EUROPEAN CYBER SECURITY ORGANISATION

WG5 PAPER

European Cybersecurity Education and Professional Training: Minimum Reference Curriculum

SWG 5.2 I Education & Professional Training

May 2022 (version 2.0)

www.ecs-org.eu

ABOUT ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders across EU Member States, EEA / EFTA Countries and H2020 associated countries, such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

For queries in relation to this document, please use wg5_secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

Copyright Notice

TABLE OF CONTENTS

Executive Summary

Background: There is a growing need for a skilled cybersecurity workforce. Various studies across the globe from industry and academia confirm that the cybersecurity workforce demand is very high and that it is difficult to hire competent professionals. The 2021 edition of the annual Cybersecurity Workforce Study published by (ISC)² [1] states that the shortage of cybersecurity professionals is 2.72 million globally which, although having decreased from 3.12 million the year prior, is still a significant number. For this study, (ISC)² surveyed 4,753 cybersecurity professionals working with small, medium and large organisations throughout North America, Europe, Latin America (LATAM) and Asia-Pacific (APAC), and while an IT background remains the most common career pathway taken into cybersecurity (47% of participants), slightly more than half of cybersecurity professionals got their start outside of IT— 17% transitioned from unrelated career fields, 15% gained access through cybersecurity education and 15% explored cybersecurity concepts on their own. The study also shows that the number of cybersecurity professionals in Europe grew from 830,187 in 2020 to 1,086,146 in 2021 which is a positive trend but more still needs to be done to address the skills gap. Overall, outside of APAC, the study showed that the cybersecurity skills gap continues to grow and that the need for more professionals in the field will continue to grow.

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" [2] 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".

Minimum Reference Curriculum: The minimum reference curriculum is based on the overarching best practices, ECSO WG5 expert group's empirical studies, recognised framework including European Cyber Security Body of Knowledge (CyBOK), IEEE guidelines, European Joint Research Centre (JRC) & ENISA reports, and ECSO papers, among other state-of-the-art resources and working-life practices. CyBOK [3] is a total of 19 comprehensive Knowledge Areas (KAs) to inform and underpin education and professional training for the cybersecurity sector. The minimum reference curriculum also uses EU Member States' working-life recommendations, best practices and successful case studies. The minimum reference curriculum provides a unified and common understanding between different parties involved in cybersecure societies, broad understanding and common language for cybersecurity within Europe and its working-life communities. The guideline adopts an evidence-based competence framework and structure which is presented in the minimum reference curriculum. It includes the subject name, brief subject description, subject content and topics, learning outcomes, and potential job roles/career paths.

Competence Framework and Methodologies: The competence framework and pedagogical methodology is based on the European Qualification Framework (EQF) and European Credit Transfer and Accumulation System (ECTS) recommendations and requirements. The work is the outcome of 10 years of research, innovation and evidence-based best practices conducted by European scholars and professionals [4].

Target groups: This guideline is for cybersecurity learners, higher education institutes, practitioners, professional training and workforce development providers, and employers. It fills the gap between industry and academia in practice to help the skills and competence development of the cybersecurity workforce. It also consolidates relevant communities for an effective and efficient human resources capacity and capability building effort. The guideline can be easily used to tailor cybersecurity education and professional training to the needs of professional life.

Takeaway and outcome: In addition to providing guidelines to the target groups mentioned above, this document can serve as a reference and recommendation document for the EU's Cybersecurity Competence Centre, the European Commission, European cybersecurity practitioners, European Union Agency for Cybersecurity (ENISA) and other relevant EU agencies. Overall, this is a compact and effective hands-on guideline for cybersecurity education and professional training curriculum to targeted groups including academic institutes, professional training providers, employers, working-life communities, cybersecurity human resource managers and learners.

1. Introduction

Background and overview: The European Commission is increasingly including cybersecurity as a main priority in its security and digital policy documents *"The EU Security Union Strategy for 2020 to 2025 succeeding the European Agenda on Security (2015-2020), focuses on priority areas where the EU can bring value to support Member States in fostering security for all those living in Europe, notably including cybersecurity"* [5].

If we analyse the context, modern businesses and organisations can suffer significant financial and operational damage with any security breach. The ever-increasing technology-driven modern business has greater cybersecurity threats and risks. For example, many independent studies are reporting that data breaches, cyberattacks and cybercrimes are costing close to the USD 500-600 billion globally in the year 2018-2019. The recent study by Ponemon Institute [6] showed that on average annual losses to companies that suffered a successful cyber-attack globally were US $3.86 million. Secure digital systems play the most important role to empower businesses, such is the importance of cybersecurity in today's world. Cybersecurity needs urgent attention from decision makers, top managers and leaders to continue thriving in the 21st century [7].

A competent and skilled workforce plays a pivotal role in making businesses and communities thrive. The European Union Agency for Cybersecurity (ENISA) published a report on European Cybersecurity Skills Development in EU. The report and research findings clearly manifest the importance of education and professional training, "*Studying cyber security and to produce graduates with 'the right cyber security knowledge and skills'. Many of the current issues in cyber security education could be lessened by redesigning educational and training pathways that define knowledge and skills which students should possess upon graduation and after entering the labour market"* [8].

The minimum reference curriculum can play a proactive and pivotal role in providing feasible solutions for European cybersecurity workforce capacity-building through cybersecurity education and professional training programmes. The uniqueness of this minimum reference curriculum guideline is that it combines the best practices of industry and academia to meet the needs of professional life through a truly practitioner's approach. This is an ongoing effort to leverage on the cybersecurity body of knowledge (CyBOK) framework [3] along with professional certifications.

Scope of the paper: The paper includes the guidelines relative to the competence & skills development framework along with pedagogical methodologies for the higher education programme requirements (compatible with the qualifications frameworks for the European Higher Education Area) including the European Qualification Framework (EQF, learning outcomes-based framework) and European Credit Transfer and Accumulation System (ECTS, validations of learning outcomes). This paper presents high-level descriptions on this matter and provides a minimum reference curriculum covering a wide range of cybersecurity knowledge areas needed for the workforce to conduct their day-to-day activities and tasks, in addition to providing sustainable cybersecurity workforce solutions. Overall, this paper presents clear evidence-based practitioner guidelines for cybersecurity subject structures, subject descriptions and objectives, key content and topics, as well as learning outcomes. The paper is intended to be a living document to be regularly updated based on inputs from the cybersecurity community and developments in the field. Currently, ECSO WG5 foresees a new release of the Minimum Reference Curriculum every 6 months.

2. Mapping with Best Practices, Current Frameworks and Market Analysis

Best practices and state-of-the-art: This paper provides best practices and solutions for cyber-security practitioners and businesses and has been developed using various sources and market analyses of the state-of-the-art. It does not aim to reinvent the wheel but tries to fill the gaps beyond the state-of-the-art. In the following, we highlight the key frameworks, best practices and state-of-the-art that were considered while developing this paper:

2.1 European Commissions JRC Technical Report on Proposal for a European Cybersecurity Taxonomy

About JRC report: This report [9] was published in 2019 with the goal of "aligning the cybersecurity terminologies, definitions and domains into a coherent and comprehensive taxonomy to facilitate the categorisation of EU cybersecurity competencies." The proposed Cybersecurity Taxonomy envisages a three-dimensional view as depicted in Figure 1. The JRC report considers existing frameworks and state-of-the-art, including the US NICE framework, IEEE Cybersecurity curriculum and others (references in JRC report). Our paper considers those as part of the JRC recommended best practices and they are therefore not explicitly described hereafter.

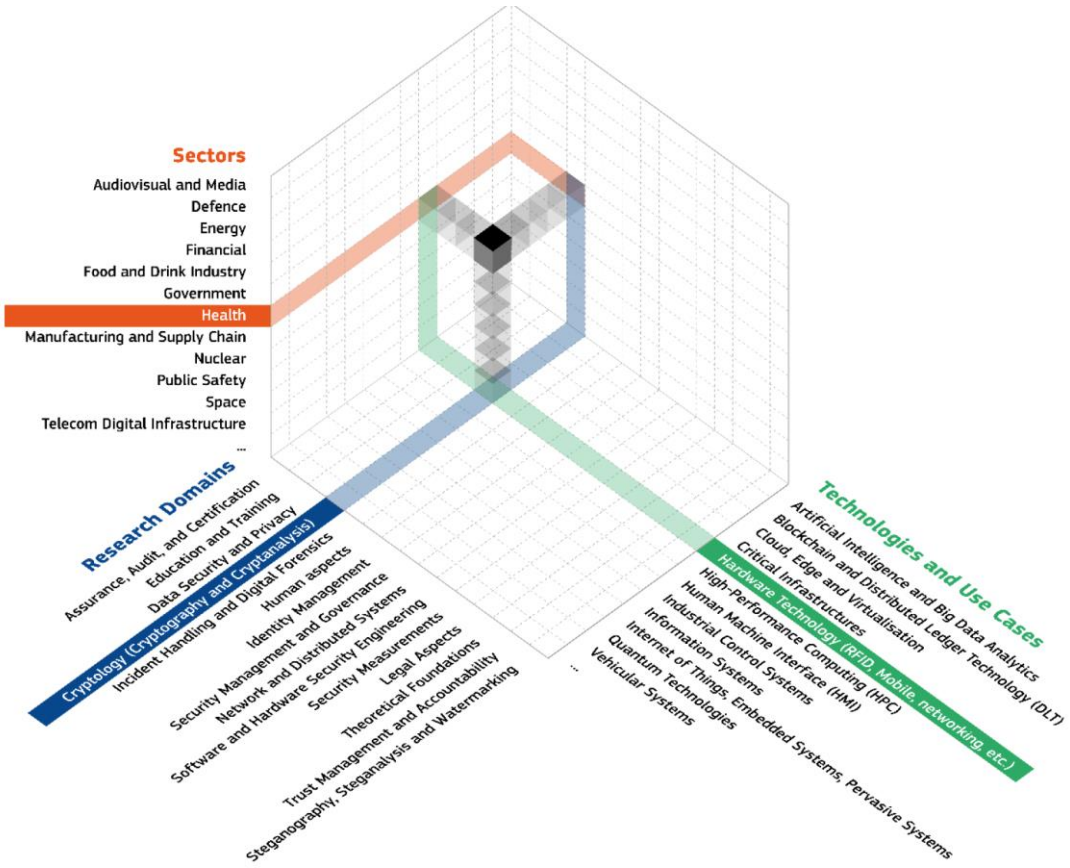

Figure 1: European Commission's JRC- Proposal of Cybersecurity Taxonomy

2.2 ENISA Reports (The European Union Agency for Cybersecurity)

About ENISA: "The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure."

This paper considers previous development work including the following reports and collaborative workshops, meetings, seminars and collective development work with ENISA.

- Cybersecurity Skills Development in the EU (2020)
- Status of privacy and NIS course curriculum in EU Member States (2015)
- Roadmap for NIS education programmes in Europe (2014)

2.3 European Cyber Security Body of Knowledge and IEEE Framework

About CyBOK: The CyBOK project [3] originated as a European research and innovation project. The CyBOK framework brings cybersecurity in line with the more established sciences by distilling knowledge from major internationally recognised experts to form a Cyber Security Body of Knowledge that will provide much-needed foundations for this emerging topic. The CyBOK development work is heavily combined with IEEE working group work. Most of the scientific based work is aligned with the IEEE Cybersecurity guidelines. Therefore, it is evident that the CyBOK model represents a similar approach and similar outcomes as IEEE's work.

"The Cyber Security Body of Knowledge (CyBOK) aims to codify the foundational and generally recognised knowledge on cyber security. In the same fashion as SWEBOK, CyBOK is meant to be a guide to the body of knowledge; the knowledge that it codifies already exists in literature such as textbooks, academic research articles, technical reports, white papers, and standards. Our focus is, therefore, on mapping established knowledge and not fully replicating everything that has ever been written on the subject. Educational programmes ranging from secondary and undergraduate education to postgraduate and continuing professional development programmes can then be developed on the basis of CyBOK. There are 19 Knowledge Areas (KAs) of the CyBOK into a coherent overall framework (https://www.cybok.org)."

Scope: A comprehensive total of 19 Knowledge Areas (KAs) known as Cyber Security Body of Knowledge (CyBOK) to inform and underpin education and professional training for the cybersecurity sector (see Figure 2). This paper has adopted the 19 knowledge areas within its curriculum, in addition to other recommended knowledge areas.

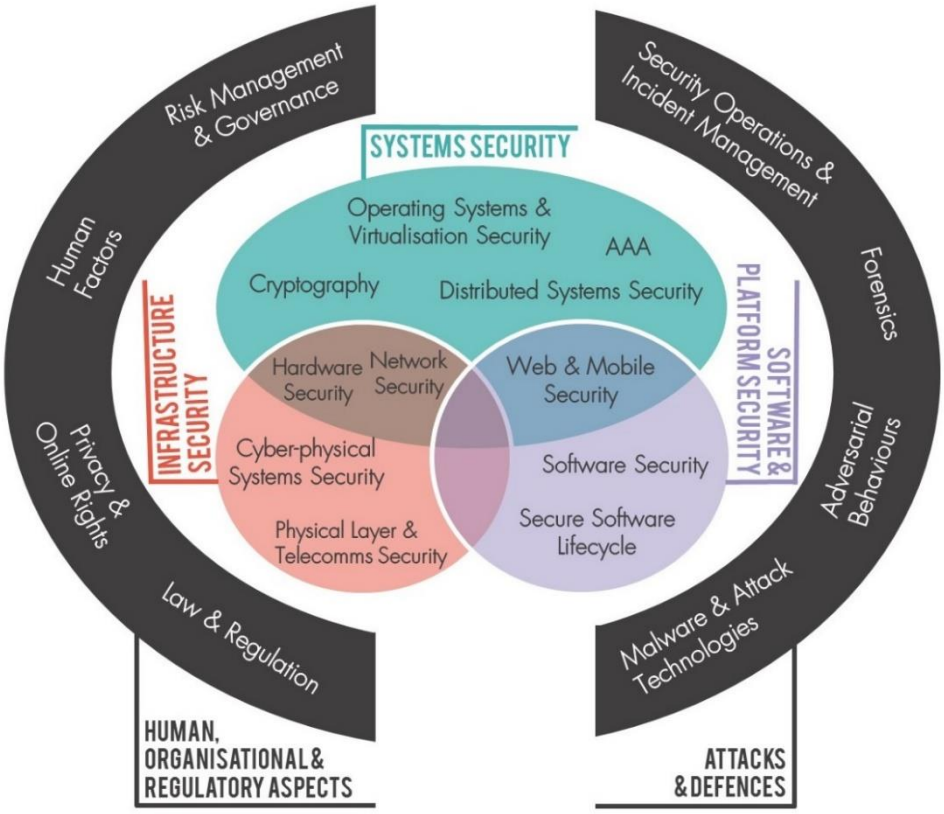

Figure 2: European Cyber Security Body of Knowledge (CyBOK aligned with IEEE work)

2.4 ECSO Reports, Practitioners Input and Empirical Market Analysis

About ECSO WG5: ECSO's working group (WG) 5 on "education, training, awareness, and cyber ranges" aims to contribute towards a cybersecurity capability and capacity-building effort for a cyber resilient next generation (NextGen) digital Europe, through increased education, professional training, skills development, as well as actions on awareness-raising, expertise-building and gender inclusiveness. The paper considers previous development work including the following reports, workshops, meetings, seminars, EU cybersecurity expert insights, and qualitative data through WG communication channels.

- Position paper: Gaps in European Cyber Education and Professional Training (2018)
- Cybersecurity Awareness Trainings: A Practical Guide (2018)
- EHR4CYBER - Information and Cyber Security Professional Certification (2018; update 2020)
- Building the Future European Cybersecurity Awareness Campaigns: Outcome paper from ECSO workshop (2019)
- ECSO, CYBERSEC4EUROPE, ECHO, SPARTA, CONCORDIA - Report: Results of Simulation-based Competence Development Survey (2019)

- Understanding Cyber Ranges: from Hype to Reality (2020)

The collective development work also leverages the benefits of scholarly work from this paper's editor and the following table depicts the knowledge base analysis of the literature studies.

Table 1: Scholarly Work and Knowledge Base

Database Source	**Gathering information: Keywords for Title, Abstract and Full Text for state-of-the-art (SOTA)**	**Re-representing Identifying the most relevant work beyond state-of-the-art (BSOTA)**	**Developing insight Implementing a sense-making loop and extracting new insights**
ACM	219	24	
Emerald Insight	85	9	
Google Scholar	98	11	
IEEE Xplore	175	12	**68**
Science Direct	95	8	
Wiley Digital Database	35	4	
Total:	**707**	**68**	**68**

The basis for this paper includes European perspectives and market needs, especially as ECSO has over 270 members, out of which around 150 members and almost 300 individual experts are part of WG5 (as of May 2022). Additionally, ECSO WG5 development work includes a specialised European Human Resources Network for Cyber (EHR4CYBER) that addresses European market analysis and practitioners' current needs. The WG member s represent the industrial and market needs. The empirical data and information reflect the collective development work including experts' views, comments, suggestions, observations, and presentations at seminars, workshops and general WG5 discussions.

3. Curricula Development Methodologies and Process

The methodology for this curriculum development adopted a combined approach considering pedagogical philosophy, thought models, and scientific approaches as described below:

3.1 Practitioners' analytical reasoning and applied science method

The curriculum development used the practitioners' analytical reasoning and the applied science approach. It includes (1) desktop research and scientific literature reviews, (2) qualitative and quantitative data collections from experts, practitioners and working-life collaborators, (3) analysis 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 3) along the timeline of the last 5 years with a pilot implementation [10].

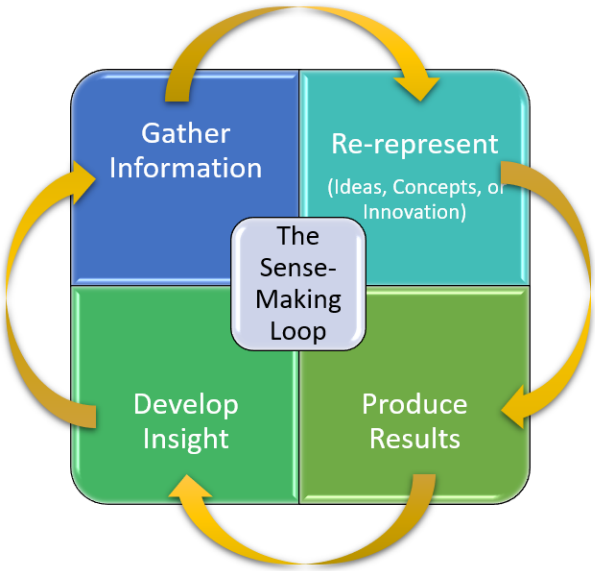

Figure 3: Analytical Reasoning & Applied Science Method[1]

3.2 Pedagogical philosophy

The minimum reference curriculum is prepared adopting the underlying European competency and learning outcome-based pedagogical philosophy from Bloom's taxonomy [11]. Our qualitative data

[1] Source of the image: Scholarly work of the ECSO WG5 Co-chair Paresh Rathod (Laurea-Finland)

suggested that practitioners find it difficult to comprehend Bloom's taxonomy using a cybersecurity competency framework. This led to an effort to simplify Bloom's taxonomy pyramid.

Competence is an umbrella term that includes ability, knowledge, and behaviour to perform an act. Further, the Oxford Dictionary of Sport Science and Medicine defines competence as "*a basic psychological need to be able to succeed at optimally challenging tasks and achieve a desired outcome."*

The practice model starts from the bottom fact-finding layer and builds towards the top layer of creating new solutions.

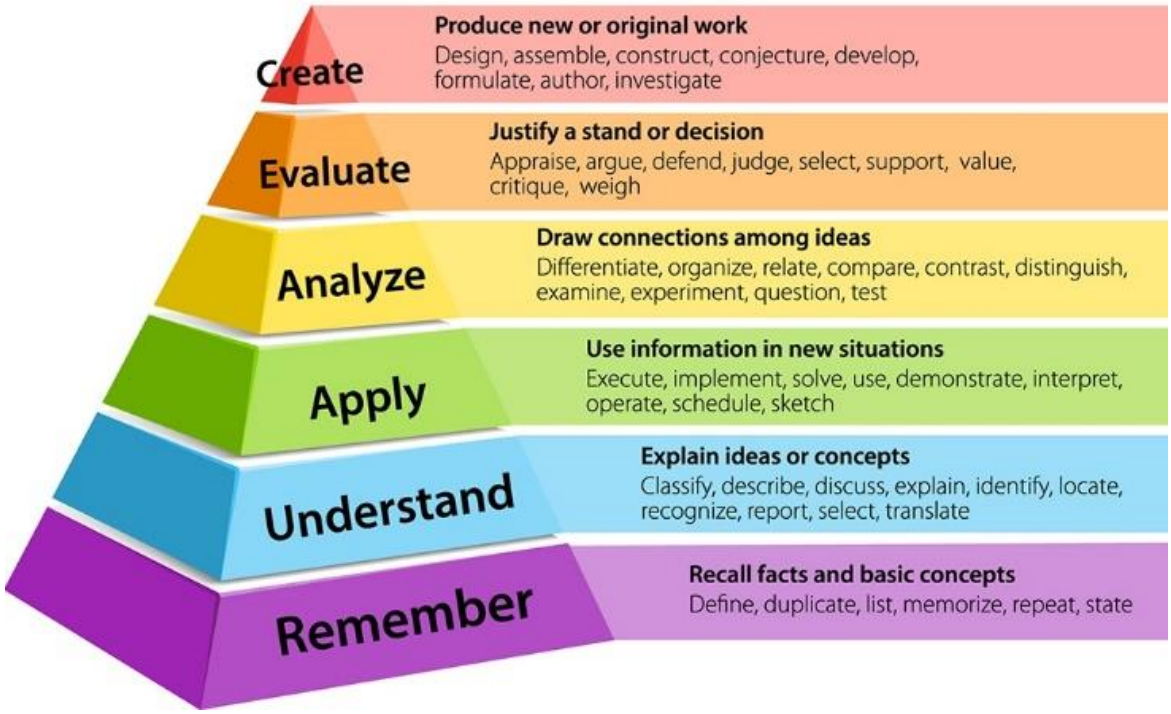

Figure 4: Simplified Bloom's Taxonomy[2]

3.3 European competence-based approach and practitioners' model

This paper presents an evidence-based and practitioner model with a simplified Bloom's taxonomy into three key competence and skills development phases offered within basic, intermediate and advanced cybersecurity subjects. Bloom's taxonomy is divided into three competence levels: knowledge, skills, and practice.

The ever-increasing cybersecurity challenges require a broad understanding of cybersecurity professional competencies. The thought model and simplified competence framework aims to provide a clear understanding of the depth of learning outcomes needed in professional life.

[2] Source of the image: Kraus-Anderson University

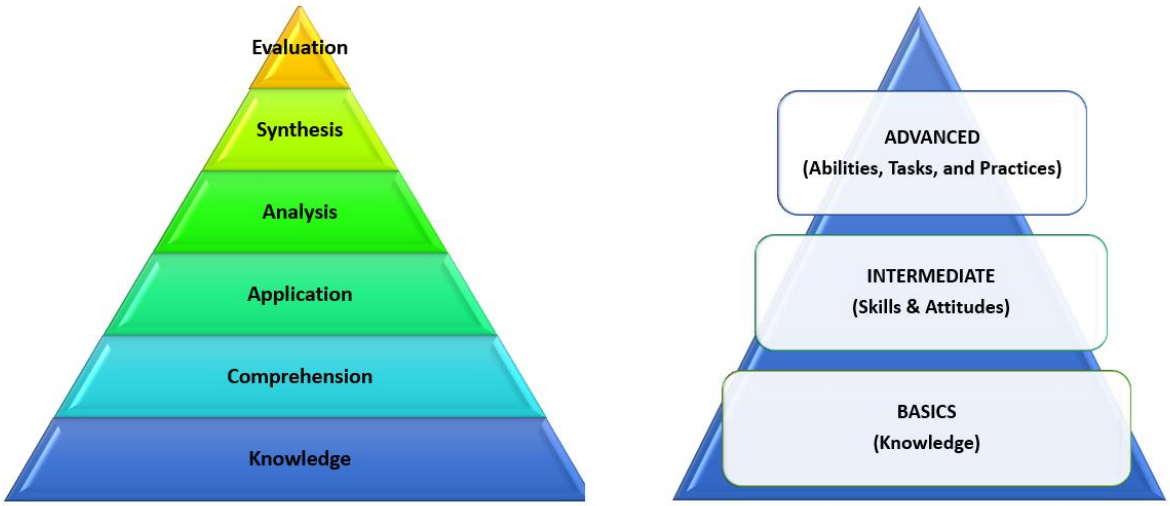

Figure 5: Practitioners' Views on Bloom's Taxonomy[3]

The minimum curriculum includes basic, intermediate and advanced level subjects. Basic subjects offer broad cybersecurity principles, knowledge and comprehension. The intermediate-level subjects offer applications and analysis of cybersecurity skills along with attitudes. The advanced level subjects offer more deep competences including synthesis, professional proficiency and evaluation of cybersecurity working-life abilities, as well as practices in day-to-day tasks.

In the above overview, the different logical competency levels are presented. The following Table 2 presents the different levels of competencies adopted from the European e-Competence Framework (e-CF) [12] for both knowledge, skills and practice levels.

In addition, our long-term research confirms the needed revision of the competence model to make it more relevant to working-life practices. This makes it more practical and relevant to the needs of the cybersecurity industry. A proposal in this respect is presented in the following Figure 6.

[3] Source of the image: Scholarly work of the ECSO WG5 Co-chair Paresh Rathod (Laurea-Finland)

Level	Knowledge	Skills and Attitudes	Abilities, Tasks and Practices
5	Exceptionally comprehensive and detailed knowledge and understanding of the subject	Carrying out the activity in a very complex context while guiding others in the implementation	Outstanding professional proficiencies covering all levels of cybersecurity practices including people, processes and technologies aspects
4	Very extensive and detailed knowledge and understanding of the subject	Carrying out the activity in a complex context	Solution oriented and highly efficient cybersecurity professional approaches and practices covering people, processes and technologies aspects
3	Knowledge and understanding of the subject in detail	Carrying out the activity in a difficult context	Detail oriented and hands-on practices in all cybersecurity aspects including people, processes and technologies
2	Knowledge and understanding of all major cyber security aspects	Carrying out the activity in a simple context	Carrying out professional work in more than one aspect of the cybersecurity practices
1	Basic knowledge and understanding of the subject	Carrying out the activity in a simple context under guidance	Intern or junior level professional practices under the supervision of level-3 or higher professionals

Table 2: Extended European e-Competence Framework (e-CF) for Cybersecurity Competencies

Figure 6: Working-life Competence Practice Model[4]

[4] Source of the image: Scholarly work of the ECSO WG5 Co-chair Paresh Rathod (Laurea-Finland)

3.4 Minimum knowledge, skills and competence requirements

The cybersecurity field is one of the fastest-growing, in-demand and cross-sectoral fields. The prospects of working in the cybersecurity professional domain demands a minimum know-how to perform the job. ECSO and many studies confirm that prospective candidates must have a minimum knowledge, skills and competences to pursue a cybersecurity career [2][17][19][25]. This reference curriculum highly recommends overarching minimum professional requirements before taking the cybersecurity specialisation career path with European minimum reference curriculum courses.

Overarching minimum professional prerequisites: The prospective candidate must have an overall understanding of information and communication technologies (ICT), digital competences and applications in the working-life, including businesses, organisations and individual usage. Figure 7 presents the key elements of the European digital competence framework (EU DigComp 2.1) [27] which can be used as an overarching minimum requirement basis for prospective candidates:

Figure 7: Working-life Competence Practice Model from DigComp 2.1

Competence levels: The minimum curriculum includes basic, intermediate and advanced level courses. More detail is given in section 3.3 and the practical application within the course templates is further explained below (section 5). The pre-requisites for the basic courses outlined include EU DigComp 2.1 topics such as fundamentals on programming, computer architecture and networking, operating systems and databases. It is evident that intermediate and advanced courses should have the basic courses as pre-requisites. This approach helps the effective cybersecurity upskilling and professional development.

4. Curriculum Content Structure

The curriculum is organised in a simplified and consolidated structure within the basic, intermediate and advanced competence clusters as shown below:

Figure 8: High-level Curricula Structure and Contents[5]

(1) Cybersecurity Principles and Management: including human, organisational and regulatory aspects

(2) Cybersecurity Tools and Technologies: including security methods, tools and techniques, as well as use of cyber ranges for training/skills development

(3) Cybersecurity in Emerging Digital Technologies: including artificial intelligence (AI), cyber forensics, machine learning, virtual reality (VR), smart technology, cloud, digital leadership and professional proficiency

(4) Offensive Cybersecurity Practitioners: Mainly cybersecurity and threat analysis in practice including offensive-defensive, cyber ranges & cyber drills, forensics, Internet of Things (IoT), and blockchain

---

[5] Source of the main image: Scholarly work of the ECSO WG5 Co-chair Paresh Rathod (Laurea-Finland)

The thumbnail images from Bing Creative Commons Image Bank

4.1 Cybersecurity cluster-01: Cybersecurity Principles and Management

Description: The key objective of the cluster is to understand, plan and implement information and cybersecurity management in an organisation considering the people, processes and technologies. Another useful objective of the module is to gain an understanding of the modern ICT infrastructure and the operations in modern communication networks. The module will also enable the student to plan a comprehensive information and cybersecurity strategy and risk management system for an organisation. In addition, the module offers possibilities of gaining the knowledge and skills to enhance the security of ICT networks by using security by design principles.

The content of this module will provide comprehensive knowledge to apply the principles of information and cybersecurity management, risk management, safeguarding and formulating continuity plans. After completing this module, the student should be able to plan security ICT network and services and anticipate future security threats based on structural vulnerabilities in IP networks.

4.2 Cybersecurity cluster-02: Cybersecurity Tools and Technologies

Description: The objective of this cluster is to learn and apply cybersecurity tools and techniques. The module focuses on educating and training the students to provide capabilities against vulnerabilities, risks and threats in cyberspace.

The participant will learn important practices used to safeguard information systems, application and enterprise networks of companies in cyberspace. Further, the students will also learn important practices used to protect data and enterprise systems against cyber threats. The students will gain knowledge and skills to manage vulnerabilities, threats and risks within organisations' information networks and cyberspace. The students can acquire knowledge and skills of cybersecurity technologies and current practices. Cyber ranges hands-on practice is provided in this module within educational platforms.

4.3 Cybersecurity cluster-03: Cybersecurity in Emerging Technologies

Description: The objective of this cluster is to equip the students with cybersecurity tools, techniques and technologies for working-life practices. This module focuses on cybersecurity practitioner competences.

The students will learn important practices used in cutting-edge cybersecurity. The module facilitates the best practices for current and future trends of cybersecurity including AI, IoT, cloud, digital businesses and digital leaderships.

4.4 Cybersecurity cluster-04: Offensive Cybersecurity Practitioners

Description: The objective of this cluster is to equip the learners with knowledge of offensive and defensive cybersecurity practices. This module focuses on cybersecurity practitioner competences including threat analysis and cyber ranges.

The participant will learn important practices used to safeguard against any cyber-attacks and mitigating cyber catastrophic incidents. Cyber ranges and cyber drills hands-on knowledge and practices are provided in this module within educational platforms. The module helps students to put into practice advanced cyber defence techniques linked to working-life practices including hackathon projects, research & innovation projects, business projects and operating cyber ranges.

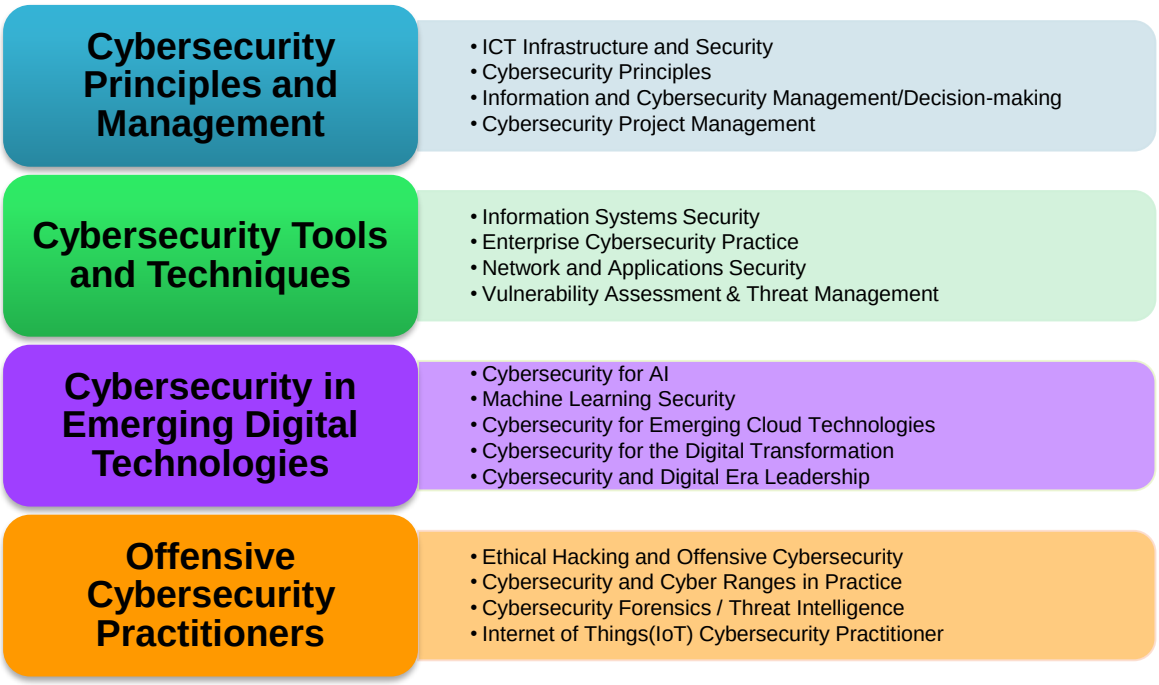

Figure 7: High-level Modules and Subjects [6]

[6] Source of the main image: Scholarly work of the ECSO WG5 Co-chair Paresh Rathod (Laurea-Finland)

5. Reference Curriculum

The proposed curriculum can be based on the following detailed contents.

5.1 Template of subject description and details

The following table template has been used to illustrate the subject details in this minimum reference curriculum.

<table>
<tr><th colspan="2">Subject code (EU CybersecurityXX-EUCSxx) – Subject Name</th></tr>
<tr><td colspan="2">Competence Level: Basic, Intermediate or Advanced (based on section 3.4 guidelines)</td></tr>
<tr><td colspan="2">Briefly about the subject:

Possible alternative subject names:
Name 1
Name 2</td></tr>
<tr><td>Subject contents and topics</td><td>Learning outcomes (competencies)</td></tr>
<tr><td rowspan="2">- Topic 1
- Topic 2</td><td>The student is able to (can apply knowledge and has skills to):
- Learning outcome 1
- Learning outcome 2</td></tr>
<tr><td>Suitable job roles/career path:
Engineer
Security Assistant
Other
Note: Minimum experiences not included due to the fact it depends on individual organisations’ perspectives.</td></tr>
<tr><td colspan="2">Mapping with the professional certifications
Pro 1
Pro 2

Mapping with frameworks such as:
CyBOK, eCF, ENISA cybersecurity skills framework, etc.

NOTE: The mapping confirms the equivalent knowledge of the candidates</td></tr>
</table>

5.2 List of subjects and details

The following tables describe each subject the following information: (1) Subject code and name, (2) Proposed ECTS, (3) Alternative names, (4) Subject contents and topics, (5) Learning outcomes (competencies), (6) Mapping with professional certifications, and (7) Suitable job roles.

<table>
<tr><th colspan="2">EUCS01 - ICT Infrastructure and Security</th></tr>
<tr><td colspan="2">Competence Level: Basic</td></tr>
<tr><td colspan="2">The subject is proposed to be 5 ECTS.

Alternative names:
Computer Network
Network Applications
Information Infrastructure and Security</td></tr>
<tr><td><u>Subject contents and topics</u></td><td>Learning outcomes (competences)</td></tr>
<tr><td rowspan="2">> Computer network concept
> Information and communications technology (ICT) network concepts
> Open System Interconnection (OSI) model
> ICT Network Technologies
> ICT Network Installation and Configuration
> ICT Network Media and Topologies
> ICT Network Management
> ICT Network Security Foundations</td><td>The student is able to
- design secure enterprise networks
- implement functional ICT networks
- configure, manage, and maintain essential network devices to create resilient networks
- comprehensive analysis of the existing network configurations
- implement network security, standards, and protocols
- management of virtual networks
- appropriate solutions of ICT network relevant troubles</td></tr>
<tr><td>Suitable job roles/career path:
Junior Network Administrator / Computer Technician / Network Field Technician / Help Desk Technician
Junior System Engineer / System Engineer / IS Consultant
Network Support Specialist / Network Field Engineer / Network Analyst</td></tr>
<tr><td colspan="2">Mapping with professional certifications:
ISC^2 SSCP (Systems Security Certified Practitioner)CCNA (Cisco Certified Network Associate) Security
CompTIA Network+</td></tr>
</table>

EUCS02 - Cybersecurity Principles

Competence Level: Basic / Intermediate

The subject is proposed to be 5 ECTS.

Alternative names:
Introduction to Cybersecurity
Introduction to Information Security
Introduction to Information and Cybersecurity

Subject contents and topics	**Learning outcomes (competences)**
> Cybersecurity concepts > Key cybersecurity body of knowledge (CyBOK) > Threats, attacks and vulnerabilities > Security technologies and tools > Security architectures and designs > Identity and access management approaches > Risk management principles > Cryptography and PKI concepts > Professional, legal and ethical aspects of cyber security > Data privacy and online rights > Cyber threat intelligence > Web navigation security > Social engineering and targeting mobile security > Cyber hygiene > Malware and malware detection	The student is able to demonstrate the knowledge and abilities of - global challenges: cyber threats, risks and attacks landscape - pivotal role of the cyber security domains and its best practices - cyber security risk management and governances - The holistic cyber security: people, processes and technologies - fostering cyber security culture with consolidating human and social factors - professional, legal and ethical practices in cyber security - thriving in the digital and technology driven modern businesses: the best practices for privacy and online rights - recognise the main cyber-attack techniques **Suitable job roles/career path:** Cybersecurity Helpdesk Assistant Junior Cybersecurity Analyst Systems Administrator / Network Administrator / Security Administrator Junior IT Auditor/ Penetration Tester Security Specialist / Security Consultant/ Security Engineer Software developer

Mapping with professional certifications:
ISC² SSCP (Systems Security Certified Practitioner)
ISC² CSSLP – (Certified Secure Software Lifecycle Professional)
CompTIA Security+
ISACA CSX-F: Cyber Security Fundamentals
CCNA CyberOps (Cisco Certified Network Associate - CyberOps)
CCNP (Cisco Certified Network Professional) Security
NCSP-F (NIST Cyber Security Professional Foundation)

EUCS03 - Information and Cybersecurity Management

Competence Level: Basic / Intermediate

The subject is proposed to be 5 ECTS. The subject can be extended to 10 ECTS with comprehensive coverage of information security management body of knowledge with practice learning activities.

Alternative names:
Cybersecurity Decision-Making and Management
Information Security Management
Management of Information Security
Cybersecurity Management

Subject contents and topics	**Learning outcomes (competences)**
> Regulatory issues > Information security governance > Cost-benefit analysis of risk mitigation >Wider IT frameworks (e.g. COBIT 5) > Information Risk management > Information Security Program Development & Management > Information Security Incident Management > Disaster recovery > Cybersecurity awareness techiniques	The student is able to demonstrate the knowledge and abilities of - information security governance principles - risk management, incident management and compliance principles - information security programme development and management principles - analysing typical information security management related problems and draw solutions to them **Suitable job roles/career path:** Cybersecurity Manager Information Security Manager Risk Management Professional Security Management Professional Risk Analyst / Assessor

Mapping with professional certifications:
ISC² CISSP (Certified Information Systems Security Professional)
ISC² CISSP - ISSMP (Certified Information Systems Security Professional - Information Systems Security Management Professional
ISC² CAP (Certified Authorization Professional)
ISACA CISM (Certified Information Security Manager)
E|ISM (EC-Council Information Security Manager)
ISO/IEC 27001-P (EXIN Information Security Management ISO 27001 Professional)
Mile2 CISRM (Certified Information Systems Risk Manager)
Mile2 CISSM (Certified Information Systems Security Manager)

EUCS04 - Cybersecurity Project Management

Competence Level: Intermediate

The subject is proposed to be 5 ECTS.

Alternative names:
Information Security Management
Management of Information Security
Cybersecurity Management

Subject contents and topics	**Learning outcomes (competences)**
> Cybersecurity Project Foundation > Cybersecurity Project Life Cycle > Project Constraints > Project Team Management, Communication and change management > Project tools, documentation and presentation > Risk management plan	The student is able to demonstrate the knowledge and abilities of - taking sole responsibility for working as a member of cybersecurity research or business project team - project management body of knowledge (PMBoK) practices or equivalent practices - planning, implementing and documenting cyber security research or business project - presenting research results in the academic and business format - manifesting cybersecurity professional practices in the community
	Suitable job roles/career path: Cybersecurity Manager Information Security Manager Project Coordinator or Manager Project Team Member Business Analyst Manager, Director, Team Leader

Mapping with professional certifications:
ISC^2 CISSP - ISSMP (Certified Information Systems Security Professional - Information Systems Security Management Professional
CompTIA Project+
Project Management Professional (PMP)
ISO/IEC 27001-E (EXIN Information Security Management ISO27001 Expert)
GCPM (Certified Project Manager)

EUCS05 - Information Systems Security

Competence Level: Advanced

The subject is proposed to be 5 ECTS. The subject can be extended to 10 ECTS with comprehensive coverage of information systems security body of knowledge with practice learning activities.

Alternative names:
Systems Security / Data Systems Security
Enterprise Systems Security
Information and Data Security

Subject contents and topics	**Learning outcomes (competences)**
>Operations security >Telecommunications and network security >Information security governance and risk management >Software development security >Cryptography >Steganography >Security architecture and design >Access control >Business continuity and disaster recovery planning >Legal, regulations, investigations and compliance >Physical and environmental security >Security in software lifecycle	The student is able to demonstrate the knowledge and skills of - code of security professional ethics and confidentiality, integrity, and availability, - security fundamentals and terminologies - cryptographic systems, life cycles, techniques, and methodologies for cryptography and cryptanalysis - identity and access services in the enterprise and provisioning life cycle - data and information systems security - physical and corporate facility security - enterprise security and risk management practices including governance, compliance, and business continuity planning
	Suitable job roles/career path: Chief Information Security Officer (CISO) Cybersecurity Officer Cybersecurity Consultant Cybersecurity Director **Note:** Minimum of 5 years professional experience required.

Mapping with professional certifications:
ISC² CISSP (Certified Information Systems Security Professional)
ISC² CISSP - ISSAP (Certified Information Systems Security Professional - Information Systems Security Architecture Professional
ISC² CISSP - ISSEP (Certified Information Systems Security Professional - Information Systems Security Engineering Professional
ISC² CISSP - ISSMP (Certified Information Systems Security Professional - Information Systems Security Management Professional
ISC² SSCP (Systems Security Certified Practitioner)
CRISC (Certified In Risk and Information Systems Control)
Mile2 CISSO (Certified Information Systems Security Officer)

EUCS06 - Enterprise Cybersecurity Practice

Competence Level: Advanced

The subject is proposed to be 5 ECTS. The subject can be extended to 10 ECTS with comprehensive coverage of enterprise cybersecurity body of knowledge with practice learning activities.

Alternative names:
Enterprise Network Security
Advanced Enterprise Security

Subject contents and topics	**Learning outcomes (competences)**
> Organisational Security and Privacy Policies > Enterprise Risk Management Process > Enterprise Network and Security Components, Concepts, and Architectures > Enterprise Security Controls for Host and Server Devices > Mobile Devices Security Solutions > Software Security Controls > Enterprise Security Assessments, Incident Response and Recovery > Hosts, Storage, and Applications in the Enterprise > Cloud and Virtualization Technologies in the Enterprise > Advanced AAA Technologies > Cryptographic Techniques > Secure Communication and Collaboration Solutions > Applying Research Methods for Trend and Impact Analysis > Implementing Security Activities across the Technology Life Cycle > Diverse Business Units and Enterprise Integration	The student is able to demonstrate the knowledge and skills of - enterprise security and advanced risk management - enterprise security operations and architecture - identify threats, vulnerabilities and risks associated enterprise network - outline common attack tactics, techniques used when hacking enterprise network, applications and wireless networks - outline security controls for information systems against common threats - technical integration and solutions of Enterprise Cybersecurity - research, development and collaboration within enterprise security **Suitable job roles/career path:** Chief Information Security Officer (CISO) Cybersecurity Officer Cybersecurity Consultant Security Architect Technical Lead Analyst Application Security Engineer Security Engineer

Mapping with professional certifications:
ISC² CISSP (Certified Information Systems Security Professional)
ISC² CISSP - ISSAP (Certified Information Systems Security Professional - Information Systems Security Architecture Professional
ISC² CISSP - ISSEP (Certified Information Systems Security Professional - Information Systems Security Engineering Professional
ISC² CISSP - ISSMP (Certified Information Systems Security Professional - Information Systems Security Management Professional
CompTIA CASP (Advanced Security Practitioner)

EUCS07 - Network and Applications Security

Competence Level: Advanced

The subject is proposed to be 5 ECTS. The subject can be extended to 10 ECTS with comprehensive coverage of Network and Applications offensive-defensive security body of knowledge with practical learning activities.

Alternative names:
Network Security / Applications Security / Enterprise Network Security/
Enterprise Applications Security
Offensive Cyber Security

Subject contents and topics	**Learning outcomes (competences)**
> Offensive and Defensive Security & Introduction to Ethical Hacking > Ethical Hacking Process: Footprinting and Reconnaissance, Scanning Networks, Enumeration, Vulnerability Analysis & System Hacking > Malware Threats > Sniffing & Social Engineering > Denial-of-Service & Session Hijacking > Evading IDS, Firewalls, and Honeypots > Hacking Web Servers & Hacking Web Applications > Database Security & SQL Injection > Hacking Wireless Networks > Hacking Mobile Platforms > IoT and OT Hacking > Cloud Computing > Cryptography	The student is able to demonstrate the knowledge, skills and abilities of - the role of ethical hacking in the offensive and defensive network and applications security - hacking phases and life cycle including foot-printing, reconnaissance, scanning networks, enumeration, vulnerability analysis and system hacking - security controls including information assurance, information security, network segmentation, defence-in-depth, and security policies - access control mechanisms, data leakage, leak prevention, and data loss prevention - preventing malware threats and social engineering - common web application and server threats and hacking - SQL injection and the role of hacking - wireless and mobile hacking and prevention tools **Suitable job roles/career path:** Chief Information Security Officer (CISO) Cybersecurity Officer / Cybersecurity Consultant

Mapping with professional certifications:
S-EHP (SECO-Institute's Ethical Hacking Practitioner)
CompTIA Pentest+
OSCE (Offensive Security Certified Expert)
eCPTX (eLearnSecurity Certified Penetration Tester eXtreme)
Mile2 C)PEH Certified Professional Ethical Hacker
CPEH (GAQM Certified Professional Ethical Hacker)

EUCS08 – Vulnerability Assessment & Threat Management	
Competence Level: Advanced	
The subject is proposed to be 5 ECTS. **Alternative names:** **Systems Security / Information and Data Security** **Cybersecurity Analysis** **Cybersecurity Threat Management**	
Subject contents and topics	**Learning outcomes (competences)**
> Threat Management > Vulnerability Management > Cyber Incident Response > Security and Architecture Tool Sets > Attack cycle > The role of the analyst in cyber threat intelligence > Attribution	The student is able to demonstrate the knowledge, skills and abilities of - network architecture and reconnaissance principles - select appropriate tools for network reconnaissance and vulnerability analysis - threat identification and threat mitigation principles - analyse network vulnerabilities with network reconnaissance and analysing tools - security incidents investigation and monitoring principles - present the results of network reconnaissance and vulnerability analysis in professional format
	Suitable job roles/career path: Cybersecurity Analyst Threat Intelligence Analyst Security Engineer Application Security Analyst Incident Response or Handler Compliance Analyst Threat Hunter
Mapping with professional certifications: **ISC² CISSP (Certified Information Systems Security Professional)** **ISC² CISSP - ISSAP (Certified Information Systems Security Professional - Information Systems Security Architecture Professional** **ISC² CISSP - ISSEP (Certified Information Systems Security Professional - Information Systems Security Engineering Professional** **ISC² CISSP - ISSMP (Certified Information Systems Security Professional - Information Systems Security Management Professional** **ISC² SSCP (Systems Security Certified Practitioner)** **CompTIA CySA+ (Cybersecurity Analyst)** **CPSA (CREST Practitioner Security Analyst)** **CESA (Lunarline Certified Expert Security Analyst)** **OPSE (OSSTMM Professional Security Expert)** **Cisco Certified CyberOps Professional certification (CBRCOR + CBRFIR)**	

EUCS09 - Cybersecurity for Artificial Intelligence (AI)	
Competence Level: Advanced	
The course is proposed to be 10 ECTS. **Alternative names:** **Smart cybersecurity / Intelligence cybersecurity** **Use of AI in cybersecurity** **Cybersecurity and the role of AI**	
Subject contents and topics	**Learning outcomes (competences)**
> Data science and security concept > Knowledge Representation > Knowledge Based Systems > Expert Systems > Types of machine learning > Data and its pre-processing > Types of Learning > Tools and Technologies > Regression > Decision Trees > Naive Bayes > Support Vector Machines > Clustering > Neural Networks > Neural Coding > Reinforcement Learning > Big Data Processing > Deep Learning > Tools and Technologies > Convolutional Neural Networks > Recurring and Recursive Neural Networks > Distributed AI / Multi-Agent Systems > Federated Learning > Ensemble Methods	The student is able to - become aware, understand and apply different techniques for data science, data pre-processing steps and its security implication. - become aware, understand and apply different machine learning techniques: supervised, unsupervised and reinforcement learning. - understand and apply different techniques for ingestion, storage and processing of big data - understand and apply different deep learning techniques - understand and apply federated learning and distributed AI - know and understand a real problem of medium or high complexity and analysing, investigating, designing, implementing, experimenting, reviewing, testing, synthesising, and evaluating in order to solve this problem using the methods presented in the course - understand different types of problems such as events correlation, impact propagation, intelligent SIEM Types of Problems: - intrusion detection - detection of inappropriate web and email contents - modelling the behaviours of devices, users, and network to learn specific patterns and detect anomalous behaviours - user and entity behaviour analytics
	Suitable job roles/career path: AI Cybersecurity Expert Threat Intelligence Analyst Data Security Scientist/Expert
Mapping with professional certifications **Cybersecurity Artificial Intelligence (CS_AI) Certificate Program: Higher Education Institutes (HEIs)** **ISACA CET—Certified in Emerging Technology Certification**	

EUCS10 – Machine Learning Security	
Competence Level: Advanced	
The course is proposed to be 5 ECTS. **Alternative names:** **Protecting AI systems** **Safe and Secure Machine Learning** **Trustworthy AI** **AI security**	
Subject contents and topics	**Learning outcomes (competences)**
> Artificial Intelligence threats > AI risks identification > Adversarial Learning > Generative Neural Networks > Explainable AI > Explainable vs black-box models > Verification and Validation of AI >AI ethics >AI abuses and their implications	The student is able to - understand and identify the threats and risks of using AI for CS - defend against adversarial learning - design adversarial-aware AI systems - use explainable AI techniques - become aware of the strategies to use to verify AI and evaluate the safety of its usage - become aware of explanation of biases with data collection & usage in relation to ethics - become aware of the history of AI abuses and the implications those have
	Suitable job roles/career path: Cybersecurity Analyst Threat Intelligence Analyst Security Engineer Application Security Analyst
Mapping with professional certifications **Cybersecurity Machine Learning Certificate Program: Higher Education Institutes (HEIs)** **ISACA CET—Certified in Emerging Technology Certification**	

EUCS11- Cybersecurity for Cloud Technologies	
Competence Level: Advanced	
The course is proposed to be 5 ECTS. **Alternative names:** **Cloud Computing** **Cloud Auditing**	
Subject contents and topics	**Learning outcomes (competences)**
>Cloud concepts, design and development >Network and cloud attack techniques >Defense systems: Anti-Malware, IPS, SandBox and Debugging >Cryptography and steganography >Risk analysis and management >Main threats: traditional attacks, ransomware, DOS and DDOS, Advanced Persistent Threats (APT). >Web Application Attacks: Cross Site Scripting (XSS) >Techniques, tools and technologies for Cloud security (including cloud data and application security using the OWASP model) >Cloud Computing Privacy Issues	The student is able to - understand and explain cloud concepts, architecture and design - understand and apply practices of operating systems, servers, clouds and relevant infrastructures (e.g., languages, software and emerging technologies, programming) - apply hands-on coding and scripting and programming skills (e.g., languages, software and emerging technologies, programming and other) - apply the cloud platform, Infrastructure, data, and application security - understand and apply regulations, legal, risk and compliance standards/methodologies/tools/guidelines/best practices relevant to cloud computing **Suitable job roles/career path:** Cybersecurity Analyst Threat Intelligence Analyst Security Engineer Application Security Analyst Risk Manager Cloud Computing Expert Cloud Auditor
Mapping with professional certifications **ISC² Certified Cloud Security Professional (CCSP)** **CompTIA Cloud+** **CompTIA Cybersecurity Analyst (CySA+)**	

EUCS12- Cybersecurity for the Digital Transformation	
Competence Level: Advanced	
The course is proposed to be 5 ECTS. **Alternative names:** **Digital Transformation in Modern Era** **Digital Transformation Cybersecurity**	
Subject contents and topics	**Learning outcomes (competences)**
>Digital transformation concepts: technology evaluation, societal-business-regulatory complexity, sophisticated cyber-threats and attacks, and resource management > Onlife Manifesto: being human in a hyperconnected era >Foundation and Revolution of AI, Machine Learning and IoT >Foundation and revolution of Cloud, Blockchain and Big Data >Foundation and revolution of Cybersecurity and Emerging Cutting-Edge technologies >Digital transformation in practice and their impacts in society, business, communities and governments >Market trends on digital transformation and impact on cybersecurity >Leadership and management practices in digital transformation	The student is able to - understand and explain digital transformation concepts and foundation including benefits, challenges and opportunities. - understand and explain the impact of digital era and information and communication technologies (ICTs) on the human condition. How it demands the need of digital transformation - explain and discuss digital transformation and its associated practices, models and technologies - application practices of contemporary technologies associated with Digital Transformation - cultivate organisational thinking of cyber secure digital transformation domains, digital capabilities and adoption considerations - foster the adoption of Digital Transformation practices and technologies to business process improvements and optimisation - ensure the organisation growth and competitiveness in digital era with next generation cybersecurity **Suitable job roles/career path:** Digital Transformation Innovator Digital Transformation Expert Digital Transformation Leader Digital Transformation Evangelist
Mapping with professional certifications **None**	

EUCS13- Cybersecurity and Digital Era Leadership	
Competence Level: Intermediate	
The course is proposed to be 5 ECTS. **Alternative names:** **Leadership in the Cyber Secure Digital Era** **Digital Era Leader** **Next Generation European Leadership** **Chief Innovation Officer / Leader**	
Subject contents and topics	**Learning outcomes (competences)**
>Online Manifesto: being human in a hyperconnected era >Leading the organisation in the disruptive digital era: Different leadership styles >Leadership and management practices in digital and innovation era: innovation, growth, inclusion, collaboration and modern business strategy: Digital competences >Creative, playful and transformational leadership and modern business strategy: Human-centric innovation >Digital readiness in modern era and innovation organisations >Effective communication and presenting in digital era >Managing global and diverse teams with impactful co-creation, co-innovation and social responsibilities >Leading from the front for the cyber secure practices of innovation, social media, cutting-edge technologies and tools	The student is able to - understand and explain the impact of digital era and information and communication technologies (ICTs) on the human condition. How it demands the need of digital era leadership - understand and explain generational leadership styles, digital competences and human-centric innovation thinking - rethink the leadership model for digital ear with innovation, growth, inclusion, and collaboration practices - support and help next generation digital leaders to perform their best with new venture, innovation, transformation and lead without titles - cultivate innovation, experimenting, entrepreneur spirit and risk taking for new service innovations as part of one-step ahead business strategies - foster initiative, creativity, curiosity, growth mindset, collaboration, grit, social responsibility and next generation leadership - ensure accountability, credits and progress for the diverse teams - ensure the organisation's growth and competitiveness in the digital era **Suitable job roles/career path:** C-Suite Leaders CEO and MD of Innovative Firms Global Advisory Board Member Board Member for Innovative Firms
Mapping with professional certifications **INSEAD Digital Ear Leadership Programme**	

EUCS14 - Ethical Hacking and Offensive Cybersecurity

Competence Level: Advanced

The subject is proposed to be 5 ECTS.

Alternative names:
Ethical Hacking
Offensive Cybersecurity
Pen testing

Subject contents and topics	Learning outcomes (competences)
> Professional and Ethical Hacking skills and responsibility > Penetration testing process and tools > Passive information gathering > Active information gathering > Vulnerability scanning and finding exploits > Exploits and hacking attacks > Client and server-side attacks > Fixing exploits and securing systems > Ethical hacking process documentations and suggestions > Ethical hacking, social responsibilities and secure society	The student is able to - take sole responsibility for working as a member ethical hacker team - participate and act ethically as a member of team, community and working-life partners - apply hacking techniques information gathering techniques targeted ICT systems and services - utilise the tools and technique for penetration testing process to exploit the vulnerabilities including local and remote client and server-side attacks - practice SQL injections, XSS exploits and tunneling techniques on web application and servers. - manifest cybersecurity offensive and ethical hacking professional practices - apply practitioner skills in the community
	Suitable job roles/career path: Ethical Hacker Penetration Tester Technical Vulnerability Analyst /Assessor Offensive Cybersecurity Practitioner Offensive Cybersecurity Expert

Mapping with professional certifications:
CompTIA Pentest+
PEH Certified Professional Ethical Hacker
OSCE (Offensive Security Certified Expert)
S-EHP (SECO-Institute's Ethical Hacking Practitioner)

EUCS15 – Cybersecurity and Cyber Ranges in Practice	
Competence Level: Advanced	
The subject is proposed to be 5 ECTS. **Alternative names:** **Cyber Ranges and Hackathons** **Offensive Cybersecurity** **Ethical Hacking**	
Subject contents and topics	**Learning outcomes (competences)**
> Cyber range concepts, architectures, and applications > Professional and ethical skills and responsibility > Teamwork participation and contribution > Collaboration and cooperation with working-life partners > Ethical hacking and hands-on skills including reconnaissance, network pen testing, access control, software, database and capture the flag. > Project documentation and presentations > Exercises and scenarios for simulations, virtual or cyber range environments	The student is able to - take sole responsibility for working as a member cybersecurity analyst team - offer a way of learning cyber sec and working on a project together (project target varies including research, innovation, business, cyber ranges, cyber drill or cyber defense projects) - participate and act ethically as a member of team, community and working-life partners - take up the responsibility to set up own research lab online like own digital cyber security playground - select appropriate tools and strategies for network reconnaissance and vulnerability analysis projects in real exercise or company environment - test out new tooling and benchmarking endpoint detection and response (EDR) vendor systems against known detection technologies - present the results of network reconnaissance and vulnerability analysis in a professional format - analyse critically the outcome of the project - manifest cybersecurity professional practices and apply practitioner skills in the community
	Suitable job roles/career path: Ethical Hacker Penetration Tester Offensive Cybersecurity Practitioner Cybersecurity Trainer Cyber Ranges Expert
Mapping with professional certifications: **S-EHP (SECO-Institute's Ethical Hacking Practitioner)** **CompTIA Pentest+** **OSCE (Offensive Security Certified Expert)** **eCPTX (eLearnSecurity Certified Penetration Tester eXtreme)** **PEH Certified Professional Ethical Hacker**	

EUCS16 - Cybersecurity Forensics / Threat Intelligence	
Competence Level: Advanced	
The course is proposed to be 5 ECTS. **Alternative names:** **Cyber Threat Intelligence** **Digital Forensics**	
Subject contents and topics	**Learning outcomes (competences)**
> Digital forensics investigations > Legal aspects and analysis methodologies >"Offensive" computer security >Explore techniques and technologies for image analysis and processing >Computer networks, protocols and analysis techniques >Network and software hacking techniques >Data analysis and recovery >Virtualisation and its implications for forensic analysis >Forensic analysis on mobile devices and in the IoT domain >Risk management	The student is able to - work ethically and independently; not influenced and biased by internal or external actors - explain and present digital evidence in a simple, straightforward and easy to understand way for non-technical people - know about evidence gathering and the crucial documentation steps they need to take & safeguard against evidence tampering - develop detailed investigation reports - carry out activities as an expert (independently, ethically, impartially, conscientiously, competently and in a trustworthy manner) - identify the limits of their expertise and act accordingly (e.g. identifying and comparing persons and objects visible on digital images, interpreting audio fragments, photogrammetry) - understand criminal law, and criminal investigation - establish “Chain of Custody” reports with relevant legal aspects **Note:** The key learning outcome is to learn the ethical and professional skills for evidence gathering and the crucial documentation steps they need to take & safeguard against evidence tampering, so their way of handling things can have an impact (positively or negatively) in court.
	Suitable job roles/career path: Digital Forensics Investigator Digital Forensics Analyst / Examiner Cyber Forensics Analyst / Expert Computer Forensics Specialist /Investigators /Technician / Examiner Cyber Threat Intelligence Expert
Mapping with professional certifications **GIAC Certified Forensic Examiner (GCFE)** **GIAC Cyber Threat Intelligence (GCTI)** **CompTIA Pentest+** **eCPTX (eLearnSecurity Certified Penetration Tester eXtreme)**	

EUCS17 – Internet of Things (IoT) Cybersecurity Practitioner	
Competence Level: Advanced	
The course is proposed to be 5 ECTS. **Alternative names:** **Internet of Things (IoT) Security** **Cybersecurity of IoT**	
Subject contents and topics	**Learning outcomes (competences)**
> Internet of Things and pervasive technology concepts > IoT Lifecycle: Conceptual Phase to Retirement Phase > Design and implement privacy-aware & secure IoT devices: Security by Design > Threats and risks to IoT devices and lifecycle > Create secure, manageable, and compliant IoT products > Release and deploy verified IoT products > Secure IoT production environment and products > Internet of Things compliance, regulatory and legal framework	The student is able to - explain and present concepts of embedded devices, wearable gadgets, pervasive technology and the Industrial Internet of Things - explain and present IoT lifecycle with examples including conceptual, development, production, utilisation, support, and retirement phases - abilities to create relevant and risk-based security requirements for IoT products and related services using security by design principle - carry out security good practices for full IoT lifecycle considering actors, processes and technologies - understand IoT compliance, regulatory and legal framework **Suitable job roles/career path:** IoT Cybersecurity Expert
Mapping with professional certifications **ISC^2 CSSLP – (Certified Secure Software Lifecycle Professional)** **CTIA IoT Cybersecurity Certification** **Eurosmart IoT Certification Scheme**	

6. Key takeaways from the Minimum Reference Curriculum

In reviewing the modules in this paper and considering ECSO's 2020 paper on cyber ranges, a clear takeaway is that we can consider the use of cyber ranges explicitly as a regular hands-on learning method for all the skills development modules/subjects of the Minimum Reference Curriculum. Simulation labs are already used for teaching but outside or without a cyber range, running teaching labs is not a sustainable learning method nor a fully accessible one (especially considering the campus access restrictions brought on by COVID-19). ECSO WG5 therefore encourages a wider adoption and use of cyber range-based services by learners, training providers, and employers alike. This will allow a shift from the still elite platform/technology perception to more accessible educational environments, in line with other available learning methods in cybersecurity such as taught education, self-learning and continuous professional development.

ECSO and its members foresee the benefits and contribution of this report towards European cybersecurity capacity building efforts and will update the report based on inputs from the wider cybersecurity community and in line with complementary frameworks such as ENISA's upcoming Cybersecurity Skills Framework.

Annex

Example: CISO profile
Sample usage: Case of possible usage of combining ECSO paper with EU nations' perspective.

Following work is Based on the Dutch CISO profile [17] mapped to e-CF [6] and integrating ECSO paper elements. The combination creates a working-life case of cybersecurity professional profiles and curricula.

Profile title	**CORPORATE SECURITY OFFICER (CISO)**		
Summary statement	Defines the information security strategy and organises and manages the organisation's information security in line with the organisation's needs and risk appetite.		
Mission	Defines the organisation's information security strategy, based on a risk management approach and anticipating the information security threat landscape, trends and business needs. Sets up the information security organisation and determines and assigns necessary resources. Initiates and coordinates information security deployment and integration throughout the organisation. Ensures an appropriate level of information security and information security behaviour based on the organisation's needs and risk appetite. Is recognised as the information security strategy expert by internal and external stakeholders.		
Deliverables	**Accountable**	**Responsible**	**Contributor**
	• Information security strategy • Information security organisation and expertise • Business continuity organisation • Adapt information security to other security domains • Compliance with information security requirements and architecture • Information security awareness across the organisation • Organisation's	• Information security project portfolio • Corporate information security activities and projects • Monitoring the relevant risks for the organisation • Monitoring compliance with policy, legislation and regulation • Coordinated response after major information security or ICT incidents • Corporate information security policies, standards, methods and techniques	• Risk management strategy • Information systems governance • Service Level Agreements • Information security architecture

	risk readiness for emerging information security and ICT risks • Information risk analyses, security designs and solutions • Information security assessments, tests, reviews and audits		

Main tasks	• Define the organisation's strategy for information security • Organise information security and the necessary expertise • Ensure adaptation of information security to other security domains, including privacy protection, physical security and continuity management • Establish a business continuity organisation • Coordinate the response to serious information security or ICT incidents • Provide an information security project portfolio • Initiate and coordinate corporate information security activities and projects • Provide corporate information security policies, standards, methods and • techniques • Monitor and ensure the quality of information risk analyses, security designs and solutions • Monitor and ensure compliance with information security requirements and architecture and consistent application of Security-by-Design and Privacy-by Design • Monitor and ensure information security awareness throughout the organisation • Monitor the relevant risks for the organisation • Ensure the organisation's risk readiness for emerging information security and ICT risks • Monitor and ensure the quality of information security assessments, tests, reviews and audits • Monitor the extent to which the organisation complies with information security policy, legislation and regulations on the basis of assessments, tests, reviews and audits • Inform senior general management on the status of information security and incidents, and present improvement proposals	
e-Competences (from e-CF)	D.1. Information Security Strategy Development	Level 4
	E.3. Risk Management	Level 3
	E.4. Relationship Management	Level 3
	E.8. Information Security Management	Level 4

General competences	G.1. Leadership	Level 3
	G.3. Communication and persuasion	Level 3
	G.5 Organisational sensitivity	Level 3
	G.6. Management	Level 3
	G.7 Analytical skills	Level 4
	G.8 Integrity	Level 3
Education and experience	• A completed relevant Master study[7] or equivalent level of knowledge and skills • Five years' work experience in an information security position • Five years' work experience in a management position	
KPI	An appropriate level of information security and information security awareness based on the organisation's needs and risk appetite.	

In the above overview, different competency levels are presented, as used in the eCF framework. Below the explanation is given for the different levels, for both knowledge and skill level.

Level	Knowledge	Skills
5	Exceptionally comprehensive and detailed knowledge and understanding of the subject	Guiding others who carry out the activity in a very complex context
4	Very extensive and detailed knowledge and understanding of the subject	Carrying out the activity in a very complex context
3	Knowledge and understanding of the subject in detail	Carrying out the activity in a difficult context
2	Knowledge and understanding of all major aspects of the subject	Carrying out the activity in a simple context
1	Basic knowledge and understanding of the subject	Carrying out the activity in a simple context under guidance

This provides the required levels of knowledge and skills. It is not yet possible to determine what this entails and how we transfer this knowledge. For this, knowledge and skill statements have been set up. These statements are still high level, but already more detailed. These learning outcomes enable training providers (both education institutes and commercial training providers) to set up relevant courses. The statements are also robust and relatively independent of time, as they don't mention specific models and technologies.
As an example, for years the relevant privacy EU legislation was provided by the EU Data Protection Directive (Directive 95/46). In recent years, it has been replaced by the General Data Protection Regulation. The statement on knowledge of relevant legislation does not need the change, the actual training however needs to be updated. The actual training can be based upon relevant Bodies of Knowledge like CyBOK.

One example is provided below, for both the knowledge and the skill part. The example is provided for D1: Information Security Strategy Management.

[7] A Master study in economic, exact, technical or human sciences domain.

Knowledge and skill (e-CF)	Learning outcomes	
Has knowledge of / is familiar with	Has knowledge of and insight in	CISO
K0 the principles and models for organization and strategy development when relevant for information security.	D1.K0.1 The most important principles and models from organization science, their characteristics and applications.	4
	D1.K0.2 The most important principles and models for strategy, governance and alignment, their characteristics and applications.	3
	D1.K0.3 The most important models, methods and techniques for financial systems, their characteristics and applications.	4
	D1.K0.4 The most important principles and models for information security, their characteristics and applications	4
	D1.K0.5 The principles and advantages / disadvantages of standardization	4
K1 potential and opportunities of relevant norms and 'best practices'.	D1.K1.1 potential and opportunities of relevant norms and 'best practices'	4
	D1.K1.2 Relevant laws and regulations with respect to information security.	4
Is capable of	**Is Capable of**	
S1 Development and critical analysis of the company strategy with respect to information security.	D1.S1.1 Creating a vision on information security for a specific organization.	4
	D1.S1.2 Creating a strategy on information security for a specific organization.	4
	D1.S1.3 Reading and judging of a strategy for information security.	4
	D1.S1.4 Presenting and explaining of a strategy for information security.	4
	D1.S1.5 Creating a business case for parts of information security	4

References

[1] (ISC)² (2021) Cybersecurity Workforce Study 2021: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

[2] European Cyber Security Organisation (2018), « Gaps in Education & Professional Training », https://ecs-org.eu/documents/publications/5fdb282a4dcbd.pdf

[3] European Cyber Security Body of Knowledge (2019): https://www.cybok.org/

[4] Rathod, P. (2019). Towards European Cyber security Professional Work-force Development Framework– successful practices and outcomes of the European Case, APWG EU Symposium on Electronic Crime Research (eCrime 2019 EU), Barcelona, Spain

[5] EU Security Union Strategy: connecting the dots in a new security ecosystem (2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379

[6] Ponemon Institute (2021), Cost of a Data Breach Report, https://www.ibm.com/security/data-breach

[7] Rathod, P. and Hämäläinen, T., (2017) A Novel Model for Cyber security Economics and Analysis. In IEEE Inter-national Conference on Computer and Information Technology (CIT) (pp. 274-279). IEEE.

[8] European Union Agency for Cybersecurity (2020), Cybersecurity Skills Development in the EU, https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

[9] European Commission's Joint Research Centre (2019), A Proposal for a European Cybersecurity Taxonomy, https://publications.jrc.ec.europa.eu/repository/handle/JRC118089

[10] Rathod, P., Kämppi, P. (2020). Cybersecurity Workforce Capacity Building: a case of specialisation studies within the undergraduate programme. In ICCWS 2020 15th International Conference on Cyber Warfare and Security. USA, AC and publishing limited.

[11] Armstrong, P. (2010), Bloom's Taxonomy. Vanderbilt University Center for Teaching, https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/

[12] European e-Competence Framework, https://www.ecompetences.eu

[13] EU Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[14] Cybersecurity Education Curricula 2017 (CSEC 2017) : http://csec2017.org

[15] Cyber Education Project (CEP) : http://cybereducationproject.org/about/

[16] Anderson, L. W., & Krathwohl, D. R. (2001). A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives. New York: Longman

[17] Curricula Recommendations. Association for Computing Machinery (ACM). Retrieved from http://acm.org/education/curriculum-recommendations

[18] Cybersecurity curriculum 2017: curriculum guidelines for undergraduate degree programs in cybersecurity. Technical report Draft version 0.5, ACM Joint Task Force on Cybersecurity Education (2017). http://www.csec2017.org/csec2017-v-0-5

[19] Lehto, M. (2018). Cyber Security Education and Research in the Finland's Universities and Universities of Applied Sciences. In Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications (pp. 248-267). IGI Global.

[20] National Initiative for Cybersecurity Education, National Cybersecurity Workforce Framework, ver. 2.0, https://www.nist.gov/file/359261

[21] Parrish, A., Impagliazzo, J., Raj, R. K., Santos, H., Asghar, M. R., Jøsang, A., ... & Stavrou, E. (2018, July). Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. In Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (pp. 36-54).

[22]Rathod, P., Kämppi, P. (2020). Applying LEAN Principles to Improve Introductory Cybersecurity Online Subject: Findings from the Pilot Study. In SITE 2020 10th International Conference on Society for Information Technology & Teacher Education. USA, Association for the Advancement of Computing in Education (AACE).

[23] M. Spruit and F. van Noord, “Job profiles for information security 2.0”, Dutch Association of Information Security Professionals (PvIB), version 2.0, 2017

[24] European Cyber Security Organisation (2020), Understanding Cyber Ranges: from Hype to Reality, https://ecs-org.eu/documents/publications/5fdb291cdf5e7.pdf

[25] European Cybersecurity Agency ENISA (2020), “Cybersecurity Skills Development in the EU”, https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

[26] European Cybersecurity Agency ENISA (2021), “Addressing Skills Shortage and Gap through Higher Education”, https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education

[27] European Union Joint Research Centre (2017, “DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use”, https://publications.jrc.ec.europa.eu/repository/handle/JRC106281

ACKNOWLEDGEMENT

The European Cybersecurity Organisation's (ECSO) WG5 aims to contribute towards a cybersecurity capability and capacity-building effort for a cyber resilient next generation (NextGen) digital Europe, through increased education, professional training, skills development, as well as actions on awareness-raising, expertise-building and gender inclusiveness. This development work has been conducted with partners from across Europe including industry, working-life practitioners, academia, researchers and scholars. Overall, ECSO has around 270 EU members, with at least 150 member organisations and 300 individual experts contributing to WG5.

The following is a special acknowledgement of the active contributions in various capacities from ECSO WG5 members.

EXPERT CONTRIBUTIONS:
SWG 5.2 co-chairs: Marcello Hinxman-Allegri (Silensec, Italy), Paresh Rathod (Laurea University of Applied Sciences, Finland), Carmel Somers (ICT Skillnet, Ireland)
WG5 colleagues: Antonio Alvarez (Atos, Spain), Giorgio Giacinto (CINI, Italy), Dr. Tero Kokkonen (JAMK, Finland), Olaf Maennel (TTU, Estonia), Donato Malerba (UNIBA, Italy), Sanjana Mehta (ISC², UK), Prof. Isabel Praça (ISEP, Portugal), Kari Rannikko (CybExer, Estonia), Jan Wessels (Rabobank, Netherlands), and WG5 members

EDITOR AND PRIMARY AUTHORS
Paresh Rathod, Co-chair ECSO WG5 (Laurea University of Applied Sciences, Finland)

HEAD OF SECTOR AND FACILITATOR:
Nina Olesen (ECSO, Brussels). @ ECSO WG5 has the right to update, edit or delete the paper and any of its contents as the field of cybersecurity is evolving all the time.

REVISIONS MADE IN VERSION 2 (MAY 2022):
Correction of typos, formatting, and (minor) wording throughout document
Updating of figures/statistics
Addition of Section 3.4 Minimum knowledge, skills and competence requirements
Adjustment of titles and headlines in course descriptions
Addition of ISC² certifications in course descriptions

ECS
EUROPEAN CYBER SECURITY ORGANISATION

> JOIN ECSO

29, RUE DUCALE - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE : WWW.ECS-ORG.EU