoc sector-specific seminars, on-demand mini-technological courses, and crisis management training.

CSP syllabus

every training module will be accompanied by a syllabus that will include information like Learning Outcomes; Who should attend; Relative conventions and standards; Prerequisite competencies (skills & knowledge); Training module outline; List tools/access rights of tools, manuals, handbooks and handouts the delegates receive during the training; Training tools that will be used; Assessment methods; Exams; Study time (physical and online learning).

A standard template for a CSP syllabus will be finalised in D4.1 ('CyberSecPro Training Operational Plan'), and it will be used in all CSP training modules.

CSP training material

corresponds to all material that will be used by the educator/trainer to provide the CSP training module.

CSP sector-specific training modules

CSP training modules that will concentrate on the sectors of health, maritime, and energy. The modules will be shaped around real-life challenges in collaboration with the HEIs, companies and industries adapting their content and approach to the specific knowledge areas, and parametrizing the training tools and practical exercises accordingly.

CSP syllabus

every training module will be accompanied by a syllabus that will include information like Learning Outcomes; Who should attend; Relative conventions and standards; Prerequisite competencies (skills & knowledge); Training module outline; List tools/access rights of tools, manuals, handbooks and handouts the delegates receive during the training; Training tools that will be used; Assessment methods; Exam; Study time (physical and online learning).

A standard template for a CSP syllabus will be finalised in D4.1 and it will be used in all CSP training modules.



CSP knowledge areas

The knowledge areas listed were based on the CyBoK Skills Framework, JRC recommendation and mainly from the European Cybersecurity Organisation report based on industry-academia cooperation and development work. However, the project will be further aligned with the ECSF and the market Analyses outcomes.

CSP practical skill

The initial studies confirm the challenges of interpreting the knowledge areas, skills, and competencies differently across EU nations and organisations. Therefore, CSP D2.1 follows the guideline from the European Cybersecurity Skills Framework definition, “The demonstrated ability to apply knowledge, skills, and attitudes to achieve observable results”.

CSP competence

The initial studies confirm the challenges of interpreting the knowledge areas, skills, and competencies differently across EU nations and organisations. Therefore, CSP D2.1 follows the guideline from the European Cybersecurity Skills Framework definition, “The ability to carry out managerial or technical activities and tasks on a cognitive or practical level; knowing how to do it.”

CSP training tools

Training tools that will be used in the training of the CSP modules (the assessment of the various tools, selection and portfolio will occur in T.2.3).

CSP training format

CSP training format describes the way how modules will be provided OnDemand, Web-based, Live Online, In Person, Hybrid/mix,

CSP Dynamic Curriculum Management System

Includes all the procedures and processes that CyberSecPro will use to manage the curriculum portfolio. The open-source learning platforms Moodle and/or e-class will be used (since the academic partners already use it in the academic programmes) for the CyberSecPro DCM integration. It will entail the entire curriculum creation, evaluation, review, approval, and promotion processes. regulation compliance (e.g., GDPR).

The main requirements of the CyberSecPro DCM will be flexibility and responsiveness to the continuously changing cybersecurity market needs. Overall, CSP Dynamic Curriculum Management (DCM): The online Dynamic Curriculum Management (DCM) is an online tool that will be integrated by parametrisation of the Moodle or e-class open-source learning platform where the cybersecurity market needs will be monitored, and curricula will be managed.



1 Introduction

Cybersecurity will continue to pose a significant challenge for the foreseeable future for companies and industries of all sizes and in all sectors of human endeavours. Existing studies and several market analyses [1]– [3] have shown that our digitally connected world faces a growing workforce shortage of qualified professionals and practitioners to take on specific work roles and duties related to cybersecurity. Cybersecurity workforce shortage and skills gap has remained a concern for professionals in the field of cybersecurity, both in the private and the public sectors [1]– [6].

To bridge the cybersecurity skills gap, it is of paramount importance that the European Union (EU), EU nation governments, academia and industry take appropriate initiatives to develop the Cybersecurity workforce and professionals. In view of the above, the Collaborative, Multimodal and Agile Professional Cybersecurity Training Program for a Skilled Workforce in the European Digital Single Market and Industries Project (CyberSecPro for short) promotes a series of new activities in the area of cybersecurity practical skills development, which focuses on identifying current European-wide initiatives to stem skills gap and workforce shortage. CyberSecPro aims to enhance cybersecurity practical skills among Cybersecurity professionals, trainers, and educators. CyberSecPro seeks to address the gap between academic degrees, working life, and market demanded cybersecurity skills-set necessary in NextGen European digitalisation efforts and provide best practices for cybersecurity training programmes.

1.1 Background

As highlighted above, the global shortage of cybersecurity professionals and a gap between the supply and demand of cybersecurity skills cannot be overemphasised. The EU is not immune from these cybersecurity-related issues due to lack of cybersecurity professionals and overall cybersecurity capacity. To this end, several studies have been conducted to find ways of addressing these two key issues. In the EU, the European Commission (EC) and its agency, the European Union Agency for Cybersecurity (ENISA), took the initiative to commission cybersecurity workforce-development targeted projects. One of the initial European Commission's Joint Research Centre (JRC) report, 'Cybersecurity Taxonomy' is intended to align the cybersecurity terminologies, definitions, and domains to facilitate the categorisation of EU cybersecurity competencies. The effort continues with some notable pilot projects including the Cyber Security Competence for Research and Innovation (CONCORDIA), CyberSec4Europe, REWIRE, ECHO, and Strategic Programs for Advanced Research and Technology in Europe (SPARTA), among others.

However, while the CONCORDIA and CybeSec4Europe projects, among other goals, focused on boosting cybersecurity competence and providing a federation of cyber ranges across Europe to facilitate cybersecurity training facilities within the project consortium, ECHO, REWIRE, and SPARTA projects focused on developing cybersecurity workforce skills frameworks and corresponding cybersecurity curricula that helps training providers deliver cybersecurity training. The proposed curricula were derived from the frameworks. ENISA, on its part, has spearheaded several efforts [7]– [11] and further galvanised and consolidated some of the results of these EU-funded initiatives to develop an European Cybersecurity Skills Framework (ECSF). The ECSF defined cybersecurity job profiles and their associated tasks, knowledge areas, skills and competencies. A brief review of these projects is presented in the later part of this report.



The ECSF is now recognized as the EU-based cybersecurity framework that aims at guiding higher education providers and professional training vendors in cybersecurity workforce skills development. Unlike other frameworks ECSF is targeting the cybersecurity workforce approach. One of the goals of CyberSecPro includes implementing the ECSF in practice. The CyberSecPro would entail specifying and developing a market-targeted cybersecurity syllabus and programme specification that implements the ECSF. The outcome of the current research serves as input to the ECSF validation process.

1.2 Scope

CyberSecPro aims to bridge the gap between degrees, working life, and marketable cybersecurity skill-set necessary in the EU's digitization efforts and provide examples of best practices for cybersecurity training programmes. The scope of this report is limited to the provision of cybersecurity workforce skills frameworks and market skills demand analyses. The report analyses existing cybersecurity skills frameworks and various private-public-government initiatives to address the cybersecurity skills shortage and bridge the gap between skills supply and demand. The report also provides an initial assessment that serves as a basis for specifying and establishing future development directions for the CyberSecPro professional training programme.

1.2.1 Relationship with Other Work Packages

CyberSecPro consists of six work packages. This document (Deliverable 2.1) is within Work Package 2 (WP2) and Task 2.1. Other tasks in WP2 are, namely, Task 2.2, "Practical Cybersecurity Skills Offered in EU Academic Programmes," Task 2.3, "Technological Tools and Academic Trainings," and Task 2.4, "CyberSecPro Professional Training Programme Requirements and Specifications." The outcomes of the current report lay the foundation for the overall project. Therefore, an analysis of the results of Task 2.1 and Task 2.2 will potentially indicate the gaps in cybersecurity skills demanded by the market and supplied by HEIs. Furthermore, while Task 2.3 ascertains the state of affairs of current technological tools and training provided by partners in the CyberSecPro Consortium, Task 2.4 aims at specifying and developing a cybersecurity professional training programme that is empowered by the outcomes of Task 2.1/Task 2.2 and addresses skills demanded by the labour market.

The CyberSecPro programme specification produced by WP2 serves as input to the CyberSecPro curriculum portfolio development (Work Package 3). Work Package 3, therefore, develops the required cybersecurity training modules. Work Package 4 (WP) involves planning and offering the CyberSecPro professional training programme to various industry and sector trainees. Work Package 5 (WP5) deals with programme evaluation, benchmarking and best practices. In contrast, Work Package 6 involves programme dissemination, exploitation, sustainability, and market take-up. Work Package 1 (WP1) deals with overall CyberSecPro management.

1.2.2 Purpose and Objective

This report is produced within the context of CyberSecPro Work Package 2, "CyberSecPro Professional Programme Analysis." It provides the outcomes of Task 2.1, "Cybersecurity Market Skills and Competencies Analysis." The high-level objective of this report is derived from the aim of Work Package 2/Task 2.1 as follows: To conduct cybersecurity competencies, skills, knowledge, and values that the market needs from the existing and future workforce.

This CyberSecPro deliverable D2.1 report provides valuable insights into the current state of cybersecurity skills in Europe. This deliverable captures the cybersecurity skill sets needed by the markets, the practical skills offered in the EU academic programmes and the gaps between demand and supply of practical skills. Special attention will be given to the three industrial sectors: health, energy, and maritime. The deliverable reflects the outcomes of tasks T2.1 and T2.2.



1.3 Methodology and Development Process

The CyberSecPro project targets the implementation approach at the market driven and practitioner's methods rather than rigorous theoretical scientific approach. Therefore, development methodology uses a combination of practical and applied research, including an integrated research model that uses multiple theories to explain a phenomenon, multiple methods to collect data on a phenomenon, and a combination of quantitative and qualitative data Analyses. The research methodology used is a comprehensive and rigorous approach. The development process was also well-structured and iterative, which allowed for the continuous improvement of the solutions and results.

1.3.1 Research Methodology:

The research methodology used in this study was a combination of practical and applied research. This involved using multiple theories to explain a phenomenon, multiple methods to collect data on a phenomenon, and a combination of quantitative and qualitative data. The specific research methods used included:

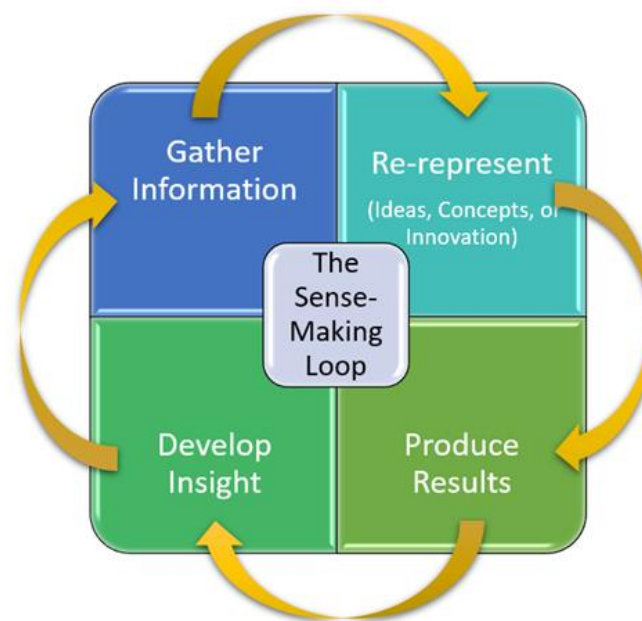


Figure 1: CyberSecPro D2.1 Development Methodology [40]

- A systematic literature review and desk research
- Observation and Analyses of industry and expert discussions
- Observation and Analyses of workshops and seminars
- Market demand surveys with industry professionals
- Analyses of practical skills offered by the European academic programmes



1.3.2 Development Process

The development work used the practical and applied research model as shown in the figure below. It includes (1) desk research, scientific literature reviews, and experts' input (2) qualitative and quantitative data collections from experts, practitioners, and working-life collaborators, (3) Analyses of the information and re-represent, (4) producing initial solutions and results, (5) application and developing insights. The complete process has been iterated with the sense-making phases (see Figure 1) along the project progress phase.

One of the critical goals of this study is to investigate and analyse cybersecurity workforce knowledge and skills demanded by the labour market (demand market analysis). Therefore, this chapter presents the methodologies adopted and followed to arrive at the outcomes provided in this report.

1.3.3 Desk Research, Literature Review and Expert Inputs

The project team embarked on initial desk research to explore existing cybersecurity workforce skills development frameworks designed to enable governments and education providers to tackle the cybersecurity skills shortage and skills gap. Although a cybersecurity frameworks review does not directly answer the question of what cybersecurity skills are demanded in the market, a review of cybersecurity frameworks can reveal current and emerging cybersecurity knowledge areas and skills together with their associated job profiles.

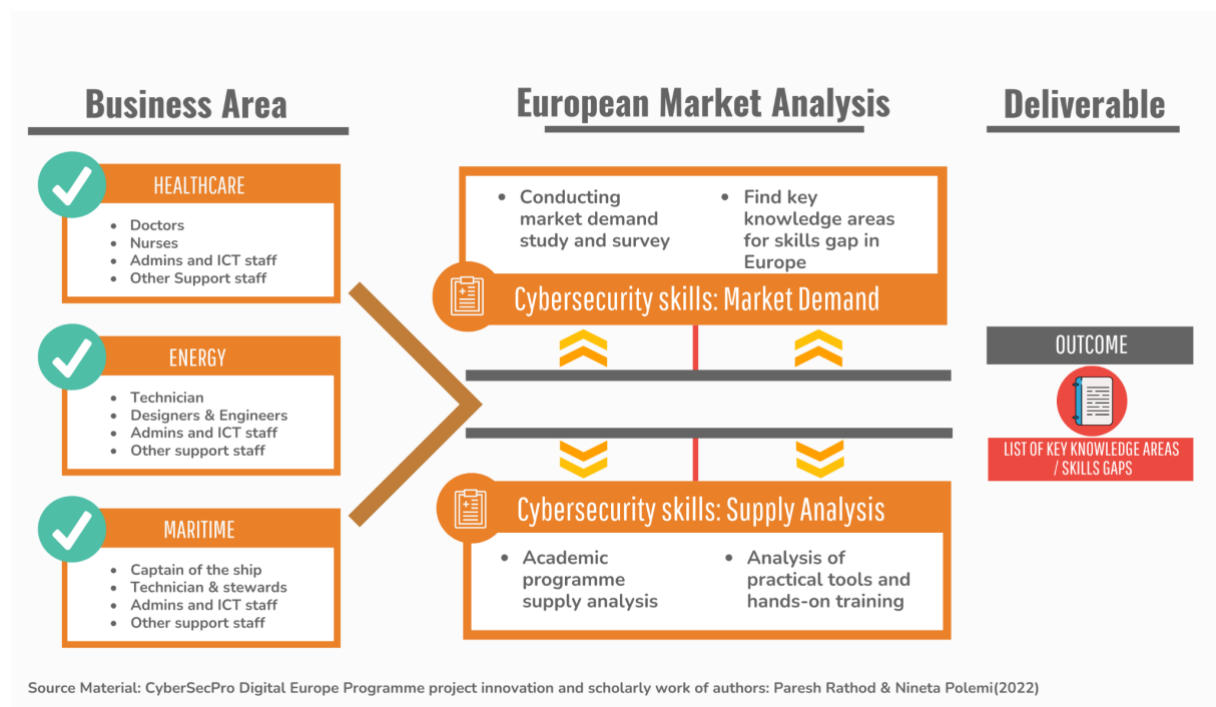


Figure 2: CyberSecPro Practical Skills Gaps in Europe: Development Work Process

The team utilised systematic and general literature review strategies in searching for papers that reported any concrete and visible form of cybersecurity workforce development initiative, including frameworks, guidelines, and directives. The review leverages the outputs of scholarly work available in reputable knowledge databases such as Europa Portal, European Commission Publications, ACM, Emerald Insight, Google Scholar, IEEE Xplore and Science Direct. The highlight of this desk research effort is an evidence review of EU's cybersecurity-funded projects (e.g., SPARTA, REWIRE, ECHO, ECSO and others.) that are targeted at developing the EU cybersecurity workforce and bridging the skills gap. **The aim was not to reinvent the wheel but to harness knowledge from the projects' results towards**



Introduction

developing a professional cybersecurity training programme that meets current labour market demands. The desk research outcome partly served as an input to the development of the quantitative, qualitative, and blended research as it indicated relevant themes within various existing skills frameworks that can be explored.

1.3.4 Market Demand Survey: Practitioner’s Approach

In order to assess and determine the cybersecurity knowledge areas and skills demanded in the labour market and the key sectors of energy, maritime and health, a survey was conducted. The tool adopted for the survey was a questionnaire. The survey type was cross-sectional, as participants were surveyed at one point in the time horizon. The survey was also designed according to a goal definition template to ensure that critical aspects of the market Analyses are captured. Furthermore, the study adopted a convenience sampling method via an online-based questionnaire. This approach ensures that time is saved in disseminating the surveys. An online survey also increases the external validity of survey results since participants are not limited by geographical location.

1.4 Structure of the Report

The rest of this report is structured as follows. Section 2 presents an overview and brief Analyses of the existing cybersecurity skills frameworks and other initiatives. Both EU and non-EU-based frameworks are explored, in addition to strategies, other frameworks, directives and guidelines on cybersecurity workforce development. Section 3 presents the CyberSecPro market demand survey results and Analyses. It describes the survey instrument and its lifecycle, as well as the results and implications of the survey. Section 4 presents the Analyses and prioritisation of cybersecurity knowledge areas and skills. Finally, section 5 provides conclusions and recommendations for a cybersecurity professional programme specification.



2 Cybersecurity Skills Framework and Relevant Initiatives

Compared to other long-established computing disciplines, cybersecurity is a relatively new and rapidly evolving discipline coupled with an increasing demand for a skilled workforce. As a result, government, public and private organisations have proposed several cybersecurity skills frameworks and other initiatives to address the widely reported workforce shortage and skills gap. This chapter presents an Analyses of the existing cybersecurity skills frameworks and other initiatives including strategies, directives and guidelines on cybersecurity workforce development.

A cybersecurity skills framework provides stakeholders with a shared understanding of the cybersecurity ecosystem and also guides the development of a cybersecurity governance structure. The most useful and popular cybersecurity frameworks often embody cybersecurity job roles and their associated cybersecurity knowledge areas, skills, abilities, tasks, and competencies. Apart from cybersecurity frameworks, other initiatives, such as guidelines and strategies, may be deployed to address workforce skills challenges. Given current and emerging cyber threats, there is a need to provide a cybersecurity professional training programme (programme with skilling, upskilling and reskilling possibilities) that addresses the needs of organisations as they strive to protect their infrastructure. A cybersecurity framework plays a vital role in addressing the above demand.

This section reviews existing cybersecurity skills frameworks and initiatives geared towards workforce skill development and their importance to CyberSecPro skilling, reskilling, and upskilling approach. The CyberSecPro project conducted a comprehensive analysis and some of the sample images are depicted in [Annex B: Analyses Work](#).

2.1 International and Non-EU Cybersecurity Skills Frameworks

This section considers cybersecurity workforce skills frameworks developed and implemented outside the European Union.

2.1.1 National Initiative for Cybersecurity Education (NICE) Framework

The NICE cybersecurity skills framework was commissioned by the National Institute of Standards and Technology (NIST) in partnership with the US academia and the private sector. It is a national resource to assist in developing the US cybersecurity workforce. The NICE framework serves as a guide for training cybersecurity professionals. It also provides standards and best practices for the US cybersecurity landscape. NICE's mission is to “energize, promote, and coordinate a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development.”

The NICE Framework is comprised of the following elements:

- Categories (7)– Typifies a high-level and principal grouping of common cybersecurity functions
- Specialty Areas (33) – Distinct areas of cybersecurity work or function.
- Work Roles (52) – Detailed groupings of cybersecurity work comprising specific knowledge, skills, and abilities (KSAs) required to perform tasks in a Work Role. KSAs are NICE’s framework attributes that cybersecurity professionals require to perform their work roles.

Table 1 presents a high-level summary of NICE’s key classifications. Each NICE category consists of specialties, and each specialty consists of one or more cybersecurity work roles. Full details of the framework, especially the KSAs for each cybersecurity work role, are provided in [12].



Cybersecurity Skills Framework and Relevant Initiatives

NICE FRAMEWORK - NIST Special Publication 800-181

Cybersecurity Workforce Categories (7)

Specialty Areas (33) – Distinct areas of cybersecurity work

Work Roles (52) – The most detailed groupings of IT, cybersecurity, or cyber-related work, which include specific *Knowledge, Skills, and Abilities*

(KSA's) required to perform a set of *Tasks*.

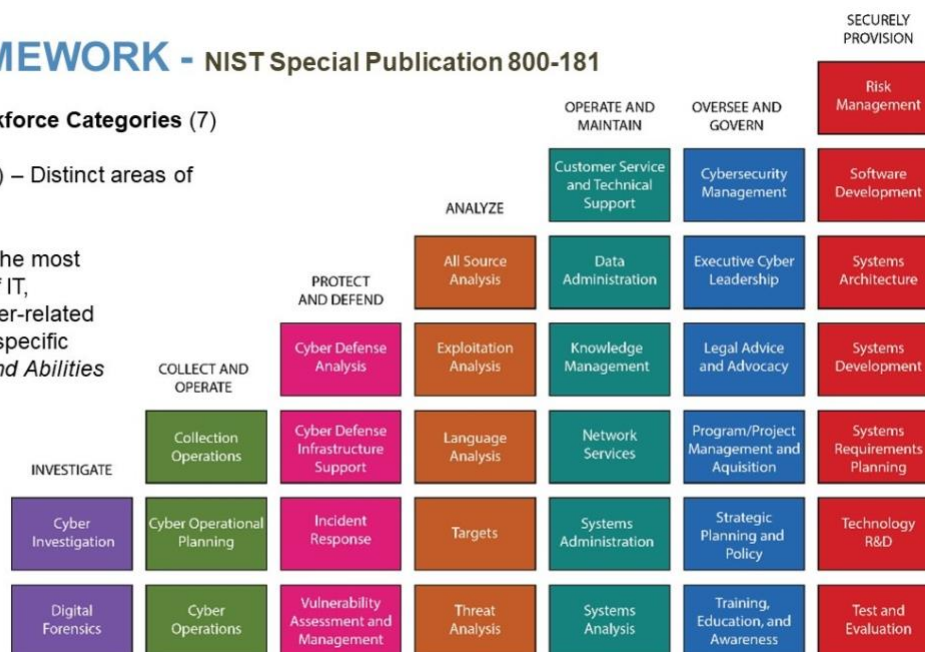


Figure 3: NICE Framework

The NICE framework has established itself as a widely referenced cybersecurity governance standard that has birthed other countries' frameworks and private and public organisations. An interesting feature of the NICE framework is that it captures the interdisciplinary nature of a cybersecurity governance initiative, thus making it quite complex and overwhelming. The US cybersecurity ecosystem inspired the NICE framework. The implication is that if the NICE framework is adopted, it should be adapted to suit the country's or sector's peculiarities.

Table 1 : Summary of NICE Framework Classification

Category	Speciality Areas	No of Work Roles
Analyse	All-Source Analyses, Exploitation Analysis, Language Analysis, Targets, Threat Analysis	8
Collect and Operate	Collection Operations, Cyber Operational Planning, Cyber Operations	6
Investigate	Cyber Investigation, Digital Forensics	3
Operate and Maintain	Customer Service and Technical Support, Data Administration, Knowledge Management, Network Services, Systems Administration, Systems Analysis	6
Oversee and Govern	Cybersecurity Management, Executive Cyber Leadership, Legal Advice and Advocacy, Program/Project Management	14



	and Acquisition, Strategic Planning and Policy, Training, Education, and Awareness	
Protect and Defend	Cyber Defense Analysis, Cyber Defense Infrastructure Support, Incident Response, Vulnerability Assessment and Management	4
Securely Provision	Risk Management, Software Development, Systems Architecture, Systems Development, Systems Requirements Planning, Technology R&D, Test and Evaluation	11

For instance, in some EU cybersecurity development projects [9], [12]– [14], the NICE framework was adapted to accommodate the peculiarities and needs of the EU. Additionally, like other frameworks, we observed that the NICE framework is not industry or organisation-size specific, thus making it applicable across the board. Given the comprehensive nature of NICE, it can yet serve as a reference framework for the CyberSecPro curriculum development programme in union with ENISA’s framework

2.1.2 ACM, IEEE, AIS SIGSEC, IFIP Cybersecurity Curricula Guidelines (CSEC2017)

The Association for Computing Machinery (ACM)/Institute of Electrical and Electronics Engineers (IEEE) curriculum models emerged in the 1960s to address the changing employment landscape applied to the field of computer technology [15]. The first curricular model resulting from the collaboration between organisations was the Computing Curricula (CC) published in 1991 [16], providing a guide for Computer Science (CS) and Computer Engineering (CE). Subsequently, the CC2001 [17] and CC2005 [18] reports appeared to unify in a single document the computing disciplines recognized at their corresponding times (2001 and 2005, respectively).

The impact of CC2005 was more relevant in the literature, as it made it possible to differentiate between computing disciplines and to include other emerging disciplines such as cybersecurity. As a result, the Joint Task Force (JTF) on Cybersecurity Education CSEC published 2017 the CSEC2017 JTF [1] in order to provide a way to establish or restructure the curricular model (denoted as a volume in [19]) required within the cybersecurity discipline, and that would enable profiling the profession of experts in that field. For that reason, it is widely recommended not to forget the application of essential theoretical concepts (the knowledge) applied through practical activities.

As everything revolves around “knowledge”, CSEC2017 bases its approach on eight Knowledge Areas (KAs), also known as “essentials”:

- Data Security / Data Essentials;
- Software Security / Software Essentials;
- Component Security / Component Essentials;
- Connection Security / Connection Essentials;
- System Security / System Essentials;
- Human Security / Human Essentials;
- Organisational Security / Organization Essentials; and
- Societal Security / Societal Essentials.

Each of these KAs is structured in interrelated Knowledge Units (KUs), also known as topics, such that:



Cybersecurity Skills Framework and Relevant Initiatives

- Data Essentials is in turn based on five KUs: basic cryptography concepts; end-to-end secure communications; digital forensic; data integrity and authentication; and data erasure.
- Software Essentials with six KUs: fundamental design principles; least privilege, open design, and abstraction; security requirements and the roles they play in design; implementation issues; static, dynamic analysis; configuring, patching; and ethics, especially in development, testing, and vulnerability disclosure.
- Component Essentials with six KUs: vulnerabilities of system components; component lifecycle; secure component design principles; supply chain management; security testing; and reverse engineering,
- Connection Essentials with five KUs: systems, architecture, models, and standards; physical component interfaces; software component interfaces; connection attacks; transmission attacks.
- System Essentials with eight KUs: holistic approach; security policy; authentication; access control; monitoring; recovery; testing; and documentation.
- Human Essentials with five KUs: identity management; social engineering; awareness and understanding; social behavioural privacy and security; personal data privacy and security.
- Organization Essentials: risk management; governance and policy; laws, ethics, and compliance; and strategy and planning.
- Societal Essentials: cybercrime; cyber law; cyber ethics; cyber policy; and privacy.

As can be seen, CSEC2017 adds an important interdisciplinarity connotation within the curricular programmes by covering other areas surrounding cybersecurity such as law, ethics and human factors. Apart from this, CSEC2017 is also characterised by providing some other aspects of interest, such as [16]: (i) a clear vision of cybersecurity competence; (ii) an appropriate structure for the cybersecurity discipline by developing a thinking model that defines the boundaries of the discipline and outlines the key dimensions of the curriculum structure; (iii) an alignment of academic programmes with industry needs in cybersecurity; (iv) implications of a broad global audience of stakeholders through ongoing community involvement during the development process; (v) a curricular guide comprehensive enough to support a wide range of programme types; and (vi) a curriculum guide that is based on fundamental principles that provide stability, but is structured in a way that offers flexibility to support the evolving needs of the programme.

While it is very true that in 2020 Cyber2yr2020 emerges [20] to support cybersecurity curriculum models for two-year programmes, its focus is to date very limited compared to CSEC2017. This is why CSEC2017 remains the most applied approach within the cybersecurity field, where CSEC2017 volume advocates incorporating [19]: (i) a solid computer science-based foundation (e.g., in computer science, information technology); (ii) crosscutting concepts that are broadly applicable across the range of cybersecurity specialisations; (iii) a body of knowledge containing essential cybersecurity knowledge and skills; (iv) a direct link to the range of specialisations that meet workforce demand; and (v) a strong emphasis on ethical conduct and professional responsibilities associated with the field. However, it is also prudent to highlight the relevance of the rubrics provided by Cyber2yr2020 that help cybersecurity trainers/teachers to know the degree of achievement of the knowledge in cybersecurity. This degree of achievement only applies to competencies, as Cyber2yr2020 replaces the idea of topic with competencies.



2.1.3 Singaporean Cybersecurity Skills Framework

Like the EU Competence framework, the Singaporean skills framework [21] was jointly developed by a Singapore government agency Infocomm Media Development Authority (IMDA) and SkillsFuture Singapore (SSG). The framework considered feedback from stakeholders within the Singaporean ICT industry. It is a broad skills framework that targets a range of stakeholders, including employers and education providers. The key objective of the framework is to advance professionalism, provide career opportunities and empower stakeholders to make informed decisions within the ICT sub-sector.

The Singaporean framework [21] broadly categorises seven core skills development areas, including cybersecurity. The other categories include Data and Artificial intelligence, Operations and Support, Infrastructure, Software and Applications, Strategy and Governance, and Sales and Marketing. Besides the classifications and descriptions provided in the framework, the framework generally provides pathways to several careers in ICT. Overall, the framework identified seven core tracks based on emerging trends, including cybersecurity. Under the cybersecurity track, seven sub-tracks, including Governance Risk and Control, Vulnerability Assessment and Penetration Testing, Security Operations, Forensics Investigation, Incident Response, Design and Engineering, and Threat Analysis, were defined. The cybersecurity track features 15 job profiles grouped in a hierarchical structure (see Figure 2) of three layers. The Chief Information Security role occupies the top layer of the framework. Other managerial cybersecurity roles are in the second layer, and their respective subordinating roles appear in the third layer. The Associate Security Analyst sits at the lowest layer and is under the roles of Security Operations Analyst, Forensics Investigator and Incident Investigator, and Senior Security Engineer.

Additionally, the framework identified and described several technical and soft skills and competencies for each cybersecurity job role. It also provided proficiency levels for each technical skill and competence. The proficiency levels and their definitions underscore the autonomy and administrative role of each respective cybersecurity job role. Critical Work Functions and Key Tasks for each job role are also provided. What is apparently missing from the framework is cybersecurity knowledge areas that may inform framework adopters and implementers in their design of training modules.

2.1.4 Australian Cybersecurity Skills Framework

In July 2019, the Australian Signals Directorate (ASD) introduced the ASD Cyber Skills Framework (ASD-CSF). It is intended to be used as a tool for assessing, maintaining, and monitoring the cybersecurity workforce's skills, knowledge, and attributes. The ASD-CSF defines cybersecurity job roles, capabilities and skills required to support ASD's cybersecurity missions. In addition, the framework serves as an enabler of the recruitment of cybersecurity professionals and a provider of cybersecurity career pathways. It aligns cybersecurity skills, knowledge, and attributes with Australian and international cybersecurity standards [22].

The development of the ASD-CSF was inspired and guided by industry, government frameworks and standards. The core frameworks relied on include the Chartered Institute of Information Security (CIISec) framework [2], The Skills Framework for the Information Age (SFIA) [23], and the Australian Public Service Commission Integrated Leadership System (ILS). Based on these frameworks and emerging trends in the cybersecurity ecosystem, the ASD-CSF cybersecurity roles, capabilities, and proficiency levels were reviewed and proposed. As a result, the ASD-CSF is built on five foundational elements: Cyber role definitions, Capability and skills definitions, Proficiency levels, Career pathways, and learning and development pathways.



Cybersecurity Skills Framework and Relevant Initiatives

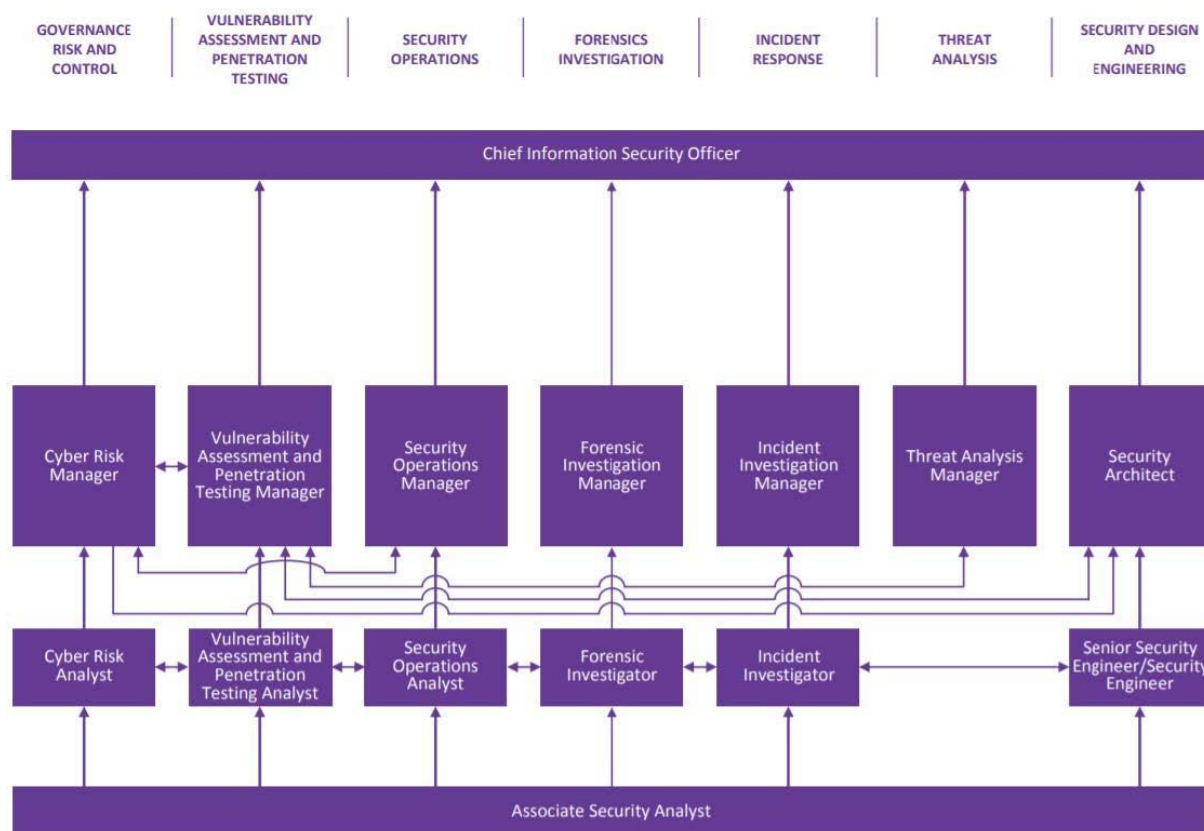


Figure 4: Cybersecurity Career Paths [21]

The ASD-CSF contains four cybersecurity disciplines and nine cybersecurity roles grouped under each related domain. Table 2 summarizes these disciplines and their respective roles. Proficiency levels defined and mapped under the ASD-CSF include Level 1 (Learner), Level 2 (Novice), Level 3 (Practitioner), Level 4 (Senior Practitioner), Level 5 (Principal Practitioner), and Level 6 (Expert Practitioner).

The ASD-CSF proposed nine unique core capabilities based on the earlier-mentioned base frameworks. In addition, a capability is used to group related skills. It is observable in the ASD-CSF that some skills are further grouped under sub-capabilities. However, the occurrence of this sub-grouping is negligible. The proposed capabilities are suggestive of high-level cybersecurity knowledge areas that ASD-CSF focuses on. Moreover, these capabilities are specified for each cybersecurity job role, which may not have all identified capabilities. These capabilities are listed as follows.

- Information Security Governance and Strategy
- Threat Assessment and Information Risk Management
- Systems Development and Implementation
- Assurance: Audit, Compliance and Testing
- Operational Security Management
- Incident Management, Investigation and Forensics
- Information Security Research
- Management, Leadership, Business and Communication



- Specialist Advice

Concerning skills, ASD-CSF proposed several skills and categorised them under each cybersecurity capability. With colour coding, various proficiency levels required to perform each skill are mapped to the respective skill. The full details of the proposed skills are provided in [22].

Table 2 : ASD-CSF Disciplines and Roles

S/N	Cybersecurity Discipline	Job Roles
1	Cyber Security Operations	Incident Response; Operations Coordinator
2	Cyber Security Analysis	Malware Analyst, Intrusion Analyst, Cyber Threat Analyst
3	Cyber Security Architecture	Cyber Security Advice and Assessment, Vulnerability Researcher
4	Cyber Security Testing	Penetration Tester, Vulnerability Assessor

Furthermore, the ASD-CSF provides a cybersecurity career pathway for current and next-generation cybersecurity professionals. Based on the framework, professionals can ascertain the skills and capabilities they currently possess and the skills and capabilities they need for increased employability. It also gives training providers and professionals an indication of relevant cybersecurity job roles in demand. The CyberSecPro professional training programme may follow a similar approach in mapping out career pathways for upcoming cybersecurity professionals.

Despite the release of the ASD-CSF, ASD yet recommends that the ASD-CSF be read in union with other cybersecurity skills frameworks, especially the NICE framework. The ASD-CSF has been the basis for other Australian agencies to develop their cybersecurity workforce occupational profiles, including the Defense People Group and the Australian Public Service Commission and Digital Transformation Agency

2.1.5 Canadian Cybersecurity Skills Framework

TECHNATION is a not-for-profit Canada's national information and communication business association. One of its main goals is to champion the development of Canada's digital economy. With support from the Cybersecurity Talent Alliance, Cybersecurity Industry Professionals, the Canadian Center for Cyber Security, the Government of Canada, and the U.S National Initiative on Cybersecurity Education, TECHNATION developed and released a Cybersecurity Workforce National Occupation Standards (CWNOS) [24] in 2020. Because cybersecurity remains a relatively new and still emerging discipline, the CWNOS purpose is to define occupation standards for the Canadian cybersecurity labour market based on emerging trends. Like every other cybersecurity skills development initiative, CWNOS aims to close the cybersecurity skills shortage gap within the Canadian cybersecurity ecosystem.

The NICE framework and the Canadian cybersecurity curriculum guide formed the Canadian Cybersecurity Skills Framework (C-CSF) bedrock. Although the CWNOS and C-CSF [25] maintain the seven specialities of the NICE framework, what distinguishes them from the NICE framework is the additional classifications it established. It leverages NICE via its simplification and use of a business-oriented lens in recognizing cybersecurity talent from an organizational viewpoint. For instance, the specialities of *Oversee and Govern*, *Design and Develop*, *Operate and Maintain*, *Protect and Defend* are



Cybersecurity Skills Framework and Relevant Initiatives

classified as Business-oriented roles (BoR). On the other hand, Investigate, Analyze, Collect and Operate specialities are classified as Specialized Cybersecurity Work Domains (SCWD). Relative to other occupations, the C-CSF considers BoR as Core Cybersecurity Roles that are conducted full-time and require unique knowledge, skills, and abilities.

The C-CSF requires all cybersecurity roles to possess the following (see Table 3) common competencies at the primary application level.

Table 3 : ASD-CSF Disciplines and Roles

S/N	Cybersecurity Discipline
1	IT systems and networking
2	Systems architecture and models
3	Internet protocols, systems and devices
4	Cybersecurity foundations (e.g., Integrated security framework, Cybersecurity strategies and approaches etc.)
5	Problem-solving and complex thinking in dynamic environments
6	Maintaining broader security situational awareness
7	Self-awareness regarding knowledge, skills and abilities required to respond to business, threat and technical changes
8	Continuous learning to support currency in knowledge of emerging threats, technological innovations in security, and the changing cybersecurity landscape.
9	Communications (oral and verbal) suited to organizational context including drafting and writing technical reports
10	Strategic thinking and business acumen to include understanding the business and risk context for cybersecurity
11	Teamwork/collaborating with others including non-cybersecurity professionals
12	Ethics and professional responsibilities
13	Cybersecurity training and awareness within their domain

Following Table 4 presents a summary of BoR in terms of job roles and the number of required competencies (KSAs). The C-CSF grouped knowledge, skills, and abilities (KSAs) under the umbrella of competencies, thus making it difficult to ascertain the distinctions between these characteristics. The KSAs are further grouped as basic or advanced in their application.



Table 4: Core C-CSF Roles and Competencies

Job Roles	Basic KSAs	Advanced KSAs
Chief Information Security Officer (CISO)	5	9
Information Systems Security Officer	5	7
Information Security Auditor	2	14
Security Architect	-	20
Security Engineer/Security Engineering Technologist	-	37
Secure Software Assessor	4	17
Security Testing and Evaluation Specialist	2	16
Operational Technology Systems Analyst	12	10
Supply Chain Security Analyst	5	10
Information Systems Security Developer	13	10
Security Automation Engineer/Analyst	-	19
Cryptanalyst / Cryptographer	6	10
Identity and Authentication Management Support Specialist	7	6
Encryption/ Key Management Support Specialist	6	13
Data Privacy Specialist / Privacy Officer	4	8
Information Systems Security Manager	1	9
Cybersecurity Operations Analyst -Tier 1	16	8
Tier II Analyst - Malware Specialist	-	6
Tier III – Threat Hunter	-	10
Cybersecurity Incident Responder	17	19
Cybersecurity Operations Technician	9	5
Vulnerability Assessment Analyst	8	8
Penetration Tester	-	17
Digital Forensics Analyst	-	14

The SCWD within the C-CSF is intended to support the cybersecurity missions of Canadian national security, armed forces, and providers of critical infrastructure sectors. These roles which are adopted from NICE include Threat/Warning Analyst, Exploitation Analyst, All-Source Analyst, Mission



Cybersecurity Skills Framework and Relevant Initiatives

Assessment Specialist, Target Developer, Target Network Analyst, Multi-Disciplined Language Analyst, All Source-Collection Manager, All Source-Collection Requirements Manager, Cyber Intel Planner, Cyber Ops Planner, Partner Integration Planner, Cyber Operator, Cyber Crime Investigator, Law Enforcement/Counterintelligence Forensics Analyst, and Cyber Defense Forensics Analyst. The grouping of these roles and their associated KSAs are fully provided in the NICE framework. However, the framers of the C-CSF suggest that these roles do not commonly appear in the wider Canadian job market.

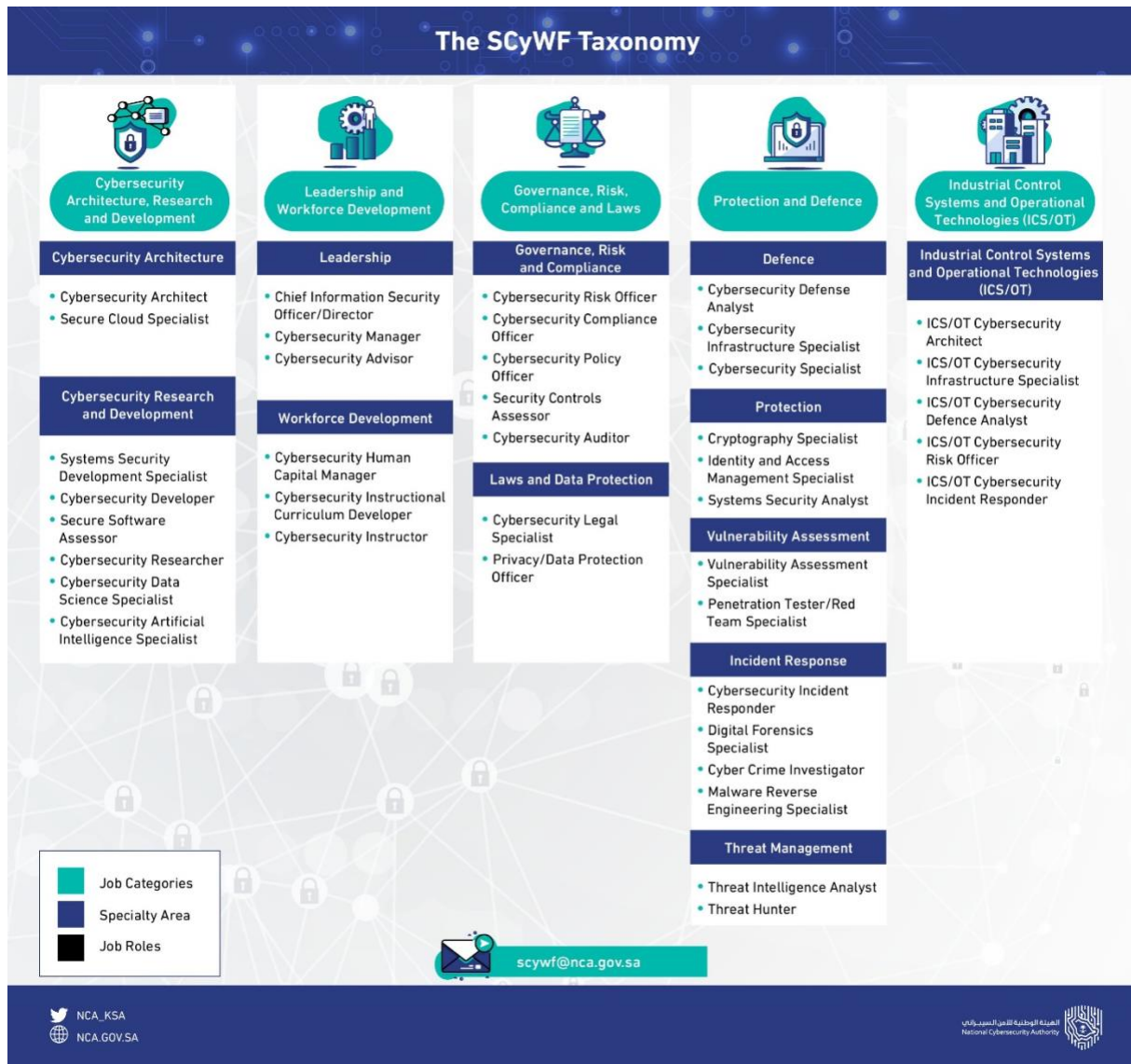


Figure 5: Saudi Arabia- SCyWF Cybersecurity Taxonomy [26]

The C-CSF also identified several cybersecurity roles related to other organisational functions. The C-CSF termed these roles as Cybersecurity Adjacent Roles (CAR) because they primarily contribute to cybersecurity missions on an ad-hoc basis. C-CSF argues that because CAR requires some cybersecurity skills and abilities, they may not typically be recognized as cybersecurity specialists. The C-CSF's CAR



and its associated competencies are fully described in [24]. These cybersecurity roles may apply in large IT-enabled organisations where they form a small part of the responsibilities within the organisation.

The re-classification of cybersecurity specialities and job roles in the C-CSF reflects the complex nature of the NICE framework. The C-CSF further suggests the unbundling of the NICE framework and adapting it to accommodate the peculiarities of the cybersecurity ecosystem it is deployed in.

2.1.6 Saudi Arabian Cybersecurity Skills Framework

The Saudi National Cybersecurity Authority (NCA) is responsible for defending and protecting the country's cyber ecosystem. The NCA, therefore, is charged with building the Saudi cybersecurity workforce in terms of developing cybersecurity education and providing professional training, including professional standards and frameworks. Given this mandate, the NCS has developed a cybersecurity skills framework (SCyWF) following the NICE cybersecurity workforce framework.

Though the SCyWF [26] was inspired by NICE, it presents cybersecurity categories and job roles that are quite different from NICE's. The SCyWF defines a job role as a set of cybersecurity tasks required to perform a cybersecurity job. Besides defining a set of tasks, it lists KSAs needed to perform the tasks. A speciality area in the SCyWF framework refers to a group of job roles serving a specific cybersecurity function and having common TKSAs. On the other hand, a category within the SCyWF refers to a group of speciality areas, including associated job roles that serve related cybersecurity functions. It is important to note that, unlike the NICE's framework, the SCyWF does not consider non-cybersecurity job roles. Figure 3 presents an overview of SCyWF taxonomy.

Table 5 presents a summary of SCyWF's offering in terms of cybersecurity job roles, knowledge areas (speciality, according to SCyWF) and skills. In addition to common job roles and specialities that are provided in other frameworks, SCyWF proposed job roles and skills for ICS/OT. SCyWF did not consider cybersecurity professional or generic skills.

Table 5: Summary of SCyWF

S/N	Job Roles	Main Knowledge Area	KAs No.	Technical Skills No.
1	Chief Information Security Officer/ Director	Leadership	23	8
2	ICS/OT Cybersecurity Incident Responder	Incident Respondent	32	74
3	Cybersecurity Legal Specialist	Laws and Data Protection	17	1
4	Threat Intelligence Analyst	Threat Management	43	16
5	Cybersecurity Architect	Cybersecurity Architecture	74	19
6	Cybersecurity Auditor/	Governance, Risk and Compliance	28	47
7	Cybersecurity Instructional Curriculum Developer	Workforce Development	24	6



Cybersecurity Skills Framework and Relevant Initiatives

8	Cybersecurity Developer	Cybersecurity Research and Development	45	16
9	Cybersecurity Researcher	Cybersecurity Research and Development	36	7
10	Cybersecurity Risk Officer	Governance, Risk and Compliance	27	3
11	Digital Forensics Specialist	Incident Response	46	22
12	Penetration Tester/Red Team Specialist	Vulnerability Assessment	34	19
13	Secure Cloud Specialist	Cybersecurity Architecture	31	3
14	Systems Security Development Specialist	Cybersecurity Research and Development	48	11
15	Cybersecurity Data Science Specialist	Cybersecurity Research and Development	33	27
16	Cybersecurity Artificial Intelligence Specialist	Cybersecurity Research and Development	16	7
17	Cybersecurity Manager	Leadership	58	4
18	Cybersecurity Advisor	Leadership	52	5
19	Cybersecurity Human Capital	Workforce Development	22	2
20	ICS/OT Cybersecurity Architect	Industrial Control Systems and Operational Technologies	81	21
21	Cybersecurity Instructor	Workforce Development	31	30
22	Cybersecurity Compliance Officer	Governance, Risk and Compliance	15	2
23	Cybersecurity Policy Officer	Governance, Risk and Compliance	19	2
24	Security Controls Assessor	Governance, Risk and Compliance	56	59
25	Privacy/Data Protection Officer	Laws and Data Protection	16	5
26	Cybersecurity Defense Analyst	Defense	72	23



26	Cybersecurity Infrastructure Specialist	Defense	30	14
27	Secure Software Assessor	Cybersecurity Research and Development	46	10
28	Cybersecurity Specialist	Defense	31	15
29	Cryptography Specialist	Protection	48	10
30	Identity and Access Management Specialist	Protection	39	4
31	System Security Analyst	Protection	48	9
32	Vulnerability Assessment Specialist	Vulnerability Assessment	38	17
33	Cyber Crime Investigator	Incident Response	24	4
34	Malware Reverse Engineering Specialist	Incident Response	33	21
35	Threat Hunter	Threat Management	37	32
36	ICS/OT Cybersecurity Infrastructure Specialist	Industrial Control Systems and Operational Technologies	39	18
38	ICS/OT Cybersecurity Defense Analyst	Industrial Control Systems and Operational Technologies	81	24
39	ICS/OT Cybersecurity Risk Officer	Industrial Control Systems and Operational Technologies	37	5

2.1.7 Indian Cybersecurity Skills Framework

The Data Security Council of India (DSCI) is a not-for-profit industry organization that is tasked with data protection in India. In collaboration with the Indian government and public and private organizations, DSCI contributes to cybersecurity policy advocacy, thought leadership, and capacity building. In DSCI's effort to strengthen thought leadership in cybersecurity and data privacy, DSCI has proposed several cybersecurity best practices and a framework [27] that enables the training of the Indian cybersecurity workforce.



Cybersecurity Skills Framework and Relevant Initiatives

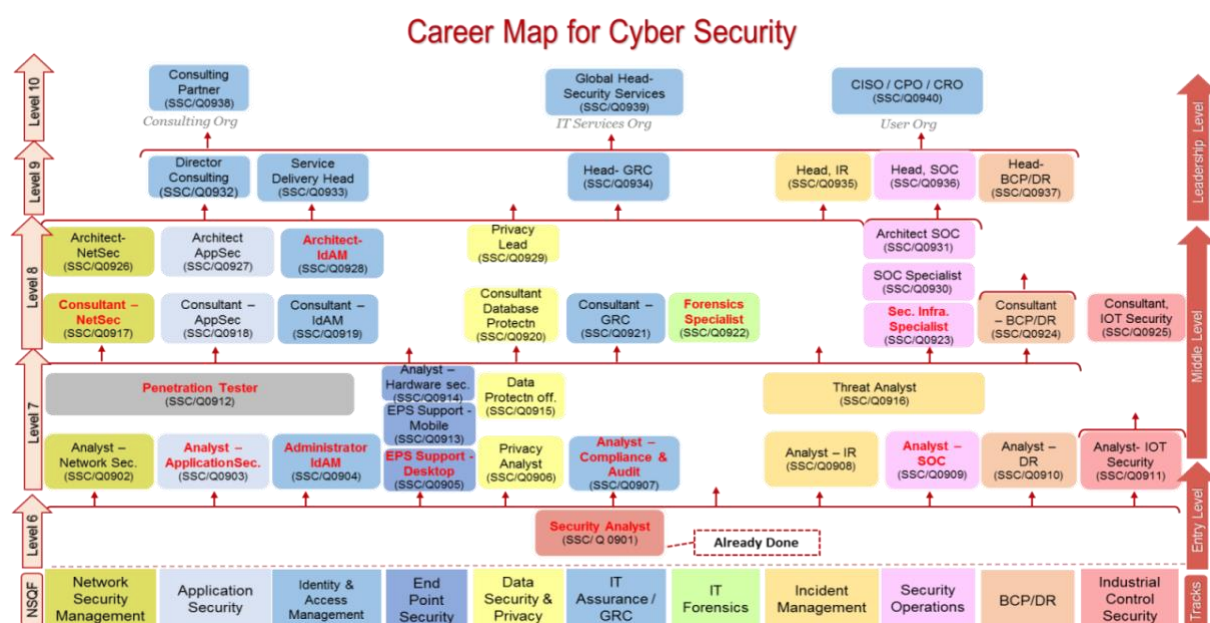


Figure 6: DSCI Cybersecurity Career Map [27]

In its recent collaboration with the IT/ ITeS Sector Skills Council, DSCI has been working towards bridging the cybersecurity workforce shortage and skills gap within the Indian cybersecurity ecosystem. DSCI, the IT/ITeS Sector Skills Council and the Indian Ministry of Skills & Entrepreneurship Development are working towards developing the Indian cybersecurity workforce under the aegis of the National Skills Development Corporation (NSDC).

Table 6: Summary of DSCI cybersecurity framework

S/N. Job roles	Main Knowledge Area / Specialty	No. of KAs	No. of Technical Skills	No. of Professional Skills
1) Forensics Specialist	Identify, preserve, and seize digital/electronics devices or records for investigation of possible breach or crime	24	7	9
	Extract relevant data or information from digital forensic evidence	26	7	9
	Analyze information or data extracted from digital forensic evidence	24	7	9



	Report and present the results of a forensic investigation	23	3	9
2) Penetration Tester	Test, run exploits to identify vulnerabilities in networks	29	9	11
	Identify and analyse exposures and weaknesses in applications and their deployment	20	5	11
	Make reports based on test results and make enhancements to existing security solutions	22	6	11
3) IT Security Infrastructure Specialist	Configure cyber security infrastructure components	23	7	11
4) IT Analyst Compliant Audit	Identify and report compliance issues with respect to cybersecurity	25	5	11
	Maintain compliance to information security policies, regulations and standards and address risk issues	22	6	11

Based on the NSDC's skills framework, DSCI, in collaboration with the industry, developed a career map for the cybersecurity sector and further proposed ten cybersecurity job roles. The cybersecurity career map is provided in Figure 4. The proposed job roles include Analyst Compliance; Audit Forensics Specialist; Penetration Tester; Analyst Application Security; Analyst End Point Security; Analyst Identity & Access Management; Analyst Security Operations Centre; Security Infrastructure Specialist; Architect Identity & Access Management, and Consultant Network Security.

Table 6 summarises DSCI's cybersecurity framework regarding job roles, knowledge areas (units according to DSCI) and skills. To keep the current report manageable, we do not highlight the actual knowledge areas and skills; instead, we capture the high-level knowledge domain. Additionally, we did not include knowledge areas outside the cybersecurity landscape. Due to the many knowledge areas and skills provided in DSCI's documentation, we recommend that the reader find full details in the referenced source.



2.2 EU-Based Cybersecurity Skills Frameworks and Development Work

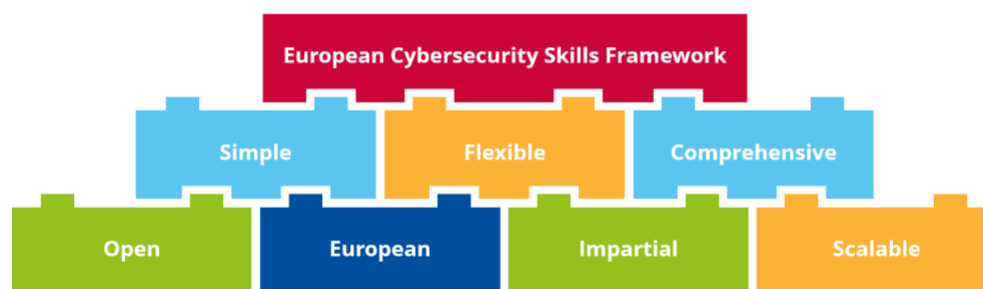
Several EU-based cybersecurity skills frameworks have been developed across Europe to enhance workforce skills development. This section reviews these frameworks and highlights how they might impact CyberSecPro.

2.2.1 ENISA European Cybersecurity Skills Framework (ECSF)

The ECSF is a result of a joint work of the European Union Agency for Cybersecurity (ENISA) [28] with members of the Ad Hoc Working Group [5] to create a common framework that helps identify and assign tasks, competences, skills, and knowledge to cybersecurity-specific roles. Both the framework [29] and its "User Manual" [30] detail the features of the approach, with the aim of creating a common understanding among all parties involved in the cybersecurity field, in addition to addressing the current gap between academia and the workforce in the labour market.

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

Principles



This framework offers:

- To create a common understanding of the roles, competencies, skills and knowledge
- To facilitate cybersecurity skills recognition
- To support the design of cybersecurity related training programs

Figure 7: European Cybersecurity Skills Framework Principles [29]

Specifically, the ECSF groups all cybersecurity-related roles into twelve profiles:

- Chief Information Security Officer,
- Cyber Incident Responder,
- Cyber Legal, Policy and Compliance Officer,
- Cyber Threat Intelligence Specialist,
- Cybersecurity Architect,
- Cybersecurity Auditor,
- Cybersecurity Educator,
- Cybersecurity Implementer,
- Cybersecurity Researcher,
- Cybersecurity Risk Manager,



- Digital Forensics Investigator, and
- Penetration Tester.

Each of these profiles is examined separately to determine the specificities of their relevant roles, competencies, synergies, and dependencies. More particularly, the approach aims to highlight for each profile: possible alternative titles, summary statement, mission, deliverable(s), main tasks, key skills (including soft skills and ethics), key knowledge, and to link the main competencies of the profile with those set out in the well-known e-Competence Framework (e-CF) [31]. This framework, with 41 competencies (in Information and communications technology (ICT)) compiled in the UNE-EN 16234-1:2021 standard, is the basis for the ECSF to build solid and reliable professional profiles in cybersecurity.



Figure 8: European Cybersecurity Skills Framework: Job Profiles [29]

As stated above, the ECSF offers a shared understanding of the pertinent roles and responsibilities, competencies, abilities, and knowledge needed, makes it easier to identify cybersecurity skills, and aids in the creation of training programmes connected to cybersecurity.

1. Use of the ECSF ensures a common terminology and shared understanding between the demand (workplace, recruitment) and supply (qualification, training) of cybersecurity professionals across the EU.
2. The ECSF supports the identification of the critical skill sets required from a workforce perspective. It enables providers of learning programmes to support the development of this critical set of skills and helps policymakers support targeted initiatives to mitigate the gaps identified in skills.
3. The framework facilitates an understanding of leading cybersecurity professional roles and the essential skills they require, including soft skills, along with the legislative aspects (if any). It



Cybersecurity Skills Framework and Relevant Initiatives

enables non-experts and HR departments to understand the requirements for resource planning, recruitment and career planning in supporting cyber-security.

4. The framework promotes harmonisation in cybersecurity education, training, and workforce development. At the same time, this common European language in the context of cybersecurity skills and roles connects well with the entire ICT professional domain.
5. The ECSF contributes to achieving enhanced shielding against cyberattacks and guaranteeing secure IT (Information Technology) systems in society. It provides a standard structure and advice on how to implement capacity building within the European cybersecurity workforce.

2.2.2 JRC European Cybersecurity Centres of Expertise Map

The JRC cybersecurity taxonomy was necessitated by the need to have a standardised definition of cybersecurity coupled with a transparent identification of its domain of development and application. A cybersecurity taxonomy is a necessary enabler of the classification of cybersecurity competencies. It stimulates the competitiveness of the EU's cybersecurity capabilities and capacity[32].

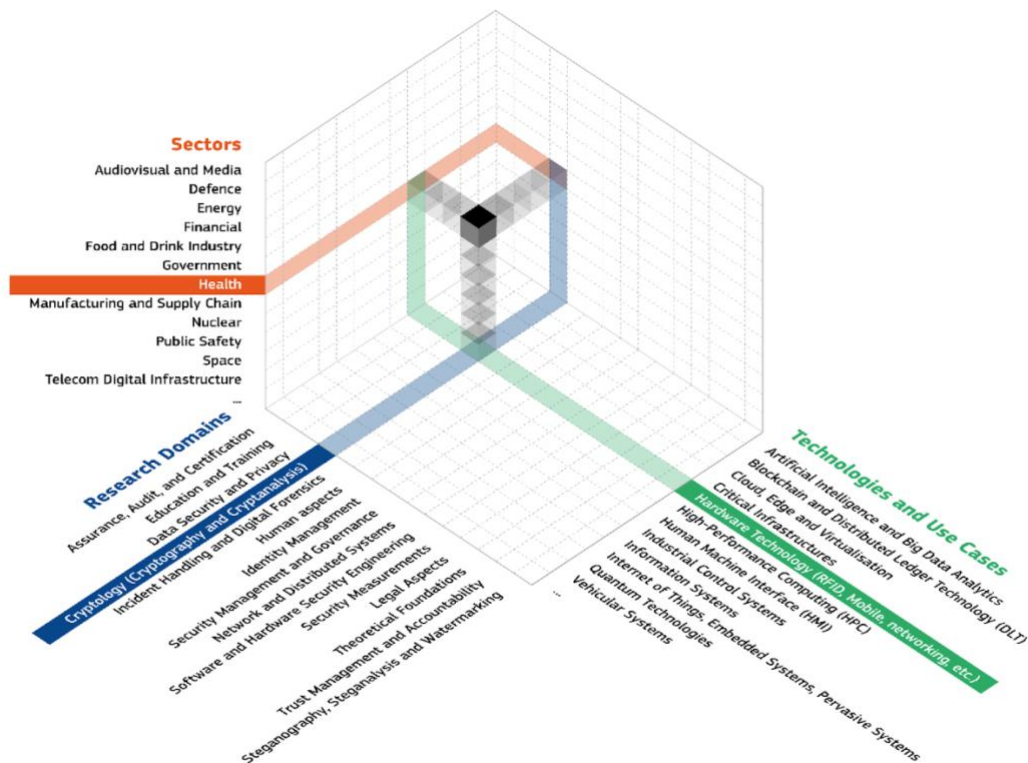


Figure 9: JRC Cybersecurity Taxonomy

According to JRC, the common European cybersecurity Taxonomy will serve to

- Support knowledge management activities
- Enable effective communication among EU HEIs and the cybersecurity community
- Serve as a cornerstone in future cooperation efforts among cybersecurity stakeholders and
- Support governance of future EU cybersecurity initiatives.



The JRC cybersecurity taxonomy results from an extensive literature review. The taxonomy aims at aligning terminologies and definitions of cybersecurity knowledge domains while factoring in the peculiarities of the EU cybersecurity ecosystem.

Figure 9 presents a visual view and summary of the JRC taxonomy, which reflects a three-dimensional matrix comprising three core elements of cybersecurity domains, sectors, applications, and technologies. According to JRC, the three-dimensional structure of the taxonomy is not static but open to modifications, given the rapid changes in the digital world.

The JRC taxonomy provides a classification of cybersecurity applications from a broad perspective, as evidenced by the inclusion of human and non-technological aspects. This implies that the knowledge, skills, and abilities required in the cybersecurity domain are not a focus of the taxonomy. It can be observed from the taxonomy that some of the domains align with notable cybersecurity knowledge areas and competencies. The JRC taxonomy is yet recognized within the EU as a benchmark framework for cybersecurity domain classification across Europe, although it is not a cybersecurity workforce-development-oriented taxonomy. Thus, the JRC taxonomy does not replace other workforce-oriented frameworks but can always be used together.

2.2.3 Cybersecurity Body of Knowledge (CyBOK)

CyBOK is an initiative of the National Cybersecurity Center (NCSC) [33], applicable for any higher education programme (undergraduate and graduate) including secondary education and professional development programmes. Its main purpose is to “codify the foundational and generally recognised knowledge on cyber security” to address the knowledge in cybersecurity [34]. This type of coding translates into addressing cybersecurity knowledge through the collection and classification of information available in the literature, such as standards, scientific research papers, manuals, technical reports, and white papers. Thus, the objective of CyBOK is to map and adapt existing knowledge instead of replicating content (from scratch) on a particular cybersecurity KA [19].

So far, there are two versions of the initiative available at [35], CyBOK 1.0 and CyBOK 1.1. The first version, released in October 2019, contemplates nineteen KAs classified in five different domains as shown below; while CyBOK 1.1, released in July 2021, adds two new KAs (marked with an asterisk in the same table) to CyBOK 1.0, in addition to including one major and one minor revision of the previously identified KAs. In other words:

- Domain 1: Human, Organisational & Regulatory Aspects ⇒ Risk Management & Governance, Law & Regulation, Human Factors, and Privacy & Online Rights).
- Domain 2: Attacks & Defences ⇒ Malware & Attack Technologies, Adversarial Behaviours, Security Operations & Incident Management, and Forensics).
- Domain 3: Systems Security ⇒ Cryptography, Operating Systems & Virtualisation Security, Distributed Systems Security, Formal Methods for Security (*) and Authentication, Authorisation & Accountability.
- Domain 4: Software and Platform Security ⇒ Software Security, Web & Mobile Security, and Secure Software Lifecycle.
- Domain 5: Infrastructure Security ⇒ Applied Cryptography (*), Network Security, Hardware Security, Cyber-Physical Systems, Physical Layer and Telecommunications Security.

Figure 10 also illustrates these five application domains from a more visual point of view, where we can also see that there are certain dependencies between the KAs. For example, Domain 3 coincides with Domain 5 through “Hardware Security and Network Security”, and the same for Domain 4 with “Web & Mobile Security”.

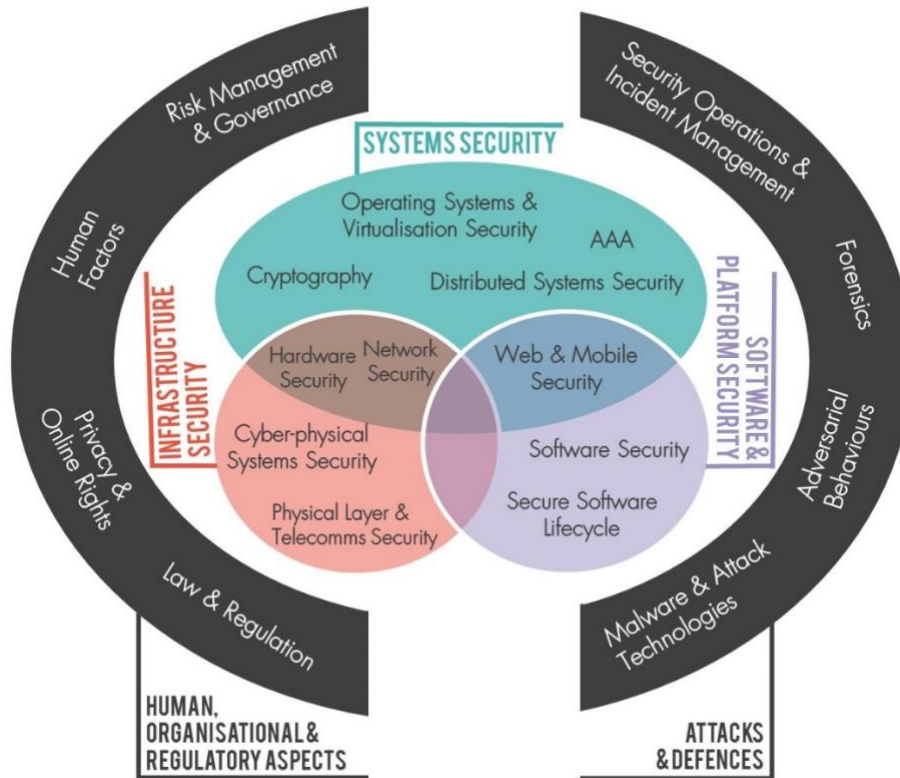


Figure 10: European Cybersecurity Body of Knowledge (CyBOK) Clusters [35]

2.2.4 European e-Competence Framework (e-CF)

The European e-Competence Framework [31] broadly classifies 41 competencies for ICT professionals. Furthermore, the e-CF maps competencies, skills, and proficiency levels to their European job profiles based on an established common language. The e-CF competencies are classified based on five ICT business areas related to the European Qualifications Framework (EQF) European Committee for Standardization currently maintains the e-CF. It has remained one of the gold standards for European HEIs and organizations in the private and public sectors [28]- [36].

The e-CF exhibits a hierarchical structure containing three significant dimensions, which we briefly now highlight.

- The five e-CF competence areas - the five ICT business processes that informed the e-Competence areas include Plan, Build, Run, Enable, and Manage.
- The e-CF competencies - 41 competencies identified and included
- Proficiency levels – 5 proficiency levels adapted from the EQF to indicate performance for each competence and its associated job role.

The e-CF identified 28 ICT job roles. However, only a handful of the 28 job roles may be considered cybersecurity core positions. These roles were mapped to their related competencies and proficiencies within the e-CF. Other frameworks have adopted these competencies, e.g., the ENISA skills framework. Although the e-CF is broad and not targeted at cybersecurity education, it is instructive for CyberSecPro to draw inspiration from the e-CF when developing its cybersecurity professional training programme.



It is also worth noting that the e-CF’s mapping of tasks to competencies and proficiency levels for each given job role could be a good approach to consider when developing the CyberSecPro curriculum.

2.2.5 European Skills, Competencies, Qualifications and Occupations (ESCO)

ESCO is a multilingual classification of EU skills, competencies, qualifications, and occupations. ESCO aims to identify, describe, and classify professional occupations and associated skills essential to the EU job market, education, and training. Currently, ESCO has provided descriptions of 3008 occupations and 13890 associated skills. The document providing these descriptions is available in all official EU languages, including Norwegian, Ukrainian, and Arabic. In addition to delivering multilingual classification, ESCO also aims to facilitate job mobility across Europe to enable an integrated and efficient labour market.

The ESCO systematic classification represents relationships among different concepts categorized in terms of occupations, skills, competencies, and qualifications. For each given occupation, ESCO provides a description and alternative label as well as essential and optional knowledge, skills, and competencies required for the occupation. The skills pillar is designed around knowledge, skills, attitudes, values, and language skills [37]. Furthermore, skill reusability level criteria are included in each skill and competence description for each given occupation.

The current ESCO classification identified about 25 occupations that are related to cybersecurity, providing their description, knowledge, and skills. The related occupations listed in Table 7 have about 300 knowledge and skill descriptors. Some of the skills and knowledge are indicated as either optional or essential. The ESCO classification may be considered too broad even though a good attempt was made to capture cyber and information security occupations.

Table 7: ESCO Cybersecurity Occupations

Cybersecurity Occupations	
ICT Security Manager	ICT Resilience Manager
Chief ICT Security Officer	ICT Security Consultant
ICT Security Administrator	ICT Security Technician
Chief Information Officer	Webmaster
Database Administrator	ICT Network Engineer
Chief Technology Officer	Digital Forensics Expert
ICT Network Administrator	ICT System Administrator
Data Entry Clerk	Enterprise Architect
Database Designer	Chief Data Officer
ICT Technician	IT Auditor
ICT Technician	ICT Disaster Recovery Analyst
Industrial Mobile Devices Software Developer	Communication Infrastructure Maintainer



The ESCO classification may be compared with frameworks like the ECSF, especially concerning cybersecurity knowledge and skills and their associated job profiles. Like the Czech framework, ESCO provides open data that allows external data sources to utilize it. Providing alternative labels for identified occupations and competencies could enhance users' ability to extract and compare ESCO's job profiles with other cybersecurity frameworks. It is also observed that each ESCO-identified occupation is mapped to the International Standard Classification of Occupations (ISCO-08) unit group, an internationally acceptable standard. This mapping enabled national and non-European classification standards to leverage ESCO's classification.

2.2.6 European Cybersecurity Organisation Working Group (ECSO)

ECSO is a European multi-sectoral organisation aiming to develop cybersecurity communities and build the European cybersecurity ecosystem. ECSO collaborates with Europe's cybersecurity public and private sectors. Also included in this collaboration are large corporations, small and medium-scale companies and start-ups, research centres, HEIs and a host of other collaborating entities. ECSO [38] emphasised the notable issue of the cybersecurity-related skills gap and highlighted problems with the shortage of cybersecurity professionals. Some of these problems include the increasing vulnerability of societies and organisations, and skills shortages in HEI, among other problems. The fact that HEIs and professional training centres offer skills that do not address cybersecurity labour market needs gave rise to ECSO's call for developing a cybersecurity framework and close collaboration with all stakeholders.



Figure 11: ECSO Market Demanded Cybersecurity Domains [40]

Furthermore, ECSO established five working groups that enable it to carry out its cybersecurity development initiatives, including workforce skills development. As it concerns CyberSecPro, one of the key working groups to highlight in this report is the Skills and Human Factors group (Working Group 5). ECSO, via the Working Group 5 (WG5) initiative [39], aims to provide education, professional training, skills development, and expertise-building across the European cybersecurity landscape. The long-term vision of ESCO is to have a cyber-resilient, informed and gender-inclusive digital Europe.



European Industry-Academia Joint Workforce and Engagement: The agile and changing cyber environment sets high requirements for workforce awareness, competence, and skillsets. The European Cyber Security Organisation’s consolidated industry, academic, and public sector partnership (composed of around 270 members) is reflected in the development activities of Working Group 5 on “Education, Awareness, Training, and Cyber Ranges” and the Task Force “European Human Resources Network for Cyber” (EHR4CYBER). Cybersecurity education and professional training is one of the key solutions to the shortage of the cybersecurity workforce. Common requirements and a broad understanding between industries and academia for the cybersecurity education and professional training requires common curriculum guidelines. The European Cyber Security Organisation’s 2018 analysis paper on “Gaps in Education & Professional Training and Certification” also clearly indicated this need. In the scope of its SWG 5.2 on “Education & Training”, ECSO would like to provide a viable and sustainable solution with this guideline paper: “European Cybersecurity Education and Professional Training: Minimum Reference Curriculum”.

ECSO’s ongoing work within WG5 revolves around cybersecurity capacity building including cyber ranges to facilitate training and enhance operational competence. Also ongoing is the development of minimum cybersecurity curricula guidelines for HEI and professional training vendors. ECSO’s curriculum proposal is provided in [40]. ECSO worked closely with industry and academia communities to develop one of the pioneering work relevant to European Cybersecurity Workforce Capacity building efforts and common understanding releasing a report and guideline titled, “European Cybersecurity Education and Professional Training: Minimum Reference Curriculum”. ECSO development work identified the market demanded key domains for cybersecurity workforce development as depicted in the Figure 11. The development work is significantly aligned and contributed in the CyberSecPro innovation proposal work. Other ECSO WG5 efforts include supporting HR, skills verification and contributing to Europe’s cybersecurity skills framework. Creating cybersecurity awareness through its cyber hygiene and gender diversity programmes is also ongoing.

2.2.7 ECHO Cybersecurity Skills Framework (ECHO-CSF)

The European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO) is one of the four pilot projects of the European Commission. ECHO is a platform to share knowledge and develop a common European cybersecurity strategy. The 30 partners of the ECHO consortium are drawn from various sectors, including health, transport, manufacturing, ICT, education, energy, telecom, defence, and civil protection. ECHO’s key objective is to strengthen the EU’s cyber defence and enhance the EU’s technological sovereignty via collaboration [41]. As part of its fundamental objective, ECHO develops the EU’s cybersecurity ecosystem that supports secure cooperation, protects EU citizens against cybersecurity threats, and the overall development of the European cybersecurity market.

The main themes within the ECHO project are summarised as follows:

- ECHO Governance Model: Management of direction and engagement of partners (current and future)
- ECHO Multi-sector assessment framework: Transverse and inter-sector needs assessment and technology R&D roadmaps
- ECHO Cyber skills Framework and training curriculum: Cyber skills reference model and associated curriculum
- ECHO Security Certification Scheme: Development of sector-specific security certification needs within the EU Cybersecurity Certification Framework from ENISA
- ECHO Federated Cyber Range: Advanced cyber simulation environment supporting training, R&D and certification
- ECHO Early Warning System: Secured collaborative information sharing of cyber-relevant information

Among other ECHO outputs, the ECHO cybersecurity skills framework and federated cyber ranges are themes that resonate well with CyberSecPro. The ECHO cybersecurity skills framework (ECHO-CSF)



[12] proposes a skills model for ICT and cybersecurity professionals who are tasked with defending and protecting ICT infrastructure and other operational technologies in sectors such as health, maritime, and energy. Additionally, it seeks to provide practical tools to aid the design and development of training programmes that meet the labour market's needs.

The ECHO-CSF (see Figure 12) consists of four self-describing components: the contextualization model, learning outcomes, assessment methodology, and generic curriculum. The ECHO-CSF also captured the relationships and progression from one component to the other. ECHO-CSF adopted a high-level modular approach and appropriate learning methods and tools to arrive at its proposed curriculum. The adopted approach enabled triangulation of the expectations of trainees, the programme content, and the capacity of the training vendor. It also allows each training module to have a tailored pedagogy to achieve learning outcomes and progression between the ECHO-CSF framework components.

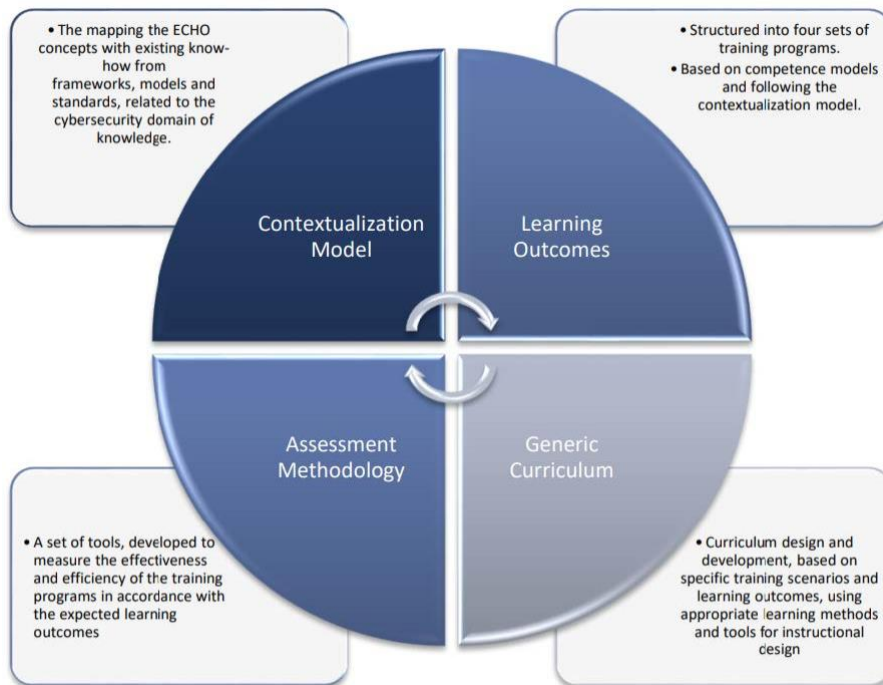


Figure 12: ECHO Cybersecurity Framework

Built around the NIST NICE framework function groups (identity, protect, detect, response, recover), the ECHO-CSF curriculum provides four training programmes designated as training modules. These training modules form the bedrock of the ECHO training cybersecurity pathways. It is also important to note that the primary goal of the curriculum is to provide guidelines for improving the competencies of IT professionals to detect, contain, assess, and deal with cyber-attacks while leveraging ECHO's assets. Based on the ECHO-CSF curriculum, training programmes have been developed for the health, energy, and maritime sectors and organizations.

For each programme module, ECHO's curriculum maps tasks, knowledge, and skills. Knowledge and skills are considered learning outcomes of the module. For example, Table 8 presents a sample of some general and unmapped knowledge areas and skills for the programme module Identify. The knowledge and skills are targeted at training professionals expected to implement cybersecurity risk-related functions such as risk assessment and management, risk prevention, and other functions. These tasks,



knowledge and skills were adopted from the NICE framework as they carried their original identification numbers. The complete mapping and description of each training module are provided in [21].

Table 8: Sample Knowledge and Skills for Identity Module

Cybersecurity Occupations	Cybersecurity Occupations
K0008: Knowledge of applicable business processes and operations of customer organizations	S0038: Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system.
K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	S0372: Skill to translate, track, and prioritize information needs and intelligence collection requirements across the extended enterprise.
K0164: Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes).	S0085: Skill in conducting audits or reviews of technical systems.
K0006: Knowledge of specific operational impacts of cybersecurity lapses.	S0038: Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system.
K0150: Knowledge of enterprise incident responsibilities.	S0372: Skill to translate, track, and prioritize information needs and intelligence collection requirements across the extended enterprise.
K0012: Knowledge of capabilities and requirements analysis.	S0085: Skill in conducting audits or reviews of technical systems.

2.2.8 Cybersecurity cOmpeteNCe fOR Research aND InnovAtion (CONCORDIA)

Commissioned in 2019, CONCORDIA[42] is among the four European Commission-funded cybersecurity pilot projects. CONCORDIA is a consortium of 46 partners drawn from academia and industry. The key goals of CONCORDIA are as follows.

- Development of a platform that enables the creation of cyber ranges across Europe that, in turn, provides training facilities to the consortium and other stakeholders.
- To share cybersecurity scenarios and best practice guidelines.

It is expected that partners will, through the project, enhance cybersecurity training capabilities for professionals (education ecosystem), strengthen the cybersecurity ecosystem and represent real-world cyber threat scenarios in a virtual environment. Cyber ranges within the consortium include Research Institute CODE, Masaryk University, RISE, Universite de Lorraine, and Airbus.

In order to enable the sharing of cybersecurity information across academic, industrial and other organisations, especially as it involves the European cybersecurity emergency response team (CERT), CONCORDIA's purpose is to create a European threat intelligence platform. To realise this initiative,



Cybersecurity Skills Framework and Relevant Initiatives

sector-specific threat intelligence platforms would have to be developed to address the needs of that sector. Table 9 summarises some of CONCORDIA's key and initial public reports on its deliverables since the project's inception. There is still major ongoing work; final reports on these major deliverables are still expected. For instance, reports on the threat intelligence platform, design, and development of the European Secured Resilient and Trusted Networked Ecosystem and cybersecurity roadmap for Europe are yet to be released.

Table 9: CONCORDIA's Reports on Key Deliverables

Paper Title	Objective and Outcome
Designing and Developing European Secure, Resilient and Trusted Ecosystem (ESRTE) [43]–[45]	Conduct excellent academic research to stimulate publication of the scientific result in reputable journals and conferences related to cybersecurity, organisation of cybersecurity events, play a leading role in the organization of the scientific community, contribute to standardization, open research data and code shared via GitHub
Cybersecurity Workforce Diversity [46]	Introduces objectives CONCORDIA targets to address to enable women's inclusion in the cybersecurity domain within Europe. Design of actions to support women's inclusion.
Cybersecurity Roadmap for Europe [47]	Presents CONCORDIA's Cybersecurity Roadmap for Europe
DDoS Clearing House Platform [48]	Describes the concept of Anti-DDoS Coalitions and the DDoS Clearing House, a platform for sharing measurements of DDoS (meta) data between organizations.
Exploitation, dissemination, certification, standardization[49]	Reports on activities performed by the CONCORDIA project on exploitation, dissemination, communication, certification and standardization, within the WP 5



2.2.9 Cybersec4Europe

Like ECHO, CyberSec4Europe is yet another European Commission pilot project comprising 43 partners drawn from 22 EU countries. It is a research and innovation project that is aimed at "designing, testing and demonstrating governance structures for a future European Cybersecurity Competence Network." The project relies on some of CERN's best practices and the capabilities and experience of project partners.

Table 10: CyberSec4Europe Work Package 6 Deliverables

Paper Title	Objective and Outcome
Case Pilot for WP2 Governance [50]	Provides a review of European Cyber Security Massive Open Online Courses (MOOCs) and defines quality assurance criteria for MOOCs to be branded CyberSec4Europe MOOCs.
Education and Training Review [51]	Presents a review of university-based European MSc programmes in cybersecurity with a later view to identifying and prioritizing cybersecurity skills needed at the university level and investigation of existing curricula
Design of Education and Professional Framework [52]	Presents a review of relevant European Cybersecurity related professional education frameworks and develops a framework for assessing skills and competencies required for difference cybersecurity job profiles.
Flagship 1 [53]	An online-only cybersecurity exercise targeted at project partners
Flagship 2 [54]	A cross-border online-only cybersecurity exercise for project partners.
Final Educational and Assessment Framework [54]	Development of European-based cybersecurity education and assessment framework, including guidelines and tools to support the design of capability-building instruments

A broad objective of CyberSec4Europe is to consolidate and project cybersecurity capabilities necessary to secure and maintain European democracy and the integrity of the single digital market.

This overall objective is further broken into policy, technical and innovation objectives. CyberSec4Europe's technical objective, which is to "revolutionize the spectrum of education and training in cybersecurity by developing a novel cybersecurity skills framework model for both education providers and employers leading to a better cybersecurity workforce," aligns with CyberSecPro.



Considering this, and within Work Package 6 (Cybersecurity Skills and Capability Building) of the project, several deliverables have been achieved with respect to cybersecurity professional education. The project kicked off in 2019, and Table 10 summarises some of the project's outputs related to CyberSecPro.

2.2.10 Strategic Programmes for Advanced Research and Technology in Europe (SPARTA)

SPARTA is another EU-funded cybersecurity project that was commissioned in 2019 to, among other objectives, develop a cybersecurity workforce skills framework [13] and a cybersecurity curriculum [19], [55], [56]. Another key objective of SPARTA was the development of threat intelligence models, including advanced methodologies and technologies required to identify and fight multilayer complex cybersecurity attacks. According to [3], the development of cybersecurity workforce skills is fundamental to the comprehension of complex and emerging cybersecurity threats

The NIST's NICE framework inspired SPARTA's cybersecurity skills framework (S-CSF). However, S-CSF majorly aimed to accommodate EU peculiarities that were not considered in NICE since NICE is a USA-based cybersecurity skills framework. These peculiarities are mainly related to the EU's general data protection regulation compliance (GDPR). SPARTA's efforts are geared towards closing the cybersecurity skills gap by providing a basis for developing a European cybersecurity skills framework. Other key initiatives that informed S-CSF include ENISA's cybersecurity education map, the European e-competence framework, and the joint research consortium of EU cybersecurity centres of expertise map. To be well-informed and as a good foundation for the development of the S-CSF, the SPARTA team mapped the JRC cybersecurity domains with the NICE framework. The mapping result supported the use of NICE as a basis for developing S-CSF from the perspective of the EU cybersecurity ecosystem.

Towards creating an EU-compliant cybersecurity skills framework, the SPARTA project team considered: 1) EU regulations (GDPR), 2) Aligning the S-CSF references to relevant EU legal documents, and 3) Introducing cybersecurity job roles as legislated by each EU member state. In adapting the NICE CSF to the EU's legal and regulatory landscape, S-CSF focused on modifying the Data Protection Officer (DPO) role, which appeared to align with the NICE Privacy Officer role. Because of the overlapping functions of the NICE Privacy Officer role with the GDPR DPO role, the S-CSF included the GDPR DPO role as a distinct role that demands accountability and special reporting. The roles of Cyber Policy and Strategy Planner and Executive Cyber Leadership were modified in S-CSF to read as Cyber Privacy Policy and Strategy Planner and Executive Cyber Privacy Leadership. Table 11 and Table 12 present the S-CSF adaptation of NICE CSF to accommodate EU rules and regulations.

The S-CSF maintained the same structural representation (categories, specialities, work roles) provided in the NICE CSF. Compared to NICE CSF, the only difference in S-CSF work roles is the inclusion of Data Protection Officer and Cyber Security Officer roles unique to each EU Member State. Similarly, cybersecurity knowledge, skills and abilities provided in NICE CSF are also retained in SPARTA CSF.



Table 11: Knowledge Adaptation of NICE CSF to EU Legal Landscape

U.S Law Specific in NICE CSF	EU Law Specific in S-CSF
Knowledge of information security systems engineering principles (NIST SP 800-160).	Knowledge of information security systems engineering principles (NIS directive)
Knowledge of Privacy Impact Assessments.	Knowledge of Privacy Impact Assessments (e.g., Data Protection Impact Assessment (DPIA)).
Knowledge of legal governance related to admissibility (e.g., Rules of Evidence). Knowledge of national legal acts related to admissibility.	Knowledge of national legal acts related to admissibility.
Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)	Knowledge of Supply Chain Risk Management Practices (e.g., INT/681-EESC-2013-165325)
Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Knowledge of EU Law's, directives, Regulations, Decisions, Recommendations, Opinions.
Knowledge of Personally Identifiable Information (PII) data security standards.	Knowledge of General Data Protection Regulation (GDPR)
Knowledge of Personal Health Information (PHI) data security standards.	Knowledge of the General Data Protection Regulation (GDPR) ²⁸ directive definition for health data for data protection purposes.

2.2.11 REWIRE Cybersecurity Skills Framework

The REWIRE project is an EU-funded cybersecurity workforce development initiative. Some of the key objectives of the project include: 1) conduct an analysis of current cybersecurity skills frameworks in terms of competencies, qualifications, and occupations b) Based on the European Skills, Competencies, Qualifications and Occupations (ESCO) and other existing competence frameworks, revise and develop cybersecurity job roles and their associated demanded skills. The REWIRE project also aims to inform and enhance ENISA's cybersecurity skills framework.

In order to produce the REWIRE cybersecurity skills framework, the project team mainly relied on a review of existing cybersecurity skills frameworks and cybersecurity job analysis tools. The job analyser tool was used to analyse cybersecurity job ads and enable the identification of cybersecurity job roles, knowledge, skills, and competencies.



Table 12: Cybersecurity Roles Adaptation of NICE CSF to EU Legal Framework

Role	U.S Law Specific in NICE CSF	EU Law Specific in S-CSF
Authorizing Official/Designating Representative	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009).	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (NIS Directive).
Security Control Assessor	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (i.e. as described in NIS Directive).
Communications Security (COMSEC) Manager	Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS).	Individual who manages the Communications Security (COMSEC) resources of an organization (NIS Directive) or key custodian for a Crypto Key Management System (CKMS).

One of the early key contributions of the REWIRE project is the identification of gaps in ENISA’s ECSF. One of such gaps is the need to create a hierarchical structure between proposed cybersecurity job roles. According to [14], a hierarchical structure enables the elicitation of vital information (e.g., job role definition, minimum skills, knowledge, and e-competencies required to implement a role, knowledge, skills, and e-competencies needed to switch between roles, among others) necessary for effectively defining and classifying a job role. On this basis, REWIRE recommends that job roles be re-categorized into three levels “Junior, Middle, Senior” and their associated relevant skills.

Following their hierarchical structure, the project team identified the e-competencies required of each ENISA’s ECSF job role (see full details in [14]). An e-competence is either mandatory or optional. The gaps identified motivated the project team to deconstruct ENISA’s ECSF job roles to ensure a shared



understanding and use of the same language. The deconstruction exercise resulted in a list of cybersecurity tasks (134), skills (158) and knowledge (140). At this juncture, these lists of tasks, skills and knowledge were not mapped to any job profiles but were subsequently mapped according to REWIRE’s recommendations. For each ENISA job role, REWIRE project team proposed an adaptation or change to some of ENISA’s ECSF offerings or outright removal. In another case, the relevant information is added to the current information in ENISA’s ECSF proposal. Full details of the proposed changes and other recommendations are provided in [14].

Table 13 and Table 14 summarise REWIRE’s recommended changes to ENISA’s ECSF. The tables focus mainly on cybersecurity job roles, skills, knowledge, and competencies.

Table 13: REWIRE Cybersecurity Skills Recommended Changes

S/N	ENISA ECSF job roles	REWIRE Alternative Job roles proposed	No. of skills adaptations proposed	No. of new skills included
1	Chief Information Officer	Information Security Manager/Chief ICT Security Officer/ICT security manager/Information systems security manager	7	30
2	Cyber Incident Responder	Incident response engineer/Cyber incident/crisis manager/Blue team member/Incident management team member (white)/Member of the IRT	1	7
3	Cyber Legal, Policy & Compliance	Privacy Compliance Manager/Cyber Legal Advisor/Cyber Security Advice and Assessment	2	19
4	Cyber Threat Intelligence Specialist	None	2	4
5	Cybersecurity Architect	Security Architect/Senior Security Architect/Information Security Architect/IT Security Architect/Cyber Security Architect	1	23
6	Cybersecurity Auditor	Information Security Auditor/Information Security Risk and Compliance Auditor	0	19
7	Cybersecurity Educator	Digital Educator/Cyber Instructor	1	10
8	Cybersecurity Implementer	Cyber Defense Infrastructure Support/ICT security specialist/Cybersecurity Engineer/Security Specialist	1	10
9	Cybersecurity Researcher	None	1	2



Cybersecurity Skills Framework and Relevant Initiatives

10	Cybersecurity Risk Manager	Cyber Risk Manager/Information Security Risk Manager	16	0
11	Digital Forensic Investigator	Incident responder/Security Incident Response Engineer/Malware analyst/CTI analyst	2	8
12	Penetration Tester	Red Teamer	3	2

Table 14: REWIRE Cybersecurity Knowledge and Competencies Recommended Changes

S/N	ENISA ECSF job roles	No. of knowledge areas adaptations proposed	No. of new knowledge areas included	No. of competences adaptation proposed	New competences included
1	Chief Information Officer	10	46	0	9
2	Cyber Incident Responder	3	12	0	4
3	Cyber Legal, Policy & Compliance	2	24	0	4
4	Cyber Threat Intelligence Specialist	0	5	0	5
5	Cybersecurity Architect	4	12	0	5
6	Cybersecurity Auditor	0	11	0	3
7	Cybersecurity Educator	3	4	0	3
8	Cybersecurity Implementer	7	6	0	8
9	Cybersecurity Researcher	6	1	0	6
10	Cybersecurity Risk Manager	2	0	1	0
11	Digital Forensic Investigator	3	8	0	2
12	Penetration Tester	3	4	0	0

Apart from REWIRE's proposed modifications and inclusions of new skills, knowledge areas and competencies, most of ENISA's ECSF proposals were primarily retained by REWIRE.



2.3 EU and Member States: Notable Cybersecurity Strategies, Guidelines and Directives

This section is presenting a review of cybersecurity workforce development initiatives embarked upon by CyberSecPro consortia member participant European countries. The report cannot cover all the European countries due to lack of access to correct information in local European languages, therefore, the report presents only from CyberSecPro partners representing European countries below.

2.3.1 EU Member State Initiatives: Austria

The Austrian Cyber Security Strategy was first developed in 2013 and has been regularly expanded and new parts added. The latest published version dates from 2021 and essentially includes the changed political situation and the European developments in the field of cyber security. The strategy had to be adapted to the new definition according to the NIS Directive and the NIS2 Directive in order to ensure the functioning of the internal market. At the political level, it was recognised that cyber security is a cross-cutting issue for the entire state and for this reason requires coordination structures that require cooperative collaboration and thus models. At the strategic level, the Federal Chancellery (BKA) oversees coordination and works together with national, European and international coordination bodies across sectors and departments. Furthermore, the Federal Ministry for European and International Affairs (BMEIA) acts in close cooperation with the BKA at the international level within the framework of foreign and security policy. Domestically, the security ministries, the Federal Ministry of the Interior (BMI) in the context of maintaining public peace, order, and security in the area of cyber security and combating cybercrime, and the Federal Ministry of Defence (BMLV), which in turn is responsible for military national defence in cyberspace, work together. This resulted in close coordination between the ministries in charge of cyber security at the strategic and operational levels. However, other ministries whose sphere of action is affected may be involved. This is ensured by the Federal Ministries Act (BMG).

The structures established in Austria for the security of network and information systems for coordination at the political, operational, and strategic levels (see picture) The operational level continuously prepares situation reports for the coordinated deployment of cyber forces and management of cyber incidents. The following teams were formed from this structure: "Operative Coordination Structure (OpKoord)" and the core element "Inner Circle of the Operative Coordination Structure (IKDOK)". These are organisationally led by the Federal Ministry of the Interior and, in the event of a crisis, form a direct interface to the national cyber crisis management (CKM). The CKM is a platform for interdepartmental coordination. In principle, the Federal Ministry of the Interior is responsible for all crisis cases. However, should a situation arise in the course of the cyber crisis in which sovereignty-threatening attacks are carried out, the leadership and thus the operational command will be transferred to the Federal Ministry of Defence. The Cyber Security Steering Group (CSS) and the Cyber Security Platform (CSP) also operate at the strategic level. The CSP is a central exchange and cooperation platform for the economy, science, and public authorities.

Current and future challenges: A future-oriented cyber security policy enables the enormous opportunities and potentials of digitalisation to be used comprehensively and securely. For this reason, the following challenges for Austria were identified and described in the cyber security strategy:



Cybersecurity Skills Framework and Relevant Initiatives

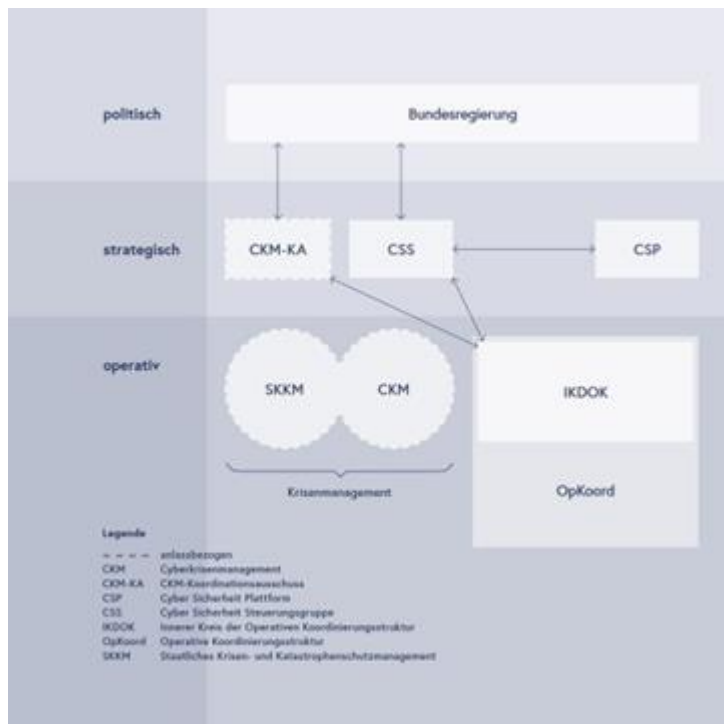


Figure 13: Austria- Operative Coordination Structure

(1) Threats that are the result of the misuse of information technology (IT) State and non-state actors use cyberspace as a field of action for ideologically, politically, and criminally motivated cyber-attacks. These range from cybercrime to cyber espionage, which can occur independently or as part of hybrid threat scenarios, to cyber warfare. The deliberate use of the IT-supported information space for the purpose of manipulating, influencing and destabilising democratic opinion-forming processes also falls into this area. [57]

(2) Threats that are the result of improper use of IT In addition to the improper and malicious use of IT, improper use can also lead to challenges. Improper use usually

arises due to a lack of user knowledge. In addition, carelessness, and negligence on the part of users lead to the realisation of numerous risks. These can only be countered to a limited extent even with security technologies. Insufficient preparation for attacks as well as negligent operation of IT makes companies and organisations particularly easy targets. This applies to the entire value creation and production process, including all "suppliers" involved. The latter must be comprehensively assessed during risk management [57].

(3) Threats that are the result of IT dependency challenges arise not only from insecure IT products and services but also from the increasing dependency on their availability. Thus, even the failure of originally secure technologies can lead to economic damage and threats. In this sense, the use of cloud technologies, for example, can bring new risks. In relation to the increasing dependency, the lack of skilled workers in the field of cyber security also poses a challenge. Digitalisation will increase dependency on IT in the future, and new challenges will arise in the face of the digital geopolitics of states, the complexity of internet governance, scarcity of resources and increasing dependency on space infrastructure [57].

(4) Threats from new technologies the digitisation of areas and processes that have not previously used IT creates new security-related challenges. In addition, the displacement of IT applications previously in use by new technologies can also lead to such challenges. This is expected in the future, especially through developments in the field of artificial intelligence (AI), the Internet of Things (IoT) and other Emergent and Disruptive Technologies (EDT), such as quantum technology. Likewise, the functional change of IT can also encompass new risks, especially if previously supporting IT applications become a supporting or controlling component. In addition to security-related challenges, this is often accompanied by technical and ethical issues [57].



Vision and goals of the Austrian cyber security strategy: Austria has decided on a nationwide cyber security policy and the creation of a secure cyberspace, which in turn is seen as part of comprehensive national defence and security provision. For this reason, it has the task of guaranteeing state sovereignty to the outside world. This results in the following vision: The long-term creation of a secure cyberspace as a contribution to increasing the resilience of Austria and the European Union through a whole-of-government approach [57].

The following goals can in turn be derived from this: 1) Austria has sufficient financial and human resources to prevent cyber threats and incidents, to recognise them as such, to defend against them and to prosecute such attacks; 2) Austria has the capacity to protect and defend its critical information systems and infrastructures in the event of a crisis; 3) In Austria, cyber security is perceived as a joint task of society, the economy and the state; responsibilities and competences are clearly defined and lived by all those involved; 4) Austria has an overall national cyber situation; cyber security competences are strengthened and promoted in all areas of society, life and work, and awareness is created; 5) In Austria, citizens can safely participate in social and political life in cyberspace; 6) Austria has clear legal and operational possibilities to offer a secure and attractive business environment in cyberspace and, if necessary, to ensure adequate law enforcement; 7) Austria is actively engaged in the cyber domain and works intensively with all stakeholders at national, European and international level; 8) Austria can ensure its digital sovereignty in cooperation with the EU and contribute to the strategic autonomy of the EU; 9) Austria has a coordinated and networked research and development landscape in the field of cyber security; 10) Austria trains a sufficient number of cybersecurity professionals to increase cybersecurity resilience, meet labour market demand and sustainably combat cybercrime; 11) Austria actively contributes to the application and strengthening of international standards for cyberspace; 12) Austria takes a whole-of-government approach to steadily develop its legal framework to increase cybersecurity and combat cybercrime [57].

2.3.2 EU Member State Initiatives: Belgium

Cybersecurity Strategy and Focus Areas: In May 2021 the Belgian Center for Cybersecurity released Belgium's Cybersecurity Strategy 2.0. This strategy is outlined by six strategic objectives to be achieved for the years 2021-2025. The aim of these objectives is to encapsulate the multiple trajectories that Belgium is committing to pursue in the following years in order to rise to the challenge that latest technological developments pose whilst still empowering and protecting its population and critical sectors. These six strategic objectives are briefly described below:

- **Strengthening the digital environment and increasing trust in the digital environment:** Belgium plans to reinforce the digital environment and increase its trust level by investing in strengthening its national network infrastructure, adopting more secure internet standards, and laying the groundwork for across-the-board standardisation of cybersecurity certifications, products, and services. Furthermore, to foster expertise and knowledge and to assist intelligence and security agencies, R&D projects will be endorsed, and Cyber Green Houses are being established.
- **Arming users and administrators of computers and networks:** Another focus area of the cybersecurity strategy for Belgium revolves around the people that manage and monitor the proper function of underlying infrastructures. To be successful in this venture Belgium has already taken the initiative by raising awareness and engaging users and administrators of computers and networks regarding current threat and vulnerability trends, concurrently, Belgium is in the process of disseminating cybersecurity guidelines and best practices for the proper disclosure and enumeration of threats and vulnerabilities along with their mitigations.
- **Protecting Organizations of Vital Interest from all cyber threats:** Belgium also plans to protect organisations hosting critical infrastructure of vital interest from all cyber threats. Having adopted the disseminated cybersecurity guidelines and best practices, some steps to further enhance current security include optimising information exchange and alerting systems.



Cybersecurity Skills Framework and Relevant Initiatives

Also, the improvement of the current protection of critical international institutions will be enhanced by building incident response procedures and exhaustively testing them in cyber defence exercises.

- **Responding to cyber threats:** Belgium has committed to improving their member-state's capacity to respond to cyber threats by firstly strengthening defensive capabilities in the cyber domain as well as improving and arming its repressive arm with the intention to swiftly respond to cybercrime. Furthermore, Belgium is aiming to map and identify potential threat sources and remain vigilant against their existing techniques and tactics. In the same direction, they have made a commitment to accurately and with purpose identify and attribute cyberattacks to the responsible actors and take actions to disrupt existing or developing criminal cyber infrastructure.
- **Improving public, private, and academic collaborations:** Another vital focus point of the Belgian strategy is promoting coordination and collaboration between the public, private and academic sectors. This goal can be achieved through the reinforcement of the Cyber Security Coalition in order to develop a unified pipeline that can shape the future of cybersecurity through the propagation of proper hierarchies and procedures.
- **Making a clear international commitment:** As the final strategic point of the Cybersecurity Strategy 2.0, Belgium offers a clear, open commitment to support the EU and NATO in promoting a free, open, and secure internet. Consequently, the strategy prescribes for Belgian authorities to work closely together and actively participate in international and intra-European organisations such as the Cyber Security Coalition, as well as ENISA, the agency of cybersecurity in Europe, which holds a particular importance for Belgium's initiatives.

Cybersecurity Education, Skills, and Workforce Development: Many key actions prescribed under the Cybersecurity Strategy 2.0 are introduced with the purpose of educating security professionals and increasing held knowledge within educational institutes and private sectors. These actions are developed across the board; from raising awareness of younger people towards STEM and security-related fields, training security professionals within the public and private sector, as well as increasing the level of security education provided within educational institutes.

Furthermore, R&D investments in educational institutes will be increased in the Cybersecurity field with the purpose of enabling research in this sector and empowering the development of training material, provision of training and exchange of knowledge. European initiatives will play an important role in fulfilling these objectives, some of the key actions along this direction are described below:

Raise awareness and engage: The government of Belgium, intends to safeguard its citizens against potential cyber threats by implementing a multifaceted action plan that seeks to educate the public on the effective use of technical protection measures and cultivate a culture of vigilance to better detect and defend against cyber-attacks. This comprehensive approach includes raising public awareness on the criticality of cybersecurity through a variety of means, as well as the dissemination of informative resources and guidelines via the CCB's (Centre for Cybersecurity of Belgium) public facing portal, www.safeonweb.be, as well as promoting citizen participation in reporting suspicious emails to the dedicated email address suspicious@safeonweb.be.

Furthermore, the CCB, in its pivotal role, is not only organising annual awareness campaigns but also collaborating with other European initiatives such as ENISA's European Cyber Security Month. The primary aim is to motivate the public to be active in securing themselves through multiple awareness-raising campaigns ranging from webinars to guides and the cybersecurity KIT, all designed to empower citizens to take proactive measures to safeguard their digital footprint. In addition, the streamlining of communication channels between citizens and cybersecurity service providers is being prioritised, which will undoubtedly facilitate the swift and effective handling of security incidents.

Promote coordination and collaboration: Multiple of the new directives for cybersecurity in Belgium have introduced novel assignments of obligations to a variety of stakeholders that encompass the public,



private, and scientific sectors. Coordination efforts within these actors will be led by the national authority, CCB. To facilitate an exchange of knowledge and response to emerging threats, extant or new platforms will be utilized. Additionally, recurrent industry events provide experts with the opportunity to communicate experiences and insights directly to each other. It is anticipated that the resulting open and structured dialogue will bolster CCB's capacity to better map the dynamic landscape of cybersecurity and evolving technologies.

Supporting the Cyber Security Coalition: The Cyber Security Coalition, an initiative in Belgium, has garnered a hundred members from diverse backgrounds, including academia, public agencies, and the private sector, who collectively collaborate to combat the ever-increasing threat of cybercrime. By sharing knowledge and experiences, organizing cross-sector initiatives, raising awareness, promoting expertise, and making policy recommendations, this Coalition serves as a formidable force in ensuring the safety of the digital landscape. And, in a show of support, the government, including the CCB, pledges to actively back the coalition in its pursuits.

Strengthening the cyber skills of intelligence and security agencies: To effectively counter the ever-increasing cybersecurity threats, it is imperative that intelligence and security services cultivate the requisite capabilities and skills. This, in turn, necessitates the employment of highly trained technical experts who can serve as their primary defence against such threats. In order to attract the necessary talent, alternative recruitment and employment strategies must be evaluated and implemented. This includes the provision of flexible recruitment options and competitive remuneration packages to enable these experts to compete with the offerings of specialized companies and large multinationals. Furthermore, it is imperative that technical cybersecurity experts receive top-notch training from government departments to guarantee their proficiency and continued motivation.

Cybersecurity Capacity and Capability Building Initiatives: Belgium's multi-faceted approach to combating cyber threats is both proactive and focuses on innovation. The member-state's leadership acknowledges the constantly changing nature of these threats and has implemented new cybersecurity directives to equip organisations with the necessary tools and knowledge to combat them effectively. These following directives are aimed in increasing the capacity and capabilities of individuals within private and public organisations:

Increasing capability, sharing guidelines, and developing innovation: Belgium has taken a proactive stance in the fight against cyber threats. With the recognition of the rapidly evolving nature of these threats, the country has put new cybersecurity directives in place to ensure that organisations are equipped with the knowledge and tools necessary to combat them. To this end, the CCB has developed an Online Cybersecurity Reference Guide, which provides basic and advanced recommendations based on international standards, to help organisations develop a robust cybersecurity strategy.

However, guidelines alone are not enough. Belgium is also in the process of creating a framework for companies to evaluate and certify the security of their ICT products, services, and processes, in line with the EU Cybersecurity Act 2019. This framework will establish a National Cybersecurity Certification Authority (NCCA), which will coordinate expertise, authorise certificates, and establish cooperation with relevant authorities. Additionally, the country is focusing on developing a cybersecurity recognition mechanism for SMEs, which will emphasise basic cybersecurity requirements and best practices. This multi-faceted approach is intended to boost customer confidence in the security of the digital environment, particularly in strategic sectors, where an integrated approach combining IT, physical protection, and staff screening is recommended.

But the fight against cyber threats also requires innovation and collaboration. This is where the concept of establishing a “Cyber Green House” within Belgium, which will play an important role by developing secure and controlled environments for testing and developing new cybersecurity technologies and practices. By providing a platform for cybersecurity professionals to work together to innovate and test new technologies, strategies, and policies, improvements will be made to the speed of innovation, reducing the risk of cyber threats, and creating a community of experts to share knowledge and best practices. In this way, Belgium is not only reacting to cyber threats, but also proactively working to stay ahead of them.



Develop an appropriate defensive and repressive capability: In response to the rapidly evolving cyber threat landscape, Belgium is taking proactive steps to bolster its defensive and repressive capabilities. The expansion of cyber capabilities within the General Information and Security Service and the Ministry of Defence, prioritised by the government, aims to provide a comprehensive understanding of the cyber threat landscape, and protect against it. To this end, an additional component will be added to the library of the Belgian Ministry of Defence's public-facing tools that focuses exclusively on cyber threats, with the goal of enhancing understanding of both the risks and opportunities of the digital world.

This component will have a multifaceted role, including supporting society during hybrid crises and contributing to NATO's vision of cyberspace as a new operational domain for military and intelligence operations. The latter reflects the increasing use of the internet as both a target and tool in international conflicts.

In parallel with this defensive strategy, Belgium is also working to develop a robust repressive capacity. This involves implementing new cybersecurity directives aimed at reducing the country's vulnerability to cyber attacks. The government is building mechanisms to develop integrated capacity and expertise at all levels of the police, ensuring that prosecutor's offices and courts are equipped with the necessary resources and personnel to effectively investigate, prosecute, and sanction cybercrime.

To guide these efforts, an extensive policy on cybercrime has been put in place. The objective of these measures is to rapidly and effectively respond to cybercrime, thereby enhancing Belgium's security in the digital age. As the cyber threat continues to grow, Belgium recognizes the need to stay ahead of the curve, both defensively and repressively.

Mapping international threats, sharing information about threats and securing international institutions: In today's ever-evolving cyber landscape, identifying and monitoring potential sources of international cyber threats is critical. Belgium, recognizing this, has introduced new cybersecurity directives that emphasise the importance of continuous assessment and monitoring of cyber intentions and capabilities. However, keeping up with the evolving tactics, techniques, and procedures of cyber attackers is not the sole focus of this action, as evaluating the effectiveness of our means of protection against these threats is equally important.

To stay ahead of the curve, Belgium's Cyber Security Coalition, along with sectoral authorities and professional organisations, will keep organisations informed of significant risks through timely warnings for emerging cyber threats and vulnerabilities. Meanwhile, the Computer Emergency Response Team and the national CSIRT will work with internet service providers to detect, analyze, and inform users of security issues. This is just one part of a comprehensive approach to informing the public, with BE-Alert, provided by the National Crisis Centre, serving as a critical tool for sending alerts to the public.

Furthermore, the national cybersecurity authority, CCB, has an Early Warning System in place to receive and distribute threat information to Organizations of Vital Interest. The responsibility of identifying, regulating, and monitoring these organisations falls to each sector's authorities, with the CySSAP consultation platform helping to improve and optimise the exchange of information. This is especially important for organisations with cross-border dependencies, as effective communication and cooperation are critical to providing effective protection and response to cyberattacks at a multi-national level.

Belgium's new cybersecurity directives aim to improve protection for vital organisations that support international institutions like NATO and the EU. With these institutions facing an increasing number of cyber threats, effective protection and response require good communication and cooperation. With these measures in place, Belgium is taking important steps to safeguard against cyber threats in an increasingly interconnected world.



Exercises for incident preparedness: Belgium's approach to improving cyber readiness combines both national and international cooperation. To ensure the effectiveness of its Cyber Emergency Plan, the plan is annually evaluated and adjusted with the coordination of the CCB. Regular exercises are conducted to test the plan's resilience and to identify any weaknesses that may arise. Such exercises involve Belgian security forces, government departments, and Organizations of Vital Interest, with the coordination of the CCB, FPS Foreign Affairs, NCCN, and the Ministry of Defence.

Moreover, Belgium has taken additional measures to handle incidents with national impact through the implementation of new cybersecurity directives. The National Cyber Emergency Plan is an integral part of these directives, which should enable national organisations such as CERT.be, the Integrated Police Services, and the National Crisis Centre to respond quickly and effectively to any cyber incidents. Legal investigations are immediately initiated and incidents with national impact are escalated to Rapid Reaction Teams, where other services and partners are also efficiently engaged. This holistic approach ensures that Belgium is well-equipped to handle any cyber incidents that may arise both domestically and abroad.

Disrupting criminal cyber infrastructure and improving attribution: Belgium's new cybersecurity directives are focused on disrupting criminal cyber infrastructure and attributing cyberattacks to individuals, groups, or states. The goal of disrupting criminal cyber infrastructure is to dismantle the business models of cybercriminals by neutralising their infrastructure, detecting compromised systems, and notifying their owners. In addition, Belgium seeks to protect public and corporate communications while sharing intelligence among security agencies. Cybercriminals often reuse attack techniques and software from the Dark Web and operate under the cloak of anonymity, making it difficult to combat their high-tech or large-scale cyberattacks.

Attribution of cyberattacks is a critical issue for Belgium and is also a hot topic in international politics. Organisations such as NATO, EU, and UN are currently discussing this matter. However, determining attribution remains a political and sovereign decision that has far-reaching foreign policy implications. To address this, Belgium has established a coordinated national procedure for thoroughly analysing and deciding on attribution, which requires capacity building. This approach will ensure that Belgium is equipped to attribute cyberattacks to the appropriate individuals, groups, or states, while also safeguarding its own national interests.

In summary: Belgium's Cybersecurity Strategy 2.0, having been disseminated since 2021, proves to be an effective one, focusing on multiple aspects of society, industry, and education that can help predict, prevent, and thwart cyber attacks. Effective tools for informing and engaging the public have already been provided and multiple layers of infrastructure, public and private sector initiatives are driven to propagate awareness and a proactive approach to security for the public, employees and leadership roles.

Relevant to CyberSecPro, many of the initiatives under the new strategy are aimed at increasing investment and activity in the Cybersecurity education by engaging research, development, and academic stakeholders and driving forward the creation and dissemination of public-facing, as well as specialised security training material, as well as enabling and organising training events for individuals in the public and private sector alike.

2.3.3 EU Member State Initiatives: Cyprus

In 2018, the Digital Security Authority (DSA) of Cyprus was appointed as the Single Point of Contact in relation to the NIS Directive and provided with the supervisory authority of the National, Governmental, and sectoral CSIRTs in Cyprus. The DSA publishes a Cybersecurity Strategy for the Cypriot Republic. The latest version of this document was published in 2020 and is available on DSA's website [58].

The purpose of the Cybersecurity Strategy of the Republic of Cyprus is the protection of the critical information infrastructures of the state and the operation of the country's communication and information technologies with the required levels of security, for the benefit of each user, the economy, and the country. It covers actions related to governance, crisis response and management, awareness



building, research and development, education, and international cooperation. The strategy defined activities to be carried out in 15 distinct thematic areas, the most relevant to education and training being: Thematic Area: 9 - Awareness - Creation of a Security Culture, Thematic Area: 10 - Education and Training and Thematic Area: 12 - Collaborations with the private sector. For each of these thematic areas, activities are also identified within the document.

Specifically, the following activities are identified:

- Activity 14. Implementation and promotion of a National Awareness Programme on cybersecurity covering all digital users (employees of the private or public sector as well as society at large). Within this activity, the application of a strategy for children, parents and educators shall be promoted, as well as the establishment of a “centre” for secure computing skills coordinated by the Cyprus Pedagogical Institute and the Ministry of Education, sport and Youth.
- Activity 15. Personnel development activities.
 - Identification of suitable and available training programmes and certifications for security professionals.
 - Promotion and exploitation of national and governmental training programmes.
 - Development of training programmes and skills development for cybersecurity experts/professionals and others.
 - Adoption of skills certifications in the official governmental job descriptions.
 - Promotion of training programmes within the schools (aiming at igniting the interest of children in cybersecurity and informing them regarding relevant career choices).
 - Promotion and support of Higher Academic Institutions in the development of relevant degrees and courses.
 - Targeted activities aiming to alleviate the gender gap in cybersecurity.

Regarding activity 14, an awareness campaign especially targeting children was also developed by the DSA and within 2022 the DSA participated in the European co-funded project CYberSafety [59]. The Cyprus Safe Internet Center - CYberSafety [59] has been operating since July 1, 2016, under the coordination of the Cyprus Pedagogical Institute [60], utilising European funding, within the framework of the Better Internet for Children Program Kids. The European CYberSafety project brings together the main national stakeholders to create a culture of safer internet, empowering creative, innovative, and critical-thinking citizens in the digital society. Its aim is to provide safer internet for children in Cyprus.

In particular, the Center is supported by the Awareness and Information Center [61], which develops rich educational/information materials, resources and tools, as well as organized campaigns to empower children, young people, parents and teachers, with skills and knowledge about Internet safety. At the same time, the Center is supported by the Helpline and Complaints Line 1480, which provides information, advice and support to children, young people, parents, and educators, on issues related to the use of digital technologies and the Internet (e.g., cyberbullying, excessive Internet use, online seduction (grooming), child sexual abuse and exploitation content, racist material).

Based on the 2021 Activity Report [62], during this year, the relevant working groups and sub-groups will converge in order to proceed with the implementation of the relevant activities. It is also expected to start mapping the current state of cybersecurity-related issues; both in school and academic education as well as in matters of certification and training. In addition, the process will begin in order to draw up, first the profiles of the graduates and then the profiles of the professionals, so that define, in a clear way, the knowledge and skills required of everyone in subjects’ cyber security.



Seminars have taken place on the issues of "Information security risk Management in critical infrastructures", and the "Train the Trainers" awareness programme in cooperation with the Ministry of Defense. Moreover, on the occasion of European Cyber Security Month, DSA has organized in cooperation with various organizations the following activities: A seminar on "Cybersecurity essentials for SMEs" in collaboration with the Cyprus Chamber of Commerce and Industry, and an awareness campaign (ASPIS II) in collaboration with the Cyprus Police and the Cyprus banking association on Cyber fraud, phishing, smishing, vishing and ransomware.

During the presentation of the event "REWIRE 1st Info Day - CY" [14], Mr. Diamandis Zafeiriadis, the head of DSA, mentioned that the DSA has internally reviewed and adopted the relevant ECSF (European Cybersecurity Skills Framework) in the internal operation of the DSA. By decision of the Council of Ministers, dated 21 December 2021, the Digital Security Authority (DSA) has been designated as the National Cybersecurity Coordination Centre (NCCC-CY) for the Republic of Cyprus. The mission of the NCCC is to provide knowledge and facilitate access to the know-how on cybersecurity industrial, technological and research issues. The NCCC acts as the national contact point for the Cybersecurity Community and supports the European Cybersecurity Competence Centre (ECCC) in fulfilling its mission and objectives. The activities of the NCCC-CY have not fully started yet, but it has been announced that EU co-financing of the development of the NCCC-CY has been secured through the N4CY project [63]. The DSA, moreover, organises training courses on specific Cybersecurity related skills and knowledge. For example, "Cyber Security Essentials for SMEs" was carried out in collaboration with the Cypriot Commercial and Industrial Chamber [62].

Finally, the National Security Authority, in collaboration with the Department of Administration and Personnel, the Cyprus Academy of Public Administration (CAPA) and the Open University of Cyprus, organises workshops on Electronic Security / Cybersecurity for all Public Servants who are authorised to handle Classified Information. NSA has organised an Information Day for the Security Officers of the Ministries and State Services and a workshop on "Risk Management, Principles and Guidelines" with the participation of several officers of the Public Health Service and executives of the Ministry of Defence and National Guard.

Initiatives for Cybersecurity workforce skills: The department of the public sector that is responsible for certifying specific working skills is called AvΑΔ (Αρχή Ανάπτυξης Ανθρώπινου Δυναμικού). They have recently realised a framework for the development of specific prototypes that formulate workforce professional skills. The prototypes cover a broad range of different professions, among different working sectors. The goal is to reach, soon, the target of 167 prototypes of workforce skills. Some of them are related to Computer Science and IT, but they are not specifically bound to cybersecurity. For instance, there is a prototype for the Administration of IT Systems and Networks [64]. Additionally, there is the Cyprus Qualifications Framework [65], which formulates the necessary educational levels required for acquiring specific degrees. Again, there is no direct connection to cybersecurity, but only a formal framework that allows establishing educational programmes with common goals as prerequisites.

Academic Programmes Related to Cybersecurity: Cyprus has several public and private higher-level institutions that provide implicitly, or explicitly educational training related to Cybersecurity. Here we list some of the representative programmes.

- **University of Cyprus¹:** The University of Cyprus is one of the major public higher-educational schools in Cyprus and it offers several graduate programmes in Computer Science with

¹ University of Cyprus: <https://www.cs.ucy.ac.cy/index.php/education/postgrad>



emphasis in Computer Science, Data Science and Artificial Intelligence. In all graduate programmes there are courses available related to Cyber Security.

- **UCLan²:** University of Central Lancashire in Cyprus has a graduate programme dedicated to Cyber Security. The programme appeals to people with an interest in understanding various topics of computer security, such as cyber warfare, cyber defence, ethical hacking, network forensics and information security management.
- **European University of Cyprus³:** University of Cyprus. The European University of Cyprus offers a graduate programme to Cyber Security. The graduate programme addresses the increasing demand for innovative approaches to the complexities and multidisciplinary character of cyber security policy and practice. The programme can be offered also through distance learning.

2.3.4 EU Member State Initiatives: Czech Republic

Cybersecurity Strategy and Focus Areas: The National Cyber and Information Security Agency oversees the Czech national cybersecurity strategy. The Czech Republic currently has a cybersecurity strategy [66] billed to operate until 2025. The strategy has a corresponding action plan [67] that is intended to facilitate its successful implementation. The Czech cybersecurity strategy and its driving action plan make it imperative for government to secure all public and private infrastructure. However, based on the strategy, there appear to be no explicitly designated government areas of focus or priority. The Czech strategy, like every other strategy, provided several strategic goals. Some of the strategic goals include:

- Securing infrastructure
- Providing a high-quality education system
- Creating a broad base of experts,
- Developing capabilities
- Preventing and combating crime
- Information sharing, coordination, and cooperation
- Cooperation between the state, private sector, and citizens

Cybersecurity Education, Skills, and Workforce Development: A cybersecurity skills framework was developed to address cybersecurity education and labour market needs. This is in furtherance to the strategic goals of providing high-quality education and creating a broad base of experts. The Czech National Qualifications Framework in Cybersecurity (CNQFC) classifies cybersecurity qualifications and professional roles according to their required knowledge, abilities, and skills. It is a comprehensive, unified basis for developing the Czech cybersecurity workforce to combat current and emerging cyber threats. It is, therefore, a common reference point for national cybersecurity capacity development.

The current version 1.0 of the CNQFC [68] identified seven professional Work Role Categories, corresponding Specializations, and individual Work Roles. Each work role has associated competencies

² UCLan: <https://www.uclancyprus.ac.cy/postgraduate-course/msc-cybersecurity/>

³ European University of Cyprus: <https://euc.ac.cy/en/programs/master-cybersecurity-online/>



(59), Requirements (1000), and Tasks (over 1000). Furthermore, each work role requirement is classified as an Ability, Knowledge, or Skill.

Table 15 : Summary of CNQFC Work Role Categories and Specialisations

Work roles	Specifications	Work
Roles in development and planning	8	27
Operational and administration roles	8	13
Supervisory, leadership, educational and support roles	6	22
Roles in protection against cyber security threats within the CERT team	6	6
Analytical roles	5	9
Roles in collection operations	2	8
Investigation	2	5

Table 15 summarizes the work role categories and the number of specializations in each category. There are about 90 job roles grouped according to related work role categories and specializations.

Table 16 : Summary of CNQFC Investigations Work Role Category and Work Roles

Work roles	Competencies	KAs	Skills
Cybercrime Forensics Analyst	Digital Forensics, Computer Languages, Critical Thinking, Data Analysis, Information Systems and Network Security, Operating System, Problem Solving, Information Technology Assessment, Intelligence Analysis, New Technology Fluency, Telecommunications, Web Technology Fluency	34	22
Cybersecurity Forensics Analyst	All the above in addition to: Network Management, Vulnerabilities Assessment	60	25
Malware Analyst	All the above in addition to: Computer Network Protection, Data Management, Database Administration, Incident Management, Information Management, Mathematical Reasoning, Network Management, Requirements Analysis, Risk Management, Software Testing and Evaluation, Systems Testing and Evaluation, Target Development, Threat Analysis, Vulnerabilities Assessment	14	27
Cybercrime Investigator	Digital Forensics, Critical Thinking, Data Management, Data Security, Information Management, Information Systems and Network Security, Information Technology	15	11



	Assessment, Law, Policy, and Ethics, Communication, Problem Solving, Requirements Analysis, Target Development, New Technology Fluency, Threat Analysis		
--	---	--	--

Cybersecurity competencies are also classified as either technical, organizational, leadership, or professional. Given the extensive detailing of the CNQFC classification, this report cannot provide a summary that fully covers the most granular details of the framework to keep the report size more manageable. For instance, Table 16 presents a sample summary of the competencies, knowledge, and skills of some work roles under the Digital Forensics specialization and the Investigation work role category. The table does not include the abilities and tasks specified for each work role. It is also important to note that the CNQFC specifies competencies by associating them with identified abilities, knowledge, and skills. This level of classification is not included in Table 16

A unique characteristic of the CNQFC is its development and optimization via an interactive web platform that is publicly available. As an open data platform, it provides an opportunity for external applications and data structures to maximise its potential. A comprehensive and well-structured database of the CNQFC is provided in [68].

The CNQFC was developed under the ENISA's initiative. It was significantly inspired by the NICE framework and revised to meet its national cybersecurity workforce development demands. The CNQFC's vast classification may also serve as a good reference point for the EU cybersecurity workforce development apart from ENISA's framework. It is important to note that besides the CNQFC, based on our search, there is yet no other EU-Member State cybersecurity workforce development framework.

2.3.5 EU Member State Initiatives: Denmark

Cybersecurity Strategy and Focus Areas: Denmark's Ministry of Finance released the Danish National Strategy for Cyber and Information Security 2022-2024 and describes targeted efforts to improve processes, technology, and behaviour, regular risk analyses, prioritising protection, and understanding the potential consequences of a data breaches. The report suggests that technology-related measures include increasing IT infrastructure and process, expertise, and regularly identifying and repairing system vulnerabilities. It also includes behavioural strategy recommendations in order to raise user knowledge of cyber threats and provide staff training programmes that teach safe internet behaviour.

Decentralised cyber and information security units (DCIS) and focused initiatives have increased cyber security in Denmark and its six important sectors (energy, health, transport, telecoms, finance, and maritime). Denmark's government agencies must also follow ISO/IEC 27001 and a set of technical minimum standards for risk-based information security management. Danish cyber and information security goals are presented in the report and prioritises ICT infrastructure security for key social functions. The national policy calls for a corporate partnership to boost ICT security in Danish businesses and make it one of Denmark's strengths through public-private collaboration and information sharing. "Virksomhedsrådet for It-sikkerhed," a business advisory board, makes monthly



recommendations to the government and business community on improving ICT security and data handling.

Major cyber crises affecting many sectors may activate the National Operative Staff (NOST, whose permanent members include the Danish National Police, the Danish Security and Intelligence Service, and the Danish Defence Intelligence Service/the Centre for Cyber Security). The Centre for Cyber Security may assist concerned firms. To prevent cyberattacks and uncover attack techniques and weaknesses, the Centre for Cyber Security may conduct technical investigations. Major cyberattacks necessitate ICT security investigations. Police and the Centre for Cyber Security collaborate to achieve this. A major incident affecting numerous industries requires effective communication coordination. The DCOK, under the NOST, coordinates this job. The DCOK distributes and synchronises important information to the public and media. The DCOK creates temporary units to inform the public about specific events. The Centre for Cyber Security is the national authority on IT security. The institution advises on preventive and mitigation measures. The Centre for Cyber Security infrastructure and Internet security service can identify and warn of sophisticated cyberattacks against subscribed authorities and enterprises. The Centre for Cyber Security alerts relevant organisations about cyber threats. The centre creates national and sector-specific situation reports and threat assessments.

Denmark's government's policy targets four strategic objectives to build a stronger and more secure digital Denmark.

- 1) Secure social functions in order to maintain important social services and economic activities in a crisis if critical ICT infrastructure is down. And to respond quickly to significant cyberattacks. Financial cybercrime is rising. The police's Nationwide Centre for IT-related Economic Crime (LCIK) has received 70,000 financial cybercrime reports since its December 2018 initiation.
 - Since 2016, government agencies must implement ISO/IEC 27001's information security management best practices. Over 30% of agencies have not implemented the standard.
 - 40% of Danish SMEs have inadequate digital security for their risk profile, and many lack fundamental protections. Thus, Danish businesses—particularly SMEs—must improve their digital resilience.
- 2) Prioritisation of developing awareness and knowledge on cyber and information security and educational developments to improve skills for all levels of society (individual, public and private entities, government agencies). The report Information Security among Danes 2020 found that cyber and information security knowledge is lacking among the general public and government and corporate employees, and that society needs to train more people and build capacity to meet cyber and information security demands.
- 3) Public-private collaboration. Government agencies and businesses must collaborate and share threat and incident information. Centralised coordination of specialised consultation for government agencies and corporations is needed. Also, the Danish Business Forum for Digital Security supports the government's efforts to improve Danish businesses' digital security. The forum advises the government and business sector and works with the government to develop and implement tangible strategies to improve digital security in the Danish business sector.
- 4) Actively fighting cybercrime globally. Denmark's goal is to enhance international collaboration within the European Union, United Nations, and NATO, and among nations that share similar values. Denmark joined The Hague Security Delta in June 2016 to promote cooperation with other European regions by bringing together public and private parties, academia, and R&D organisations to boost innovation and economic growth. Karup and CenSec are Denmark's clusters.

Cybersecurity Education, Skills, and Workforce Development: The Council for Digital Security advocates for security and privacy with 20 private and academic organizations. Dansk IT represents



Danish IT professionals, including cyber security. Danish companies need engineers, computer scientists, biostatisticians, and other digitally skilled workers, according to the national policy. A technology pact by the Danish government encourages young people to study technology and digital skills. Over a decade, the government wants 20% more STEM students to graduate from vocational or higher education programmes.

Cybersecurity education objectives: Denmark is dedicated to education-based digital judgment and competence development for students. This is done with the targeted child, youth, and teacher security awareness campaigns. Also, the development of ongoing education and training programmes, instructional materials, and cyber and information security awareness campaigns for instructors, learners, and students is currently being developed.

Higher Education and Performance Indicators: There are two higher education programmes dedicated to cybersecurity:

- 1) Technical University of Denmark – Master Degree in Cyber Security (60 ECTS) established in 2020. Each year 60 students are admitted, and the study has a focus on system security, network security, component security, and SW security.
- 2) Aalborg University – master’s degree in cyber security (120 ECTS) established in 2020. Each year 60 students are admitted to the degree with the focus on system security, network security, component security, and SW security.

Cybersecurity Capacity and Capability Building Initiatives: Recent developments include the government-allocated funding for technological research, including funds for the RESEARCH2025-team (FORSK2021) project under the Ministry of Higher Education and Science (New technological possibilities under the Innovation Fund Denmark). The focus is on generating knowledge about new models and tools to assess threats, knowledge to bolster the infrastructure against attacks, and knowledge to help improve the ability of authorities and businesses to find attackers.

2.3.6 EU Member State Initiatives: Estonia

Cybersecurity Strategy and Focus Areas: Estonia's cybersecurity strategy, Cybersecurity Strategy - Republic of Estonia (EE), was implemented in 2019. It defines the long-term vision, objectives, priority action areas, responsibilities, and duties for activity planning and resource allocation for 2019–2022. It involves Estonia's civilian, military, public sector, critical infrastructure service providers, sectoral entrepreneurs, and academia.

Estonia's Digital Agenda 2020 guided the Cybersecurity Strategy. The cybersecurity strategy's goals and indicators are intended for four years, with an interim review in 2020 at the end of the Digital Agenda.

The revised plan addresses 13 of the 15 ENISA self-assessment strategic goals.

- Cybercrime security and privacy balance
- Citizen awareness
- Critical information infrastructure protection
- National cyber contingency plans



- International cooperation
- Incident response capability
- Institutionalised public agency cooperation
- Baseline security requirements
- Incident reporting mechanisms
- R&D
- Cybersecurity exercises
- Training and education

The Estonian Information Security Association (EISA) promotes university-business-government collaboration. The strategy emphasises the ideal launch of new cooperation based on relevant capabilities with an administrative support structure for cross-sectorial participation in bidding on international contracts and competition to establish the preconditions for export and research financing. Enabling the military industry to participate in EU defence initiatives like the European Defence Fund and European Defence Industrial Development Plan is another step.

Estonia has strong, innovative, research-based, and globally competitive cybersecurity enterprise and R&D, spanning essential state competencies. Estonia excels in cybersecurity, especially secure communications, in universities, commercial organisations, and the governmental sector. Improving collaboration and coherence between research, enterprise, and government to strengthen the capacity to apply university developments to the private sector and state services. Estonia's small market can speed up product development for society-level products. To achieve the strategic goal, academics, private enterprises, and government must cooperate. Educational institutions will ensure that strategic priorities will govern R&D in academia and the corporate sector, ensuring state-level capabilities. The Estonian Information Security Association (EISA) promotes university-business-government collaboration.

Cybersecurity Education, Skills, and Workforce Development: Digital competence state curricula outline cybersecurity knowledge and abilities for youth. Both basic and upper secondary school curricula, coupled with methodological materials, have been developed for training bases. Unfortunately, there is a state-wide dearth of motivated and skilled teachers, and schools and teachers rarely share cybersecurity responsibilities.

127 upper secondary and 22 vocational institutions teach national defence subjects, according to 2018 data. Cyber and internal security are considered natural parts of national defence studies, however, the number of courses planned for these topics is insufficient. So, the policy promotes cyber defence courses in general education schools to develop students. The goal is to integrate cybersecurity with information science syllabi and promote in-depth cyber defence studies in as many upper secondary schools as possible to prepare for the official education of cyber specialists. ICT-interested kids can join robotics and programming groups, but cybersecurity clubs are rare. A Küber Naaskel (competition)-based extracurricular cybersecurity programme for talented youngsters is used to identify prospects to develop a pool of cybersecurity military recruits for conscription.

Based on the OSKA research on cyber competencies in ICT core professions, a systematic analysis of cyber defence workforce needs will be generated. The report does not map the workforce needs for cybersecurity specialists specifically sought by the state and private sector, which is important for planning student places, determining academic areas with greater potential, and determining the need for continuing education for top specialists, including external training and industrial PhD studies. A comprehensive study on cybersecurity workforce needs will inform policy recommendations. The studies will help organisations and institutions improve talent development, ensuring current curricula and graduates have the correct skills.



Higher Education and Performance Indicators: The Tallinn University of Technology offers a bachelor's degree (180 ECTS) in Cyber Security Engineering. Upon completion of the bachelor's degree, students would be able to work as IT specialists and become a member of the computer emergency readiness team. Upon completion of the curriculum, students will:

- develop an understanding of the concept of the IT systems life cycle
- master the life cycle of systems development as follows
- perform programming, testing, and distribution of an infosystem with a focus on administration and security
- under supervision perform IT systems security testing based on standards and best practices
- apply the processes ensuring IT systems security and participate in the design and development of these systems
- recognise the basics of IT administration, and administer development and testing environments adhere to the ethical norms of the field

The curriculum is designed to provide higher education in the broad domain of cybersecurity, integrating software development and IT systems administration. Graduates of this curriculum will be able to independently design, operate, and manage secure IT systems. Estonia has a collaboration of two universities (Tallinn University of Technology and Tartu University) that offer a Programme MSc in Cybersecurity (120 ECTS). This programme was established in 2009 and admits 60 (including 25 international) students per year. The programme provides students with core skills in wide aspects of the security of information systems and specialised skills in the chosen specialisation (Cybersecurity, Digital Forensics, Cryptography). The programme is taught jointly by the two largest public universities in Estonia. The Cybersecurity and Digital Forensics studies are concentrated in Tallinn, while the specialisation in Cryptography is concentrated in Tartu. Upon successful completion of the programme, students will receive a joint degree signed by both universities - TalTech and the University of Tartu. Students get a unique chance to study under high-level cybersecurity practitioners from Estonian universities, industry, law enforcement, CERT, and the NATO Cooperative Cyber Defense Centre of Excellence. The programme conveys the specialist knowledge and professional skills needed on a career path leading to high-end technical roles (e.g., security analyst, architect, or research engineer; security incident handler, or digital forensic expert in a law enforcement agency) or managerial roles (e.g., project/team leader or technology officer). The studies are also an excellent addition to a previous background in legal studies or law enforcement, leading to unique career opportunities. Great networking possibilities and collaboration with leading specialists in the field will present graduates with a range of career opportunities. The studies can also be continued at the doctoral level.

The direct follow-up curriculum at TalTech is the Information and Communication Technology (IAQD) PhD programme. The number of cybersecurity doctorates defended has risen from 1.7 PhDs per year (during the period 2014-2017) to 2.5 doctorates (2019-2022).

Cybersecurity Capacity and Capability Building Initiatives: Estonia has developed several public services to build knowledge and competencies for the public that includes all ages and levels of prior knowledge and for recruitment to possible careers within cybersecurity. This includes digital services for information and education, activities, and games and competitions.



Targalt Internetis (50% funded by the EU) has two aims: teaching the general public about cybersecurity issues through tasks and information, and an internet site that aims at teaching teachers, parents, and children smart internet use.

For the general public, the Targalt Internetis project provides information on cybersecurity while also offering tasks and activities in cryptography, hardware reverse engineering, and coding. Here, users can test their knowledge, interact with safe systems, and test their cybersecurity skills and competencies.

For teaching teachers, children, and parents about cybersecurity, interactive games focusing on issues such as internet use, data protection, social media use, smart devices, and cyberbullying are offered to help students build competencies in behaviours that help protect personal data and internet safety practices. This is done by:

- training sessions and seminars for children, parents, teachers and social workers, and awareness-raising events for the public
- the drafting of training and awareness-raising materials for children, teachers, and parents
- creative competitions for children and students
- assistance and counselling from the Children's Helpline
- providing a web-based hotline (www.vihjeliin.ee), which allows Internet users to provide information about web environments which contain inappropriate materials for children
- cooperation among different stakeholders in Estonia and Europe and participation in the INHOPE and INSAFE cooperation networks.

The CyberSec Stories, developed by the Tallinn University of Technology Center for Digital Forensics and Cyber Security, is a platform that consists of 54 cases about cybersecurity and helps to raise overall awareness in the cyber hygiene area that is open to public users.

Projects for recruitment of cybersecurity personnel: Women in Cybersecurity - role models for girls: Developed by Start-up Estonia and Kredex, and supported by the Estonian Ministry of Defense, Smart Internet Project and Connecting Europe, the Women in Cybersecurity Role Models for Girls project offers educational content that is tailored to the experiences of female students in grades 7 through 12. The most exemplary research and projects pertaining to IT and cybersecurity challenges have been compiled and presented in a manner that is both engaging and relevant to educators, who are instrumental in reaching female students within their academic institutions. The project identifies educational pathways required to excel in the field of IT/Cybersecurity.

2.3.7 EU Member State Initiatives: Finland

Cybersecurity Strategy and Focus Areas: The current Finnish Cybersecurity Strategy has been adopted by the State Council in 2019. The Strategy is based on the general principles of Finland's cyber security strategy of 2013. The strategy and its implementation are also part of the implementation of the EU Cyber Security Strategy. The Finnish Cyber Security Strategy 2019 [69] sets out the key national objectives for the development of the cyber environment and the safeguarding of related vital functions. The reform and implementation of the strategy are based on the Government Programme.

The three strategic guidelines are the following: 1) international cooperation, 2) better coordination of cyber security management, planning and preparedness, and 3) developing cyber security competence. A cyber security development programme extending beyond government terms will improve the allocation of resources and improvement of cooperation for cyber security. According to the first guideline international cooperation Finland will take care of its cyber environment, supported by active international and EU cooperation. It is Finland's interest to cooperate closely with other international



actors on a multilateral, regional and bilateral basis including technical and political cooperation and dialogue. Better coordination of cyber security management, planning and preparedness guideline states that Finland's cybersecurity will be improved through development programmes and cooperation to promote its design and monitoring. Developing cyber security competence – Day-to-day skills and top specialists ensuring cyber security. National cybersecurity expertise will be ensured by identifying skills needs and strengthening training and research.

Finland is focusing on development programme to improve the overall state of cyber security. The government resolution on Cyber Security Development Programme. The aim of the Programme is to provide guidance for the cyber security development extending across sectoral borders and government terms. The Development Programme includes both a concrete implementation plan and an impact analysis. The Programme covers the period from 2021 to 2030. Besides, the higher education has special emphasis on developing education programmes, professional training and awareness actions plan to fill the gaps of cybersecurity skills and expertise shortage.

Cybersecurity Education, Skills, and Workforce Development: Finland has implemented a national level cyber security competence development programme from schools to higher education. The curriculum is targeting to meet the standards and learning outcomes of national and international certification programmes. For example, Finnish schools are encouraged to leverage the benefits of the European Union's recommendation on minimum cyber security education for school children. In Finland, the higher education institutes including traditional Universities and University of Applied Science offers graduate, postgraduate, doctoral, and professional education programmes.

Cybersecurity-focused higher education degree programmes (Bachelor's and Master's) are offered in several Universities and Universities of Applied Sciences: University of Oulu, University of Turku, University of Jyväskylä, Jyväskylä University of Applied Sciences, Laurea University of Applied Sciences, Turku University of Applied Sciences, and South-Eastern Finland University of Applied Sciences. In addition, Aalto University has recently started a research and development effort toward making cybersecurity a civic skill in the EU through national cybersecurity curriculums [70]. On the one hand, the traditional universities offer more technical-oriented education programmes including Master of Engineering (MEng) to Master of Sciences (MSc) degrees. For example, University of Jyväskylä, Aalto University, JAMK University of Applied Sciences, University of Turku and South-Eastern Finland University of Applied Sciences. On the other hand, Laurea University of Applied Sciences is offering a fully online cybersecurity degree programme in cross-sectoral management and technological solutions for information and cybersecurity. The curriculum is mapped with the suggestions from industrial partners while designing the cyber security curriculum at Laurea University of Applied Science. The curriculum is directly mapped with the market demand and industry professional certifications. Finland heading towards more transformation of higher education where HEIs are cooperating closely with industries and working-life partners [140].

The National Cyber Security Centre Finland (NCSC-FI) develops and monitors the operational reliability and security of communications networks and services. NCSC-FI provides situational awareness of cyber security and comprehensive instructions for private individuals, organisations, and companies as well as for cyber security professionals to keep information safe. All the instructions are available and continuously updated on the NSCS-FI web page [71] in Finnish, Swedish and English.



Cybersecurity Capacity and Capability Building Initiatives: Finland has realised there is huge gap in cybersecurity skills, expertise, and professional competences across the board. To address these challenges, the action plan rolled out with following segmentations:

- Training and Exercises: General awareness of the basics of cybersecurity needs to be part of daily life in the digital information society.
- Better information and cybersecurity skills for citizens: The National Defence Training Association of Finland will annually organise a cybersecurity curriculum for basic courses open to all citizens as well as continuing education and special training for professionals.
- Basic skills in cyber security and the digital environment – general education and professional training for school children and teachers: As a part of multiliteracies, teachers’ continuing education will develop and advance contents associated with information and cyber security. These awareness contents and programmes delivered to school children across the nation.
- Higher education and specialised programmes: The government aims to integrate higher education institutes (HEIs) to address the challenge of skills, expertise, and professional competences.

These are few of many capacity building efforts with general users including and not limited to citizens, public and school children benefits the European cyber secure society and digital agenda of European Union. For cyber security professionals, NSCS-FI instruction covers the following content: (1) how to detect web shells (2) collecting and using log data (3) criteria for assessing the information security of cloud services (4) assessing ISO/IEC 27001 information security management system maturity in social welfare and healthcare organisations (5) deployment of cybermeter in social welfare and healthcare organisations (6) criticality classification of functions and information systems in social welfare and healthcare organisations (7) information security and data protection requirements for social welfare and healthcare procurements (8) decommissioning of outgoing services

Additionally, to the instructions provided by NCSC-FI, the Ministry of Social Affairs and Health has published the “Cyber Security Guidance for operators in the healthcare and social welfare sectors” [72]. The guidance will be updated as and when necessary. Other published directives exist also e.g., “Cyber Security in the social welfare healthcare” [73] by Jyväskylä University and, “Cyber Security in healthcare” [74] and “Cyber disruption management” [75] by Jyväskylä University of Applied Sciences. These publications are focused on cybersecurity in the healthcare environment, how to be prepared, how to manage the disruptions and resilience after a cyber disruption. According to the Survey of the cyber maturity of industries 2022, a national summary report by The National Emergency Supply Agency of Finland, in Finland the healthcare branch shows good basic level maturity, being able to manage cyber security with support by different data protection controls and quality standards.

Maritime operators and seafarers have requested clear, concise, and practical instructions and checklists that can be easily understood and implemented onboard vessels. The National Emergency Supply Agency of Finland in collaboration with The Finnish Shipowners’ Association has published 2021 a report on Finnish Maritime Cybersecurity Maturity as well as maritime cybersecurity best practices both for the ships and shipping companies. The best practices have been created so that maritime operators can get a good start with improving their cybersecurity posture and take the necessary steps to be in line with the International Maritime Organisation (IMO) cybersecurity risk management requirements.

A few years ago, the key players in the energy industry recognized the need to improve the cyber security and awareness of their industry on a sector-oriented basis, so that the cyber experiences and know-how of pioneering companies would be shared even more directly with companies that need it. As a result,



The National Emergency Supply Agency of Finland launched a new sector-specific project (KYBER-ENE 1 [76]) in the fall of 2017 and a follow-up project (KYBER-ENE 2) in the summer of 2018, which focused on the most important development targets identified in the energy sector:

- Starting cyber security work in companies
- Development of property management and perception
- Safe utilisation of IoT
- Cooperation, disruption management and cyber training

Initiatives for cyber security training and auditing: Finland has initiated specialised programmes for the very specific professional skillsets, for example, national security auditing professional training and risk manager training. Following is few to mentioned:

Katakri [77] – Information Security Audit Tool for Authorities published by National Security Authority (NSA) of Finland, provides an information security audit tool for Finnish authorities and organisations that can be used to assess the organisation’s ability to protect national or international classified information. Katakri is divided into three areas 1) the Security Management component which aims to ensure that the organisation has an effective IT security management system and adequate personnel security procedures for the protection of classified information 2) the physical security component which describes the security requirements for the physical environment of the classified information and 3) the technical Information Security component describes the safety requirements for the technical data processing environment. The technical component includes the telecommunications section, information system security section, and safety operation section

Instructions for organising cyber exercises [78] is a manual for cyber exercise organisers provided by NCSC-FI. It is a practical manual on organising cyber exercises where the insights have been gathered into one dossier. The exercise manual is suitable for both an organisation organising its first exercise as well as an organisation with vast experience in organising exercises for the search of new methods and points of view. NCSC-FI has also published a cyber exercise scenario manual which includes 20 different scenarios for supporting the exercises.

Kybermittari – Cybermeter [80] which is a tool that helps corporate managers to visualise the maturity level of important operational cybersecurity capabilities per domain and objective. Kybermittari has been customised for companies and organisations operating in Finland, and it is based on international measurement models for cybersecurity capabilities.

Cyber weather [81] is an NCSC-FI report which is published monthly. The report is targeted at actors who work with information security issues at different levels of organisations. The report summarises key cyber events of each month in a concise and easy-to-understand form.

Finnish Broadcasting Company YLE produces 10-minute-long podcasts **Team Whack** [82] Everything is hackable – The podcasts visualise in an understandable way our everyday vulnerabilities to cyber-attacks.



2.3.8 EU Member State Initiatives: France

France has identified the cybersecurity skills gap for several years. As a result, the French national cybersecurity agency ANSSI has developed, within its internal training centre, several initiatives to develop cybersecurity skills in France.

The first and foremost initiative is the SecNumEdu label [83]. This label is granted by ANSSI to training programmes that train cybersecurity professionals (i.e., degrees that are granted to people that will be directly able to be cybersecurity practitioners). The label is requested by a training organisation, which needs to file an application containing a significant amount of information: level of degree granted (Licence or Master), number of theoretical and practical training hours and levels in 15 areas of cybersecurity, and information about the jobs that alumni have obtained. The label is granted by ANSSI for 5 years, and the training programme is listed in the ANSSI directory of training programmes. It is important to note that a training programme needs to ensure a minimal level (1 - meaning introduction - only a few theoretical hours) in all domains of cybersecurity. To be eligible, a training programme must focus on cybersecurity and devote almost all its training hours to cybersecurity. The ANSSI directory lists about 80 training programmes, 1/3rd L and 2/3rd M. It is estimated that almost all training programmes in cybersecurity in France have requested the SecNumEdu label.

From this tool, ANSSI has derived a SecNumEdu-FC label [84] for executive education. This label targets upskilling and reskilling, with dedicated training curricula providing expertise in a specific domain. In this label, a training programme can ignore some of the cybersecurity fields required by ANSSI.

The second initiative is the CyberEdu programme [85]. This programme was initially launched by ANSSI to support the introduction of cybersecurity in digital training programmes. The objective of this programme was to ensure that all digital skills training programmes would include some notions related to cybersecurity. Since it is difficult to ensure that digital training programme operators have the skills to teach introduction to cybersecurity, ANSSI subcontracted a group of schools to create training material for introduction to cybersecurity and released it freely to the community. All training organisations delivering classes on digital technologies are encouraged to provide an introduction to cybersecurity to their trainees. ANSSI has transferred the operation of CyberEdu to an external association which maintains the teaching content.

The third initiative is the ESSI degree (Cybersecurity Expert) [86]. This degree is granted by ANSSI to French civil servants having followed its one-year internal training programme. In order to increase the number of alumni, ANSSI has partnered with two institutions in France, and delivers the ESSI degree to alumni of these institutions, under conditions that are negotiated periodically.

The two first initiatives have seen wide deployment in France. The last one remains confidential and with a limited scope.

ANSSI also operates the cybersecurity jobs observatory [87] and publishes a yearly report on the state of the job market.



2.3.9 EU Member State Initiatives: Germany

Cybersecurity Strategy and Focus Areas: The German government adopted the 2021 Cyber Security Strategy⁴ on September 8, 2021. It followed the strategies of 2011 and 2016 and aimed to provide a framework for cyber security in Germany for the following five years. The strategy includes four areas of action:

- (1) “Remaining safe and autonomous in a digital environment” focussing on citizens and society;
- (2) “Government and private industry working together” aiming to strengthen cyber security in private industry in general, but also focussing on critical infrastructures;
- (3) “Strong and sustainable cyber security architecture for every level of government” focussing on government stakeholders involved in cyber security;
- (4) “Germany's active role in European and international cyber security policy” focussing on enhancing the foundations and instruments of cyber security policy on an international level in e.g. the European Union (EU) and the North Atlantic Treaty Organization (NATO).

The areas of action comprise 44 strategic objectives. It is specifically pointed out that their implementation is subject to the availability of allocated budgetary resources. In this context it is worthwhile to note that the German federal election on September 26, 2021 led to a substantially changed German government in December 2021: The parties previously staffing the Federal Chancellery (CDU) and the Ministry of the Interior (the ministry chiefly responsible for the cybersecurity strategy, CSU) are not part of the government anymore. The coalition contract between the three governing parties (SPD, Grüne, FDP)⁵ includes a section on cybersecurity linking it closely to the digital rights of citizens. This section also mentions the goals to further develop the Cyber Security Strategy and to make the Federal Office for Information Security (BSI) more independent (currently it is still subordinated to the Ministry of the Interior).

On the German federal level there are three entities with a special relation to cybersecurity:

- (1) The Federal Office for Information Security (BSI, www.bsi.bund.de);
- (2) The Federal Commissioner for Data Protection and Freedom of Information (BfDI, www.bfdi.bund.de);
- (3) The National Coordination Centre for Cybersecurity linking to the European Cybersecurity Competence Centre (ECCC) as part of the network of national coordination centres (NCC-DE, <https://www.bmi.bund.de/EN/topics/it-internet-policy/ncc-de/ncc-de-node.html>).

Both the BSI and the BfDI are publishing annual reports on the state of affairs in their areas of responsibility. As Germany is a federal republic consisting of 16 constituent states (“Länder”) the tasks of both the BSI and the BfDI are mirrored in these states as appropriate. It is to be noted that the German

⁴ Cyber Security Strategy for Germany 2021, Published by Federal Ministry of the Interior, Building and Community; <https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf>

⁵ Mehr Fortschritt wagen, Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, Koalitionsvertrag 2021 - 2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90/Die Grünen und den Freien Demokraten (FDP); https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf



constitution (Basic Law, “Grundgesetz”) considering the experiences with German centralized governments in the 20th century placed major responsibilities into domain of the constituent states. This includes e.g. the areas of culture (including language, the education system and media) and law enforcement.

Consequently, one can expect German initiatives to be well synchronised with European activities, as this is a strategy overarching governmental changes, but special attention is given to civil rights (possibly more than in some other EU member states), and implementations may differ between different German constituent states.

Germany's Cybersecurity Skills Landscape: Like the EU, Germany has a diverse cybersecurity skills landscape, with stakeholders from the private and public sectors, civil society, and associations all playing a role.

School and university education are in the responsibility of the constituent states. The federal government has the ability to fund special initiatives like research centres or digitalisation strategies, but the institutional and legal decisions are with the constituent states. Fields like vocational training, training assistance, and continuing education can be influenced by federal labour law.

A German education model not necessarily mirrored EU-wide is the so-called “Dual model” of vocational training that combines specialised education of 2 to 3 years in a company (following a regulated educational contract) with specialised school education. The concluding examination follows federally standardised criteria. The specialisation area closest to cybersecurity is “Fachinformatiker” (Informatics expert for a subject area). So far four subject areas have been defined: application development, system integration, digital networks and networking, and data and process analysis. The subject areas consider cybersecurity to some degree; a specific subject area “Cybersecurity” does not exist. As rationale one should consider that the typical participants of vocational training are taking this training after ten years of school and in an age of less than 20. So the non-existence of a specific subject area “Cybersecurity” mirrors the reluctance to offer Bachelor specialisations in cybersecurity: the respective students first need to learn the respective basics, before specialisations beyond make sense.

Germany is facing a shortage of professionals both in ICT and in cybersecurity and both in the ICT core sector and the various ICT application sectors. This is leading to rising wages across the country and increased competition between employers, both in the public and private sector.

As an example, BSI is competing with the private sector and other institutions in the public sector for qualified personnel. Therefore it is highlighting its mission for government, business, and society. In particular, it aims to convince ICT professionals to work with BSI. To do this, BSI's HR department conducted various media campaigns to spread its message and provide insights into the work and profiles of its employees. BSI also offers a variety of opportunities for students, such as scholarships, internships, and thesis mentoring.

BSI uses a range of tools to attract potential candidates and develop the skills of employees, including:

- Onboarding procedures;
- Leadership Development Programme;
- Assessment Center for leadership positions;
- Internships in different divisions of BSI and cooperation with other national agencies;
- Networking initiatives: BSI supports national and international networks.



2.3.10 EU Member State Initiatives: Greece

The National Cybersecurity Authority of Greece offers a cybersecurity handbook [88] containing best practices in technical and organisational risk management measures and addressed to public sector organisations as well as medium and large private enterprises. Chapter 12 of the handbook is dedicated to cybersecurity skills and awareness needs. In this chapter, it was emphasised that it is necessary to Implement the national training programmes on a regular basis, to improve the skills and awareness of employees on cybersecurity issues.

This national document emphasises that employees play a critical role in the security of networks and information systems and that the lack of training and corresponding responsibility for this issue poses various types of threats to organisations. Examples of such attacks include social engineering attacks, Insider threats.

The guidance to the Greek stakeholders is to develop a cybersecurity training and awareness policy that addresses the purpose, scope, roles and responsibilities, procedures for implementing the policy and the relevant protection measures. Organise a training programme to increase the skills and awareness of your employees in cybersecurity issues, which should be conducted at least twice a year. The training material should include:

- how to interact with the corporate network, systems, and data in a secure manner,
- authentication best practices, such as creating strong passwords and applying multi-factor authentication,
- train employees to identify social engineering attacks, such as phishing emails, impersonated phone calls, etc.
- being able to recognize evidence of system breaches and incidents arising from insider threats.

The handbook urges to periodically conduct a cybersecurity awareness training programme addressed to distinct roles and targeting different employee categories based on business activities and the level of technical expertise; Perform a knowledge gap analysis of employees to develop a plan of sequential training; Periodically conduct exercises that simulate cyber security incidents and their impact.

There are various cybersecurity master programmes in Greece as reported in the ENISA CyberHEAD database [89]. Also, national cybersecurity exercises (named “PANOPTIS” are organised since 2011 [90]. Greece is also participating in various NATO cyber defence exercises e.g. “Cyber Coalition”, “Locked Shields” since 2009 and various other exercises e.g. ENISA CyberEurope and “Crossed Swords 16”. Building practical skills and capabilities is a main national concern.

Chapter 14 of the handbook describes in detail the cybersecurity technical assessments. In this chapter, there is a clear explanation of the need for and the way to perform periodic assessments of the technical and organizational measures that are deployed in the organization’s network and information systems. Security assessments offer valuable assistance to organisations in identifying gaps and vulnerabilities in technologies, processes, and human behaviour. Especially in the modern Internet environment, where technology is rapidly evolving and the attacker methods get even more sophisticated, conducting such assessments can reveal critical weaknesses that could be fatal to an entity's assets and reputation. This assessment will examine the overall organisation’s ecosystem and will try to understand if (1) the patch management process is not timely implemented because unpatched systems are identified even though



the corresponding patch has been already officially released, (2) the required countermeasures to mitigate new forms of attack widely studied and recognized by the research community have not yet been implemented and finally (3) the employees exhibit dangerous behaviour and ignorance about social engineering attacks (e.g. phishing emails), although the organization's security policy explicitly mentions the obligation to conduct regular cybersecurity awareness training programmes.

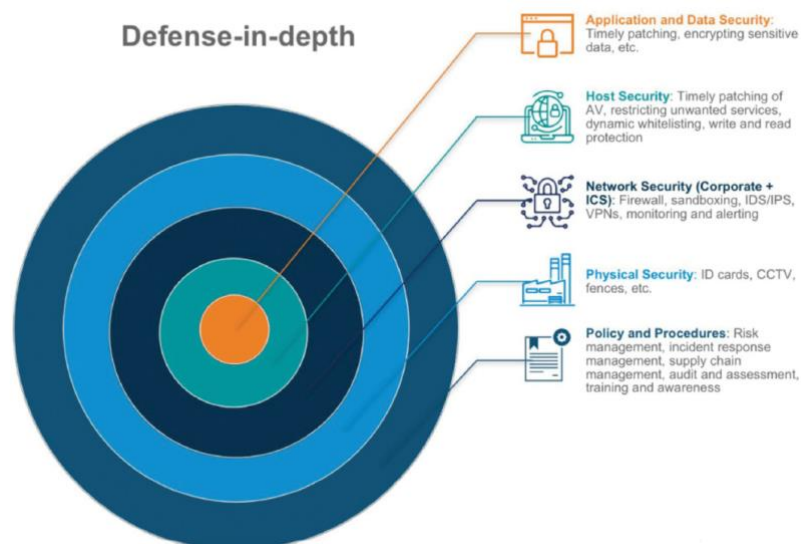


Figure 14: Cybersecurity Defence-in-depth approach of Greece

Regarding the cybersecurity assessments, three (3) main categories are described in this national cybersecurity handbook. These are: **(i)** Vulnerability scanning, **(ii)** Vulnerability assessment, **(iii)** Penetration testing or ethical hacking and **(iv)** Red team / blue team exercises. Going into more technical details, while delivering Vulnerability scanning, IT assets (network, systems, applications, etc.) are scanned using automated tools to detect known vulnerabilities and insecure settings. Scanning can be done in an authenticated or non-authenticated way. Since automated scans are mainly signature-based, the results may include some false positives. Based on the final report, patches are installed with the appropriate priority. Vulnerability assessment is a systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation [91]. It is performed in an automated and non-automated way (manually) and results in the identification and confirmation of all the vulnerabilities of the systems in scope, but without exploiting them. Penetration testing or ethical hacking is an authorized cyber-attack simulation for the purpose of assessing the security of networks and information systems. The penetration test model techniques are used in the real world and extend vulnerability assessment to the fact that, under controlled conditions, an attempt is made to exploit them in order to gain unauthorized access to the system and determine the impact on business operations and critical data [92]. Finally, when the cybersecurity assessment is focused on Red team / Blue team exercises, it means that the red teaming mimics real cyber threat actors by using the same tactics, techniques, and procedures. The purpose is to train and measure the effectiveness of people, processes and technologies used to defend the organisation [93]. "Red team" is the name of the team conducting the attack, while the "Blue team" is the group of people in charge of the defence (Security Operations Centre staff, incident response team, etc.).



The guidelines for a complete cybersecurity assessment framework cover several aspects. The goal is to work on development and documentation covering two (2) broad topics: (i) a cybersecurity technical assessment policy that addresses purpose, scope, roles, and responsibilities, (ii) procedures for implementing the policy and the relevant protection measures. In addition, organisations have to perform (i) automated vulnerability scans on a regular basis (e.g. once a month) to identify potential vulnerabilities and unpatched systems on your corporate assets and network, (ii) a full vulnerability assessment of your network and information systems on a periodic basis (e.g. at least once a year), (iii) a full penetration test on your network and information systems on a periodic basis (e.g. once a year) and after a confirmed cybersecurity incident and (iv) "red team - blue team" exercises on a periodic basis (e.g. once a year) to simulate cyber-attacks accomplished by well-known high-profile cybercrime groups.

In order to have an effective defence in-depth strategy, this must include mechanisms at a technical level, as well as organisational/administrative measures. This overall strategy should be focused on: (1) Policies and procedures (risk analysis, user training, supply chain management, etc.), (2) Access restrictions (least privilege, need-to-know, etc.), (3) Network security (network segmentation, firewalls, intrusion detection systems, VPNs, etc.), (4) Device protection (antivirus, application whitelisting, etc.), (5) Application and data protection (patching, data backup, encryption, etc.). Following a sequential layering of a “defence-in-depth, as it is graphically illustrated in Figure 13, we can have a holistic and complete “defence-in-depth” architecture [94].

2.3.11 EU Member State Initiatives: Italy

The contributors from CyberSecPro (Italy) partners are not aware of any specific Italian cybersecurity initiatives that differ in terms of strategy, education, or development efforts from the general EU efforts on this topic. The main authors suggesting referring the main EU initiatives as overarching Italy and other EU national initiatives. Further, the main author summarises previous development work conducted with ENISA for the Italian national initiatives as below:

Cybersecurity Strategy and Focus Areas: The Italian government adopted the 2022 Cybersecurity Strategy on March 8, 2022. It provides a framework for cybersecurity in Italy for the next five years. The strategy focuses on four areas of action: society, private industry, government, and international affairs. A total of 44 strategic objectives have been set within these action areas. The strategy will be evaluated in a transparent and measurable way to track progress in each area.

Cybersecurity Education, Skills, and Workforce Development: Italy has a diverse cybersecurity skills landscape, with stakeholders from the private and public sectors, civil society, and associations all playing a role.

School and university education are mainly the responsibility of the regions, but the national government also plays a significant role. Shared responsibility between the regions and the national government is particularly important in the fields of non-school vocational training, training assistance, and continuing education.

A key strategic actor for cybersecurity skills is the National Cybersecurity Committee (CCN), which was established in 2016. The CCN advises the national government on cybersecurity issues and brings together high-level representatives from the national and regional levels, as well as the private sector.



The CCN is increasingly drawing on expertise from society, private industry, and the research community. Invited experts speaking on individual strategic topics provide background for discussion and for drawing up recommendations for action. The Italian IT sector is also facing a shortage of IT professionals. This is leading to rising wages across the country and increased competition between employers, both in the public and private sectors.

As an example, the National Cybersecurity Agency (CAN) is competing with the private sector by highlighting its unique mission for government, business, and society as the national cyber security authority. In particular, we aim to convince IT professionals to work with the ACN. To do this, the ACN's HR department conducts various media campaigns to spread our message and provide insights into the work and profiles of our employees. The ACN also offers a variety of opportunities for students, such as scholarships, internships, and thesis mentoring. The ACN Human Resource Development uses a range of tools to attract potential candidates and develop the skills of employees

Other Italian initiatives and observations: The Italian government is investing in the development of key enabling technologies, such as artificial intelligence and blockchain, to improve cybersecurity and create new opportunities for the digital economy. The Italian government is working to establish partnerships with the private sector, research institutions, and other European countries to promote collaboration and knowledge-sharing in the field of cybersecurity. These partnerships will help to accelerate the development of new cybersecurity solutions and to ensure that Italy is at the forefront of the global cybersecurity landscape.

The Italian government is committed to investing in cybersecurity and emerging technologies. These investments will help to protect Italy from cyberattacks and to create new opportunities for the digital economy.

2.3.12 EU Member State Initiatives: Netherlands

Cybersecurity Strategy and Focus Areas: The Netherlands is in a prime position to benefit from digitalization and keep up the country's forefront digital services and activities released cybersecurity strategy 2022-2028. The Netherlands' cybersecurity strategy is based on four pillars:

- Pillar I: Cyber resilience of the government, businesses, and civil society organisations
- Pillar II: Secure and innovative digital products and services
- Pillar III: Countering cyber threats posed by states and criminals
- **Pillar IV: Cybersecurity labour market, education and cyber resilience of the public**

Education and skills focus: The Dutch cybersecurity strategy has identified skills development efforts as one of the important pillars. Netherlands wants to ensure that there are enough cybersecurity specialists and workforce to address any cyber treats and risks. The government wants to invest in education and training, and it wants to raise awareness of cybersecurity issues among the public.

The Dutch approach to cybersecurity is based on public-private cooperation, as security in the digital domain can only be achieved through collaboration with the business community. This cooperation requires a clear division of responsibilities between public authorities, the business community, and citizens, based on existing laws and regulations. An integrated approach to cybersecurity is favoured, requiring joint efforts from the business community, social organisations, and various government bodies to address both existing and emerging issues, and set five priorities:

1. Be more aware of cyber threats so that we know and understand them.



Cybersecurity Skills Framework and Relevant Initiatives

2. Ensure sufficient cyber expertise is available on the labour market so that we can meet the challenges we face.
3. Be aware of and understand risks and threats.
4. Legislation to ensure that frameworks are clear and verifiable.
5. Review of the national cybersecurity system to ensure effective and efficient use of cyber capabilities.

The National Cyber Security Agenda emphasises the importance of knowledge sharing and promoting information sharing between the public and private sectors to strengthen cybersecurity and resilience across the board. Fundamental and applied research into cybersecurity is also needed to develop the Dutch cybersecurity knowledge position. The digital domain is not confined by national borders, and a more secure digital domain is one of the Netherlands' priorities at the EU and NATO levels. The National Cyber Security Agenda, in combination with other strategies, provides guidance for the further development of Dutch efforts in international forums.

Cybersecurity Education, Skills, and Workforce Development: The Netherlands places great importance on knowledge development, especially in the field of cybersecurity, to protect their society from digital threats. There is a need to maintain and deepen high-quality cybersecurity knowledge development in the country through investments in research and education. The shortage of skilled personnel in the cybersecurity field in organisations also needs to be addressed. There is a growing demand for innovative solutions to cybersecurity issues, and citizens and businesses need to continuously renew their knowledge to protect themselves from digital threats. Efforts have been made to raise awareness among the public and smaller businesses, but more public-private cooperation is needed to improve the effects of these efforts. A guide containing basic security measures for citizens and small businesses could be developed to further develop their digital skills. For example, one of the important examples below:

Human Capital Agenda ICT + CS4NL: Regional initiatives for upskilling and lifelong education in the digital sector 2021-2025.

The Human Capital Agenda ICT has made a plan to train and retrain an additional 36,000 people training and upskilling, involving more than 4,000 additional companies. The aim is to work on talent development and bring more people with the right ICT knowledge and skills onto the labour market.

CS4NL is formed in cooperation with ministries, such as Defence, J&V and EZK, and supports effective cybersecurity innovation and knowledge development and distribution within the Dutch cybersecurity ecosystem. The programme addresses demand-driven innovation needs from the market and at different readiness levels. The programme and calls are demand-driven, as the top sectors have submitted innovation needs with their constituencies through use cases. The 7 themes defined are: Security by Design, Secure Data-Driven Working, Secure Connectivity, OT/IT Security, Cyber Risk Management, System or Chain Security and Awareness, Knowledge and Skills.

Cybersecurity Capacity and Capability Building Initiatives: The Netherlands will invest in cybersecurity research through a multi-year public-private approach. Digital skills, including media literacy and cybersecurity, will be a focus area in the review of the primary and secondary education curriculum. The government will encourage the development of digital skills in employees and citizens



and ensure continuity and cohesion between various awareness campaigns. The latest insight in behavioural sciences will be considered.

The Netherlands is investing in fundamental and applied cybersecurity research through a multi-year public-private approach, aiming to improve cybersecurity knowledge development. The government is encouraging the development of digital skills and media literacy, including cybersecurity, in primary and secondary education curriculums.

- A National Coordination Centre (NCC-NL) will be set up at the Netherlands Enterprise Agency (RVO) as part of the European Cybersecurity Competence Centre and Network (ECCCN).
- Strengthen and expand organisations within the Landelijk Dekken Stelsel (Nationwide Network of Cybersecurity Partnerships).
- Encourage SMEs to use tools, such as risk scans, and products and security recommendations, including possible courses of action. This could be achieved via trade associations, for example through the public-private platform Samen Digitaal Veilig (Digitally Safe Together).
- The programme Informatie veilig gedrag in de zorg (information security behaviour in the healthcare sector) provides healthcare institutions with ways to promote the secure handling of information.
- The Netherlands Institute for Curriculum Development (SLO) has been tasked with working with the teaching profession to develop specific core objectives for basic skills, including cybersecurity skills, for both primary and secondary education. These detailed core objectives will be submitted to the House of Representatives in a bill in 2025.
- Educational institutions will develop upskilling and reskilling programmes to enhance employees' cybersecurity expertise. To this end, they will work alongside the business community and other relevant parties. Any obstacles or limitations in that collaboration that stem from legislation will be identified and examined to see how they can be resolved.
- Development of an ICT dashboard for education and the labour market also provide sufficient insight into regional shortages of cybersecurity specialists.
- Through the 'Human Capital Agenda ICT', the government aims to increase the supply of cybersecurity and ICT specialists to the labour market, and enhance the quality of that supply. This will be done in close collaboration with the business sector, regional and local government organisations and educational institutions.

2.3.13 EU Member State Initiatives: Norway

Cybersecurity Strategy and Focus Areas: Public security in the civilian sector is managed by the Norwegian Ministry of Justice and Public Security. The Ministry supervises the Government's policy for cyber security [95], including national cyber security requirements and recommendations for public and private firms, since it is the responsible institution for national cyber security in the civilian sector.

In the defence industry, cyber security is supervised by the Norwegian Ministry of Defence (MoD). The MoD has access to a wide range of methods to handle these tasks, including the creation of regulations and required competencies, supervision of operations, as well as advising all sectors.

Norwegian interests and essential societal activities are dependent on expanding and increasingly complex digital infrastructures. One of the main challenges in determining digital vulnerability is the length and lack of transparency of the digital value chains, which span several industries and borders.

Therefore, emphasis on cooperation and partnerships among relevant stakeholders at the national and international levels is prioritized in order to address the national cybersecurity concerns.



The Norwegian Ministry has identified these strategic goals as fundamental:

1. Norwegian companies digitalize in a secure and trustworthy manner and are able to protect themselves against cyber incidents
2. Critical societal functions are supported by a robust and reliable digital infrastructure
3. Improved cyber security competence is aligned with the needs of society
4. Society has improved ability to detect and handle cyber attacks
5. The police have strengthened their ability to prevent and combat cybercrime

There are multiple government agencies with cross-sectoral cybersecurity responsibilities. It is essential to guarantee that these actors cooperate effectively. The Joint Cyber Coordination Centre (Felles cyberkoordineringssenter, FCKS), which comprises representatives from NSM, the Norwegian Intelligence Service, the Norwegian Police Security Service (PST), and the National Criminal Investigation Service (Kripos), is one of the most important collaborative hubs. FCKS aims to improve the nation's ability to detect and withstand significant cyber-attacks, provide strategic analysis, and maintain a comprehensive assessment of cyberspace's threats and risks. The Norwegian Ministry has identified three areas for cybersecurity collaborations: public-private, civilian-military, and international collaboration.

Public-private partnership: The government cannot accomplish cyber security on its own, and cooperation with industry is essential, as they possess the necessary skills and resources and serves as a catalyst for digitalization and innovation. All businesses are responsible for ensuring their own cyber security, but the reliance of society on digital solutions is needed to establish stronger international and cross-sector partnerships and cooperations. This public-private cooperation is guided by the following principles:

- The authorities and the business community work together to identify and discuss cybersecurity challenges and to exchange experiences about them.
- This cooperation should carry obligations for both parties and be based on transparency, trust and mutuality.
- The authorities contribute to establishing a business community where cyber security services are in demand, developed and provided.
- When building up national capacity in cyber security, it should be facilitated for inclusion of capabilities from the business community

Civilian-military collaboration: The defence sector relies on digital infrastructures and services provided by the civilian sector, therefore, cyber security challenges in the private sector are of military importance as it may influence Norway's capacity to manage security and political crises and military operations. In the worst-case scenario, cyber-attacks on civilian infrastructures could threaten Norway's capacity to protect national security.

Norway developed the "Totalforsvaret" (Total Defence) which includes both military and civilian support for the Armed Forces. The contribution of the Armed Forces to public security also correlates to an enhanced capacity to protect state security, given that a well-functioning civilian society and robust public security serve as a crucial foundation for an effective military defence. To address common cyber security challenges, the military and civilian sectors must develop close collaborations. This includes conducting exercises on crisis management, developing joint competencies, mutual incidence



communication, and exchanging information on threats and vulnerabilities. Norway has adopted NATO's prioritisation of civil emergency preparedness and civil-military collaboration which includes emergency preparedness, crisis management, and resilient critical societal functions.

In order to achieve these goals, the following guiding principles have been identified for use:

- Civilian support of the Norwegian Armed Forces in the event of cyber security challenges in times of crisis and armed conflict is provided within the framework of the Total Defence concept.
- Companies in the defence sector work with civilian counterparts to identify, exchange experience about and find solutions to cyber security challenges that may be of significance to the ability to carry out military operations.
- Companies in the defence sector and the civilian sector should make use of each other's capacities to address common cybersecurity challenges.
- Companies in the defence sector share information and experience with their counterparts in the civilian sector in order to raise the level of national security.

International Cooperation: The objective of Norway's international cyber policy (Internasjonal Cyberstrategi for Norge, 2017) is to serve Norwegian interests, guarantee robust and predictable framework conditions, and contribute to preventing and protecting against cyber threats and vulnerabilities while achieving a balance between transparency, security, robustness, and freedom in digitalisation.

Since cross-border digital value chains are mutual dependencies that challenge national authorities' national security and economic aspects through cyber-crimes and cyber-attacks from both state and non-state actors, Norway needs to participate in international forums to strengthen cyber security on a global scale through the following principles:

- The authorities work with other nations to reinforce Norwegian ability to prevent, detect, alert, and handle cyber incidents.
- The authorities promote international cooperation on cyber security, agreements on state behaviour in cyberspace, and collaboration on combating cyber-crime in international arenas such as the UN, NATO, the EU, the OECD and the OSCE. In addition, dialogue is established with other states bilaterally and at the regional level, including Nordic collaboration.
- The authorities ensure active Norwegian participation in relevant international arenas to ensure the Internet remains an open, accessible, secure, and robust platform, based on international standards and collaboration between authorities, the business community, academia and other parts of civilian society.
- The authorities ensure close coordination between bodies that represent Norway in arenas where international cyber security policy and cooperation on cyber-crime and handling cyber incidents are developed.

Cybersecurity Education, Skills, and Workforce Development: The Norwegian Ministry of Justice and Public Security is responsible for coordinating public security in the civilian domain, outlining government policy for cybersecurity, including national requirements and recommendations for public and private companies.

The strategic goal for competence in the national strategy is improving cybersecurity competency aligned with the needs of society. Competence and knowledge of threats, vulnerabilities, and effective countermeasures are prerequisites for protecting digital assets from cyberattacks. Individuals,



Cybersecurity Skills Framework and Relevant Initiatives

businesses, and authorities must have access to information regarding cybersecurity challenges and appropriate countermeasures. As a result, cybersecurity specialisation is given top priority due to its essential importance to national security. The national strategy for 2019 lays out the objectives and conditions for the long-term development of cybersecurity capacities, including research, development, education, and measures designed to increase business and citizen awareness.

To achieve the required competencies and competency development, the following goals have been identified:

- Establish attractive and competent research environments for prominent researchers and post-graduates.
- The number of specialists in cybersecurity meets the needs of the labour market and accommodates national security considerations.
- Cybersecurity competence is sufficiently addressed in study programmes where ICT constitutes a key component, including ICT and technology courses, as well as study programmes in other disciplines that include cybersecurity to a relevant extent.
- Good post- and supplementary education in ICT and cybersecurity at vocational colleges, universities, and university colleges.
- Cybersecurity is included in relevant professional training courses and vocational courses to a sufficient extent.
- Pupils and apprentices have digital skills including competencies that enable them to experience life skills and succeed in further education, working life and participation in society.
- Private individuals have knowledge and skills that provide them with good judgement of digital issues and that protect them from their privacy and assets online.

Norway offers two undergraduate programmes that focus on cybersecurity, and six (6) post-graduate degrees that include a focus on information and digital security, digital infrastructures, communication technology, and cybersecurity. Norway also offers two doctoral training programmes (PhD) in information security and communication technology.

To help support education, the Norwegian Center for Cyber and Information Security (CCIS), which is a partnership of major national cyber security stakeholders with access to various financial and human resources, works closely with the Norwegian University of Technology (Norges teknisknaturvitenskapelige universitet; NTNU) where one of its primary responsibilities is to ensure that cyber security education is available at all levels, from elementary institutions to postgraduate universities. The CCIS/NISlab also directs the

Cybersecurity Capacity and Capability Building Initiatives: The Norwegian National Security Authority (NSM) is the national specialist organisation for cyber security as well as the national warning and coordination body for significant computer attacks on society's vital infrastructure and other essential societal functions. NSM operates the national response function for severe computer attacks against essential infrastructure (NorCERT) and the national warning system for digital infrastructure (VDI). The National Cyber Security Centre (NCSC) is a division of the Norwegian Security Authority and serves as the country's cyber security centre and CERT. It is the national cyber security centre of Norway and the location of the national CERT; NorCERT, where severe computer assaults against



critical infrastructure and data are managed. It was established to enhance Norway's digital domain resilience and is the point of contact for ICT threats and cyber security incidents.

The Norwegian Data Protection Authority serves as both a supervisory and representative authority. The Data Protection Authority is an independent administrative body entrusted with monitoring privacy regulations and ensuring that the rights of individuals are not violated by the use of personally identifiable information. The Norwegian Communications Authority (Nkom) is responsible for the security and readiness of electronic communications networks and services.

The Norwegian Centre for Information Security (NorSIS) is an independent organisation working to enhance cyber security knowledge and understanding, for example by providing advice and guidance to private individuals and businesses (especially SMEs).

2.3.14 EU Member State Initiatives: Spain

Cybersecurity Strategy and Focus Areas: Order PCI/487/2019 [96], published in the BOE (Boletín Oficial del Estado) on April 30th 2019, which includes the "National Cybersecurity Strategy 2019" (also available in [97]), establishes the general guidelines on cybersecurity and addresses the objectives established in the National Security Strategy of 2017. To this end, the new strategy prioritizes a series of purposes, such as: (i) strengthening capabilities to face cyber threats; (ii) fostering cybersecurity culture; (iii) boosting the Spanish cybersecurity industry; and (iv) achieving and maintaining technological and professional knowledge, skills, experience, and capabilities.

To achieve these purposes, five strategic objectives are also defined in line with the objectives of the 2017 strategy [97]:

1. Security and resilience of ICT systems for the public sector and essential services.
2. Secure and reliable use of cyberspace against illicit or malicious use.
3. Protection of the business and social ecosystem and citizens.
4. Culture and commitment to cybersecurity, and empowerment of human and technological capabilities.
5. International cyberspace security.

Of these five objectives, we highlight the fourth one, whose purpose is to address [96]: the culture of cybersecurity; the training of professionals in accordance with the conditions of the labour market and its demand; the development of professionals with their own skills; the need for specialized training and qualifications; the generation of knowledge; the development of R&D&I activities in cybersecurity; and the promotion of the use of certified products and services.

In turn, this fourth objective is supported by Action Line 5 [97]: "strengthen the Spanish cybersecurity industry, and the generation and retention of talent to enhance digital autonomy", and Action Line 7: "develop a cybersecurity culture". Both lines are subject to a set of actions, of which we stress some specific actions to Action Line 5, such as (i) update/develop cybersecurity competency frameworks that are able to respond to the needs of the labour market; (ii) identify the current needs for professional competencies in the field of cybersecurity, fostering, on the one hand, academic collaboration and training, and, on the other hand, professional accreditation and certification; (iii) add cybersecurity professional profiles in future public job descriptions; and (iv) detect, encourage and retain cybersecurity talent.



Cybersecurity Education, Skills, and Workforce Development: several universities offer official higher education programmes (bachelor's and master's degrees) focused on cybersecurity, but also other intuitions that provide specialized courses in cybersecurity. For that reason, the Spanish National Institute of Cybersecurity (INCIBE, Instituto Nacional de Ciberseguridad) [98] regularly updates the catalogues [99] and [100], one with information on these institutions and another on education and training programmes through undergraduate, graduate and specialized courses.

More information on the university training offered for bachelor's and master's degrees can also be found in the report [101] prepared by INCIBE together with the National Observatory of Technology and Society (ONTSI, Observatorio Nacional de Tecnología y Sociedad) [102]. The report, mainly focused on the analysis and diagnosis of cybersecurity talent in Spain, points out that cybersecurity training is more widespread in masters (on-site and online) than in degrees (on-site), with more than 75 masters available for 2020-2021 (time of the study for the report). The report's diagnosis is quite extensive and detailed, where it not only reviews the current state but also offers guidelines to boost supply and highlights the main limiting factors to generating or retaining talent. Some of these factors are, for example, the gender deficit (only 18% of students are women), the lack of early vocation, or the lack of trainers specialised in the field of cybersecurity. More information about the focus group, the methodology of the study and its exploration can be found in [98].

Likewise, the quality of university degrees (bachelor's and master's degrees), curricula, courses, and teaching in general, including those related to cybersecurity, is also fundamental. For that reason, they are subject in Spain to continuous monitoring by the National Agency for Quality Assessment and Accreditation (ANECA, Agencia Nacional de Evaluación de la Calidad y Acreditación). This agency, created in 2001 under the Organic Law of Universities 6/2001 [103], is in charge of the evaluation, certification and accreditation of the Spanish university system with the aim of its continuous improvement and adaptation to the European Higher Education Area (EHEA), as stated in [104]. This evaluation, certification and accreditation process is carried out in different phases and under different programmes: the VERIFICA programme [105] to evaluate the design of the degree in line with the EHEA and in compliance with the legislation [106]; the MONITOR programme [107] to establish external evaluations and supervise the implementation of the degrees; and the ACREDITA programme [108] to renew the official degree status. All instructions are available on the ANECA website [104], both in Spanish and English.

Cybersecurity Capacity and Capability Building Initiatives: as regulatory measures, it is worth mentioning that some cybersecurity profiles along with their responsibilities and relationships are already regulated. For example, the role of the “responsible for information security” is regulated since 2021 in RD (Real Decreto) 43/2021 [109] with applications in the private and public sectors. Its article 7 (RD 43/2021) details its main functions, which correspond, amongst other things, to the capacity to elaborate, supervise and develop security policies, manage, and act, as well as connect with the competent authorities. In information systems, these tasks must be treated differently from the other responsibilities within an organisation as also stated in Article 11 of RD 311/2022 [110], whose functions must be well established within the security policies. Also, the “data protection delegate”, commonly known as “Data Protection Officer” (DPO), is also regulated through Article 39 of Regulation (EU) 679/2016 [111], as well as the responsibility for security and liaison of Critical Infrastructures in Law 8/2011, Article 16 [112].



On the other hand, INCIBE in its proposal to promote strategies and support the culture of cybersecurity, and the identification, attraction, development, and retention of national talent, promotes several initiatives. One of them is the provision of a set of recommendations on how to address key challenges to intensify cybersecurity in Spanish organizations. These recommendations are available in [113], where the main stakeholders are entities from the public, private and academic sectors. For the latter stakeholder, they recommend: (i) aligning training programmes with business needs; (ii) strengthening soft skills within training programmes; (iii) modifying access requirements for current training programmes; and (iv) promoting the training of trainers/professors in cybersecurity, as discussed above.

One way to address these challenges, and especially the first one, is through the application of standardised strategies such as the use of the new ECSF [114] to articulate roles, tasks, knowledge, and skills in concordance with the labour market, as also indicated in [113]. On this website, INCIBE remarks that there are two initiatives at the national level that will give value to this new framework to define homogeneous cybersecurity profiles aligned with the profiles expected at the European level. The first initiative corresponds to the "Academia Hacker INCIBE" [113] to precisely create homogeneous profiles through a free training programme. In contrast, the second initiative corresponds to the creation of a National Cybersecurity Forum (FNC, "Foro Nacional de Ciberseguridad") [115] as one of the measures of Order PCI/487/2019 [96]. The forum seeks to bring together experts and organisations from the public and private sectors to support cybersecurity culture, industry and R&D&I, training and talent in cybersecurity; and all of them aligned with the measures predetermined in [96]. To do this, FNC is composed of five Working Groups (WGs) [115], where one of them is mainly focused on "education, training and talent" so as to promote cybersecurity training according to market needs.

Continuing with the professional orientations and their capabilities, INCIBE is one of the main institutions of reference at the national level. In [116], it is possible to find, for example, an infographic containing a guide to accessing the sector from a professional point of view; i.e.: either (i) by specialisation through training; (ii) the sharing of ideas, experiences and knowledge through the creation of specific communities and participation in events; (iii) certification; (iv) participation in cybersecurity challenges and competitions; and (v) self-learning. INCIBE also promotes many other initiatives for the community such as the CyberCamp (to identify and promote talent in cybersecurity), the Summer BootCamp (to train experts in CERTS, cybersecurity forces and bodies, and policymakers), the Ciberemprede or CyberSecurity Ventures (to foster entrepreneurship in the field of cybersecurity) as also indicated in [117].

Similarly, the CCN-CERT (Information Security Incident Response Capability of the National Cryptologic Center – CCN, Centro Criptológico Nacional) [118] offers a set of initiatives to enhance cybersecurity within organizations, whose functions were established in Law 11/2002 [119], [120]. As indicated on its website [119], the CCN-CERT addresses a set of actions to protect classified information and sensitive information, preserve the Spanish technological heritage, train experts, and implement security policies and procedures. For that reason, a set of guidelines about how to use the technologies for the different sectors, including universities, are given in [121], but also good practices, training courses and awareness programmes [122]. For these last three aspects, the CCN establishes a set of essential actions to support: (i) continuous training through its own training plan, comprising courses established on the basis of current needs; (ii) self-training through the implementation of webinars and online course retransmission platforms; (iii) awareness and talent through the establishment of practical challenges and the use of platforms and simulators as means of support; (iv) cyber advice on different topics (threats, social networks, and use of technologies); and (v) good practices, published in three languages (Spanish, English and French).



Last but not least, and beyond cybersecurity, it is worth highlighting the Framework of Reference for Digital Competence in Education ("Marco de Referencia de la Competencia Digital Docente", MRCDD) [123] to address the basic digital skills of professors/trainers. The framework applies the European Framework for the Digital Competence of Educators (DigCompEdu) [124] to standardise and review the digital competencies of professors/trainers regardless of the subject or the stage or type of education they teach. One of the competence areas to be developed within the MRCDD is precisely the protection of personal data, privacy, security, and digital well-being.

2.3.15 Summary- European National Cybersecurity Initiatives

The European member states have realized that they need to continue to put more effort into collectively building a strong cybersecurity workforce. The current market needs confirm that the European Union (EU) nations are facing a cybersecurity skills shortage. The recent release of the market-demanded European Cybersecurity Skills Framework (ECSF) helps to create a common understanding of the skills and knowledge required for cybersecurity workforce roles. European-level initiatives will help to consolidate policy and decision-making for more skills development efforts. However, much more is needed at the European national level. For example, at the national level, many EU countries are developing their own initiatives.

The CyberSecPro study confirms that there is a need to address the cybersecurity skills shortage across Europe and continue to put more development efforts into areas such as partnerships between academia and industry, specialized training programmes, support for cyber competitions, and public-private partnerships.

Here are some specific examples of what the EU member states can do to address the cybersecurity skills shortage:

- Invest in education and training. This includes providing financial support for students and professionals who want to pursue careers in cybersecurity, as well as developing and delivering high-quality cybersecurity training programmes.
- Create incentives for businesses to hire cybersecurity professionals. This could include tax breaks, government subsidies, or other financial incentives.
- Promote cybersecurity awareness and education among the public. This will help to create a more informed and security-conscious population, which will make it more difficult for attackers to succeed.

By taking these steps, the EU member states can help to close the cybersecurity skills gap and protect themselves from increasingly sophisticated cyberattacks.



2.4 Private Sector Cybersecurity Workforce Development Initiatives

This section considers cybersecurity workforce development frameworks proposed by organisations in the private sector.

2.4.1 SANS Institute

The SANS Institute (officially the Escal Institute of Advanced Technologies) is a US-based for-profit company established in 1989. SANS is a trusted industry player that provides information security and cybersecurity professional training, certifications, research, and other consultancy services.

SANS Institute is primarily known for its cybersecurity training programmes, which are generally considered high quality. It offers in-person, online and self-paced training courses covering various cybersecurity topics at different levels of expertise. SANS also conducts research on various cybersecurity topics to help organisations worldwide better understand and defend against cyber threats and offers free access to a large collection of security research documents.

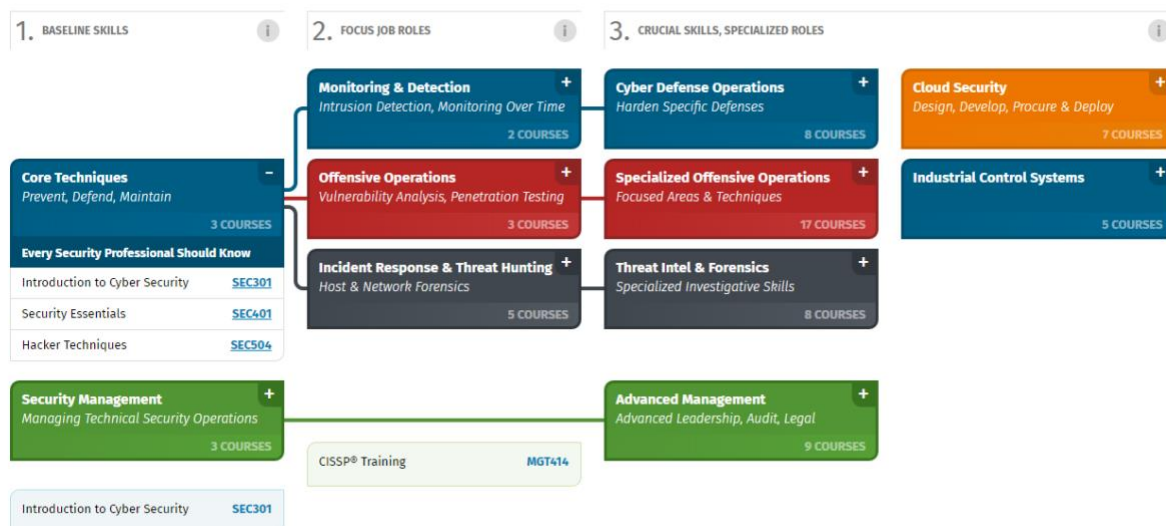


Figure 15: SANS Cybersecurity Roadmap Summary [125]

In order to facilitate its delivery of professional cybersecurity training programmes, SANS developed a web-based interactive cybersecurity skills roadmap [125]. SANS provides over 80 professional cybersecurity courses in focus areas (also identified as skills paths) such as cloud security; cyber defence and blue team operations; cybersecurity and IT essentials; digital forensics and incident response; industrial control systems security; open-source intelligence; penetration testing and red teaming; purple team, security management, legal and audit. The roadmap is partitioned into three main divisions: a) Baseline Skills, b) Focused Job roles, and c) Crucial Skills, Specialised Roles. The above figure summarises the SANS roadmap. The associations in the roadmap indicate that the baseline skills are prerequisites for attaining high-level responsibilities (focused job roles). As a result, trainees can further acquire crucial skills and assume specialised roles.

SANS' skills roadmap identified 25 cybersecurity job profiles under the earlier focus areas. However, besides the summary in Image 15 and cybersecurity courses offered by SANS, the roadmap does not appear to provide details about knowledge areas, competencies, abilities, and tasks associated with each job role.



2.4.2 ISACA

ISACA is a global professional association and learning organisation that has existed for over 50 years. Headquartered in the US, ISACA operates in 188 countries. The organisation aims to "inspire a safe and secure cyber world" [26]. To achieve this goal, ISACA, like SANS, offers cybersecurity training, certification programmes, and other resources for cybersecurity professionals and organisations. The professional programmes offered by ISACA are broader as they focus not only on cybersecurity but other core IT areas, such as software development and project management. The organisation provides both online and in-person training options. The training programmes are intended for cybersecurity and IT professionals at different career stages, from entry-level to experienced professionals.

Table 17: ISACA Key Certification Areas

Key Areas	Typical Job Profiles
Fundamentals of Computing, Networks and Infrastructure, Cybersecurity, Software Development, Data Science	Applications Developer, Systems Engineer Database Administrator, Software Developer Computer Operator, Technical Support Specialist, PC Technician, Help Desk Analyst
Audit, control, monitor and assess IT and business systems using a risk-based approach	IT Auditor, Compliance Analyst/Programme Manager, Risk Analyst/Programme Manager, Data Protection Manager, Security Officer/Security Manager, IT Consultant
Deployment and management of enterprise, IT risk and controls	Risk and Security Manager, IS or Business Analyst, IS Manager, Operations Manager Information Control Manager, Chief Information Security or Compliance Officer
Creating and implementing technical privacy-by-design solutions	Data Analyst, Privacy Engineer, Privacy, Solutions Architect, Lead Privacy Manager, IT Consultant
Identify, Protect, Detect, Respond, Recover	Cybersecurity Analyst, DevOps, Cybersecurity Engineer, SOC Analyst, Cybersecurity, Compliance Manager, Cybersecurity and IT Advisor, Cybersecurity Investigator, Network Engineer/Architect, Vulnerability Analyst/Pen Tester



Information security, governance, managing risk, programmes and incidents	IT Architect, Security Analyst, Data Security Manager, Security and Compliance Director VP/AVP Information Security, CIO/CISO/CTO
Framework-agnostic governance, risk/benefit optimization	CIO, CTO, CISO, Senior IT Internal Auditor, Cybersecurity and Compliance, Lead Analyst—IT Governance, Risk and Compliance, Security Risk and Compliance Specialist, Information Security Compliance Manager, Governance Risk Consultant

Besides other formal reports on the shortage of skilled cybersecurity professionals and the gap in cybersecurity skills demand and supply, ISACA, through its 2019 global survey [2], further confirmed cybersecurity workforce shortage, skills gaps, and other issues in various sectors. In [126] ISACA outlined several strategies for building and growing sustainable cybersecurity teams.

In order to address the cybersecurity workforce shortage and skills gap, ISACA offers several targeted cybersecurity and IT certification programmes. ISACA's certifications are highly respected in the cybersecurity and IT industry. They are designed to validate individuals' knowledge and skills in different areas of cybersecurity. The organisation offers a variety of certifications, including the Certified Information Systems Security Professional (CISSP) certification, one of the most widely recognized and sought-after certifications in the industry. Other certifications offered include the Certified Cloud Security Professional (CCSP), Certified Secure Software Lifecycle Professional (CSSLP), and the HealthCare Information Security and Privacy Practitioner (HCISPP).

Table 17 presents ISACA's broad key areas for certification and corresponding job roles associated with the areas. Core cybersecurity roles are categorised within the key areas, including identifying, protecting, detecting, responding, and recovering. Like the SANS professional programme, cybersecurity knowledge areas, abilities, competencies, and tasks are not associated with each job role. They may have been provided within each certification bundle.

2.4.3 Information Systems Security Certification Consortium (ISC)²

The Information Systems Security Certification Consortium (ISC)² is a non-profit organization that provides cybersecurity certifications to individuals and organizations. The ISC² framework is a comprehensive set of security controls that can be used to protect information systems and data. The framework is based on the following five pillars:

- **Asset Management:** The ability to identify, classify, and protect information assets.
- **Security Governance:** The establishment of policies and procedures to manage information security risks.
- **Risk Management:** The identification, assessment, and mitigation of information security risks.
- **Security Operations:** The implementation and monitoring of security controls to protect information systems and data.
- **Incident Response:** The ability to detect, respond to, and recover from information security incidents.



The ISC² framework is a valuable resource for organizations of all sizes. It provides a comprehensive set of security controls that can be used to protect information systems and data. The framework is also flexible enough to be customized to meet the specific needs of each organization. Following are some of the benefits of using the ISC² framework:

- It provides a comprehensive set of security controls that can be used to protect information systems and data.
- It is flexible enough to be customized to meet the specific needs of each organization.
- It is based on industry best practices.
- It is supported by a large community of cybersecurity professionals.

If you are looking for a comprehensive and flexible private sector security framework, the ISC² framework is a great option. It is a valuable resource for organizations of all sizes that are looking to protect their information systems and data.

ISC² offers a variety of cybersecurity certifications for professionals at all levels of experience, from entry-level to executive.

ISC² Certifications: There are a variety of ISC² certifications available, each of which is designed to validate the skills and knowledge of professionals in a specific area of cybersecurity. Some of the most popular ISC² certifications include.

- **Certified Information Systems Security Professional (CISSP)** is the most prestigious cybersecurity certification in the world. It is designed for experienced security professionals with a broad range of knowledge and skills. CISSPs are in high demand by employers, and the certification can help you advance your career in cybersecurity. The Certified Information Systems Security Professional (CISSP) is possible with optional concentrations:
 - **Information Systems Security Architecture Professional (ISSAP)**
 - **Information Systems Security Engineering Professional (ISSEP)**
 - **Information Systems Security Management Professional (ISSMP)**
- **Systems Security Certified Practitioner (SSCP)** is a foundational cybersecurity certification for entry-level security professionals. It covers the core principles of cybersecurity, such as asset security, security architecture and engineering, communication and network security, identity and access management, security assessment and testing, security operations, and software development security.
- **Certified Cloud Security Professional (CCSP)** is a cybersecurity certification for professionals who design, implement, and manage cloud security solutions. It covers the following domains: cloud security architecture and design, cloud security operations, cloud security governance and risk management, cloud security technologies, and cloud security compliance.
- **Security Assessment and Authorization Professional (CAP)** is a cybersecurity certification for professionals who assess and authorize information systems. It covers the following domains: security assessment and authorization process, security assessment and authorization tools and techniques, security assessment and authorization standards and guidelines, and security assessment and authorization case studies.



- **Certified Secure Software Lifecycle Professional (CSSLP)** is a cybersecurity certification for professionals who develop, build, and maintain secure software. It covers the following domains: software security programme management, software development security, software testing and quality assurance, and software security assessment and remediation.
- **Healthcare Information Security and Privacy Practitioner (HCISPP)** is a cybersecurity certification for professionals who protect the privacy and security of healthcare information. It covers the following domains: healthcare information security and privacy governance, healthcare information security and privacy risk management, healthcare information security and privacy legal and regulatory requirements, healthcare information security and privacy technical controls, and healthcare information security and privacy operational controls.

Benefits of ISC² certifications: Here are some of the benefits of Information Systems Security Certification Consortium ISC² certifications:

- Increased earning potential, Improved job prospects, Enhanced credibility, Access to exclusive resources and benefits, Professional development opportunities and Networking opportunities.

With a certification from ISC², you can improve your earning potential, increase your job prospects, enhance your credibility, and gain access to exclusive resources and benefits.

2.4.4 Summary- Private Sector Cybersecurity Skills Initiatives

A primary goal of reviewing existing cybersecurity workforce skills frameworks and similar initiatives is to identify cybersecurity skills development best practices and appropriate cybersecurity competencies (knowledge areas, skills) necessary for cybersecurity professional training. The frameworks we have reviewed so far meet the above goal to various extents. For instance, while some skills frameworks are cybersecurity-specific, others are broader, including other related ICT sub-disciplines. Also, whereas some workforce development frameworks provide extensive knowledge areas and skills for various cybersecurity job roles, while other frameworks fall short of specifying the required competencies. Given these observations, it is essential to note that no single framework may achieve all the workforce development goals of an organisation or sector. Therefore, it is reasonable to consider cybersecurity-specific frameworks that provide the required competencies that cybersecurity professionals need. In this vein, the NICE and ENISA frameworks are good candidates to use as reference points. Although some of the reviewed frameworks, such as the Czech, Australian, Saudi Arabian, and Canadian frameworks, are good frameworks of reference tailored to their country-specific needs, they have the NICE framework as their bedrock. It is, therefore, even more, reasonable to adopt NICE in conjunction with ECSF. ECSF must be considered because it is an EU-based framework undergoing validation within CyberSecPro.

It is also worth reiterating that the reviewed frameworks and initiatives, especially cybersecurity-specific ones, are not sector or organisation-specific. Therefore, they apply to any organisation in any sector, irrespective of size. What is required is to adapt the framework to the workforce development needs of the organisation in the industry targeted. Furthermore, the cybersecurity competencies identified via the reviewed frameworks may not fully reflect current cybersecurity labour market demands and, therefore, may not replace a market analysis survey, as would be seen in this report's later part. However, the frameworks yet serve as baselines of cybersecurity workforce development best practices that can better inform the CyberSecPro professional training programme.



3 Cybersecurity Workforce Analyses: Market Demands

The cybersecurity industry is rapidly growing and evolving, and organisations are facing increasing cyber threats. To combat these threats, it is crucial to have a skilled workforce with diverse expertise in various areas of cybersecurity. In this section, we present the results of the market analysis survey that aimed to identify the professional profiles, knowledge areas, and hands-on skills in demand that are most needed in European organisations and companies within the health, energy, and maritime sectors.

This section describes the market analysis conducted to elicit the current practical skills and knowledge areas needed by cybersecurity workers in the three sectors. The analysis derives from a survey distributed to EU partners in the CyberSecPro consortium to further distribute to their respective networks. The responses from all countries were consolidated and analysed as-a-whole, providing a view into what cybersecurity skills gaps and education development needs exist in the European economy. The survey aimed to assess the different cybersecurity skills, competencies, and values needed in the market currently, to inform the design, development, and implementation of the CyberSecPro training programmes.

3.1 Goal of the Market Analysis Survey

The cybersecurity industry faces increasing challenges with the growing number and complexity of cyber threats. To address these challenges, a skilled and competent cybersecurity workforce is required. This survey aims to identify the hands-on skills and competencies needed in the cybersecurity industry, focusing on the health, energy, and maritime sectors.

Identifying the skills and competencies required in the cybersecurity workforce is crucial to ensuring that the industry can effectively combat cyber threats. As new technologies are developed and utilised in various sectors, the demand for cybersecurity professionals with specialised skills and knowledge has increased. Understanding the industry's specific needs can help inform education and training programmes, recruitment and retention strategies, and workforce development initiatives.

This survey will help better understand the cybersecurity workforce's needs and the specific skills and competencies required to mitigate cyber threats effectively. The results of this survey will provide valuable insights for industry professionals, policymakers, and educators regarding the skills and competencies needed in the cybersecurity workforce. In addition, they will help to inform strategies for developing a more skilled and competent workforce.

3.2 Methodology

The research design for the market analysis study is a cross-sectional survey. A survey is an appropriate method for collecting data from a large sample of participants quickly and efficiently. In addition, surveys facilitate collecting insights from professionals in different business sectors.

The survey was developed based on a review of the current literature and input from cybersecurity experts within the consortium to ensure that the questions were relevant and targeted to the industry's specific needs. The questionnaire was then pilot tested with a small group of cybersecurity professionals to provide clarity and comprehension.

The survey contained multiple-choice questions on the industry's relevant job roles and open-ended questions on the knowledge areas and hands-on skills needed by cybersecurity professionals. The



multiple-choice questions were analysed using descriptive statistics to identify the most reported skills and competencies required in the cybersecurity industry. Responses from the open-ended questions were analysed using content analysis to determine themes, specific knowledge areas, and hands-on skills needed in the industry.

While self-selection and response biases may be present due to the homogenous participant group, we believe that their background and expertise provide valuable insights into the specific needs of the cybersecurity workforce in the health, energy, and maritime sectors.

3.3 Structure and Lifecycle CSP Survey

A questionnaire was developed to identify the cybersecurity workforce's needs in terms of skills and competencies required in their sector. The survey consisted of two parts: multiple-choice questions about the European Cybersecurity Skills Framework (ECSF; see Section 2.2.1) job roles needed in the industry and an open-ended question asking for knowledge areas in cybersecurity and specific hands-on skills needed. The questionnaire was developed based on a review of current literature and from input given by cybersecurity experts (see Appendix A). The landing page of the survey is shown in Figure 14.



Figure 16: CyberSecPro Market analysis survey

Section 1: The survey collected respondents' background and demographic data (i.e., education, experience, sector), as well as contact information in case the respondents wished to hear back from the survey results. Additionally, informed consent to use the data was asked in this section. If the participant did not accept the informed consent, then their responses were not included in the analysis and deleted.



Section 2: The survey focused on the job-roles defined by the European Cybersecurity Skills Framework (ECSF). The question used in this section was, “Which of the professional profiles listed in the ECSF are most needed in your organisation/company?” ECSF roles and their descriptions were presented, and participants could select multiple responses (from 0 to 12 possible responses). Responses were analysed using descriptive statistics.

Sections 3 and 4: These sections focused on the cybersecurity knowledge areas and hands-on skills. Open-ended questions were asked, and respondents could freely suggest up to 10 knowledge areas and skills. The question regarding knowledge areas was, “Which cybersecurity knowledge areas are most needed in your business?” The question about hands-on skills was, “Which cybersecurity practical skills are most needed in your organisation/company?”

The survey link was distributed through various professional networks, social media such as LinkedIn and Twitter, and targeted email lists in 16 different EU countries. Participants were encouraged to share the survey link with their colleagues and peers in the cybersecurity. The survey remained open accept responses for four weeks and took each participant approximately 10-15 minutes to complete.

At the end of the survey response period, we received 243 responses from various European countries. The responses were then inspected and categorised to identify patterns and trends in the data. The multiple-choice questions were analysed using descriptive statistics, and the open-ended questions were analysed using content analysis.

3.4 Cybersecurity Market Survey Results

This section presents the detailed results of the survey. First, descriptive statistics of the participants are presented. Next, a breakdown of responses to the survey questions pertaining to the ECSF job roles, cybersecurity knowledge areas (KAs), and hands-on skills required by organisations from cybersecurity workers is presented. Finally, the section concludes with a discussion of the general survey results, focusing on skills and competencies required in healthcare, energy, and maritime.

3.4.1 Respondents and data

The survey consisted of four sections: multiple-choice, multiple-answer questions and open-ended (free-form) question prompts. The responses were processed using thematic content analysis. The data was cleaned and transformed into a tabular format. Possible answers in different languages than English were translated. Each response was then read and categorised individually. Then, the resulting taxonomy was reviewed by domain-area experts, and final data tables were generated.

A total of 243 participated in the survey. Of these, 235 gave their consent to data usage for further analysis. The survey asked about the respondents' work organisations to establish survey demographics. The results show that 23 % of respondents worked at large organisations, 2.9 % were professional practitioners, 8.6 % worked for government organisations, 35.4 % worked at a university or research institute, and 27.6 % were in small and medium-sized enterprises (SMEs). Sector-wise, participants were distributed as follows: 54.7 % Digital-ICT, 8.2 % maritime, 6.2 % healthcare, 4.5 % energy sector, and 26.3 % miscellaneous.

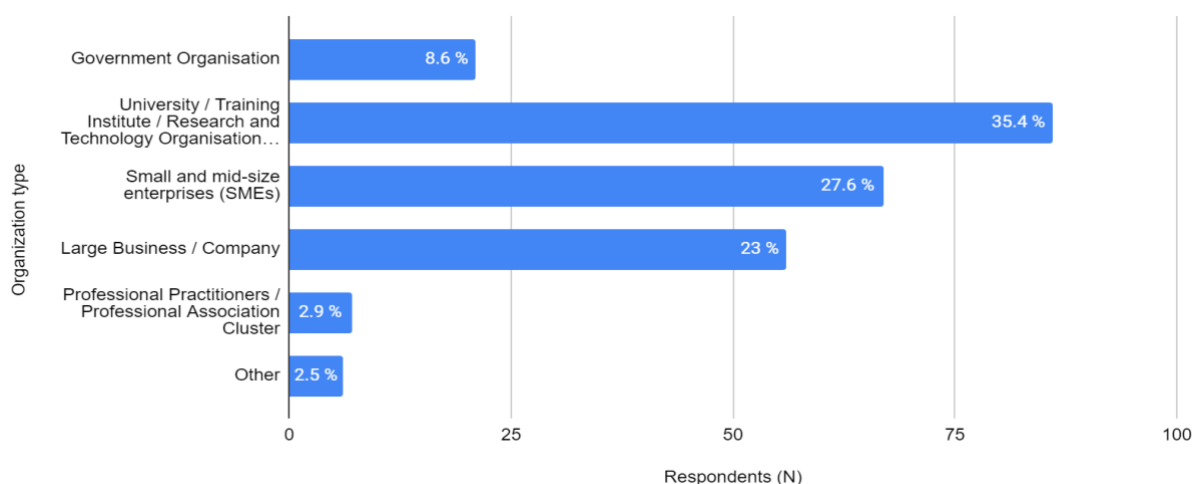


Figure 17: Respondent's Types of the Organisation

3.4.2 Cybersecurity job roles

The first part of the survey asked respondents to select the professional profiles that are most needed in their organization/company from a list of options. Profile descriptions were taken from the European Cybersecurity Skills Framework (ECSF): The options included Chief Information Security Officer, Cyber Incident Responder, Cyber Legal, Policy and Compliance Officer, Cyber Threat Intelligence Specialist, Cybersecurity Architect, Cybersecurity Auditor, Cybersecurity Educator, Cybersecurity Implementor, Cybersecurity Researcher, Cybersecurity Risk Manager, Digital Forensics Investigator, and Penetration Tester (Ethical Hacker). Table 18 presents the survey data in detail.

Table 18: Cybersecurity Job Roles Needed in the Industry (Distinguished in the Survey)

Job role / Work sector	Health (14)	Energy (10)	Maritime (20)	ICT (130)	Other (61)	Total (235)
Chief Information Security Officer	8	8	11	55	24	106 (45 %)
Cybersecurity Educator	6	2	6	59	19	92 (39 %)
Cybersecurity Architect	2	6	6	57	18	89 (38 %)
Cybersecurity Researcher	3	2	4	54	18	81 (34 %)
Cyber Legal, Policy and Compliance Officer	7	3	8	40	21	79 (34 %)
Cyber Incident Responder	4	5	10	39	20	78 (33 %)
Cybersecurity Implementor	5	5	4	47	12	73 (31 %)
Cybersecurity Risk Manager	6	6	5	33	24	74 (31 %)
Cyber Threat Intelligence Specialist	3	4	3	42	15	67 (29 %)
Penetration Tester (Ethical Hacker)	2	3	6	43	13	67 (29 %)
Cybersecurity Auditor	2	3	6	27	9	47 (20 %)
Digital Forensics Investigator	1	3	4	18	10	36 (15 %)

The most in-demand job role was Chief Information Security Officer (45 %), followed by Cybersecurity Educator (39 %), Cybersecurity Architect (38 %), Cybersecurity Researcher (34 %), Cyber Legal,



Policy and Compliance Officer (34 %), and Cyber Incident Responder (33 %). Cybersecurity Auditor (20 %) and Digital Forensics Investigator (15 %) were also often selected by the respondents.

3.4.3 Knowledge areas

Next, the survey asked respondents about knowledge areas needed in their domain. For example, respondents were asked to indicate which cybersecurity knowledge areas are currently most important. The responses were open-ended, and the data were coded using a content analysis approach. From the survey responses, we recorded a total of 1035 responses were given about knowledge areas in demand. Among these observations, 58 % were related to the Digital ICT sector, 9 % to the Maritime sector, 7 % to the Healthcare, and 5 % to the Energy sector. The remaining 21% of observations were in other, unspecified domains. Table 19 presents the most popular knowledge areas as indicated by the respondents.

Based on the responses, the most frequently mentioned topics were Cybersecurity Tools (10 % of responses), Cybersecurity Management (9 %), Cybersecurity Technologies (8 %), and Cybersecurity Principles (8 %). Among the most popular topics were also Security in Emerging Digital Technologies (6 %), Ethical Hacking (5 %), and Offensive Security (5 %).

Other topics were mentioned less frequently, but they were still fairly common. These include Cybersecurity Education and Training (3 %), Cybersecurity Regulations (3 %), Cyber Threat Awareness (2 %), Incident Response (2 %), Forensics (2 %), Threat Intelligence (2 %), Communications and Network Security (2 %), Cybersecurity for ML and AI (2 %), Penetration Testing (2%), Vulnerability Assessment (2 %), Cybersecurity Compliance (1 %), Risk Assessment (1 %), Risk Management (1%), Defensive Practitioners (1 %), Cybersecurity Management Systems (1 %), Cloud Security (1 %), Cybersecurity Architecture (1 %), Cybersecurity Engineering (1 %), and Cybersecurity Processes (1 %)

Overall, the results indicate that respondents were most interested in the knowledge areas about cybersecurity tools, management, technologies, and principles, with a wider range of topics receiving some attention but to a lesser scale. It is notable that the most valued knowledge areas are related to technical or technology knowledge, and management. This information can give indications of the respondents' needs in different knowledge areas of cybersecurity.

Note: In the following table percentages are presented in relation to the total number of observations. (Rows 28-93 are omitted for presentation clarity. The full data is presented in [Appendix B](#).)

Table 19: Cybersecurity Knowledge Areas in Demand

Knowledge areas (KA) in demand	Health (69)	Energy(55)	Maritime (91)	ICT (599)	Other fields(221)	Total (1035)
Cybersecurity Tools	5	6	8	55	29	103 (10 %)
Cybersecurity Management	6	8	0	49	25	88 (9 %)
Cybersecurity Technologies	3	5	0	52	24	84 (8 %)
Cybersecurity Principles	7	5	2	48	19	81 (8 %)



Emerging Digital Technologies	3	3	5	40	14	65 (6 %)
Ethical Hacking	5	6	0	30	13	54 (5 %)
Offensive Security	3	5	2	25	12	47 (5 %)
Cybersecurity Education and Training	4	1	0	17	6	28 (3 %)
Cybersecurity Regulations	1	0	3	15	8	27 (3 %)
Cyber threat awareness	0	1	6	12	5	24 (2 %)
Incident response	2	1	4	12	2	21 (2 %)
Forensics	1	1	0	9	7	18 (2 %)
Threat intelligence	0	0	0	14	4	18 (2 %)
Communications and Network Security	3	1	0	13	0	17 (2 %)
Cybersecurity for ML and AI	1	1	0	13	1	16 (2 %)
Penetration Testing	1	0	1	11	3	16 (2 %)
Vulnerability Assessment	2	1	3	10	0	16 (2 %)
Cybersecurity Compliance	0	0	2	12	1	15 (1 %)
Risk Assessment	0	2	3	5	5	15 (1 %)
Risk Management	3	1	2	7	2	15 (1 %)
Defensive practitioners	0	1	0	9	4	14 (1 %)
Cybersecurity Management Systems	0	0	12	0	1	13 (1 %)
Cloud Security	0	1	0	8	2	11 (1 %)
Cybersecurity Architecture	0	0	1	7	2	10 (1 %)
Cybersecurity Engineering	1	1	6	2	0	10 (1 %)
Cybersecurity Processes	0	0	8	0	2	10 (1 %)
Data protection and security	2	1	0	5	1	9 (1 %)

3.4.4 Hands-on skills

Finally, the survey asked respondents about the different hands-on skills and skillsets needed for work in cybersecurity. The question was open-ended, and respondents could record up to 10 different skills. Table 20 presents the most sought-after practical skills identified by the survey responses. As a whole, 714 observations of various skills were recorded during the analysis.

Overall, the survey results demonstrated a considerable dispersion of responses across the various categories. However, some skills were reported more than others: The top-reported needed skills were Network security control (4 %), Penetration testing (4 %), and Incident response (4 %). Other highly



Cybersecurity Workforce Analyses: Market Demands

reported needs included Cloud security (3 %), Risk management (3 %), Education and training skills (3 %), and Risk assessment (3 %).

Note: The following table presents the Hands-on Skills in Demand Based on Survey Responses (Percentages are presented in relation to the total number of observations. Rows 28-121 are omitted for presentation clarity. The full data is presented in [Appended B.](#))

Table 20: Cybersecurity Hands-on Skills in Demand

Hands-on skills in demand	Health (54)	Energy (36)	Maritime (53)	ICT (420)	Other (151)	Total (714)
Network security control	2	0	1	22	7	32 (4 %)
Penetration testing	1	0	1	26	4	32 (4 %)
Incident response	0	1	3	18	8	30 (4 %)
Cloud security	1	4	1	13	4	23 (3 %)
Risk management	5	2	1	10	5	23 (3 %)
Education and training skills	2	1	1	8	9	21 (3 %)
Risk assessment	1	2	1	12	5	21 (3 %)
Forensics	0	1	1	16	2	20 (3 %)
Network and system administration	0	2	2	12	5	21 (3 %)
Technical skills	0	0	0	10	8	18 (3 %)
Legal Training	1	0	0	12	4	17 (2 %)
Threat detection	2	0	0	12	3	17 (2 %)
Analysis and Critical thinking	1	0	0	10	5	16 (2 %)
Artificial intelligence (AI)	1	1	1	9	4	16 (2 %)
Cybersecurity architecture	0	0	2	11	3	14 (2 %)
Software security	1	1	1	13	1	17 (2 %)
Programming skills	1	0	1	9	4	14 (2 %)
Compliance	0	2	0	12	0	16 (2 %)
Vulnerability assessment	0	0	0	10	4	14 (2 %)
Communication - teamwork (soft-skills)	2	2	2	5	2	13 (2 %)
Threat understanding / knowledge	0	0	3	6	3	12 (2 %)
Operating Systems	0	1	0	8	2	11 (2 %)



Software Design Skills	0	0	0	8	3	11 (2 %)
Auditing	0	0	0	8	2	10 (1 %)
DevSecOps / DevOps	1	2	0	6	1	10 (1 %)
Management skills	0	0	2	5	3	10 (1 %)
Threat intelligence	0	0	0	9	1	10 (1 %)

3.5 Discussion

The objective of the survey was to assess and determine the cybersecurity knowledge areas and skills demanded in the labour market, with a focus on the key sectors of energy, maritime, and health. The survey was conducted through an online-based questionnaire, and to strengthen the generalisation of the results, the survey used a convenience sample of experts working in cyber security domains. The survey is considered cross-sectional across countries in the EU, with participants surveyed at one point in time.

Data from 235 responses were used to extract observations of cybersecurity knowledge areas and hands-on skills. Participants provided 1035 responses of knowledge areas in cybersecurity that corresponded to 27 categories (Table 19) of cybersecurity knowledge areas. Within the knowledge areas, 58 % of the observations were related to the Digital ICT sector, 9% were reported in the Maritime sector, 7% in the Healthcare, and 5% in the Energy. Additionally, 714 observations on hands-on skills distributed across 27 categories (Table 20) elicited 59 % of responses in the ICT sector. Other sectors, including Health (8 %), Maritime (7 %), and Energy (5 %) were less represented among the respondents, but conclusions about skills needed in these business fields could still be drawn. Next, this section discusses cybersecurity knowledge and skills in the Health, Energy, and Maritime Sectors in detail.

3.5.1 Cybersecurity Skills Required in the Health, Energy, and Maritime Sectors

The JRC cybersecurity taxonomy [19] identified several economic sectors that should be targeted for cybersecurity governance (i.e., healthcare, energy, and transportation). The mandate of CyberSecPro is to prioritise the cybersecurity workforce skills development in the healthcare, energy, and maritime sectors as specified by ENISA [39], [40]. In this regard, this section considers the cybersecurity knowledge and skills necessary to provide secure, safe health, energy, and maritime infrastructure. A primary objective of CyberSecPro is to specify and develop a cybersecurity training programme that enables cybersecurity professionals to protect operational and information technologies deployed within the target industry sectors. An intensive analysis of the sectorial cybersecurity competency and skill needs is therefore needed in order to identify and develop professional training programmes in order to meet the needs of the labour market.

In the previous sections, we reviewed existing cybersecurity frameworks developed to enable governments and public and private organisations to train 21st-century cybersecurity professionals responsible for securing and protecting critical infrastructure from malicious attacks. Based on the cybersecurity skills frameworks reviewed, we can conclude that the frameworks provided in terms of job profiles, knowledge, skills, and competencies broadly apply across all sectors and to all organisations within any sector, regardless of size or the required cybersecurity governance complexity. This conclusion aligns with the motivations of the authors of the reviewed frameworks. The reviewed frameworks can guide any organisation wishing to establish a cybersecurity governance structure where none exists.



On the other hand, a cybersecurity skills framework can help an organisation improve the security and resilience of its critical infrastructure where a cybersecurity governance structure already exists. It is important to note that our literature search did not find publications that analysed and documented cybersecurity knowledge and skills exclusive to an organisation in any sector. This information can be addressed by surveying specific sectors' knowledge areas and skills required in their workforce. This information will then highlight the need for specific cybersecurity work roles, which the CyberSecPro market skills survey addresses.

3.5.2 Cybersecurity Skills for the Health Sector

The healthcare domain comprises several multi-functional companies providing services, products, or both. This includes pharmaceutical industries, manufacturing industries, and patient care centres. Given the rapid development and integration of digital technologies, the health sector workforce needs to be continuously updated and trained. One major concern for the health sector is the reliance on access to patient data and information. Modern-day ICT-compliant healthcare infrastructure includes the assets identified in the ECHO project.

Health sector respondents identified Cybersecurity Principles (10%) as the most important area, followed by Cybersecurity Management (9%) and Cybersecurity Tools (7%). Ethical Hacking, Cybersecurity Education and Training, Communications and Network Security, and Cybersecurity Technologies were each mentioned by 4% of respondents. Ethical Hacking, Cybersecurity Education and Training, Communications and Network Security, and Cybersecurity Technologies were each mentioned by 4% of respondents. Other areas receiving between 3% and 4% of mentions included Embedded Systems, Emerging Digital Technologies, Risk Management, Incident Response, and Vulnerability Assessment (see Table 19 and Table 20).

3.5.3 Cybersecurity Skills for the Energy Sector

The energy sector is another primary focus of CyberSecPro. The core assets in the energy sector include the SCADA system and programmable logic controllers (PLCs). These assets control the manufacturing and supply of energy, among other functions. The loss of control of these devices to an attacker could result in the attacker changing set parameters, thus causing a ripple effect and crippling all related operations. The significance of this sector and the severity of the consequences of any security breach necessitated being classified as critical infrastructure. Cybersecurity professionals are responsible for securing and protecting critical infrastructure against current and emerging attacks, hence the need for a targeted professional cybersecurity programme.

Based on the survey data, cybersecurity management was the most popular knowledge area, with 15% of respondents indicating that it was important in their business sector. Other popular topics included cybersecurity tools (11%), ethical hacking (11%), cybersecurity principles (9%), cybersecurity technologies (9%), and offensive security (9%). Emerging digital technologies and risk assessment were less popular, with 5% and 4% of respondents expressing their importance, respectively. Overall, the results suggest that respondents valued a mix of managerial and technical topics, with cybersecurity management and tools being the most popular.



3.5.4 Cybersecurity Skills for the Maritime Sector

The transport sector is yet another key sector that is classified as a critical infrastructure sector. The Maritime sector is a sub-sector within transportation. In the maritime sector, operational and information technologies are required to interoperate and coordinate various shipping lines. For the logistics to work, cybersecurity can be seen as a paramount factor to consider. Operational technologies such as propulsion plants, dynamic positioning systems, and monitoring and control systems, among other systems, help to ensure a safe operational environment. However, the complex nature of these systems, especially cyber-physical systems, implies that they can become susceptible to various malicious attacks. The complex nature of the operating environment may explain the need for better management, processes, and tools for cybersecurity in the maritime sector.

The survey results reflect the state of the maritime sector as uncovered in the related literature. Based on the survey responses, the most popular knowledge areas in the maritime sector were Cybersecurity Management Systems (13%) followed by Cybersecurity Tools (9%), Cybersecurity Processes (9%), Cyber Threat Awareness (7%), and Cybersecurity Engineering (7%). Several other topics received between 3% and 5% of respondents expressing importance, including Emerging Digital Technologies (5%), Incident Response (4%), Cybersecurity Regulations (3%), and Vulnerability Assessment (3%). Overall, the results suggest that respondents valued topics related to cybersecurity management, tools, and processes, with a smaller proportion expressing interest in more technical areas such as cybersecurity engineering and vulnerability assessment.



4 Cybersecurity Practical Skills Gaps in Europe: Analyses and Prioritisation

This chapter presents the cybersecurity practical skills gap in Europe. It analyses cybersecurity frameworks, standards, current European higher education programmes and market analysis to identify key knowledge areas, skills, and competencies. The complete list of cybersecurity practical skills can be complex and interpreted differently by EU nations and organisations. Therefore, the report combines them into a list of cybersecurity practical knowledge areas and highly essential practical skills. The outcome is represented as the cybersecurity practical skills gap in Europe.

The following sections present the outcome of a cybersecurity knowledge and skills gap analysis in Europe. These knowledge areas and skills gaps resulted from a comparative analysis of market demand and supply. The market demand considers the current state of the art from Chapter 2 and the market survey from Chapter 3. The supply side comes from the analysis of cybersecurity academic programs at European Higher Education Institutions (HEIs), as presented in Section 4.3 below.

4.1 The Market Demand Side: Essential Cybersecurity Practical Skills

The following section presents the outcome of the market demand survey conducted in CyberSecPro. It identifies and presents the most essential cybersecurity practical skills found in the conducted cybersecurity market demand survey. The list combines the cybersecurity knowledge areas and skills presented in chapter 3, and essentially presented as the most essential cybersecurity practical skills reported in the market demand survey. It was reasonable to combine knowledge areas and skills because many overlapping instances were observed. This case of overlapping was also observed in the supply-side analysis. The merger of knowledge areas and skills is also due to the complexity of arriving at a comprehensive list of skills given the varying understanding and interpretation of skills by EU nations and organisations.

4.1.1 Cybersecurity Skills Demand Prioritisation Criteria:

The list of practical skills and hands-on capabilities needed in the market is presented in Table 23. The prioritisation was performed as follows:

- Responses (from data presented in Section 3) were examined and re-grouped to align with ENISA’s cybersecurity skills framework lexicon and classification.
- The resulting skills were ordered (descending) by the number of observations.
- To calculate priority levels, the maximum number of responses for each skill across all sectors is calibrated on a two-points interval scale.
- **The two-interval is simple method for the prioritisation as most of the respondent confirms the demand of the cybersecurity skills. The resulting priority categories are**
 - **In demand:** When the number of observations is below 40 (<40 or less Market Demand Survey Responses).
 - **High demand:** If the number of observations is above 40 (40 or more > Market Demand Survey Responses).
 - **The categorisation is based on number of response entries.**



Table 21 presents the outcome of implementing the above criteria. The last column in Table 21 indicates the knowledge areas and skills that were normalised and regrouped according to ENISA’s skills framework. We used not applicable to (NA) to refer to respondents’ knowledge areas and skills that appear consistently in either the knowledge or skills table.

Table 21: Cybersecurity Knowledge Areas and Hands-on Skills in Demand (Combined List from the Survey Results)

S/N	Essential Cybersecurity Practical Skills: Market Demand	No. of Observations	Priority Level	Merged Knowledge Areas and Skills (included in the main category of column 2)
1	Ethical Hacking and Penetration Testing	192	High demand	Penetration testing/Ethical hacking/Defensive Practitioners/Offensive Security/Vulnerability assessment/Vulnerability analysis
2	Cybersecurity Tools and Technologies	187	High demand	Cybersecurity tools/Cybersecurity technologies
3	Cybersecurity Management Systems: CS Management and Processes	111	High demand	Cybersecurity management, cybersecurity management systems, cybersecurity processes,
4	Cybersecurity Principles	81	High demand	NA
5	Cybersecurity Threat Management: Threat Awareness, Threat Knowledge, Threat Assessment, Threat Intelligence, Threat Detection	78	High demand	Cybersecurity threat awareness/Threat intelligence/Threat detection/Threat understanding/Threat knowledge
6	Risk Assessment and Risk Management	76	High demand	Risk assessment/Risk management
7	Emerging Technologies	65	High demand	NA
8	Cybersecurity Regulations and Compliance	58	High demand	Cybersecurity regulations/Cybersecurity compliance/Compliance
9	Cybersecurity Education and Training	49	High demand	Education and training/Education and training skills
10	Incident Response	49	High demand	Appear as both knowledge and skill
11	Communications and Network Security: Network Security Controls	48	High demand	Communication and network security/Network security control



12	Cybersecurity Forensics	38	In demand	Appeared as both knowledge and skill
13	Cloud Security	37	In demand	Appeared as both knowledge and skill
14	Cybersecurity for Artificial Intelligence and Machine Learning	32	In demand	Cybersecurity for artificial intelligence and machine learning/Artificial intelligence
15	Legal and Auditing Training	27	In demand	Legal training/Auditing
16	Cybersecurity Architecture	24	In demand	Appeared as both knowledge and skill
17	Cybersecurity Engineering	22	In demand	Cybersecurity engineer / DevSecOps / DevOps
18	Network and System Administration	21	In demand	NA
19	Technical Skills	18	In demand	NA
20	Software Security	17	In demand	NA
21	Analysis and Critical Thinking (soft/professional skills)	16	In demand	NA
22	Programming Skills	14	In demand	NA
23	Communication and Teamwork (soft/professional skills)	13	In demand	NA
24	Operating Systems	12	In demand	NA
25	Software Design Skills	11	In demand	NA
26	Data Protection and Security	9	In demand	NA

4.1.2 The Sectoral Specific Cybersecurity Knowledge Area Prioritisation: Health, Energy, Maritime, ICT and Others

This section presents the prioritisation of knowledge areas based on survey responses and for each sector. The prioritisation criteria derive from the criteria used to prioritise the combined list of knowledge areas and skills provided in Table 21. The only difference in this case is the sector specification. To prioritise cybersecurity knowledge areas according to sectors, the maximum number of responses for each skill in each sector is calibrated on a three-points interval scale. As an example, the nearest sum of the scores of each knowledge area is divided into three intervals. The upper interval is assigned a critical priority while the middle and low intervals are assigned High-demand and In-demand priority levels, respectively.

Table 22 presents knowledge areas prioritisation for health, energy, maritime and other sectors based on respondents' observations. Table 22 complements Table 22-Section Three as it prioritises knowledge areas demanded by each sector. It is important to note that Table 22 provides also ECSF-



normalised knowledge areas and skills. The normalisation process reduces ambiguity and duplicity while enhancing comprehension.

Prioritisation challenges with sectoral specific survey data: The biggest challenge in this study was the limited number of responses for the sectoral specific data of health, energy, and maritime. This resulted in different priority levels for the final outcome of the skills gaps between sectoral specific and combined practical skills gaps. The researchers considered the following criteria for the sectoral specific prioritisation:

- **In demand:** When the number of observations is below 20 (less than 20 Market Demand Survey Responses).
- **High demand:** If the number of observations is above 20 (more than 20 Market Demand Survey Responses).

The categorization is based on the number of response entries. **However, the sectoral specific prioritisation may not provide accurate results due to the limited number of responses for each sector, including health, energy, and maritime cybersecurity skills.** Therefore, the researchers suggest considering the final list of the European cybersecurity skills gaps (Figure 20) for the high demand and in demand skills level reliable results.

Table 22: Knowledge Area Prioritisation for All Sectors

Knowledge Areas	Health	Energy	Maritime	ICT	Other
Penetration Testing	In demand	In demand	High demand	High demand	High demand
Cybersecurity Tools/Technologies	In demand	In demand	In demand	High demand	High demand
Cybersecurity Threat Management: Threat Awareness, Threat Knowledge, Threat Assessment, Threat Intelligence, Threat Detection	In demand	In demand	In demand	High demand	In demand
Cybersecurity Management Systems: CS Management and Processes	In demand	In demand	High demand	High demand	High demand
Risk Assessment and Risk Management	In demand	In demand	In demand	High demand	In demand
Emerging Technologies	In demand	In demand	In demand	High demand	
Cybersecurity Regulations and Compliance	In demand	In demand	In demand	High demand	In demand
Cybersecurity Education and Training	In demand	In demand	In demand	In demand	In demand
Incident Response	In demand	In demand	In demand	In demand	In demand



Communications and Network Security: Network Security Controls	In demand	In demand	In demand	In demand	In demand
Cybersecurity Forensics	In demand	In demand	In demand	In demand	In demand
Cloud Security	In demand	In demand	In demand	In demand	In demand
Cybersecurity for Artificial Intelligence and Machine Learning	In demand	In demand	In demand	In demand	In demand
Cybersecurity Architecture	In demand	In demand	In demand	In demand	In demand
Data Protection and Security	In demand	In demand	In demand	In demand	In demand
Cybersecurity Engineering	In demand	In demand	In demand	In demand	In demand

4.1.3 The Sectoral Specific Cybersecurity Hands-on Skills Prioritisation: Health, Energy, Maritime, ICT and Other

Like the previous section, this section presents the prioritisation of skills based on survey responses for each sector under consideration. The prioritisation criteria used for knowledge areas are also applied here, except that a two-point scale interval (upper interval for High-demand priority level and low interval for In-demand priority level) is used. The reason for using a two-point interval scale is that data scores for cybersecurity skills appeared too low and too close to support a three-point interval calibration, especially in the health, energy, and maritime sectors.

Table 23 presents skills prioritisation for all sectors considered in this report and based on survey respondents' observations

Table 23: Hands-on Skills Prioritisation for All Sectors

Hands-on Skills	Health	Energy	Maritime	ICT	Other
Penetration Testing	In demand	In demand	In demand	High demand	In demand
Cybersecurity Threat Management: Threat Awareness, Threat Knowledge, Threat Assessment, Threat Intelligence, Threat Detection	In demand	In demand	In demand	High demand	In demand
Risk Assessment and Risk Management	In demand	In demand	In demand	High demand	In demand
Cybersecurity Regulations	In demand	In demand	In demand	In demand	In demand



and Compliance					
Cybersecurity Education and Training	In demand	In demand	In demand	In demand	In demand
Incident Response	In demand	In demand	In demand	In demand	In demand
Communications and Network Security: Network Security Controls	In demand	In demand	In demand	High demand	In demand
Cybersecurity Forensics	In demand	In demand	In demand	In demand	In demand
Cloud Security	In demand	In demand	In demand	In demand	In demand
Cybersecurity for Artificial Intelligence and Machine Learning	In demand	In demand	In demand	In demand	In demand
Cybersecurity Architecture	In demand	In demand	In demand	In demand	In demand
Cybersecurity Engineering	In demand	In demand	In demand	In demand	In demand
Programming Skills	In demand	In demand	In demand	In demand	In demand
Operating Systems	In demand	In demand	In demand	In demand	In demand
Communication and Teamwork (soft skills)	In demand	In demand	In demand	In demand	In demand
Software Design Skills	In demand	In demand	In demand	In demand	In demand
Management Skills (soft skills)	In demand	In demand	In demand	In demand	In demand
Legal Training and Auditing	In demand	In demand	In demand	In demand	In demand
Software Security	In demand	In demand	In demand	In demand	In demand
Network and System Administration	In demand	In demand	In demand	In demand	In demand
Analytical and Critical Thinking (Soft skills)	In demand	In demand	In demand	In demand	In demand

4.2 The Market Supply Side: Analyses of Practical Cybersecurity Skills Offered in EU Academic Programmes

This section considers cybersecurity knowledge areas and skills offered by cybersecurity academic programmes across EU HEIs and other cybersecurity professional training providers.

4.2.1 ENISA/CyberHEAD: Analyses of the European Cybersecurity Education Roadmap

In the EU and EFTA nations, the Cybersecurity Higher Education Database (CyberHEAD) is the largest certified database for higher education in cybersecurity. It has served as the primary source of information for all citizens wishing to advance their knowledge in the realm of cybersecurity.



CyberHEAD has a database of 136 cybersecurity programmes in 26 countries at all higher education levels, with master specialisations being the most offered, in online, classroom or blended deliveries.

Of the 136 programmes, only 12 programmes are both free of charge and In English (2 BSc, 10 MSc) while 40 programmes offered in English also had fees associated with the degree.

Of these, the programmes that offer teaching (N=48) that cover defined roles (i.e., ENISA, NIST, ACM) or certifications were included in the analysis.

CyberHEAD is the largest recognized cybersecurity higher education database in the EU and EFTA. Anyone seeking cybersecurity expertise development can use the database. CyberHEAD lists 136 cybersecurity programmes in 26 countries, most of which are master's degrees in online, classroom, or blended formats. Only 12 of the 136 programmes (2 BSc, 10MSc) are free and in English, while 40 of them have fees.

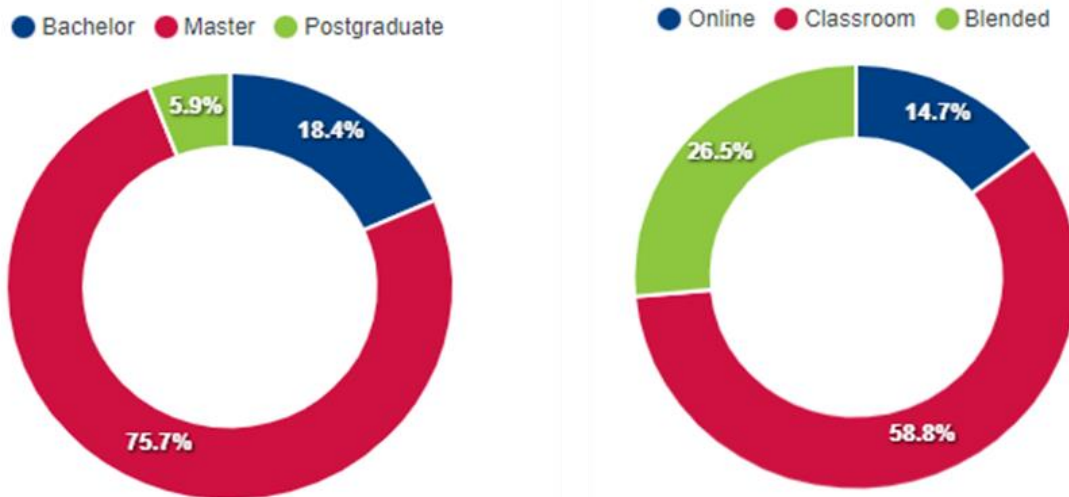


Figure 18: ENISA CyberHEAD: European Cybersecurity Higher Education Programme Summary

The Analyses comprising N=48 programmes that teach defined roles (ENISA, NIST, ACM) or certifications showed that ENISA descriptions predominated. EU offerings covered 11 of ENISA's 12 jobs except for Cybersecurity Auditor. Only 4 other framework positions were employed as career options in EU academic programmes, but they overlap with ENISA roles. ENISA's Legal Policy & Compliance officer and Data protection officer overlap with ENISA's Digital Forensic Officer and NIST IT Forensic specialist.

Table 24: Summary of Cybersecurity Academic Offerings Based on Job Roles

ENISA Roles Framework	European Academic Offering
Digital Forensics Investigator	13
Chief Information Security Officer	13



Cyber Legal Policy & Compliance Officer	10
Cybersecurity Architect	8
Cybersecurity Risk Manager	8
Penetration Tester	7
Cyber Incident Responder	4
Cybersecurity Implementer	3
Cybersecurity Researcher	2
Cyber Threat Intelligent Specialist	2
Cybersecurity Educator	2
Data protection and security officers	3
IT Forensic Expert	3
Data Protection Officer	2
Cyber Resilience Specialist	1

4.2.2 Cybersec4Europe: Analyses of the European Academic Offering

CyberSec4Europe Knowledge Framework completed July 2022, combines ideas from other frameworks, but due to the fact that CSEC uses accepted and well-established scientific vocabulary from the ACM and is considered the most appropriate for teaching and training professionals, CyberSec4Europe uses CSEC as a foundation but includes inputs from CWF, JRC, CyBOK, and ECSO. The knowledge area produced by the framework is divided into 9 knowledge areas with smaller knowledge units. The knowledge area "operate and maintain" and its corresponding knowledge unit "Customer Service and Technical Support" come from CWF; the remaining knowledge areas are all drawn from CSEC.

The ACM framework was prioritised for overlapping concepts due to its emphasis on scientific and knowledge-based terminology, while the NICE framework places greater emphasis on workforce skills and corresponding terminology. Consequently, the framework that emerged is an extension of the ACM framework, which encompasses a knowledge area titled "Customer Service and Technical Support." This knowledge area pertains to the sole speciality area of the NICE framework that was not addressed by a knowledge area of the ACM framework. The framework was centred on a moderate level of categorization, specifically the knowledge areas and knowledge units outlined in the ACM framework. The survey comprised a total of 104 education programmes that were offered by 96 educational institutions located in the member states of the European Union. The knowledge areas and sub-knowledge units are described as follows:

Survey results show that Mandatory courses cover all knowledge units. Thus, at least one education programme in the survey requires every knowledge unit. Data Security knowledge units were most identified and ranked 1-4, 9-10, and 17, where the Data Security knowledge area's Cryptography and System Security knowledge units are the most covered with a minimum coverage of 80% when using more relaxed standards. The Organisational Security and System Retirement sub-knowledge units are the least covered (only 20% coverage). Societal Security (Customer Service and Technical Support),



Organisational Security (Security Operations and Personal Security), Component Security (Component Procurement), and Connection Security (Physical Interface and Connectors) also lack coverage. Design, Privacy, Analyses, and Testing are required in less than 30% of school programmes. Large countries (Spain, Germany, France, Italy) cover over 75% of knowledge units with mandatory courses under the stricter coverage metric. But if metrics are eased, then most countries cover over 80% of all knowledge areas.

Some remarks on the results should be noted. Countries with higher subject coverage have a more balanced distribution of knowledge area coverage, while countries with lower topic coverage have an uneven distribution. However, these results are based only on whether each country has at least one educational programme for each knowledge unit. And even though mandated education programmes include most knowledge areas, some countries, i.e., Sweden and Cyprus, which rank 5th and 7th globally for mandated training, cover practically all knowledge categories except Component Security.

4.2.3 CONCORDIA: Analyses of the European Academic Offering

CONCORDIA created a framework for the European Cybersecurity Education Ecosystem. This was done by mapping the consortium's offerings that were concentrated on skill development from university and industry partners, and then contrasting those with the market's and different CONCORDIA partners' (primarily the industry partners') needs for skill development. CONCORDIA offer 30+ English courses across the EU on five pillars (see Figure 19):

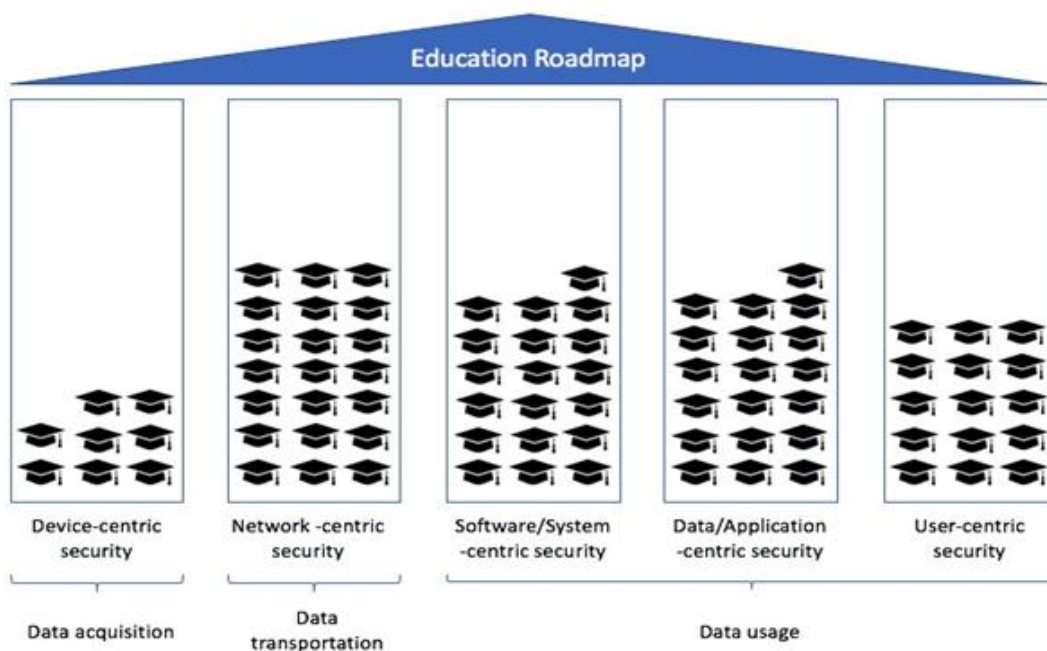


Figure 19: CONCORDIA's Five Pillars of Education Roadmap

(1) Device-centric Security: DCS focuses on securing devices that generate raw data, including embedded systems, sensors, IoT devices, and drones, as well as addressing security concerns related to IoT.



(2) Network-centric Security: NCS pertains to data transport, networking, and security concerns. Topics include DDoS protection, SDN, and encrypted traffic analysis.

(3) Software/System-centric Security: SSCS focuses on middleware, secure OS, and security by design. Malware analysis, system security validation, zero-day detection, and service dependency recognition are covered.

(4) Data/Application-centric Security: DACS focuses on data and application security, including data visualisation and securing cloud services.

(5) User-centric Security: UCS focuses on user security concerns such as privacy, social networks, fake news, and identity management.

Table 25: Summary of CONCORDIA Analysed Academic Offerings

Title	Who	What
Cyber Range: IT Ethical Hacking	Airbus Cybersecurity	Hands-on Labs on different topics and countermeasures in a simulated network.
ICS-Ethical Hacking	Airbus Cybersecurity	Hands-on Labs on different topics of threats scenarios and countermeasures in a simulated industrial environment.
Cyber Incident Handling Workshop	Airbus Cybersecurity	Table-top game to learn how to deal with cyber incidents from different perspectives.
Cyber Range: Advanced Persistent Threats and Targeted Attacks	Airbus Cybersecurity	Hands-on labs to learn current techniques of APTs and Targeted Attacks.
Cyber Incident Game	Airbus Cybersecurity	Play the hacker role: plan a cyber-attack on a classical network or an industrial network infrastructure.
Cybersecurity for business	EIT Digital	An innovative training to empower and train in improving and championing Cybersecurity for the future
Security and Privacy for Big Data	EIT Digital	Learn how to identify key security and data protection issues and how to apply privacy preserving methodologies in compliance with the current regulations
ENISA Summer School (Assisting the organization)	FORTH	Network and Information security: policy, economic, legal and research matters



CSIRT Cyber Training	Masaryk University	Hands-on tailor-made Cybersecurity training for IT administrators and CSIRT/CERT members. Everything from servers hardening to network monitoring & analysis
Capture the Flag by Team Localos	Research Institute CODE	Learn and evolve your Cybersecurity capabilities. And have fun at our Cybersecurity competition!
IT Competence Education and Training	Research Institute CODE	In our flexible Cyber Range, participants are provided with self-learning modules, individual exercises as well as defensive/offensive hands-on scenarios.
SINA Basics	Secunet	Basics and functions of the Secure Inter-Network Architecture (SINA)
TRANSITS I/II	SURFnet	Training for new and experienced computer security incident response team (CSIRT) personnel, and individuals interested in establishing a CSIRT.
Reliable Software and Operating Systems	Technical University Darmstadt	Dependability and Security Issues for SW systems
Security and the Cloud: The Issue of Metrics	Technical University Darmstadt	SW and Distributed Systems Security
ICT Security	University Mariboru	Basics; Physical security and biometrics; Cryptography basics; Secure e-commerce; Protection of communication technologies; Standards, security policies and security planning; Software security; User aspects of security and privacy
Data protection	University Mariboru	Introduction to the topic; Advanced cryptography;



		Usability and related standards; Practical aspects of data protection
ADVANCED INFORMATION SECURITY	University Mariboru	Provide in-depth knowledge on techniques for securing and protecting information, computer systems and computer networks
Data security and privacy	University Insubria	Models, tools and languages for managing access control and privacy policies/ preferences in a data management system
DATA SECURITY FUNDAMENTALS	University Insubria	Basic knowledge for the design and verification of mechanisms for data protection in information systems and networks
Internet Security Protocols	University Twente	MOOC to discuss the details of Internet security protocols, such as HTTPS, SSH, DNSSEC, IPsec and WPA
Internet attacks and defence	University Twente	MOOC to discuss how to detect and mitigate Internet attacks. Topics include DDoS, IDS and Firewalls
Certified Information Systems Auditor CISA - certification and exam preparation	SBA Research	The course helps in preparing for the exam in view of CISA certification. The Certified Information Systems Auditor (CISA) is a globally recognized certification for professionals in the areas of auditing, control and information security.
Certified Security Information Manager CISM and Certification exam preparation	SBA Research	The course helps in preparing for the exam in view of CISM certification. The Certified Information Security Manager (CISM) is a globally recognized certification for experts in the field of information security management in companies.
Certified Information Security Systems Professional CISSP exam certification preparation	SBA Research	The course helps in preparing for the exam in view of CISSP



		certification. The CISSP examination covers 8 areas of security which are necessary for the essential protection of information systems, companies and national infrastructures.
Certified Secure Software Lifecycle Professional CSSLP - certification and exam preparation	SBA Research	The course helps in preparing for the exam in view of CSSLP certification. The CSSLP certification guarantees that you have comprehensive knowledge in all areas of the secure development lifecycle.
Cybersecurity Essentials	SBA Research	The aim of the course is to provide participants with an introduction to the topics of cyber security as well as IT and information security. The course provides participants with sound basic knowledge and essential threat scenarios as well as modern solutions and methods for coping with cyber risks.
Incident Response	SBA Research	The aim is to learn tools and techniques for clarifying an APT incident. The course participants will also have the practical opportunity to investigate a simulated APT attack using hard disks and memory images.
Windows Hacking	SBA Research	The aim is to convey the most frequent and dangerous gaps in Windows networks and thus provide the necessary knowledge for securing security-relevant networks and servers.
Secure Coding in C/C++	SBA Research	This training is specially designed for C/C++ developers. It covers secure software development practices and attacks.



Web Application Security	SBA Research	The course teaches developers the most common and dangerous bugs in web application development. Testers learn how to test security aspects.
IoT Security Essentials	SBA Research	The course teaches the typical and dangerous security vulnerabilities of Internet Enabled hardware, including the OWASP IoT Top 10

CONCORDIA Courses mainly focus on Telecom and Transport industries but can have relevance to other sectors. These courses (see Table 25) are offered through the CONCORDIA platform.

4.2.4 JRC Atlas: Analyses of Cybersecurity Knowledge Areas

The JRC/ATLAS also identifies and maps EU cybersecurity centres, including research organisations, academic groups, and operational centres, based on their expertise in specific domains using the proposed taxonomy. Over 660 responses from 60 centres across Europe participated in this project. The analysis of respondents' research domains revealed that all cybersecurity domains were covered, with 39 institutions claiming to cover all 14 domains. 191 institutions reported coverage of at least 10 out of the 14 specified cybersecurity domains in the survey, but there are relevant sub-domains that are poorly investigated (i.e., post-quantum cryptography). A notable trend is a prevalence of "privacy and data protection" subdomains in top positions, indicating European research institutions' focus on this area. This outcome may be attributed to the implementation of the General Data Protection Regulation in Europe and the increased focus on privacy and data protection matters at the master's degree level. Other popular research domains such as Identity management, secure architectures, and network security, receive many counts due to the number of institutions working on them since this is a focus of general-purpose cybersecurity research activities across institutions.

Thirty-nine institutions covered all 14 cybersecurity categories, according to respondents' research domains. 191 institutions covered at least 10 of the 14 cybersecurity categories, however, post-quantum cryptography is poorly researched. Less than 1/6 of the surveyed research institutions address relevant domains such as quantum and post-quantum cryptography, trusted computing, and cybercrime, as noted on the lower end of the ranking. Nearly 400 companies selected "Cybersecurity education," as most survey respondents were from higher education institutions. European research institutions prioritise "privacy and data protection" subdomains. The European General Data Protection Regulation may explain this result. Since many universities conduct general-purpose cybersecurity research on identity management, safe architectures, and network security, these fields receive many counts.

As noted in the lower ranking, less than 1/6 of the examined research institutes address crucial domains like quantum and post-quantum encryption, trustworthy computing, and cybercrime. Results need further analysis. Europe has many horizontal research groups, which help cover multiple study topics across the continent. The subdomains show that most research institutes focus on a limited portion of each top-level cybersecurity domain's study spectrum. Table 26 depicts the summary of the common knowledge areas offered in EU academic programmes.

Table 26: Summary of Knowledge Areas from EU Academic Programmes



S/N	Knowledge Area
1	Data Security: <ul style="list-style-type: none"> • Cryptography • Digital Forensics • Data Integrity and Authentication • Access Control • Secure Communication Protocols • Cryptanalysis • Data Privacy • Information Storage Security
2	Network Security <ul style="list-style-type: none"> • Fundamental Principles • Design • Implementation • Analysis And Testing • Deployment And Maintenance • Documentation • Ethics
3	Component Security <ul style="list-style-type: none"> • Component Design • Component Procurement • Component Testing • Component Reverse Engineering
4	Connection Security <ul style="list-style-type: none"> • Physical Media • Physical Interfaces and Connectors • Hardware Architecture • Distributed Systems Architecture • Network Architecture • Network Implementations • Network Services • Network Defence
5	System Security <ul style="list-style-type: none"> • System Thinking • System Management • System Access • System Control • System Retirement • System Testing, • Common System Architectures



6	Human Security <ul style="list-style-type: none">• Identity Management• Social Engineering• Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms• Awareness And Understanding• Social and Behavioural Privacy• Personal Data Privacy and Security• Usable Security and Privacy
7	Organisational Security <ul style="list-style-type: none">• Risk Management• Security Governance and Policy• Systems Administration• Cybersecurity Planning• Business Continuity (Including Disaster Recovery and Incident Management)• Security Programme Management• Personnel Security• Security Operations
8	Operate And Maintain <ul style="list-style-type: none">• Customer Service and Technical Support
9	Societal Security <ul style="list-style-type: none">• Cybercrime• Cyber Law• Cyber Policy• Privacy

4.2.5 Mapping of Market Demand Skills with Knowledge Areas in Mandatory HEIs Courses

In order to assess the spread of knowledge areas identified from the market survey, we mapped them against knowledge areas provided via HEIs cybersecurity courses that are made compulsory for students.

It is reasonable to think that when courses or modules are made compulsory, the idea is to ensure the development of mandatory skills. However, we observed that 80% of HEIs offer 40% or less of the knowledge areas and skills from the market. To better visualise the spread, see Table 27.

For the colour coding: green => high response rate (33%), yellow => medium response rate next 33%, and red => low response rate last 34% in each sector.

Table 27: Mapping of Market Skills with HEI Skills for Mandatory Cybersecurity Courses



Knowledge Units/Skills	Percent Covered in HEI (Mandatory only)	Health	Energy	Maritime	ICT	Other
Cryptography	75%-79%					
Secure Communication Protocols	65%-69%	Red	Green		ddd	Green
Network Defence	50%-54%	Yellow	Red	Green	Green	Green
Data Integrity and Authentication	45%-50%	Red	Green			Green
Network Architecture	45%-50%	Red	Yellow	Green	Yellow	Green
System Control	45%-50%				Green	
Access Control	40%-45%	Yellow	Green		Green	Yellow
System Access	40%-45%	Yellow	Red		Green	
Risk Management	40%-45%	Red	Red	Red	Yellow	Yellow
Data Privacy	35%-39%		Green			Yellow
Fundamental Principles	35%-39%				Yellow	
Network Implementations	35%-39%	Red		Yellow	Green	Green
Digital Forensics	30%-35%		Red	Red	Yellow	Red
Cryptanalysis	30%-35%					



Design	30%-35%	Green			Yellow	Red
Implementation	30%-35%				Yellow	Red
Distributed Systems Architecture	30%-35%	Red	Yellow	Green	Green	Yellow
Network Services	30%-35%	Red	Yellow	Green	Green	Green
Common System Architectures	30%-35%		Red		Yellow	Red
Security Governance and Policy	30%-35%				Yellow	
Cyber Law	30%-35%					Yellow
Analysis and Testing	25%-29%	Red		Red	Green	Green
System Thinking	25%-29%					
Information Storage Security	20%-25%	Red	Green		Green	Yellow
Ethics	20%-25%				Yellow	
Identity Management	20%-25%				Red	
Social Engineering	20%-25%	Yellow			Green	
Personal Data Privacy and Security	20%-25%					
Analytical Tools	20%-25%	Yellow			Green	Green
Systems Administration	20%-25%				Yellow	Yellow
Privacy	20%-25%				Yellow	Yellow



Cybersecurity Practical Skills Gaps in Europe: Analyses and Prioritisation

Component Design	15%-19%					Red	
Physical Media	15%-19%	Yellow			Yellow	Yellow	Yellow
Hardware Architecture	15%-19%	Yellow			Yellow		Yellow
System Management	15%-19%					Yellow	Yellow
Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms	15%-19%	Yellow	Red			Yellow	Green
Awareness and understanding	15%-19%	Yellow	Red	Red			Green
Usable Security and Privacy	15%-19%						Green
Cybersecurity Planning	15%-19%	Green			Green	Yellow	
Business Continuity	15%-19%	Green				Red	
Cyber Ethics	15%-19%					Yellow	Yellow
Component Reverse Engineering	10%-14%						
System Testing	10%-14%				Green		Green
Social and Behavioural Privacy	10%-14%	Yellow					Green
Security Program Management	10%-14%	Green				Red	Red



Personnel Security	10%-14%	Yellow			Red	Red
Security Operations	10%-14%	Red		Green	Red	Red
Cybercrime	10%-14%				Yellow	Yellow
Cyber Policy	10%-14%				Yellow	Yellow
Deployment and Maintenance	5%-9%				Yellow	
Documentation	5%-9%				Yellow	
Component Testing	5%-9%					
Physical Interfaces and Connectors	5%-9%	Yellow		Red		Yellow
Customer Service and Technical Support	5%-9%					
Component Procurement	<5%					
system retirement	<5%		Red			

It is important to note that not all skills reported in the market analysis survey were mapped. Non-shaded areas also indicate that mappings could not be made with the affected skill because it was not reported. These are limitations that may affect the overall outcome of the analysis.

The mapping also highlights the need for cybersecurity knowledge areas and skills from the market survey that should be incorporated into HEIs courses. The HEI academic offering appears not to make provision for certain skills, including AI and soft/professional skills indicated in the survey. However, we note that some skills-set may be provided in the HEI's KSA database, which are unavailable to the authors. The analysis further indicated that mandatory courses which ensure skills training are not delivered across HEIs. For instance, 61 (of 105) responses are found within 30% of HEIs. Though this outcome is not discouraging, what is more, worrisome is the fact that 80 responses (of 120) are found in less than 30% of the HEI offerings. HEIs should be seen to achieve close to 100% adoption of mandatory components, especially components that address the findings from the market analysis.



4.3 Cybersecurity Practical Skills Gaps in Europe: Main findings

This section presents cybersecurity practical knowledge areas and skills gaps in Europe. These knowledge areas and skill gaps resulted from the comparative analysis of the market survey and the cybersecurity academic programmes offered in EU HEIs.

4.3.1 Progress Beyond the State of The Art (BSOTA)

Previously in Chapter 2, we reviewed existing cybersecurity workforce development frameworks and EU Member States' initiatives. These frameworks enabled us to identify cybersecurity competencies required of professionals. Moving on from existing frameworks and initiatives and given that cybersecurity is relatively new and fast evolving, the reviewed frameworks did not fully answer the question of what cybersecurity competencies are currently needed in the European labour market hence the need to undertake a market skills demand survey. Chapter 3 discussed the outcome of the market analysis. Furthermore, the early part of this chapter provided a combined list of the market-demand-driven cybersecurity knowledge areas and skills. Based on established criteria, these knowledge areas and skills were further prioritised and grouped according to the sectors: health, energy, maritime, ICT and other. Given that the supply-side analysis of practical cybersecurity skills offered by EU academic programmes is not sector-specific, the identification of knowledge and skills gaps will not also be sector-specific but a common list combining them as cybersecurity practical skills gap in Europe.

Further, a study by the European Union Agency for Cybersecurity (ENISA) found that there is a shortage of 2.2 million cybersecurity professionals in Europe. This gap is expected to grow to 3.5 million by 2022. The study also found that the most in-demand cybersecurity skills in Europe are in the areas of threat intelligence, incident response, and risk management. The ENISA study correlate with CyberSecPro where many areas are overlapping with CyberSecPro market demand survey results.

Many studies including CyberSecPro study confirms, there is still a significant cybersecurity skills gap in Europe, but there has been some progress in addressing the issue. The EU has taken several steps to address the gap, including funding research projects and launching the Cybersecurity Skills Academy. However, more needs to be done to close the gap and ensure that Europe is adequately prepared to meet the growing cybersecurity challenges. The CyberSecPro project and its impact will further consolidate the cybersecurity skills shortage in Europe.

4.3.2 European Cybersecurity Framework Workforce Roles: Sectoral Specific Mapping

The review of cybersecurity academic programmes offered by HEIs, and private professional training providers appear to indicate that ENISA's cybersecurity skills framework job roles are reflected in various academic programmes. To demonstrate the trend in the adoption of these work roles in each CyberSecPro target sector, we mapped ECSF and academic offerings with the data obtained from the market analysis survey. The outcome of this mapping is presented in Table 28. Following the earlier established market demand prioritisation criteria, critical knowledge areas are indicated in green, In-demand priority areas are indicated in yellow, and low-priority areas are indicated in red. The ICT and other sectors appear to dominate the chart based on the number of survey responses and knowledge areas indicated. A similar trend is observed with the practical skills (see right-hand-side of Table 28).



For the practical skills in-demand indicated in yellow, skills with high priority are indicated in green, while skills with low priority are indicated in red.

Table 28: Mapping ECSF Job Role with Academic Offerings in Each Sector

ENISA Roles Framework	#EUAcademic offerings	Knowledge Areas						Practical Skills					
		Health	Energy	Maritime	ICT	Other	Total	Health	Energy	Maritime	ICT	Other	
Digital Forensics Investigator	13	Red	Red	Red	Red	Red	Red	Red	Red	Red	Red	Red	Red
Chief Information Security Officer	13	Green	Yellow	Green	Green	Red	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Green
Cyber Legal Policy & Compliance Officer	10	Green	Red	Yellow	Yellow	Green	Yellow	Red	Red	Red	Red	Red	Red
Cybersecurity Architect	8	Red	Green	Yellow	Green	Yellow	Green	Red	Red	Red	Red	Red	Red
Cybersecurity Risk Manager	8	Green	Green	Red	Yellow	Green	Yellow	Yellow	Yellow	Green	Yellow	Yellow	Green
Penetration Tester	7	Red	Red	Yellow	Yellow	Red	Red	Green	Green	Green	Green	Green	Green
Cyber Incident Responder	4	Yellow	Yellow	Green	Red	Green	Yellow	Yellow	Red	Yellow	Red	Red	Red
Cybersecurity Implementer	3	Yellow	Yellow	Red	Yellow	Red	Yellow	Yellow	Red	Green	Yellow	Yellow	Yellow
Cybersecurity Researcher	2	Red	Red	Red	Green	Yellow	Green	Red	Red	Red	Red	Red	Red



Cyber Threat Intelligent Specialist	2	Red	Yellow	Red	Yellow	Yellow	Red	Black	Red	Red	Green	Red	Red
Cybersecurity Educator	2	Green	Red	Yellow	Green	Yellow	Green	Black	Yellow	Red	Red	Red	Red
Cybersecurity Auditor	0	Red	Red	Yellow	Red	Red	Red	Black	Yellow	Red	Red	Red	Red

4.3.3 Final Outcomes and Result: Cybersecurity Practical Skills Gap in Europe

Identifying cybersecurity skills gaps from the cybersecurity market demand and supply analysis involved creating a matrix between demand and supply data sources. To facilitate the identification of knowledge areas and skill gaps, we first consolidated and relied on cybersecurity academic programmes data provided by the ENISA CyberHEAD platform, JRC Atlas, CONCORDIA and CyberSec4Europe (see previous section).

This consolidation effort resulted in a combined list (supply side) of cybersecurity knowledge areas and skills offered by EU academic programmes (see Table 26). This merged list of knowledge areas and skills reflects terminologies and interpretations of EU academic programmes, thus presenting a challenge of arriving at a uniform, comprehensive list of skills gaps. The prioritisation level of each skill gap inherits the prioritisation level of the same skill gap in the ECSF-normalised combined list of cybersecurity knowledge areas and skills (see Table 21). **It is important to stress again that that the prioritisation in Table 21 is based on survey responses across all sectors considered in this report.**

Table 29: Comprehension of Cybersecurity Practical Skills Names

S/N	Essential Cybersecurity Practical Skills: Market Demand	Merged Knowledge Areas and Skills (included in the main category of column 2)	Comprehended New Name
1	Ethical Hacking and Penetration Testing	Penetration testing/Ethical hacking/Defensive Practitioners/Offensive Security/Vulnerability assessment/Vulnerability analysis	Same
2	Cybersecurity Tools and Technologies	Cybersecurity tools/Cybersecurity technologies	Same
3	Cybersecurity Management Systems: CS Management and	Cybersecurity management/ Cybersecurity management	Cybersecurity Management Systems (CSMS)



	Processes	systems/Cybersecurity processes/ Cybersecurity Principles	
4	Cybersecurity Principles	NA	Cybersecurity Management Systems (CSMS)
5	Cybersecurity Threat Management: Threat Awareness, Threat Knowledge, Threat Assessment, Threat Intelligence, Threat Detection	Cybersecurity threat awareness/Threat intelligence/Threat detection/Threat understanding/Threat knowledge	Cybersecurity Threat Management / Security Operations Center (SOC)
6	Risk Assessment and Risk Management	Risk assessment/Risk management	Cybersecurity Risk Management
7	Emerging Technologies	NA	Cybersecurity for Artificial Intelligence and Machine Learning
8	Cybersecurity Regulations and Compliance	Cybersecurity regulations/Cybersecurity compliance/Compliance	Cybersecurity Policy, Process and Compliance
9	Cybersecurity Education and Training	Education and training/Education and training skills	Same
10	Incident Response	Appear as both knowledge and skill	Cybersecurity Threat Management / Security Operations Center (SOC)
11	Communications and Network Security: Network Security Controls	Communication and network security/Network security control	Network and Communications Security
12	Cybersecurity Forensics	Appeared as both knowledge and skill	Same
13	Cloud Security	Appeared as both knowledge and skill	Same
14	Cybersecurity for Artificial Intelligence and Machine Learning	Cybersecurity for artificial intelligence and machine learning/Artificial intelligence	Same
15	Legal and Auditing Training	Legal training/Auditing	Cybersecurity Law and Auditing
16	Cybersecurity Architecture	Appeared as both knowledge and skill	Same
17	Cybersecurity Engineering	Cybersecurity engineer / DevSecOps / DevOps	Same



18	Network and System Administration	NA	Systems Security / Systems Administrations and Security
19	Technical Skills	NA	Cybersecurity Tools and Technologies
20	Software Security	NA	Programming Skills and Software Security
21	Analysis and Critical Thinking (soft/professional skills)	NA	Soft and Transferable Skills
22	Programming Skills	NA	Programming Skills and Software Security
23	Communication and Teamwork (soft/professional skills)	NA	Soft and Transferable Skills
24	Operating Systems	NA	Systems Security / Systems Administrations and Security
25	Software Design Skills	NA	Programming Skills and Software Security
26	Data Protection and Security	NA	Data Protection and Security

Note: Since the CyberSecPro is following ECSF, DevSecOps merged into cybersecurity engineering. Vulnerability assessment merged into Pen testing. Read may find that certain gaps are missing. However, some of the relevant knowledge areas and skills (as per analysis work) must be comprehend and merged with other to give more clear view. Some gaps on the supply side leave room for too much interpretation.

We then mapped knowledge areas and skills in Table 26 with knowledge areas and skills (demand side) provided in Table 21 to find the gaps. It should be noted that CyberHEAD's educational offering is described in terms of ENISA's job roles without explicit mention of actual knowledge areas and skills which is a limitation. On the other hand, CyberSec4Europe explicitly provided several knowledge areas hence the need to read it together with CyberHEAD, Atlas, and CONCORDIA.

From CyberHEAD's job role viewpoint, the matrix between demand and supply revealed that only a handful of academic programmes offered forensics (13), cybersecurity leadership (appeared as cybersecurity management in the survey) (13), risk management (8), cybersecurity architecture (8), and cyber legal (10) as part of their knowledge areas.

From the point of view of the market-elicited knowledge areas and skills, the outcome of the mapping implies that most academic programmes are not offering the sufficient workforce supply and knowledge areas demanded by the market. For example, “In 2022, the shortage of cybersecurity professionals in the EU ranged between 260,000 and 500,000, while the EU’s cybersecurity workforce needs were estimated at 883,000 professionals. In addition, women only amounted to 20% of cybersecurity graduates and to 19% of information and communications technology specialists [152].”



Table 30: Cybersecurity Practical Skills Gaps in Europe

S/N	Cybersecurity Hands-on Practical Skills	No. of Responses	Priority Level
1	Cybersecurity Tools and Technologies	205	High demand
2	Cybersecurity Management Systems (CSMS)	192	High demand
3	Ethical Hacking and Penetration Testing	192	High demand
4	Cybersecurity Threat Management / Security Operations Center (SOC)	127	High demand
5	Cybersecurity for Artificial Intelligence and Machine Learning	97	High demand
6	Cybersecurity Risk Management	76	High demand
7	Cybersecurity Policy, Process and Compliance	58	High demand
8	Cybersecurity Education and Training	49	High demand
9	Network and Communications Security	48	High demand
10	Programming Skills and Software Security	42	High demand
11	Cybersecurity Forensics	38	In demand
12	Cloud Security	37	In demand
13	Soft and Transferable Skills	37	In demand
14	Systems Security / Systems Administrations and Security	33	In demand
15	Cybersecurity Law and Auditing	27	In demand
16	Cybersecurity Architecture	24	In demand
17	Cybersecurity Engineering	22	In demand
18	Data Protection and Security	9	In demand

The mapping also revealed that several knowledge areas and skills provided in the educational programmes do not appear in the survey knowledge and skills list. Based on the matrix, we identified knowledge areas and skills that require more focus by EU academic programmes to help with new cybersecurity workforce and existing workforce's skilling, upskilling and reskilling. **The Cybersecurity Practical Skills Gaps in Europe list (Image-20) is compiled from the research outcomes and beyond the current state of the art (BSOTA) including analyses of market demand survey, cybersecurity framework analyses, analysis of the European cybersecurity projects and their research outcomes.**



Source: Authors - CyberSecPro-D2.1 Report: Cybersecurity Skills Gaps in Europea

Figure 20: CyberSecPro: Cybersecurity Skills Gaps in Europe

4.3.4 Summary

In this chapter, CyberSecPro study have analysed, and prioritised different cybersecurity knowledge areas and skills currently needed in the labour market. For each health, energy, and maritime sector, we established the criteria that enabled us to categorise the needs level of each identified cybersecurity knowledge area and skill. The results obtained from the market analysis survey did not indicate that certain cybersecurity knowledge areas and skills are unique to any sector. They rather indicate their applicability and need across all sectors. On the supply side, we also analysed and presented cybersecurity knowledge areas and practical skills provided by EU academic programmes and private cybersecurity training programmes. The results of the cybersecurity skills demand and supply analyses enabled us to create a matrix for the identification of cybersecurity skills gaps in Europe. Based on the demand and supply comparison, 18 cybersecurity knowledge and skills gaps were identified. As we have earlier stated, the gaps we have identified are not sector specific because the data relied upon on the supply-side was also not sector-driven unlike the demand-side data. Overall, the Cybersecurity Practical Skills Gaps in Europe table present the more pressing and urgent practical skills required in Europe.



5 Recommendation and Pointers for CyberSecPro Programme Specification

This report presented a comprehensive analysis of the practical cybersecurity skills gap in Europe and the market demand analysis for these skills. The study utilised a combination of practical and applied research, including extant research, existing cybersecurity education and training initiatives, methods published in the literature, and quantitative and qualitative data analysis. As a result, over 25 essential practical knowledge areas and practical skills in demand were identified. This included incident response, threat intelligence, and penetration testing. Special focus was given to cybersecurity in the health, energy, and maritime sectors.

The analysis of European cybersecurity higher education programmes confirms that the demand for skilled professionals outpaces supply. This report provides research insights and potential solutions to address the skills gap. In particular, state-of-the-art market needs analysis was conducted and results from the market survey were consolidated with an analysis of academic programme offerings in the EU. This effort provides a holistic overview into the cybersecurity professional skills demand and supply in the European cybersecurity workforce.

As a result, the report has distinguished many key details for improvement of cybersecurity education, including increasing investment in cybersecurity education and training, transforming higher education programmes to address market demand, and promoting collaboration between academia, industry, and government in developing cybersecurity talent. **The study emphasises the need for consolidation of cybersecurity workforce capacity-building efforts and effective dissemination of the European Cybersecurity Skills Framework (ECSF). Overall, this report highlights the need for a coordinated effort to bridge the practical skills gap and meet market demand for skilled cybersecurity professionals in Europe.**

5.1 Cybersecurity Practical Skills: Market Demand and Recommendation

The CyberSecPro market analysis survey investigated the job roles in demand and knowledge areas and hands-on skills required in the cybersecurity industry. The survey focused on the health, energy, and maritime sectors. Additionally, it also provided useful information on ICT field and other. The CyberSecPro study provides useful insights and critical recommendation as explained below:

(1) Considering the market demand and importance of workforce role based European Cybersecurity Skills Framework: First, the market demand survey investigated the cybersecurity job roles in demand. The European Cybersecurity Skills Framework (ECSF) was used as a template for the different job roles. Based on the survey, all ECSF job roles are in-demand to some extent: Chief Information Security Officers, Educators, Cybersecurity Architects, Researchers, Cyber Legal, Policy and Compliance Officers, and Incident Responders were chosen in over 30% of the survey responses. In addition, Auditors and Digital Forensics Investigators were also common choices, with 20% and 15% of the respondents indicating a need for these roles. Thus, the ECSF is a relevant framework for cybersecurity job roles. More work on the effective use of the framework is recommended. As the survey results show significant market relevance, ECSF could be used as a framework to design cybersecurity training that aligns well with industry-relevant job roles.

- **The first and foremost, CyberSecPro programme specification can leverage the benefits of workforce role based ECSF framework. The most useful step could be piloting CyberSecPro training programme that consolidates the implementation of ECSF.**

(2) Focus on the hands-on and practical cybersecurity skills: Next, the market analysis survey focused on the knowledge areas and hands-on skills. The survey aimed to identify the specific hands-on skills and competencies required in the cybersecurity industry, focusing on the health, energy, and maritime sectors. The results provided insights for developing a skilled and competent workforce



capable of effectively mitigating cyber threats. Critical focus areas for the health, energy, and maritime sectors can be recommended as follows.

In the health sector, the survey showed that in-demand knowledge areas and skills included cybersecurity principles, management, and tools, with ethical hacking, cybersecurity education and training, and communications and network security also mentioned as critical areas.

The survey results in the energy sector revealed that cybersecurity management and tools were the most popular knowledge areas, followed by ethical hacking, cybersecurity principles, cybersecurity technologies, and offensive security. Respondents valued a mix of managerial and technical topics, reflecting the need for a targeted professional cybersecurity programme to secure and protect critical infrastructure against current and emerging attacks.

As for the maritime sector, results indicated that cybersecurity management systems were the most important area for respondents, followed by cybersecurity tools and processes. Cyber threat awareness and cybersecurity engineering were also mentioned as important areas, while vulnerability assessment and cybersecurity regulations received less but still considerable emphasis.

- **The survey results also revealed that the specific hands-on and practical skills required in focused areas including health, energy, maritime, ICT and other.**

(3) Skilling, Upskilling and Reskilling- transformation of the European cybersecurity higher education programmes: After the important focus areas for development in cybersecurity were distinguished, the survey results were cross-examined with European cybersecurity education and training offerings. The first notable result of this analysis is the definition of the most critical and high-demand skills and knowledge areas for cybersecurity training programmes. For example, Cybersecurity Tools and Technologies and Ethical Hacking and Penetration Testing were considered the most important content for contemporary education and training programmes. Additionally, the following skills were deemed in high demand for educators: Cybersecurity Threat Management (Threat Awareness, Threat Knowledge, Threat Assessment, Threat Intelligence, Threat Detection), Management Skills, Cybersecurity Principles, Risk Assessment and Risk Management, Emerging Technologies, Cybersecurity Regulations and Compliance, and Incident Response.

In terms of comparing the market needs with existing cybersecurity curricula, it was determined that certain cybersecurity skills are scarcely offered in academic programmes. These skills included forensics, cybersecurity leadership, risk management, cybersecurity architecture, and cyber legal skills. Thus, there is a market need to develop programmes that include these skills and knowledge. In addition to these essential yet uncommon competencies in educational programmes, a comprehensive list of 27 knowledge and skills gaps where academic programmes could be improved.

- **The result confirms the urgent need of transforming the higher education and cybersecurity training programme towards more addressing the market needed cybersecurity working-life skills rather than academic rigor with high emphases on practical training including skilling, upskilling, and reskilling programmes.**

(4) Industry-academia cooperation: The cybersecurity landscape is constantly evolving, and the skills and knowledge required to succeed in this field are constantly changing. This makes it difficult for traditional academic institutions to keep up with the latest trends and developments. Industry-academia cooperation can help to bridge this gap by providing learners with access to the latest industry resources and expertise.

There are many benefits to industry-academia cooperation in cybersecurity education. For learners, this type of cooperation can provide them with a comprehensive understanding of the cybersecurity landscape and the skills and knowledge required to succeed. Industry partners can offer learners field-specific resources and tools, as well as real-world experience and insights from industry experts. This



can help learners to gain a competitive edge in the job market. Another aspect of the cooperation leads to current know-how and industry demanded skilling, upskilling and reskilling of the educators, professors, teachers, and trainer. There is a very effective way for this purpose using “Train the Trainer” approach. For industry partners, cooperation with academia can help them to identify and develop the next generation of cybersecurity professionals. This can help them to stay ahead of the curve in terms of cybersecurity threats and to ensure that they have the talent they need to protect their businesses.

Collaboration between industry and academia can also lead to new research and development projects that can help to advance the cybersecurity field and keep pace with evolving threats. This type of collaboration can be mutually beneficial for both parties, as it can help to ensure that the latest research is being translated into practical solutions that can be used to protect businesses and individuals.

Overall, industry-academia cooperation is a valuable tool for both learners and industry partners. By working together, they can help to ensure that cybersecurity education is more relevant, practical, and effective in preparing learners for careers in the field.

Here are some specific examples of how industry-academia cooperation can be beneficial for cybersecurity education:

- **Industry partners can provide learners with access to real-world cybersecurity challenges.** This can help learners to develop the skills and knowledge they need to solve real-world problems.
- **Industry partners can provide learners with access to industry experts.** This can help learners to get their questions answered and to learn from the best in the field.
- **Leveraging the benefits of “Train the Trainer” model** for the skilling, upskilling and reskilling of the educators, professors, teachers, and trainer. The European HEIs educators can sharpen their practical skills by working with cybersecurity industrial professionals and experts.
- **Industry partners can provide learners with internship and job opportunities.** This can help learners to gain valuable experience and to make connections in the industry.
- **Industry partners can provide funding for cybersecurity research and education.** This can help to ensure that the latest research is being translated into practical solutions that can be used to protect businesses and individuals.

There are many ways that industry and academia can collaborate to improve cybersecurity education. By working together, they can help to ensure that the next generation of cybersecurity professionals has the skills and knowledge they need to protect our world from cyber threats.

5.2 Cybersecurity Higher Education Programmes and Recommendations

Finally, other recommendations regarding pedagogy for cybersecurity education have also been established in extant literature. Pedagogic approaches cover how cybersecurity should be taught more than what the programmes should include (content). So far, this report has extensively covered the content, so it is apt to also consider how that content should be delivered.

The field of cybersecurity as part of computing education is abundant with research and documented best practices for the most effective and efficient teaching and learning (see, for example, the studies in [127]–[149]). **Takeaways from existing cybersecurity education recommendations are as follows.**

(1) Utilising awareness programmes: Security awareness programs promote responsible behaviour online, create a security culture within an organisation or community, and reduce the risk of successful cyber-attacks. They also help organisations comply with legal and regulatory requirements. Cybersecurity education can help students become responsible digital citizens, who are aware of their online behaviour and how it can impact others. Organising training early, starting with the K-12 level,



can help create a generation of informed and responsible technology users who are equipped with the necessary cyber skills.

(2) Games and gameful approaches: Games or gamification can be leveraged in cybersecurity education as an effective tool for engaging and educating learners. Games can simulate real-world scenarios and provide an environment for learners to practise and develop their skills. They can also help learners understand the consequences of their actions and reinforce good cybersecurity practices. Educators can leverage games to create engaging, immersive learning experiences that simulate real-world scenarios. Serious games can be designed to teach technical skills, such as network configuration and vulnerability assessment, as well as non-technical skills, such as decision-making and risk management. Gamification, which involves adding game elements, such as points, badges, and leader boards, to non-game contexts, can also increase engagement and motivation in cybersecurity training environments.

(3) Virtualisation and simulation: Virtual laboratories allow learners to gain hands-on experience in a controlled environment. Virtual laboratories can simulate real-world scenarios and enable learners to practise their skills and techniques without the risk of causing damage or compromising security. Learners can experiment with security configurations, run penetration testing exercises, and practice incident response protocols. Digital twins can be used for simulation and testing purposes. They can be used to simulate real-world cybersecurity scenarios, allowing learners to practise their skills and develop their knowledge in a real-like environment. Digital twins can also be used to simulate attacks, allowing learners to test and refine their defensive strategies. They can also be used to teach the behaviour of complex systems and networks, providing learners with a deeper understanding of how they function and how to secure them.

(4) Focus on industrial systems: Cyber threats to critical infrastructure, such as power plants, water treatment facilities, and transportation systems, can have significant and even life-threatening consequences. Many of these systems rely on code written decades ago, which may not have been designed with security in mind. As industrial control systems become more interconnected, they become more vulnerable to cyberattacks that can disrupt operations or cause physical harm. Developing secure code in industrial environments requires a deep understanding of both cybersecurity and industrial control systems, and training in this area can help prevent catastrophic incidents. Additionally, as more companies adopt Industry 4.0 technologies, such as the Industrial Internet of Things (IIoT), blockchain secure code development [79] will become even more critical for protecting these systems from cyber threats.

(5) Crystallise how theory is applied in practice: While theoretical concepts are essential in understanding the cybersecurity fundamentals, learners need to understand how these concepts are applied in the real world to develop practical skills and knowledge. By clarifying the practical applications of theoretical concepts, learners can better understand how cybersecurity works in the real world and develop the skills and knowledge needed to apply these concepts in practice. This approach can also help learners develop the ability to adapt to new and evolving threats. Overall, cybersecurity education that emphasises the practical applications of theoretical concepts can help learners develop a comprehensive understanding of cybersecurity and be better equipped to protect against real-world threats. By focusing on these areas in cybersecurity education, learners can develop the skills and knowledge needed to implement effective security measures and protect against real-world threats. Additionally, these areas are in high demand in the cybersecurity job market, making them valuable skills for learners to possess.

(6) Situated learning: Situated learning improves learning outcomes by engaging learners in a relatable simulation world. Educators can create virtual scenarios (for example, in a game environment) to situate



the student in a specific context, providing faster learning and better outcomes. Educators can leverage news stories and recent events to contextualise and reinforce cybersecurity concepts and skills. News stories and recent events provide real-world examples of cybersecurity threats and attacks, highlighting the importance of cybersecurity and its impact on individuals, organisations, and society. By incorporating news stories and recent events into cybersecurity education, learners can develop a deeper understanding of cybersecurity's relevance and practical applications.

(7) Inclusion and diversity: Inclusion promotes diversity of thought and enables the development of more inclusive and effective cybersecurity solutions. Neurodiverse individuals and people with disabilities can bring unique skills and perspectives to the field, such as detecting patterns and anomalies that others may miss. By creating a more inclusive environment that accommodates the needs of neurodiverse individuals and people with disabilities, we can foster a more diverse and effective cybersecurity workforce. It is important to address the inclusion of often underrepresented groups, such as women and people of colour, in cybersecurity education because diversity fosters innovation, creativity, and problem-solving. The field of cybersecurity faces a significant skills gap, and a lack of diversity can contribute to this problem. Cybersecurity threats affect everyone regardless of gender, race, or ethnicity, so it is crucial that cybersecurity professionals represent and understand the diverse perspectives and experiences of the people they are protecting.

5.3 Conclusion of the CyberSecPro D2.1 report

This CyberSecPro deliverable D2.1 report provides valuable insights into the current state of cybersecurity skills gaps in Europe. This deliverable captures the cybersecurity skill sets needed by the markets, the practical skills offered in the EU academic programmes and the gaps between demand and supply of practical skills. Special attention will be given to the three industrial sectors: health, energy and maritime. The deliverable reflects the outcomes of tasks T2.1 and T2.2. The cybersecurity skills gap is a complex problem with no easy solutions. However, there are number of things that can be done to address the gap, and CyberSecPro project work is embarking on the development journey to consolidate the European Cybersecurity Workforce with increasing the hands-on practical skills development efforts. Indeed, the cybersecurity skills gap is a serious problem, but it is one that can be solved. By taking some of the steps to address the gap within CyberSecPro project and beyond, we can make Europe a safer and more secure place.



References

- [1] D. McHenry et al., “Cyber security skills in the UK labour market 2021,” 2021.
- [2] “CYBERSECURITY WORKFORCE STUDY.” Accessed: Apr. 01, 2023. [Online]. Available: <https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx>
- [3] “State of Cybersecurity 2021,” ISACA. <https://www.isaca.org/go/state-of-cybersecurity-2021> (accessed Apr. 01, 2023).
- [4] D. Burley, M. Bishop, S. Kaza, D. S. Gibson, E. Hawthorne, and S. Buck, “ACM Joint Task Force on Cybersecurity Education,” in Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education, 2017, pp. 683–684.
- [5] ENISA, “Ad-Hoc Working Group on the European Cybersecurity Skills Framework,” 2022 2020. https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework/adhoc_wg_calls_2020 (accessed Mar. 27, 2023).
- [6] “This is what the future of cybersecurity will look like | World Economic Forum.” <https://www.weforum.org/agenda/2017/08/the-us-is-upping-its-game-against-cyber-attacks-but-the-security-industry-faces-a-huge-challenge> (accessed Apr. 01, 2023).
- [7] “Cybersecurity Education Initiatives in the EU Member States,” ENISA. <https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states> (accessed Apr. 02, 2023).
- [8] “Cybersecurity Skills Development in the EU,” ENISA. <https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union> (accessed Apr. 02, 2023).
- [9] “European Cybersecurity Skills Framework (ECSF),” ENISA. <https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework> (accessed Apr. 02, 2023).
- [10] “European Cybersecurity Skills Framework Role Profiles,” ENISA. <https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles> (accessed Apr. 02, 2023).
- [11] ENISA, “European Cybersecurity Skills Framework (ECSF) - User Manual,” Sep. 2022. Accessed: Mar. 27, 2023. [Online]. Available: <https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf>
- [12] “D2.6 ECHO CYBERSKILLS FRAMEWORK.” Accessed: Apr. 05, 2023. [Online]. Available: https://echonetwork.eu/wp-content/uploads/2021/03/ECHO_D2.6_Cyberskills-Framework.pdf



- [13] “SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf.” Accessed: Mar. 23, 2023. [Online]. Available: <https://www.sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf>
- [14] “R3.3.1. Cybersecurity Skills Framework.” Accessed: Mar. 23, 2023. [Online]. Available: https://rewireproject.eu/wp-content/uploads/2022/11/R3.3.1.-Cybersecurity-Skills-Framework_FINAL.pdf
- [15] “Curricula Recommendations.” <https://www.acm.org/education/curricula-recommendations> (accessed Apr. 05, 2023).
- [16] “Computing Curricula 1991: Report of the ACM/IEEE-CS Joint Curriculum Task Force,” Association for Computing Machinery, New York, NY, USA, 1991.
- [17] “The Joint Task Force for Computing Curricula 2001,” Dec. 2001. Accessed: Nov. 04, 2023. [Online]. Available: <https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2001.pdf>
- [18] “The Joint Task Force for Computing Curricula 2005,” Sep. 2005. Accessed: Nov. 04, 2023. [Online]. Available: <https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2005-march06final.pdf>
- [19] 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.
- [20] “Cybersecurity Curricular Guidance for Associate-Degree Programs.” ACM CCECC. Accessed: Nov. 04, 2023. [Online]. Available: <https://ccecc.acm.org/files/publications/Cyber2yr2020.pdf>
- [21] Infocomm Media Devevelopment Authority, “Skills Framework For ICT.” <https://www.imda.gov.sg/cwp/assets/imtalent/skills-framework-for-ict/index.html> (accessed Mar. 28, 2023).
- [22] “ASD Cyber Skills Framework | Cyber.gov.au.” <https://www.cyber.gov.au/acsc/view-all-content/publications/asd-cyber-skills-framework> (accessed Mar. 29, 2023).
- [23] “The global skills and competency framework for a digital world,” SFIA. <https://sfia-online.org/en> (accessed Mar. 29, 2023).
- [24] “Canadian Cybersecurity Skills Framework | TECHNATION.” <https://technationcanada.ca/en/future-workforce-development/cybersecurity/cybersecurity-skills-framework/> (accessed Mar. 23, 2023).
- [25] “The Canadian cyber security skills framework.” Canadian Centre for Cyber Security, Jan. 2023.
- [26] “The Saudi Cybersecurity Workforce Framework.” Accessed: Mar. 22, 2023. [Online]. Available: https://nca.gov.sa/scywf_en.pdf
- [27] “Cyber Security Skills | Data Security Council of India.” <https://www.dsci.in/content/skill-building/cyber-security-skills> (accessed Mar. 20, 2023).
- [28] ENISA, “European Union Agency for Cybersecurity,” 2023 2005. <https://www.enisa.europa.eu> (accessed Mar. 27, 2023).



References

- [29] ENISA, “ECSF (European Cybersecurity Skills Framework),” Sep. 2022. Accessed: Mar. 27, 2023. [Online]. Available: <https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles>
- [30] ENISA, “User Manual, European Cybersecurity Skills Framework (ECSF),” Sep. 2022. Accessed: Mar. 27, 2023. [Online]. Available: <https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf>
- [31] “European e-Competence Framework.” <https://ecfexplorer.itprofessionalism.org/> (accessed Apr. 07, 2023).
- [32] I. Nai Fovino, R. Neisse, and J. Hernandez Ramos, “A proposal for a European cybersecurity taxonomy,” European Commission, Joint Research Centre, Nov. 2019. Accessed: Aug. 04, 2023. [Online]. Available: <https://data.europa.eu/doi/10.2760/106002>
- [33] “National Cyber Security Centre - NCSC.GOV.UK.” <https://www.ncsc.gov.uk/> (accessed Apr. 06, 2023).
- [34] Awais Rashid et al., The Cyber Security Body of Knowledge. 2019. [Online]. Available: <https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf>
- [35] “CyBOK – The Cyber Security Body of Knowledge.” <https://www.cybok.org/> (accessed Apr. 06, 2023).
- [36] “European Qualifications Framework (EQF).” <https://esco.ec.europa.eu/en/about-esco/escopedia/escopedia/european-qualifications-framework-efq> (accessed Apr. 07, 2023).
- [37] ESCO, “Home.” <https://esco.ec.europa.eu/en> (accessed Apr. 03, 2023).
- [38] E. W. Ecsso, “ECSO Gaps in European Cyber Education and Professional Training”.
- [39] “Skills & Human Factors - ECSO.” <https://ecs-org.eu/activities/education-training-awareness-and-cyber-ranges/> (accessed Apr. 05, 2023).
- [40] P. Rathod, N. Olesen, et al., “European Cybersecurity Education & Professional Training: Minimum Reference Curriculum.” European Cyber Security Organisation, ECSO-Brussels, 2021.
- [41] S. EMK, “Project summary – ECHO Network.” <https://echonetwork.eu/project-summary/> (accessed Apr. 05, 2023).
- [42] “CONCORDIA,” CONCORDIA. <https://www.concordia-h2020.eu/home-2/objectives/> (accessed Apr. 07, 2023).
- [43] CONCORDIA, “Deliverable D1.1: 1st Year Report on Designing and Developing an European Secure, Resilient and Trusted Ecosystem (ESRTE).” Accessed: Jul. 04, 2023. [Online]. Available: [https://www.concordia-h2020.eu/wp-content/uploads/2020/05/D1.1-1stYearReportonDesigningandDevelopinganEuropeanSecureResilientandTrustedEcosystem\(ESRTE\).pdf](https://www.concordia-h2020.eu/wp-content/uploads/2020/05/D1.1-1stYearReportonDesigningandDevelopinganEuropeanSecureResilientandTrustedEcosystem(ESRTE).pdf)



- [44] CONCORDIA, “Deliverable D1.2: 2nd Year Report on Designing and Developing an European Secure, Resilient and Trusted Ecosystem (ESRTE).” Accessed: Jul. 04, 2023. [Online]. Available: https://www.concordia-h2020.eu/wp-content/uploads/2021/03/Deliverables_D1.2.pdf
- [45] CONCORDIA, “Deliverable D1.3: 3rd Year Report on Designing and Developing an European Secure, Resilient and Trusted Ecosystem (ESRTE).” Accessed: Jul. 04, 2023. [Online]. Available: <https://www.concordia-h2020.eu/wp-content/uploads/2022/07/CONCORDIA-D1.3.pdf>
- [46] CONCORDIA, “Deliverable D4.5: First report on Cybersecurity Workforce Diversity.” Accessed: Jul. 04, 2023. [Online]. Available: https://www.concordia-h2020.eu/wp-content/uploads/2021/03/Deliverables_D4.5.pdf
- [47] CONCORDIA, “Deliverable D4.4: Cybersecurity Roadmap for Europe.” Accessed: Jul. 04, 2023. [Online]. Available: https://www.concordia-h2020.eu/wp-content/uploads/2021/10/CONCORDIA_Roadmap.pdf
- [48] CONCORDIA, “Deliverable D3.6: DDoS Clearing House Platform.” Accessed: Jul. 04, 2023. [Online]. Available: https://www.concordia-h2020.eu/wp-content/uploads/2023/03/PREPRINT-D3-6_DDoS_Clearing_House_Cookbook.pdf
- [49] CONCORDIA, “Deliverable D5.2: 1st year report on exploitation, dissemination, certification and standardization.” Accessed: Jul. 04, 2023. [Online]. Available: <https://www.concordia-h2020.eu/wp-content/uploads/2020/05/D5.2-1stYearReportOnExploitationDisseminationCertificationandStandardization.pdf>
- [50] “D6.1 Case Pilot for WP2 Governance.” Accessed: Apr. 06, 2023. [Online]. Available: <https://cybersec4europe.eu/wp-content/uploads/2020/06/D6.1-Case-Pilot-for-WP2-Governance-V4-.pdf>
- [51] “D6.2 Education and Training Review.” Accessed: Apr. 06, 2023. [Online]. Available: <https://cybersec4europe.eu/wp-content/uploads/2020/02/D6.2-Education-and-Training-Review-V1.2-Submitted.pdf>
- [52] Karinsalo Anni, Halunen Kimmo, “Design of Education and Professional Framework.” CyberSec4Europe, Mar. 25, 2021. [Online]. Available: https://cybersec4europe.eu/wp-content/uploads/2021/06/D6_3_Design-of-Education-and-Professional-Frame-work_Final.pdf
- [53] “D6.4 Flagship 1.” Accessed: Apr. 06, 2023. [Online]. Available: <https://cybersec4europe.eu/wp-content/uploads/2021/06/D6.4-Flagship-1-v1.1-submitted.pdf>
- [54] “D6.5 Flagship 2.” Accessed: Apr. 06, 2023. [Online]. Available: https://cybersec4europe.eu/wp-content/uploads/2022/04/D6.5-Flagship-2-v1.3_submitted.pdf
- [55] J. Hajný, M. Sikora, A. V. Grammatopoulos, and F. Di Franco, “Adding European Cybersecurity Skills Framework into Curricula Designer,” presented at the Proceedings of the 17th International Conference on Availability, Reliability and Security, 2022, pp. 1–6.
- [56] J. Hajný, S. Ricci, E. Piesarskas, and M. Sikora, “Cybersecurity Curricula Designer,” presented at the Proceedings of the 16th International Conference on Availability, Reliability and Security, 2021, pp. 1–7.



References

- [57] “Österreichische Strategie für Cybersicherheit - Bundeskanzleramt Österreich.” <https://www.bundeskanzleramt.gv.at/themen/cybersicherheit/oesterreichische-strategie-fuer-cybersicherheit.html> (accessed Apr. 18, 2023).
- [58] C. Efthymiou, “Στρατηγική κυβερνοασφάλειας της Κυπριακής Δημοκρατίας,” 2020.
- [59] “Home - Cyber Safety.” <https://cybersafety.cy/> (accessed Apr. 11, 2023).
- [60] “CYPRUS PEDAGOGICAL INSTITUTE.” <https://www.pi.ac.cy/pi/index.php?lang=en> (accessed Apr. 11, 2023).
- [61] “Home - Internet Safety.” <https://internetsafety.pi.ac.cy/> (accessed Apr. 11, 2023).
- [62] “Digital Security Authority - News.” <https://dsa.cy/en/category/news> (accessed Apr. 11, 2023).
- [63] “Digital Security Authority - Approval for co-financing of the N4CY project for development of the National Coordination Center (NCCC-CY).” <https://dsa.cy/en/category/news/approval-for-co-financing-of-the-n4cy-project-for-development-of-the-national-coordination-center-nccc-cy> (accessed Apr. 11, 2023).
- [64] “ΔΓΚΑΘΙΡΤΗ ΚΑΙ ΛΔΙΣΟΤΡΓΙΑ ΤΩ ΣΗΜΑΣΟ ΔΠΑΓΓΔΛΜΑΣΙΚΩΝ ΠΡΟΝΣΩΝ ΣΗΝ ΚΤΠΠΟ, 2007-201.” Accessed: Apr. 11, 2023. [Online]. Available: https://www.anad.org.cy/wps/wcm/connect/hrda/3668bba6-2980-424b-a0b1-d84f46d19e17/Diktia.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=ROOTWORKSPACE.E.Z18_HHHAH9O0NGE980A7L632QJ0000-3668bba6-2980-424b-a0b1-d84f46d19e17-nzRp5KQ
- [65] “Homepage.” <https://www.cyqf.gov.cy/index.php/el/> (accessed Apr. 13, 2023).
- [66] “NSCS_2021_2025_ENG.pdf.” Accessed: Apr. 07, 2023. [Online]. Available: https://nukib.cz/download/publications_en/strategy_action_plan/NSCS_2021_2025_ENG.pdf
- [67] “NSKB-AP_ENG.pdf.” Accessed: Apr. 07, 2023. [Online]. Available: https://nukib.cz/download/publications_en/strategy_action_plan/NSKB-AP_ENG.pdf
- [68] “CyQUAL | National Qualifications Framework in Cybersecurity.” <https://platform.cyqual.cz/en> (accessed Apr. 04, 2023).
- [69] “Finland’s Cyber Security Strategy 2019 – Turvallisuuskomitea,” Oct. 03, 2019. <https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019/> (accessed Apr. 05, 2023).
- [70] “Finland boost education in cybersecurity skills in the EU | Digital Skills and Jobs Platform.” <https://digital-skills-jobs.europa.eu/en/latest/news/finnish-researchers-develop-curriculum-make-cybersecurity-civic-skill-eu> (accessed Apr. 05, 2023).
- [71] “Instructions and guides,” NCSC-FI. <https://www.kyberturvallisuuskampus.fi/en/ncsc-news/instructions-and-guides> (accessed Apr. 05, 2023).
- [72] S. Vuorinen, “Kyberturvallisuus Ohje sosiaali- ja terveydenhuollon toimijoille,” Jun. 17, 2019. <https://julkaisut.valtioneuvosto.fi/handle/10024/161683> (accessed Apr. 18, 2023).



- [73] M. Lehto, J. Pöyhönen, and M. Lehto, Kyberturvallisuus sosiaali- ja terveydenhuollossa. 2019. Accessed: Apr. 18, 2023. [Online]. Available: <https://jyx.jyu.fi/handle/123456789/63325>
- [74] “Terveydenhuolto – JYVSECTEC.” <https://jyvsectec.fi/fin/terveydenhuolto/> (accessed Apr. 18, 2023).
- [75] K. Sulasalmi, “Kyberhäiriöiden hallinta – Käsikirja terveydenhuollon toimijoille – JYVSECTEC.” <https://jyvsectec.fi/2021/01/kyberhairioiden-hallinta-kasikirja-terveydenhuollon-toimijoille/> (accessed Apr. 18, 2023).
- [76] P. Ahonen, J. Seppälä, and J. Pärssinen, KYBER-ENE Energia-alan kyberturvaaminen 1-2. FI: VTT Technical Research Centre of Finland, 2019. Accessed: Apr. 17, 2023. [Online]. Available: <https://doi.org/10.32040/2242-122X.2019.T353>
- [77] “Information security auditing tool for authorities – Katakri,” Ministry for Foreign Affairs. <https://um.fi/information-security-auditing-tool-for-authorities-katakri> (accessed Apr. 17, 2023).
- [78] “Instructions for organising cyber exercises”. “Kyberharjoitusskenaariot2020.pdf.” Accessed: Apr. 17, 2023. [Online]. Available: <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kyberharjoitusskenaariot2020.pdf>
- [79] P. Rathod, “Blockchain for business: Secure implementation.” Florida: International Council of E-Commerce Consultants., 2023. Available: <https://www.eccouncil.org/cybersecurity-exchange/whitepaper/blockchain-for-business-secure-implementation/>
- [80] “Kybermittari - Cybermeter,” NCSC-FI, May 11, 2021. <https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter> (accessed Apr. 17, 2023).
- [81] “Cyber Weather,” NCSC-FI, Mar. 17, 2023. <https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/cyber-weather> (accessed Apr. 17, 2023).
- [82] “Team Whack - everything is hackable | Yle Areena.” <https://areena.yle.fi/1-4664681> (accessed Apr. 17, 2023).
- [83] “SecNumedu, Labeling of higher education courses in cybersecurity,” ANSSI. <https://www.ssi.gouv.fr/en/cybersecurity-in-france/formations/secnumedu-labeling-of-higher-education-courses-in-cybersecurity/> (accessed Apr. 17, 2023).
- [84] “SecNumedu-FC, labellisation de formations continues en cybersécurité,” ANSSI. <https://www.ssi.gouv.fr/entreprise/formations/secnumedu-fc-labellisation-de-formations-continues-en-cybersecurite/> (accessed Apr. 17, 2023).
- [85] “CyberEdu,” ANSSI. <https://www.ssi.gouv.fr/entreprise/formations/cyberedu/> (accessed Apr. 17, 2023).
- [86] “Titre ESSI,” ANSSI. <https://www.ssi.gouv.fr/entreprise/formations/titre-essi/> (accessed Apr. 17, 2023).
- [87] “Observatoire des métiers de la cybersécurité,” ANSSI. <https://www.ssi.gouv.fr/entreprise/formations/observatoire-des-metiers-de-la-cybersecurite/> (accessed Apr. 17, 2023).



References

- [88] “Cybersecurity Handbook”.
- [89] “CYBERHEAD - Cybersecurity Higher Education Database,” ENISA.
<https://www.enisa.europa.eu/topics/education/cyberhead> (accessed Apr. 17, 2023).
- [90] geetha, “Εθνική Διακλαδική Άσκηση Κυβερνοάμυνας «ΠΑΝΟΠΤΗΣ 2021»,” Γενικό Επιτελείο Εθνικής Άμυνας - Επίσημη Ιστοσελίδα, Oct. 22, 2021. <https://geetha.mil.gr/ethniki-diakladiki-askisi-kyvernoamynas-panoptis-2021/> (accessed Apr. 17, 2023).
- [91] “Top 11 Best SIEM Tools in 2023 (Real-Time Incident Response & Security).”
<https://www.softwaretestinghelp.com/siem-tools/> (accessed Apr. 20, 2023).
- [92] “Security Information and Event Management (SIEM) Reviews 2023 | Gartner Peer Insights.”
<https://www.gartner.com/reviews/market/security-information-event-management> (accessed Apr. 20, 2023).
- [93] “25 Best Microsoft Active Directory Alternatives.” <https://www.winosbite.com/best-microsoft-active-directory-alternatives/> (accessed Apr. 20, 2023).
- [94] “modernciso.com | Fresh Thinking for the Modern CISO.” <https://modernciso.com/> (accessed Apr. 20, 2023).
- [95] “national-cyber-security-strategy-for-norway.pdf.” Accessed: Apr. 17, 2023. [Online]. Available: <https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf>
- [96] “BOE-A-2019-6347 Order PCI/487/2019, of April 26, which publishes the 2019 National Cybersecurity Strategy, approved by the National Security Council.”
<https://www.boe.es/buscar/doc.php?id=BOE-A-2019-6347> (accessed Apr. 20, 2023).
- [97] “National Cybersecurity Strategy.” DSN, 2019. Accessed: Apr. 20, 2023. [Online]. Available: <https://www.dsn.gob.es/en/file/2989/download?token=EuVy2INr>
- [98] “Análisis y diagnóstico del talento de ciberseguridad en España,” INCIBE, Mar. 10, 2022.
<https://www.incibe.es/diagnostico-talento-ciberseguridad> (accessed Apr. 20, 2023).
- [99] “Instituciones que imparten formación en ciberseguridad en España.” Accessed: Apr. 20, 2023. [Online]. Available: <https://www.incibe.es/sites/default/files/paginas/talento/catalogos-formacion/catalogo-instituciones.pdf>
- [100] “Formación reglada en ciberseguridad en España. Másteres, especializaciones, grados y especializaciones en Formación Profesional”.
- [101] “Análisis y diagnóstico del talento de ciberseguridad en España.” NCIBE, 2022. Accessed: Apr. 20, 2023. [Online]. Available: https://files.incibe.es/incibe/talento/INCIBE_InformeCompleto_DIAG.pdf



- [102] “Observatorio Nacional de Tecnología y Sociedad”, Vicepresidencia Primera del Gobierno y el Ministerio de Asuntos Económicos y Transformación Digital,” 2023. <https://www.ontsi.es/es> (accessed Apr. 20, 2023).
- [103] “BOE-A-2001-24515 Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.” <https://www.boe.es/eli/es/lo/2001/12/21/6> (accessed Apr. 20, 2023).
- [104] “National Agency for Quality Assessment and Accreditation of Spain,” Aneca Web. <https://www.aneca.es/aneca> (accessed Apr. 20, 2023).
- [105] “Evaluation of new degrees,” Aneca Web. <https://www.aneca.es/evaluacion-nuevos-titulos> (accessed Apr. 20, 2023).
- [106] “MINISTERIO DE UNIVERSIDADES Ministerio de Universidades, ‘Real Decreto 822/2021, de 28 de septiembre, por el que se establece la organización de las enseñanzas universitarias y del procedimiento de aseguramiento de su calidad.’” Accessed: Apr. 20, 2023. [Online]. Available: <https://www.aneca.es/documents/20123/66848/RD+822-2021.pdf/9b426b2e-c455-cd46-ee7d-fa1d218a60d4?t=1661765207185>
- [107] “Monitoring of the implementation,” Aneca Web. <https://www.aneca.es/seguimiento-implantacion-titulo> (accessed Apr. 20, 2023).
- [108] “Accreditation renewal,” Aneca Web. <https://www.aneca.es/renovacion-acreditacion> (accessed Apr. 20, 2023).
- [109] “BOE-A-2021-1192 Royal Decree 43/2021, of January 26, which develops Royal Decree-Law 12/2018, of September 7, on network security and information systems.” https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-1192 (accessed Apr. 20, 2023).
- [110] “BOE-A-2022-7191 Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.” <https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191> (accessed Apr. 20, 2023).
- [111] “REGLAMENTO (UE) 2016/ 679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO - de 27 de abril de 2016 - relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/ 46/ CE (Reglamento general de protección de datos)”.
- [112] “BOE-A-2011-7630 Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.” <https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630> (accessed Apr. 20, 2023).
- [113] “Casos de uso de los perfiles de ciberseguridad de ENISA | INCIBE.” <https://www.incibe.es/talento-hacker/publicaciones/european-cybersecurity-skills/casos> (accessed Apr. 20, 2023).
- [114] “Perfiles de ciberseguridad de ENISA | INCIBE.” <https://www.incibe.es/talento-hacker/publicaciones/european-cybersecurity-skills> (accessed Apr. 20, 2023).
- [115] “National Cybersecurity Forum - Home.” <https://foronacionalciberseguridad.es/> (accessed Apr. 20, 2023).



References

- [116] “Cómo puedes convertirte en un profesional de la ciberseguridad?” Accessed: Apr. 20, 2023. [Online]. Available: https://www.incibe.es/sites/default/files/paginas/talento/orientacion/infografia_consejos.pdf
- [117] “Orientación Profesional en Ciberseguridad | INCIBE.” <https://www.incibe.es/orientacion-profesional-ciberseguridad> (accessed Apr. 20, 2023).
- [118] “Countering Cyber Threats.” <https://www.ccn-cert.cni.es/en/> (accessed Apr. 20, 2023).
- [119] “Mission and objectives.” <https://www.ccn-cert.cni.es/en/about-us/mission-and-objectives.html> (accessed Apr. 20, 2023).
- [120] “Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.” Accessed: Apr. 20, 2023. [Online]. Available: https://www.ccn.cni.es/images/stories/normas/pdf/ley_11_2002_reguladora_cni.pdf
- [121] “Guides.” <https://www.ccn-cert.cni.es/en/guides.html> (accessed Apr. 20, 2023).
- [122] “ANGELS - Home.” <https://angeles.ccn-cert.cni.es/index.php/es/> (accessed Apr. 20, 2023).
- [123] “Marco de Referencia de la Competencia Digital Docente.” Accessed: Apr. 20, 2023. [Online]. Available: https://aprende.intef.es/sites/default/files/2023-02/MRCDD_V06B_GTTA.pdf
- [124] C. Redecker, “European Framework for the Digital Competence of Educators: DigCompEdu.” Publications Office of the European Union, Luxembourg, 2017. [Online]. Available: doi:10.2760/178382
- [125] “Cyber Security Skills Roadmap | SANS Institute: Cyber Security Skills Roadmap.” <https://www.sans.org/cyber-security-skills-roadmap/> (accessed Apr. 05, 2023).
- [126] (ISC) 2, “Strategies for Building and Growing Strong Cybersecurity Teams,” 2019.
- [127] H. Aldawood and G. Skinner, “Educating and raising awareness on cyber security social engineering: A literature review,” in 2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE), IEEE, 2018, pp. 62–68.
- [128] F. Alotaibi, S. Furnell, I. Stengel, and M. Papadaki, “A review of using gaming technology for cyber-security awareness,” *Int. J. Inf. Secur. Res.(IJISR)*, vol. 6, no. 2, pp. 660–666, 2016.
- [129] M. Canepa, F. Ballini, D. Dalaklis, and S. Vakili, “Assessing the effectiveness of cybersecurity training and raising awareness within the maritime domain,” in INTED2021 Proceedings, IATED, 2021, pp. 3489–3499.
- [130] W. Chen, Y. He, X. Tian, and W. He, “Exploring Cybersecurity Education at the K-12 Level,” in SITE Interactive Conference, Association for the Advancement of Computing in Education (AACE), 2021, pp. 108–114.
- [131] N. Chowdhury and V. Gkioulos, “Cyber security training for critical infrastructure protection: A literature review,” *Computer Science Review*, vol. 40, p. 100361, 2021.



- [132] N. Chowdhury and V. Gkioulos, “Key competencies for critical infrastructure cyber-security: a systematic literature review,” *Information & Computer Security*, vol. 29, no. 5, pp. 697–723, 2021.
- [133] M. Coenraad, A. Pellicone, D. J. Ketelhut, M. Cukier, J. Plane, and D. Weintrop, “Experiencing cybersecurity one game at a time: A systematic review of cybersecurity digital games,” *Simulation & Gaming*, vol. 51, no. 5, pp. 586–611, 2020.
- [134] P. Rathod and P. Kämppi, "Applying LEAN Principles to Improve Introductory Cybersecurity Online Course: Findings from the Pilot Study." *SITE Interactive Conference: 73-79*, 2020
- [135] M. Gálíková, V. Švábenský, and J. Vykopal, “Toward guidelines for designing cybersecurity serious games,” in *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education*, 2021, pp. 1275–1275.
- [136] T. E. Gasiba, K. Beckers, S. Suppan, and F. Rezabek, “On the requirements for serious games geared towards software developers in the industry,” in *2019 IEEE 27th International Requirements Engineering Conference (RE)*, IEEE, 2019, pp. 286–296.
- [137] M. Hendrix, A. Al-Sherbaz, and B. Victoria, “Game based cyber security training: are serious games suitable for cyber security training?,” *International Journal of Serious Games*, vol. 3, no. 1, pp. 53–61, 2016.
- [138] S. Hu, C. Hsu, and Z. Zhou, “Security education, training, and awareness programs: Literature review,” *Journal of Computer Information Systems*, vol. 62, no. 4, pp. 752–764, 2022.
- [139] J. Jeong, J. Mihelcic, G. Oliver, and C. Rudolph, “Towards an improved understanding of human factors in cybersecurity,” in *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, IEEE, 2019, pp. 338–345.
- [140] P. Rathod, "Towards Cybersecurity Professional Workforce Development Framework—successful practices and outcomes of the European Case." *eCrimeEU-EU Symposium on Electronic Crime Research*, 2019.
- [141] M. Lamond, K. Renaud, L. Wood, and S. Prior, “SOK: young children’s cybersecurity knowledge, skills & practice: a systematic literature review,” in *Proceedings of the 2022 European Symposium on Usable Security*, 2022, pp. 14–27.
- [142] X. Mountrouidou et al., “Securing the human: a review of literature on broadening diversity in cybersecurity education,” *Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education*, pp. 157–176, 2019.
- [143] R. Roepke and U. Schroeder, “The Problem with Teaching Defence against the Dark Arts: A Review of Game-based Learning Applications and Serious Games for Cyber Security Education.,” in *Proceedings of the 11th International Conference on Computer Supported Education (CSEDU 2019)*, 2019, pp. 58–66.
- [144] P. Rathod, and T. Hamalainen, “A Novel Model for Cybersecurity Economics and Analysis.” *IEEE International Conference on Computer and Information Technology (CIT)*, August 2017. <https://doi.org/10.1109/cit.2017.65>.
- [145] R. B. Sağlam, V. Miller, and V. N. Franqueira, “A Systematic Literature Review on Cyber Security Education for Children,” *IEEE Transactions on Education*, 2023.



References

- [146] B. Siemers et al., “Modern Trends and Skill Gaps of Cyber Security in Smart Grid,” in IEEE EUROCON 2021-19th International Conference on Smart Technologies, IEEE, 2021, pp. 565–570.
- [147] P. Rathod, P. Kämppi and T. Hämäläinen, "Leveraging National Auditing Criteria to Implement Cybersecurity Safeguards for the Automotive Emergency Response Vehicles: : A case study from Finland." International journal of digital content technology and its applications, 11, no. 4: 15-26. 2017.
- [148] C. Van Slyke, G. Clary, S. Ellis, and M. Maasberg, “Employer preferences for cybersecurity skills among information systems graduates,” in Proceedings of the 2019 on Computers and People research Conference, 2019, pp. 131–134.
- [149] L. Zhang-Kennedy and S. Chiasson, “A systematic review of multimedia tools for cybersecurity awareness and education,” ACM Computing Surveys (CSUR), vol. 54, no. 1, pp. 1–39, 2021.
- [150] P. Rathod, and T. Hamalainen, "Leveraging the benefits of big data with fast data for effective and efficient cybersecurity analytics systems: A robust optimisation approach." In International Conference on Cyber Warfare and Security, pp. 411-XVII. Academic Conferences International Limited, 2020.
- [151] J. Rajamäki, P. Rathod and K.Kioskli, "Demand Analysis of the Cybersecurity Knowledge Areas and Skills for the Nurses: Preliminary Findings ." 22nd European Conference on Cyber Warfare and Security, 2023, Accepted manuscript submitted for publication.
- [152] “Cybersecurity Skills Academy: a coordinated approach to boost the EU cyber workforce”, Accessed: Apr. 20, 2023. [Online]. Available: <https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy>



Annex A: Market analysis survey

The market survey information can be found below. Images are also supplied after the texts for more clarity.

=====

Introduction: This development work focuses on the cybersecurity workforce, and hands-on market skills demand analysis. The CyberSecPro survey aims to identify the cybersecurity workforce's needs, specific hands-on skills, and the competencies required in their business activities.

Survey Outline and Instructions: The survey is divided into the following sections

Section One: Introduction

Section two: Demographic Information (about organisation & background)

Section Three: European Cybersecurity Workforce Demand (specific job and role demand)

Section Four: Current Market Demands: Cybersecurity knowledge areas

Section Five: Current Market Demands: Cybersecurity Skills

Motivation and Useful Note:

>> The survey results will be used for research and provide policy guidance to the European Commission on the EU's cybersecurity workforce capacity building.

>> The survey would take about 10-15 minutes to complete.

Participation and Consent: Respondents are encouraged to answer every question in this questionnaire for the research data to be valid and fit for purpose. Your participation in the survey is considered confidential and voluntary. All data obtained as part of this survey shall be used strictly for research purposes and will be kept private and confidential as provided for in the GDPR.

Furthermore, the outcome of the survey will be anonymised and not attributable to participants. You can withdraw from the survey at any time. If you are happy to participate in this survey and have given your consent, please proceed to the next section and complete the survey.

@CyberSecPro project has received funding from the European Commission under the Digital Europe Programme (DIGITAL) – a new EU funding programme focused on bringing digital technology to businesses, citizens, and public administrations. A part of the project aims for common and public good. The project has 28 partners from 16 EU nations, Serbia and Norway.

@Contact: If you have any open question or comment kindly contact: cspwp2@dlist.server.uni-frankfurt.de

=====>> PLEASE START THE SURVEY <<=====

Section Two: Demographic Information

Background information of the organisation

Kindly provide the following information to aggregate the data for the analysis of the country's need, organisation's size, and practitioner's information.

Note: List of EU nations and other (29 options)

2) Choose Your Organisation Type

1. Government Organisation
2. University / Training Institute / Research and Technology Organisations (RTO)
3. Small and mid-size enterprises (SMEs)
4. Large Business / Company
5. Professional Practitioners / Professional Association Cluster
6. Other

3) Choose the Staff Size of Your Organisation

1. 0-10



Annex A: Market analysis survey

2. 11-50
3. 51-200
4. 201-500
5. 501-1250
6. 1251 - more
7. Other

4) Your Professional Work Sector (For example, Maritime, Health, Energy, Digital-ICT, or Other):
Select one.

1. Maritime
2. Health
3. Energy
4. Digital-ICT
5. Other

Your professional work levels. Select one.

- Executive or board member or C-level
- Management and decision-maker
- Operational
- Technical
- Junior

Section Three - European Cybersecurity Workforce Demand (specific job and role demand)

Activity: European Cybersecurity Skills Framework (ECSF)* job roles

Survey Question: Which of the professional profiles listed in the ECSF are most needed in your organisation/ company?

Activity details: Please review the following ECSF job roles. Kindly select the most relevant job roles in your company and business. We encourage you to consider the industry and workforce-oriented roles, not academic priorities. ECSF role descriptions can be found here: <https://doi.org/10.2824/859537>

Note: (1) Besides ECSF, you can also provide additional information (free form and not mandatory) in the comment section below.

***Reference:** ECSF European Union Agency for Cybersecurity. (2022). ECSF, European cybersecurity skills framework. Publications Office. <https://doi.org/10.2824/859537>



Select the most important and needed in your company:

- Chief Information Security Officer
- Cyber Incident Responder
- Cyber Legal, Policy and Compliance Officer
- Cyber Threat Intelligence Specialist
- Cybersecurity Architect
- Cybersecurity Auditor
- Cybersecurity Educator
- Cybersecurity Implementor
- Cybersecurity Researcher
- Cybersecurity Risk Manager
- Digital Forensics Investigator
- Penetration Tester (Ethical Hacker)

Any additional information you wish to provide relevant to ECSF job roles or relevant to cybersecurity market needs (Optional) _____

Section Four - Current Market Demands: Cybersecurity Knowledge Areas

Activity: The Current Cybersecurity Knowledge Areas in Demand

Survey Question: Which cybersecurity knowledge areas are most needed in your business?

Helpful clarification: The focus is more on cybersecurity knowledge areas demanded by businesses, and not academic priorities. The following image provides initial ideas of the cybersecurity areas; however, we request you to provide independent answers based on your business or organisational needs.

List from the highest to the least priority of cybersecurity knowledge areas.

Note: There is a maximum of 10 options below. All are not mandatory; you can freely fill up as per your business needs and demand.



Annex A: Market analysis survey



Cybersecurity Principles and Management

- including human, organisational and regulatory aspects
- basic subjects offering broad cybersecurity principles and management understanding, knowledge and comprehension



Cybersecurity Tools and Technologies

- including cybersecurity methods, tools and techniques
- use of cyber ranges for training/skills development
- cross-cutting intermediate-advanced level subjects offering analysis and applications of cybersecurity skills



Cybersecurity in Emerging Digital Technologies

- including cybersecurity for the Artificial Intelligence, Machine Learning, Virtual Reality and Smart Technology
- advance level subjects offer comprehensive competences including synthesis, leadership and professional proficiency



Offensive Cybersecurity Practitioners

- including cybersecurity and threat analysis in practice (Offensive-Defensive), ethical Hacking in practice, cyber ranges & cyber drills, cybersecurity forensics, Internet of Things, Blockchain

Kindly provide cybersecurity knowledge area demand- 01

Provide cybersecurity knowledge area in demand- 02

....

Provide cybersecurity knowledge area in demand- 10

Section Five - Current Market Demands: Cybersecurity Hands-On Practical Skills

Activity: The Current Cybersecurity Practical Skills in Demand

Survey Question: Which cybersecurity practical skills are most needed in your organisation/company?

List from the highest to the least priorities: **Cybersecurity Practical Skills**

Note: There is a maximum of 10 options below. All are not mandatory, and you can also provide additional relevant information at the end.

Provide cybersecurity practical skills in demand- 1

...

Provide cybersecurity practical skills in demand- 10

Any additional information regarding cybersecurity hands-on practical skills in demand for businesses (Optional)



Thank you for participating in the survey.

We will provide more insights from this study if you have supplied your email. Thank you again and best wishes!

#CyberSecPro Team

Market Analysis Survey
CYBERSECPRO <https://cybersecpro-project.eu/>

CyberSecPro: Market Need and Demand

Introduction: This development work focuses on the cybersecurity workforce, and hands-on market skills demand analysis. The CyberSecPro survey aims to identify the cybersecurity workforce's needs, specific hands-on skills, and the competencies required in their business activities.

Survey Outline and Instructions: The survey is divided into the following sections
Section One: Introduction
Section two: Demographic Information (about organisation & background)
Section Three: European Cybersecurity Workforce Demand (specific job and role demand)
Section Four: Current Market Demands: Cybersecurity knowledge areas
Section Five: Current Market Demands: Cybersecurity Skills

Motivation and Useful Note:
>> The survey results will be used for research and provide policy guidance to the European Commission on the EU's cybersecurity workforce capacity building.
>> The survey would take about 10-15 minutes to complete.

Participation and Consent: Respondents are encouraged to answer every question in this questionnaire for the research data to be valid and fit for purpose. Your participation in the survey is considered confidential and voluntary. All data obtained as part of this survey shall be used strictly for research purposes and will be kept private and confidential as provided for in the GDPR.

Furthermore, the outcome of the survey will be anonymised and not attributable to participants. You can withdraw from the survey at any time. If you are happy to participate in this survey and have given your consent, please proceed to the next section and complete the survey.

@CyberSecPro project has received funding from the European Commission under the Digital Europe Programme (DIGITAL) – a new EU funding programme focused on bringing digital technology to businesses, citizens, and public administrations. A part of the project aims for common and public good. The project has 28 partners from 16 EU nations, Serbia and Norway.

@Contact: If you have any open question or comment kindly contact:
cspwp2@dist.server.uni-frankfurt.de

====> THANK YOU VERY MUCH FOR YOUR TIME AND EFFORT <====
====>>> PLEASE START THE SURVEY <<====>>>

paresh.rathod.laurea@gmail.com [Switch account](#)

Not shared

Next Page 1 of 5 [Clear form](#)



Annex A: Market analysis survey

Market Analysis Survey

CyberSecPro: Market Need and Demand

paresh.rathod.laurea@gmail.com [Switch account](#)

Not shared

* Indicates required question

Section Two: Demographic Information

Background information of the organisation

Kindly provide the following information to aggregate the data for the analysis of the country's need, organisation's size, and practitioner's information.

Note: List of EU nations and other (29 options)

1) Select your country *

Choose ▼

2) Choose Your Organisation Type *

Choose ▼

3) Choose the Staff Size of Your Organisation *

Choose ▼

4) Your Professional Work Sector (For example, Maritime, Health, Energy, Digital-ICT, or Other): Select one. *

Choose ▼

If other: Please provide more specific information below:

Note: This survey aims for the current market demand of CyberSecPro focus areas: Knowledge Areas, Skills and importance of European Cybersecurity Skills Framework job roles.

Your answer _____

Your professional work level. Select one.

Executive or board member or C-level

Management and decision-maker

Operational

Technical

Junior

Other: _____

6) The survey results will be used only for research purposes and to provide workforce development guidelines across the European Union. *

The survey results will be anonymised and not attributable to survey respondents. Please select **"Yes"** to consent to use your survey responses in the research or **"No"** to withhold consent.

Yes

No

7) Kindly provide an email address (if you wish): This can help us with future communications or sharing updates.

Your answer _____

Back
Next
Page 2 of 5
Clear form





CyberSecPro: Market Need and Demand

paresh.rathod.laurea@gmail.com [Switch account](#)

Not shared

* Indicates required question

Section Three - European Cybersecurity Workforce Demand (specific job and role demand)

Activity: European Cybersecurity Skills Framework (ECSF)* job roles

Survey Question: Which of the professional profiles listed in the ECSF are most needed in your organisation/ company?

Activity details: Please review the following ECSF job roles. Kindly select the most relevant job roles in your company and business. We encourage you to consider the industry and workforce-oriented roles, not academic priorities. ECSF role descriptions can be found here: <https://doi.org/10.2824/859537>

Note: (1) Besides ECSF, you can also provide additional information (free form and not mandatory) in the comment section below.

***Reference:** ECSF European Union Agency for Cybersecurity. (2022). ECSF: European cybersecurity skills framework. Publications Office. <https://doi.org/10.2824/859537>

Image: European Cybersecurity Skills Framework: job roles



Select the most important and needed in your company: *

- Chief Information Security Officer
- Cyber Incident Responder
- Cyber Legal, Policy and Compliance Officer
- Cyber Threat Intelligence Specialist
- Cybersecurity Architect
- Cybersecurity Auditor
- Cybersecurity Educator
- Cybersecurity Implementer
- Cybersecurity Researcher
- Cybersecurity Risk Manager
- Digital Forensics Investigator
- Penetration Tester (Ethical Hacker)

Any additional information you wish to provide relevant to ECSF job roles or relevant to cybersecurity market needs (Optional)

Your answer

Back Next Page 3 of 5 Clear form



Annex A: Market analysis survey

Market Analysis Survey

CyberSecPro: Market Need and Demand

paresh.rathod.laurea@gmail.com [Switch account](#)

🔒 Not shared

Section Four – Current Market Demands: Cybersecurity Knowledge Areas

Activity: The Current Cybersecurity Knowledge Areas in Demand

—

Survey Question: Which cybersecurity knowledge areas are most needed in your business?

Helpful clarification: The focus is more on cybersecurity knowledge areas demanded by businesses, and not academic priorities. The following image provides initial ideas of the cybersecurity areas, however, we request you to provide independent answers based on your business or organisational needs.

List from the highest to the least priority of cybersecurity knowledge areas.

Note: There is a maximum of 10 options below. All are not mandatory, you can freely fill up as per your business needs and demand.

Cybersecurity areas: @Image from CyberSecPro project

Cybersecurity Principles and Management

- including human, organisational and regulatory aspects
- basic subjects offering broad cybersecurity principles and management understanding, knowledge and comprehension

Cybersecurity Tools and Technologies

- including cybersecurity methods, tools and techniques
- use of cyber ranges for training, skills development
- cross-cutting, intermediate advanced level subjects offering analysis and applications of cybersecurity skills

Cybersecurity in Emerging Digital Technologies

- including cybersecurity for the Artificial Intelligence, Machine Learning, Virtual Reality and Smart Technology
- advanced-level subjects offer cross-sectional competences including synthesis, leadership and professional proficiency

Offensive Cybersecurity Practitioners

- including cybersecurity and threat analysis in practice (Offender-Defender), ethical Hacking in practice, cyber ranges & cyber drills, cybersecurity forensics, Internet of Things, Blockchain

Kindly provide cybersecurity knowledge area demand- 01

Your answer

Provide cybersecurity knowledge area in demand- 02

Your answer

Provide cybersecurity knowledge area in demand- 03

Your answer

Provide cybersecurity knowledge area in demand- 04

Your answer

Provide cybersecurity knowledge area in demand- 05

Your answer

Provide cybersecurity knowledge area in demand- 06

Your answer

Provide cybersecurity knowledge area in demand- 07

Your answer

Provide cybersecurity knowledge area in demand- 08

Your answer

Provide cybersecurity knowledge area in demand- 09

Your answer

Provide cybersecurity knowledge area in demand- 10


Your answer

Any additional information regarding cybersecurity knowledge areas in demand for businesses (optional)

Your answer

Page 4 of 5





Market Analysis Survey

CYBERSECPRO <https://cybersecpro-project.eu/>

CyberSecPro: Market Need and Demand

paresh.rathod.laurea@gmail.com [Switch account](#)

Not shared

Section Five - Current Market Demands: Cybersecurity Hands-On Practical Skills

Activity: The Current Cybersecurity Practical Skills in Demand

Survey Question: Which cybersecurity practical skills are most needed in your organisation/company?
List from the highest to the least priorities

Cybersecurity Practical Skills

Note: There is a maximum of 10 options below. All are not mandatory and you can also provide additional relevant information at the end.

Provide cybersecurity practical skills in demand- 1

Your answer

Provide cybersecurity practical skills in demand- 2

Your answer

Provide cybersecurity practical skills in demand- 3

Your answer

Provide cybersecurity practical skills in demand- 4

Your answer

Provide cybersecurity practical skills in demand- 5

Your answer

Provide cybersecurity practical skills in demand- 6

Your answer

Provide cybersecurity practical skills in demand- 7

Your answer

Provide cybersecurity practical skills in demand- 8

Your answer

Provide cybersecurity practical skills in demand- 9

Your answer

Provide cybersecurity practical skills in demand- 10

Your answer

Any additional information regarding cybersecurity hands-on practical skills in demand for businesses (Optional)

Your answer

Thank you for participating in the survey.
We will provide more insights from this study if you have supplied your email. Thank you again and best wishes!
#CyberSecPro Team

[Back](#) [Submit](#) Page 5 of 5 [Clear form](#)



Annex B: Analyses work

Annex B: Analyses work

(1) The literature collections of Analyses work (below):



(2) One of the sample folder literature collections of Analyses work (below):

