Co-funded by the European Union

Project Nr. 2023-1-AT01-KA220-SCH-000166888

EnCycLEd

Enhancing Cybersecurity Literacy in Education

Cybersecurity Careers and Study Pathways Guide

21 March 2025

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

EnCycLEd

Co-funded by the European Union

PROJECT'S COORDINATOR

Leopold-Franzens-Universität
Innsbruck

www.uibk.ac.at

PROJECT'S PARTNERS

University of Macedonia
Greece

www.uom.gr

Ruprecht-Karls-Universität
Heidelberg

www.uni-heidelberg.de

SET University
Ukraine

www.setuniversity.tech

KVS
Ukraine

pkvfp.ki_ev.ua

American Farm School
Greece

www.afs.edu. gr

ASCEND Consulting
Malta

ascendconsulting.eu

Ukrainian Academy of Cyber Security
Ukraine

https://uacs.kiev.ua/

REACH Innovation
Austria

www.reach-innovation.eu

TABLE OF CONTENTS

ABOUT THE PROJECT 3

INTRODUCTION 4

Target audience groups 4
Content structure and recommended delivery 5

1. THE IMPORTANCE OF CYBERSECURITY AND ITS CURRENT SITUATION AS AN ECONOMIC SECTOR 7

1.1 Fast growing sector cross-cutting the digital economy 8
1.2 Significant skill gaps and workforce shortages 9
1.3 Female underrepresentation and consequences 11
1.4 Limited public awareness of cybersecurity as a career opportunity 12

2. OVERVIEW OF VARIOUS PROFESSIONAL ROLES AND PROFILES IN CYBERSECURITY 14

2.1 The 12 professional profiles envisaged by the European Cybersecurity Skills Framework 14
2.2 Other international frameworks structuring cybersecurity roles and their skills requirements 16

3. OVERVIEW OF VARIOUS CYBERSECURITY EDUCATION AND TRAINING OPPORTUNITIES 18

3.1 Higher Education Academic Programs 18
3.2 Professional Trainings 21
3.3 Certification schemes 23
3.4 Various online courses and training materials 27

4. TOOLS FOR CHARTING STUDY AND CAREER PATHWAYS 30

4.1 REWIRE tools focused on the European context 30
4.2 Tools focused on the American context 35
4.3 Others 38

5. CYBERSECURITY PROFESSIONALS IN PRACTICE 39

Maltese role models 39
Austrian role models 44
Ukrainian role models 47
Greek role models 51
German role models 53

6. COUNTRY SPECIFIC CYBERSECURITY OPPORTUNITIES 54

6.1 GERMANY 54

Co-funded by the European Union

6.2 AUSTRIA 63
6.3 GREECE 74
6.4 UKRAINE 78
6.5 MALTA 88
7. SPECIFIC OPPORTUNITIES FOR GIRLS 94
8. OTHER RELEVANT EUROPEAN TOOLS AND INITIATIVES FACILITATING CYBERSECURITY STUDIES AND CAREERS 96
9. SOME SECTOR SPECIFIC CYBERSECURITY CHALLENGES AND OPPORTUNITIES RELEVANT TO VET 101
9.1 HEALTHCARE 101
9.2 BUILT ENVIRONMENT.....105
9.3 ENERGY 108
9.4 TRANSPORTATION 111
9.5 AGRO-FOOD 112
9.6 EDUCATION.....112
10. SPECIFIC GUIDANCE FOR THE SCHOOL COMMUNITY 117

Co-funded by the European Union

ABOUT THE PROJECT

The EnCycLEd Erasmus+ Project aims to promote digital readiness in cybersecurity, resilience, and capacity-building in educational institutions. To achieve this, the project will promote cybersecurity literacy and awareness. It focuses on training students, schoolteachers and other teaching professions to develop key digital skills and competences.

Special focus is given to promote interconnected educational systems in Europe with cybersecurity awareness and training at High Schools, Vocational Schools, as well as at university courses, especially the ones related to the formation of future teachers. The project results are planned to go beyond the project's educational partners, taking effect also via interactions with the vast existing network of associated institutions of the partners.

The EnCycLEd consortium benefits from the diverse and profound experience of higher education partners, professional schools and associations in the topic areas of cybersecurity and didactics. The project counts with cybersecurity expertise coming from European Universities (UIBK in Austria and HU in Germany) and from a cybersecurity association (UACS in Ukraine), supported by two other Universities (UoM in Greece and SET Univ. in Ukraine) to develop and test the training materials and school curricula. Two project partners (AC in Malta and REACH in Austria) will respectively cater for the development of the project's digital platform and the project’s dissemination and network-building. EnCycLEd will devote main efforts on interacting and piloting its developments in cooperation with two European Schools (in Greece and in Austria) and with two Ukrainian educational institutions (a University dedicated to the formation of teachers and a Vocational School).

Co-funded by the European Union

INTRODUCTION

This Cybersecurity Careers and Study Pathways Guide is one of the EnCycLEd project main outputs. By highlighting cybersecurity studies and careers, the aim of this Guide is to contribute to increasing school teachers', students' and even their parents' awareness of cybersecurity opportunities, and to increase readiness and resilience to cyberattacks in general.

Discussions with various stakeholders in the cybersecurity ecosystem indicate that the overall interest in cybersecurity studies and careers is rather limited. One of the main caused for this is considered to be the insufficient awareness among students, teachers, career counsellors and parents about

- the wide scope and breadth of cybersecurity careers, as well as
- the high and ever increasing negative impacts of cyberattacks in both economic and social terms, at individual, organisational and community levels.

The increasing hybrid nature of cyberattacks, exploiting both technical issues and people's emotional states and reactions (at individual, group and societal levels) is calling for an even wider scope of educational and professional backgrounds in the cybersecurity workforce of tomorrow. Professionals with a technical ICT and engineering background need to be complemented by others with educational background in legal, regulatory, forensic, psychology, sociology, human dynamics and communications, organisational behaviour, risk and mitigation, crisis, project and general management.

Target audience groups

The specific audiences for this Guide includes:

- career counsellors and teachers - as first and direct users;
- students, and their parents – as second and third level users, preferably through the intermediation of the first user group;

Co-funded by the European Union

at secondary and high-school levels, including in vocational education and training (VET).

From a geographic perspective we focus on providing guidance relevant to our target audiences in

- the project partner countries in particular, that is Austria, Germany, Greece, Malta and Ukraine, but also to others in
- Europe in general.

Content structure and recommended delivery

The scope of this Guide is wide, as is the cybersecurity field and the range of audiences it targets. Therefore, its content has been structured and packaged in a **modular** manner, along **10 sections that can serve as separate guides for specific audience groups**. For example, audiences in Germany versus those in Malta or Greece or Ukraine; female students and their parents; students and teachers in VET.

This Guide is also mainly addressed to career counsellors and teachers, who are best placed to further explain and guide the students, and even their parents, through its content. One or more sessions with students, and separately with parents, could be organised to:

1. Introduce them to the importance of cybersecurity and current situation in this economic sector.

2. Provide an overview of the main professional roles and profiled in cybersecurity.

3. Provide an overview of the various cybersecurity education and training opportunities available across Europe and beyond.

4.Explain a number of online tools available for charting study and career pathways in cybersecurity.

Co-funded by the European Union

5. Highlight a number of cybersecurity professionals from all project partner countries (Austria, Germany, Greece, Malta, Ukraine) that can serve as role models. Discussing their study paths and career progression to date can inspire and guide students to consider cybersecurity careers.

6. Explain the country specific educational and career opportunities in cybersecurity available in Austria, Germany, Greece, Malta and Ukraine.

7. Highlight specific opportunities for girls to enter into cybersecurity.

8. Explain a number of other European tools and initiatives that facilitate cybersecurity studies and careers, from studies accreditation to job search.

9. Explore cybersecurity challenges and opportunities specific in particular sectors like healthcare, transport, energy, built environment, agri-food, education, sectors that very relevant to occupations developed through vocational education and training (VET).

This Guide also provides in section 10 further specific guidance to the overall school community, including teachers, career counsellors and other education staff. This relates to how they could, and should, better engage with students, parents and industry so as to increase their resilience to cyber threats and interest in exploring studies and careers in cybersecurity, regardless of gender, predilection for ICT and special abilities of students.

Co-funded by the European Union

1. THE IMPORTANCE OF CYBERSECURITY AND ITS CURRENT SITUATION AS AN ECONOMIC SECTOR

The more digital processes are embedded in everyday, educational and professional life, the greater the volume and criticality of the information being exchanged. This fact brings the issue of cybersecurity to the center of the frame. In the early years of the digital age, internet security was mostly confined to antivirus protection. Nowadays, internet security has many more dimensions and is associated with the security of information sources, the security of information being stored, the protection of personal data and the protection of the hardware of devices. From the aforementioned it is obvious that Cybersecurity is now a topic that has a wide range of fields and depth of scientific knowledge. Therefore, the issue of training specialized labour and scientific personnel arises and, consequently, the need to provide guidance on study and career pathways arises.

In this context, this section,

a) examines the expanding role of cybersecurity in the economy and society;

b) analyses the state of cybersecurity as a fast-growing sector;

c) highlights the significant skills and workforce deficiencies;

d) outlines the gender inequalities in the sector; and

e) stresses the need for awareness of the fact that cybersecurity is turning from a problem to be solved into a career opportunity.

In this first approach to the issue, it should not be overlooked that as digital technology and communication become part of the family, personal and educational life of young people, aged 10-18, especially during the Covid-19 and post-Covid-19 era, the need for systematic and professional protection of young people in cybersecurity issues also increases.

Co-funded by the European Union

1.1 Fast growing sector cross-cutting the digital economy

Looking at the economy and its various sectors, we can see a long list of continuously increasing use of digital technologies, communication, information and data circulation within and across all economic sectors. In 2020, the digital economy already represented 22.5% of the world economy[1].

With the Covid-19 pandemic crisis and the travel restrictions that ensued in 2020-2022 period, the need to work and study remotely that it brought, digital internet technology has been an area of ever increasing growth. In turn, this further increased the need for cybersecurity, not just in organisational but also in personal environments, and not just in specific economic sectors but in all.

Another parameter that increased the need for cybersecurity in data acquisition and management is the Internet of Things (IoT) deployment of smart devices and facilities that generate and transfer data to manage systems. In this case, security in the cyber space involves both the secure flow of information and the secure storage of data that is often personal or corporate property.

The need for environmentally friendly practices with a low environmental footprint and the ability of expanding many services into a digital form for improved accessibility is another key factor in the rapid development of smart IoT systems, and along with it the need for their secure operation.

In this context, the global cybersecurity market size is projected to grow from $193.73 billion in 2024 to $562.72 billion by 2032, at a Compound Annual Growth Rate (CAGR) of 14.3% over this period[2].

Moreover, the socio-economic impacts of cyberattacks are significant, and many are done exactly for such reason. A basic categorisation of cyber threats

[1] Accenture - Abbosh, O. & Bissell, K. 2019. https://www.accenture.com/us-en/insights/cybersecurity/reinventing-the-internet-digital-economy
[2] Fortune Business Insights – Cybersecurity Market Size, Share and Industry Analysis 2025 https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

Co-funded by the European Union

that share economic exploitation of cyberattack targets as a key element, includes:

- Threats to individuals, like:
  a) The "stealing" or "capture" of data for commercial transactions and purchases, not only in e-commerce but also in conventional commerce.
  b) Access to bank accounts for direct illegal withdrawal of funds.

- Threats to businesses:
  a) Attacks to intercept data, information and data that constitute intellectual property.
  b) Ransomware attacks, where hackers block the operation of systems and data storage spaces and demand a fee for unblocking the operation of corporate systems. These threats often also target national systems or government agencies.

- Threats to national systems: Cyber-attacks on government organisations, energy, health or transportation infrastructures and systems are aimed at
  a) intercepting important information and
  b) provoking acts of sabotage or demonstrating power in the sense of "terrorist" attacks.

1.2 Significant skill gaps and workforce shortages

Expectedly, the cybersecurity sector, with its rapidly increasing needs, has struggled to be captured as a niche and specialty occupation in the labour market mapping. Job descriptions in company organisational charts have not yet been well established. More importantly, a structured curriculum and training programme of what the job of a cybersecurity manager or technologist entails has not yet been developed. This is precisely the turning point we are at, with the prospect of better understanding and charting Cybersecurity Studies and Career Pathways now before us, opening up a new perspective on this issue.

Co-funded by the European Union

The opportunity to enter into this fast developing sector is surely significant. In 2022, the global shortage of cybersecurity experts was of 3.4 million, having increased from of 2.7 million people in 2021[3], with the 63% of the respondents to the ISC2 Cybersecurity Workforce Study claiming to have unfilled cybersecurity positions (up from 55% in the previous year). Only in Europe, the shortage of cybersecurity professionals was estimated at 260,000 in 2022, a 57% increase over 2021[4]. This study also found that although having an ICT background is still the most common pathway into cybersecurity, more than 50% of cybersecurity professionals entered the field from outside of ICT. For example, 15% of respondents said that they studied cybersecurity concepts on their own.

A study carried out by the Enterprise Strategy Group (ESG) and the Information Systems Security Association (ISSA) found out that there is a variety of factors that affect the cybersecurity skills gap, among them, the lack of a well-defined career path in cybersecurity for students.

According to the European Commission, 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.

Looking at the World Economic Forum's Global Cybersecurity Outlook report, published in January 2024, the impact the skills gap has on businesses is alarming. 36% of respondents list the skills gaps as the main challenge to achieving their cyber-resilience goals.

[3] State of Cybersecurity 2022 ISACA Report https://www.isaca.org/resources/reports/state-of-cybersecurity-2022

[4] ISC2 Cybersecurity Workforce Study 2022 https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf

Co-funded by the European Union

In the 2024 Eurobarometer on Cyber Skills[5], 45% of companies surveyed cited difficulty in finding qualified candidates as one of the main challenges in recruiting staff with the right cybersecurity skills. The survey also found that 76% of employees in cybersecurity-related roles do not have any formal qualifications or certified trainings, 34% entered the role from a non-cyber related role, while 57% absorbed the cybersecurity responsibilities into an existing role.

1.3 Female underrepresentation and consequences

Although the work environment and job descriptions do not typically include specific requirements that would justify differential representation of women in cybersecurity positions, globally only 20% to 25% of positions was occupied by women in 2023[6].

Recent research carried out by the European Union Agency for Cybersecurity ENISA[7] also indicates that only 18% of graduates and 20% of students enrolled in cybersecurity-related programs in Europe in 2020 were women.

According to the May 2024 Eurobarometer on CyberSkills, 70% of those surveyed agree that diversity and inclusion in cybersecurity are important in their respective companies. Moreover, about 66% agree that women are encouraged to take up roles and tasks in cybersecurity, but 56% of respondent companies do not have any women in cybersecurity roles.

This underrepresentation of women has two implications:

- A reduction in the input that could foster innovation in cybersecurity and

[5] https://europa.eu/eurobarometer/surveys/detail/3176
[6] ISC2 Cybersecurity Workforce Survey 2023 and Women in Cybersecurity Report https://www.isc2.org/Insights/2024/04/Women-in-Cybersecurity-Report-Inclusion-Advancement-Pay-Equity
[7] ENISA Report - Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education, 2021 https://op.europa.eu/en/publication-detail/-/publication/599fbec7-71c5-11ec-9136-01aa75ed71a1

Co-funded by the European Union

- The limitation of career-building opportunities for women in a workplace that is - otherwise - friendly and compatible for them.

Gender inequality has implications on the quality of the workforce, substantially limiting the pool of talent and skills. Finally, the underrepresentation of women in cybersecurity positions reinforces the perception and stereotype of the sector as a male-dominated field, discouraging younger women from considering cybersecurity as a viable career option.

1.4 Limited public awareness of cybersecurity as a career opportunity

While the need for cybersecurity services is constantly increasing, it is rarely being referred to as a career option by career advisors. The fact that the cybersecurity manager position is not included in the career guidance agenda does not contribute to these jobs becoming a trend in young people's choices.

This is further contributed to by the common social stereotypical belief that all cybersecurity professionals must have specialized and high-level IT and programming knowledge. There is the technical part to a cybersecurity job, but that is not the only dimension.

In reality cybersecurity work is equally about risk identification and assessment, defining and following protocols, communication and consulting, understanding of people psychology and groups dynamics (sociology), of the specific in diverse application sectors, from health and education to banking and infrastructure. All these skills and competences need to be developed and brought together, often not within one professional but within a team of cybersecurity experts.

Moreover, cybersecurity knowledge is increasingly expected from any potential employee, and thus everyone should have at least some basic knowledge and understanding of cybersecurity. Higher abilities in this area are in turn representing an asset when starting or advancing your career.

Co-funded by the European Union

Finally, the absence of cybersecurity topics in the typical curricula of secondary, high school and vocational education and training prevents pupils and students from making such a choice. This diminishes the pool of human resources and does not encourage such a choice.

This raises the need to organise information events and campaigns for parents and teachers to understand the new needs and requirements of the modern working environment which is an option for the new generation when entering the labour market.

Co-funded by the European Union

2. OVERVIEW OF VARIOUS PROFESSIONAL ROLES AND PROFILES IN CYBERSECURITY

The field of cybersecurity encompasses a diverse range of specialized roles, each addressing distinct aspects of safeguarding digital assets and ensuring the resilience of information systems. As cyber threats continue to evolve, organizations require professionals with varied expertise to address strategic, operational, legal, and educational needs within cybersecurity.

2.1 The 12 professional profiles envisaged by the European Cybersecurity Skills Framework

The European Cybersecurity Skills Framework (ECSF)[8], developed by **ENISA**, defines **12 professional roles** in cybersecurity, each with specific competencies and skills essential to the field:

1. **Chief Information Security Officer (CISO)**: Oversees an organization's cybersecurity strategy, aligning it with business objectives to ensure robust protection of digital systems, services, and assets. The CISO is responsible for strategic planning, policy formation, resource allocation, and communication with executive management.
2. **Cyber Incident Responder**: This role manages the organization's response to cybersecurity incidents, monitoring systems, and ensuring continued operations during attacks. It involves analyzing incidents, mitigating impacts, and restoring functionality according to the organization's incident response plan.
3. **Cyber Legal, Policy, and Compliance Officer**: This role ensures compliance with cybersecurity regulations, policies, and legal standards. It is crucial for managing data protection and privacy

[8] https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

Co-funded by the European Union

policies, providing legal guidance, and ensuring adherence to cybersecurity standards.

4. **Cyber Threat Intelligence Specialist**: This person gathers, processes, and analyzes threat data to produce actionable intelligence. They monitor threat tactics, techniques, and patterns, supporting defensive strategies and sharing insights with relevant stakeholders.
5. **Cybersecurity Architect**: This person designs secure infrastructure and systems, applying security-by-design principles. The cybersecurity architect develops architecture models, specifies cybersecurity controls, and ensures systems meet security and privacy requirements.
6. **Cybersecurity Auditor**: This person conducts audits to assess the effectiveness of an organization's security policies, controls, and procedures. They verify compliance with standards, identify improvements, and document audit findings.
7. **Cybersecurity Educator**: This person develops cybersecurity knowledge and skills within the organization by providing training and resources. The educator designs curricula and supports continuous learning in cybersecurity best practices.
8. **Cybersecurity Implementer**: This role focuses on deploying and managing cybersecurity solutions, including systems, software, and controls. It ensures that cybersecurity measures are operational and responsive to threats.
9. **Cybersecurity Researcher**: Investigates emerging cybersecurity threats, technologies, and vulnerabilities to support innovative security measures and enhance resilience against cyber risks.
10. **Cybersecurity Risk Manager**: This position manages cybersecurity-related risks aligned with organizational strategies. Responsibilities include assessing vulnerabilities, developing risk policies, and conducting ongoing risk assessments.

Co-funded by the European Union

11. **Digital Forensics Investigators analyze** digital evidence from cyber incidents to support investigations and legal proceedings. Their work is crucial in understanding incident causes and documenting cases for prosecution.
12. **Penetration Tester**: This person simulates cyberattacks to test the effectiveness of security controls and identify vulnerabilities that could be exploited. Penetration testers play a proactive role in strengthening organizational defenses.

These roles cover cybersecurity's strategic, operational, and educational aspects, creating a comprehensive workforce to address diverse cybersecurity needs and mitigate risks effectively.

2.2 Other international frameworks structuring cybersecurity roles and their skills requirements

The **NICE (National Initiative for Cybersecurity Education) Framework** by NIST, widely used in the United States, provides a structured approach to organizing cybersecurity roles and competencies. It categorizes cybersecurity functions across seven broad areas: **Analyze**, **Collect and Operate**, **Investigate**, **Operate and Maintain**, **Oversee and Govern**, **Protect and Defend**, and **Securely Provision**. Each category breaks down into specific **Work Roles** and associated **Tasks, Knowledge, and Skills (TKS)**, which define the capabilities required to perform effectively in these domains. The NICE Framework's competency-based structure, with a strong focus on supporting career planning, aims to create a common language and shared understanding among organizations, professionals, and educators, supporting workforce development and training programs.

Co-funded by the European Union

The NICE Framework aligns well with the ECSF[9], which similarly organizes cybersecurity roles and competencies, though it is primarily focused on harmonizing skills across the EU. Both frameworks strive to bridge the skills gap in cybersecurity by providing structured, adaptable pathways for training and upskilling. However, while ECSF is tailored to the EU's regulatory environment, NICE's global reach makes it widely applicable in educational and professional contexts beyond the U.S.

The Cyber Career Framework (CCF)[i] in the UK, developed by the UK Cyber Security Council, is a comprehensive structure designed to outline career pathways in cybersecurity. It covers 16 specialisms, detailing key aspects of each role, such as responsibilities, typical work environment, expected salary range, required knowledge and skills, and options for career progression, whether moving up the ladder or shifting laterally within the field. The framework also specifies the qualifications needed for each role, providing clarity for individuals at all career stages.

As part of its efforts, the Council introduced an interactive **Career Mapping Tool** in 2024. This tool helps candidates, including those outside the cybersecurity sector, identify transferable skills and explore compatible roles within cybersecurity. By highlighting potential pathways, the tool aims to attract diverse talent from various sectors into cybersecurity careers.

The framework is being implemented in parallel with the **Cyber Security Profession Chartered Standards (CSPCS)**, which will establish three certification levels—Associate, Principal, and Chartered—within each of the 16 specialisms. This ambitious overhaul seeks to formalize and elevate cybersecurity career standards across the UK, with full implementation expected by 2025.

[9]https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

Co-funded by the European Union

3. OVERVIEW OF VARIOUS CYBERSECURITY EDUCATION AND TRAINING OPPORTUNITIES

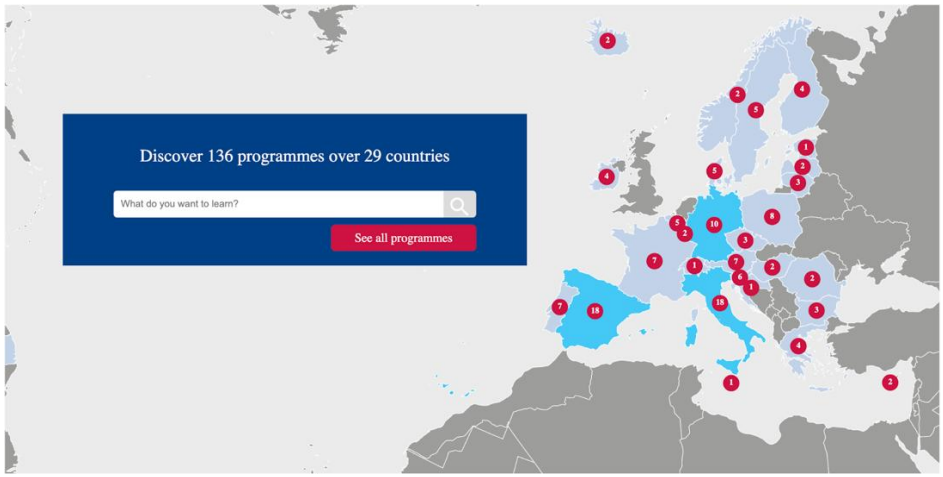
In today's digital landscape, cybersecurity education and training are paramount for developing a skilled workforce capable of defending against evolving cyber threats. This chapter explores the diverse avenues available for individuals and organizations to enhance their cybersecurity competencies, focusing on higher education academic programs, professional training courses, and certification schemes.

3.1 Higher Education Academic Programs

Higher education institutions across Europe offer a multitude of cybersecurity programs aimed at cultivating the next generation of cybersecurity professionals. Several platforms and initiatives have been established to map and promote these educational opportunities.

The European Union Agency for Cybersecurity (ENISA) maintains the Cybersecurity Higher Education Database (CyberHEAD), which is the largest validated cybersecurity higher education database in the EU and EFTA countries. This resource serves as a main point of reference for individuals seeking to start an academic journey in the cybersecurity field, allowing them to make informed decisions about higher education opportunities in cybersecurity.

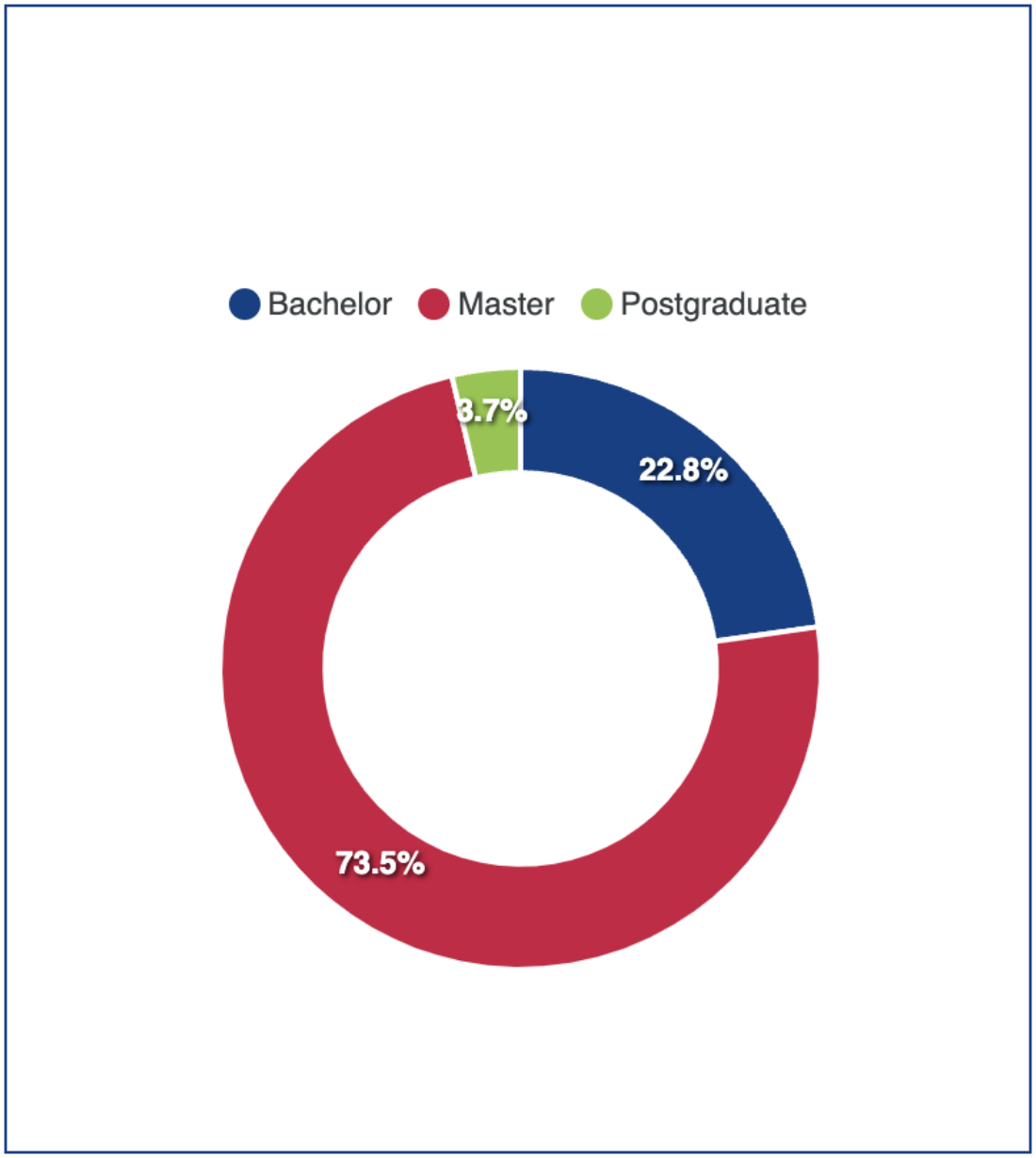
CyberHEAD provides an interactive map of cybersecurity programs in Europe.



Source: CyberHEAD screenshot

Co-funded by the European Union

As of March 2025, the map covers 136 cybersecurity programs across 29 countries. These include 100 Master degree programs, 32 Bachelor degree programs, and 5 postgraduate programs.



Source: CyberHEAD screenshot

Countries with higher concentrations of programs include Italy (18 programs), Spain (18), and Germany (10), suggesting that these countries have well-established cybersecurity education infrastructures. The search bar and the "See all programs" button allow users to explore these programs interactively based on specific learning interests.

The programs listed in CyberHEAD are linked to the 12 role profiles presented in the European Cybersecurity Skills Framework (ECSF), helping students to find a suitable path for their dream careers.

Notably, many programs offer specialized instruction and educational materials designed to support the attainment of professional certifications. Information on specific programs that include certification preparation can be found in the program description under "Preparation for Professional Certification". Additionally, individuals can search by keywords to identify programs linked to their desired certification, e.g. CISSP or CEH.

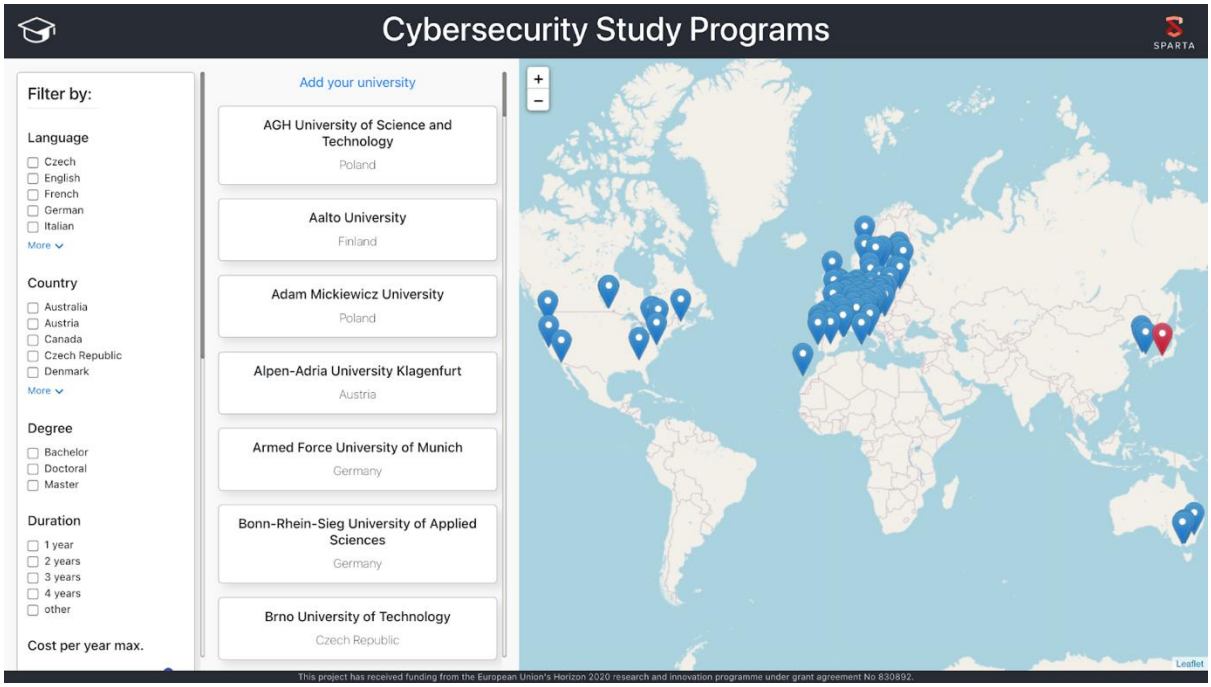
It is recommended to watch this short video to see how CyberHEAD can assist degree-seekers in selecting the academic program that aligns with their interests and aspirations.

Building on this effort to structure and standardize cybersecurity education, several complementary initiatives have been launched. For instance, the CyberSec4Europe project introduced the Cybersecurity MSc Education Survey Map. This interactive tool showcases cybersecurity master's programs across Europe.

Source: Cybersec4Europe screenshot

Co-funded by the European Union

Unlike CyberHEAD and CyberSec4Europe, which focus on mapping and structuring cybersecurity education in Europe, the EU-funded SPARTA project takes a broader perspective, providing a detailed analysis of more than 80 higher education Cybersecurity Study Programs worldwide. SPARTA's Education Map is available here.



Source: SPARTA screenshot

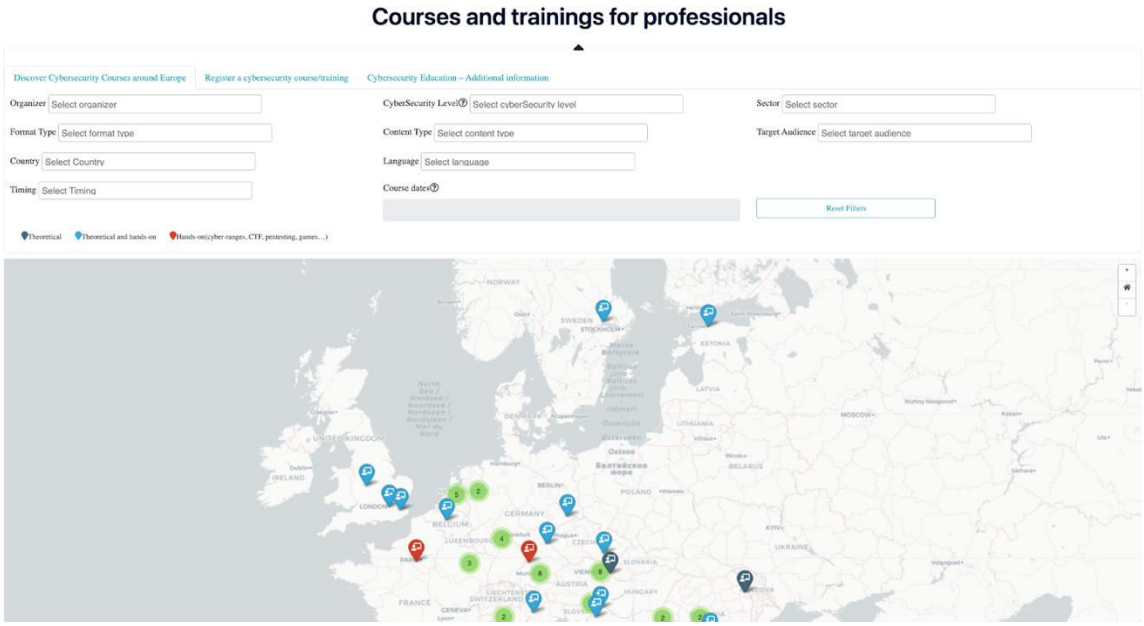
CyberHEAD, CyberSec4Europe, and SPARTA help students, researchers, and professionals explore specialized academic opportunities in cybersecurity, identifying higher education study programs that align with their career and learning objectives.

3.2 Professional Trainings

As cyber threats continue to evolve, professional training programs play a crucial role in equipping individuals with up-to-date skills and knowledge to protect organizations, critical infrastructure, and digital ecosystems. In addition to university-based cybersecurity education, short-term training programs and hands-on courses have become essential for cybersecurity professionals, students, and researchers seeking to develop practical expertise or specialize in niche areas.

One of the key resources supporting professional cybersecurity training in Europe is the [CONCORDIA map of cybersecurity courses and trainings].

CONCORDIA, an EU-funded multi-disciplinary research and innovation project in cybersecurity, launched an interactive map displaying short courses and training programs for cybersecurity professionals across Europe. This map complements the ENISA CyberHEAD database, which primarily focuses on university-related degree programs. By structuring a diverse range of cybersecurity courses and training opportunities in a single, accessible platform, CONCORDIA contributes to the development of a European Education Ecosystem for Cybersecurity, helping professionals and students find tailored cybersecurity opportunities that align with their career and educational goals.



Source: CONCORDIA screenshot

Some key features of the CONCORDIA map include:

- **Targeted training for different audiences**. The platform allows users to filter courses and trainings based on their background and objectives, ensuring students, recent graduates, freelancers, and academic researchers can find relevant cybersecurity training.

Co-funded by the European Union

- **Sector-specific cybersecurity training**. The map categorizes courses by industry focus, including finance, healthcare, telecom, defense, and transportation, allowing professionals to acquire cybersecurity knowledge relevant to their fields.
- **Flexible learning formats**. Courses and trainings are available in various formats, including:
    - **Theoretical only** – focused on conceptual cybersecurity knowledge, regulations, and frameworks.
    - **Hands-on (cyber ranges, CTF, pentesting, games, etc.)** – interactive courses featuring real-world cybersecurity challenges, including capture-the-flag (CTF) competitions, penetration testing labs, and simulated cyber-attacks.
    - **Theoretical and hands-on** – a combination of lectures and practical exercises to reinforce cybersecurity skills.
- **Skill-specific training**. The map enables learners to search for programs based on cybersecurity specialization, such as device security, network security, software security, data protection, and user-centric security.

To explore additional cybersecurity training opportunities, visit the Training section of the Digital Skills & Jobs Platform.

3.3 Certification schemes

In the rapidly evolving field of cybersecurity, professional certifications play a critical role in validating expertise, enhancing career opportunities, and ensuring industry-standard knowledge. Various internationally recognized organizations provide cybersecurity certifications tailored to different levels of experience, specializations, and industry needs:

Co-funded by the European Union

1. **C3 by CONCORDIA**. The C3 by CONCORDIA certification is designed for European cybersecurity professionals, managers, and freelancers seeking to validate their expertise. The certification covers core knowledge and skills essential for a Cybersecurity Consultant, enabling professionals to apply best practices across industries.
2. **ISC² – International Information System Security Certification Consortium.** ISC² offers some of the most recognized cybersecurity certifications globally, catering to professionals at different stages of their careers. Examples include:

- **CISSP (Certified Information Systems Security Professional)**. One of the most prestigious certifications, focusing on risk management, security architecture, and governance.
- **CCSP (Certified Cloud Security Professional)**. Specializes in cloud security operations and compliance.
- **CSSLP (Certified Secure Software Lifecycle Professional)**. Focuses on secure software development.

3. **ISACA – Cybersecurity Certifications.** ISACA's certifications are designed for professionals involved in IT security governance, risk management, and cybersecurity assurance, e.g.:
    - **CISA (Certified Information Systems Auditor).** Industry-standard for IT auditing, compliance, and risk assessment.
    - **CISM (Certified Information Security Manager).** Designed for professionals managing enterprise security programs, ideal for those seeking senior cybersecurity roles.
    - **CRISC (Certified in Risk and Information Systems Control).** Focuses on IT risk management and security controls, enhancing credibility in cyber risk and compliance.

Co-funded by the European Union

4. CompTIA Cybersecurity Certifications. CompTIA offer industry-recognized certifications, supporting professionals across various cybersecurity roles, including:

- **CompTIA Security+.** A foundational certification covering essential cybersecurity principles and best practices.
- **CompTIA Cybersecurity Analyst CySA+**. Focuses on behavior analytics and threat detection.
- **CompTIA Advanced Security Practitioner CASP+.** Designed for advanced security practitioners managing enterprise security.

5. GIAC (Global Information Assurance Certification). GIAC provides more than 30 cybersecurity certifications covering security administration, management, legal, audit, forensics, and software security. Each certification independently validates an individual's expertise in a specific area (e.g. Offensive Operations, Cyber Defense, Cloud Security, Industrial Control Systems, Digital Forensics & Incident Response, Cybersecurity Leadership), demonstrating mastery of essential cybersecurity skills and knowledge. GIAC certifications include:

- **GIAC Security Essentials (GSEC).** Covers fundamental cybersecurity concepts.
- **GIAC Certified Incident Handler (GCIH)**. Specializes in responding to cybersecurity incidents.
- **GIAC Penetration Tester (GPEN)**. Focuses on ethical hacking and penetration testing.

Co-funded by the European Union

6. SANS Technology Institute – Cybersecurity Education Pathways. SANS offers structured training with certification opportunities for professionals entering the cybersecurity field. For instance, the Applied Cybersecurity Certificate (ACS) program provides essential cybersecurity skills and certifications for career changers and students, with training available online and at live events.

7. PECB (Professional Evaluation and Certification Board). PECB provides globally recognized ISO-standard cybersecurity certifications covering information security, cybersecurity management, technical cybersecurity, AI, privacy and data protection, compliance, and others. These cover, among others:

- **ISO/IEC 27002 – Information Security Controls**. Focuses on standards and best practices for implementing information security measures.
- **ISO/IEC 27033 – Network Security.** Covers designing and ensuring network security of devices, applications, services, and end users against cyber threats.
- **ISO 37301 Compliance Management System**. Emphasises regulatory adherence.

For a comprehensive overview of cybersecurity certification options, the **CyberABILITY platform** provides a structured search tool for professionals seeking recognized credentials in the field. The platform allows users to:

- Browse available certifications across various cybersecurity domains.
- Compare certification options based on industry standards, required skill levels, and areas of expertise.
- Identify career pathways by exploring how different certifications align with specific cybersecurity roles and responsibilities.
- Access relevant training programs that prepare candidates for certification exams.

Co-funded by the European Union

3.4 Various online courses and training materials

A wide range of online courses and training materials are available to support cybersecurity education at different skill levels. These resources provide learners with flexible, accessible, and industry-relevant knowledge to prepare for careers in cybersecurity.

Below is an overview of notable online cybersecurity materials and training programs, designed to support learners at different stages of their cybersecurity journey:

- **REWIRE Vocational Open Online Courses (VOOCs).** REWIRE offers a few targeted cybersecurity training courses aligned with the REWIRE Curricula and Training Framework. These courses enhance cybersecurity competencies at different levels, equipping professionals with the expertise needed for specialized roles:
    - The **Cyber Incident Responder course**, which trains IT and security professionals to manage cybersecurity incidents (**EQF level 6**).
    - The **Cyber Threat Intelligence Specialist course**, focusing on threat detection and analysis (**EQF level 3**).
    - The **Penetration Tester course**, providing hands-on skills inconducting conduct penetration tests independently and proficiently (**EQF level 4-5**).
    - The **CISO Training Program**, which prepares professionals for executive roles in cybersecurity management (**EQF level 7-8**).
- **European Cybersecurity Month (ECSM) resources.** The European Cybersecurity Month (ECSM) campaign offers educational materials, practical advice, and online safety tips for different user groups. The platform provides customized cybersecurity resources for children, seniors, and business users, helping them develop safer online behaviors and defend against cyber threats.
- **Cyber Security Coalition – cybersecurity awareness and training opportunities.** The Cyber Security Coalition offers awareness campaigns, cybersecurity tools, podcasts, webcasts, blogs, and other types of materials

Co-funded by the European Union

that provide individuals and businesses with practical cybersecurity insights and knowledge resources.

- **CyberPhish: Safeguarding against Phishing in the age of 4th Industrial Revolution.** The CyberPhish initiative is designed to enhance phishing awareness and prevention. It features an interactive training platform, where users can test their ability to detect phishing scams through realistic simulations. This project equips learners with practical skills to identify phishing and protect themselves from online threats.
- **CYBERWISER.eu – Trainings for organizations and individuals.** CYBERWISER.eu provides cybersecurity training for professionals and organizations, offering beginner-friendly and advanced courses. The PRIMER course is a free entry-level program covering basic cybersecurity concepts and risk analysis, while more advanced paid courses provide enhanced and hands-on cybersecurity training for businesses and professionals.
- **Cybersecurity Skills Academy.** It is a European policy initiative aimed at bridging the cybersecurity skills gap. It provides a centralized hub for cybersecurity knowledge and training, featuring information about:
    - Cyber skills training and initiatives, showcasing available training opportunities, initiatives, and organizations dedicated to developing cybersecurity skills.
    - National and EU cybersecurity campuses and academies, providing access to training opportunities offered by national and EU institutions.
    - Cybersecurity certifications and skills frameworks, offering insights into certification programs and structured frameworks for defining, providing, and evaluating cybersecurity skills.
- **INCO Academy.** The INCO Academy provides cybersecurity and digital skills training and certificates in a number of areas, such as data analytics (to obtain Google Data Analytics Certificate), cybersecurity (with the prospect of acquiring Google Cybersecurity Certificate), environmental and social impact of digital technology (to receive Green Digital Certificate), and others.

Co-funded by the European Union

- **Road2Cyber.** Road2Cyber is a career-focused cybersecurity training initiative, offering a catalogue of:
  - Comprehensive training programs, covering ransomware defense, identity management, secure DevOps infrastructure, and other areas.
  - Cybersecurity insights and resources, featuring market reports, expert articles, relevant portals and tools.
- **Youth4Cyber – European Cyber Security Organisation (ECSO) Initiative.** Youth4Cyber is a cybersecurity awareness initiative targeting young people aged 6 to 26. It delivers structured training modules that teach children about cyber hygiene and online safety, while guiding young adults through cybersecurity trends and career opportunities.
- **ENISA CyberEducation Platform.** The ENISA Cybersecurity Education Platform is a learning hub for educational resources, designed for primary and secondary students. This platform helps build cybersecurity awareness from an early age and equips students with fundamental digital security skills.

These online cybersecurity training programs offer diverse learning opportunities, from basic cyber hygiene awareness to advanced technical training for professionals. By leveraging these accessible educational resources, individuals and organizations can enhance their cybersecurity skills, improve digital resilience, and prepare for careers in cybersecurity. Many of these initiatives align with European cybersecurity strategies, ensuring high-quality training and support for the growing cybersecurity workforce.

Co-funded by the European Union

4. TOOLS FOR CHARTING STUDY AND CAREER PATHWAYS

With so many cybersecurity related courses, trainings and certification programmes available, one would surely wonder which of these are best suited towards undertaking a certain type of job, or role profile in this area.

Over the last years, a number of tools have been developed and are available to guide in this sense.

4.1 REWIRE tools focused on the European context

Part of the project REWIRE Cybersecurity Skills Alliance A New Vision for Europe funded by the European Union, a CyberABILITY Platform was developed, including specific tools like the Cybersecurity Profiler and Career Path Development.

The starting point for these has been the analysis of the 12 role profiles in the European Cybersecurity Skills Framework developed by ENISA,

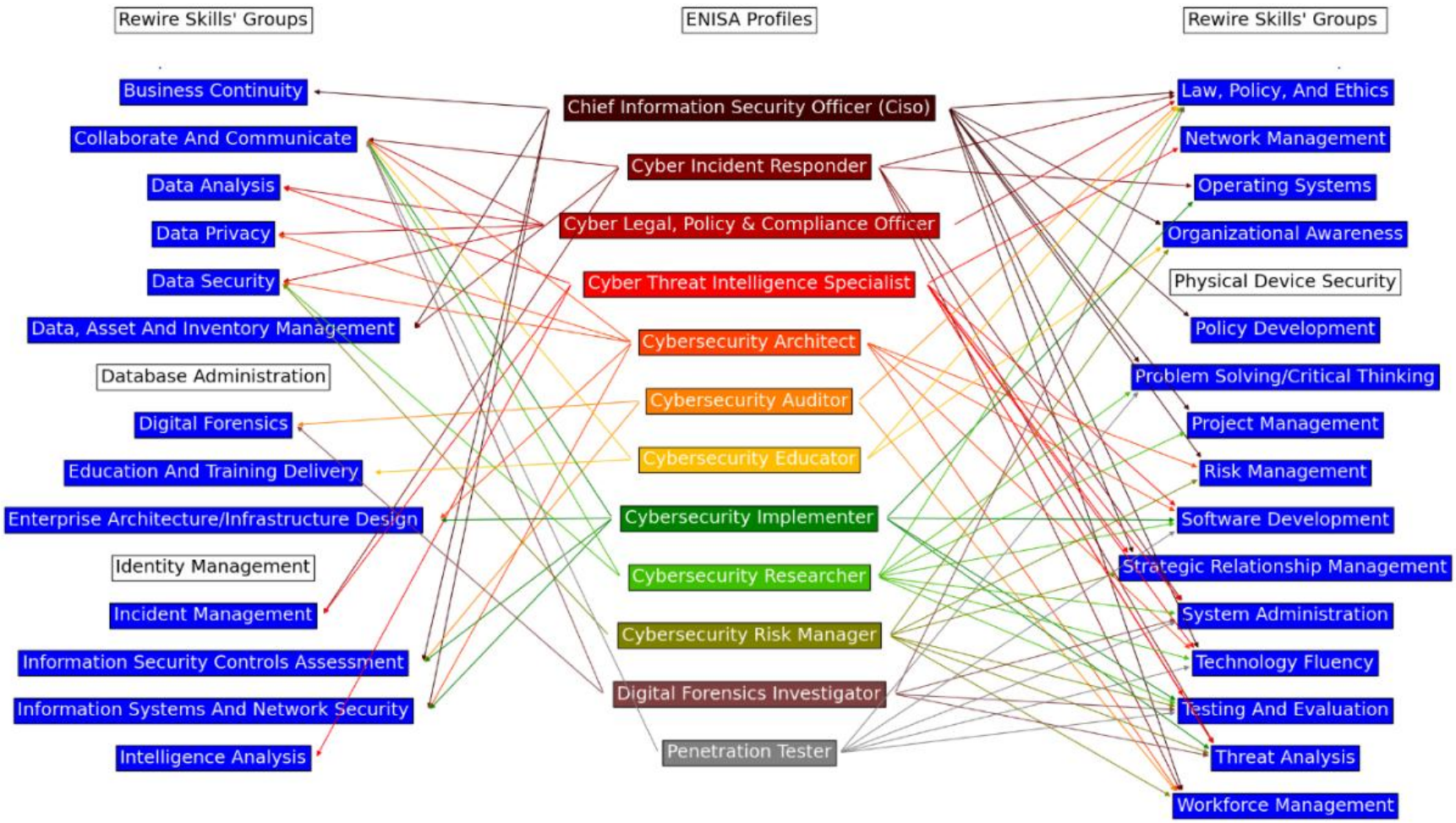
- with a view to identify the interconnections between them, and
- as a base to establish how they can link-up along career pathways.

In this sense, the almost 200 Key Skills and Key Knowledge indicated for the 12 key cybersecurity profiles in the ENISA Framework have been grouped into 31 categories, that then allowed for the easier mapping of the interconnections between these profiles / job roles based on the key skills and knowledge they have in common. The image below, extracted from the REWIRE Cybersecurity Career Pathway Analysis Report[10], outlines these interrelations across all 12 ENISA profiles. The specific skill groups required for each of the 12 ENISA profiles are also available in this Report.

[10] https://rewireproject.eu/wp-content/uploads/2022/10/R3.5.1.-Cybersecurity-career-pathway-analysis_Final_v1.0.pdf

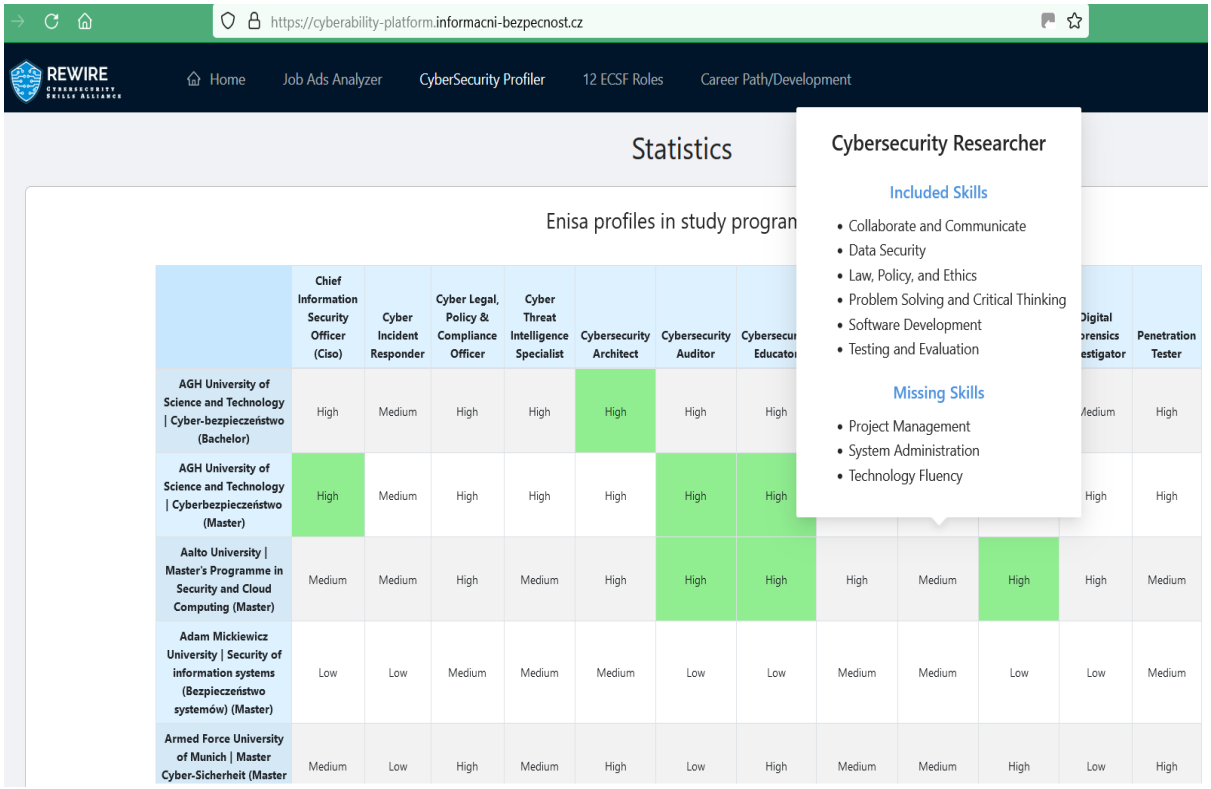
Co-funded by the European Union

Mapping the REWIRE skill groups to the ENISA profiles



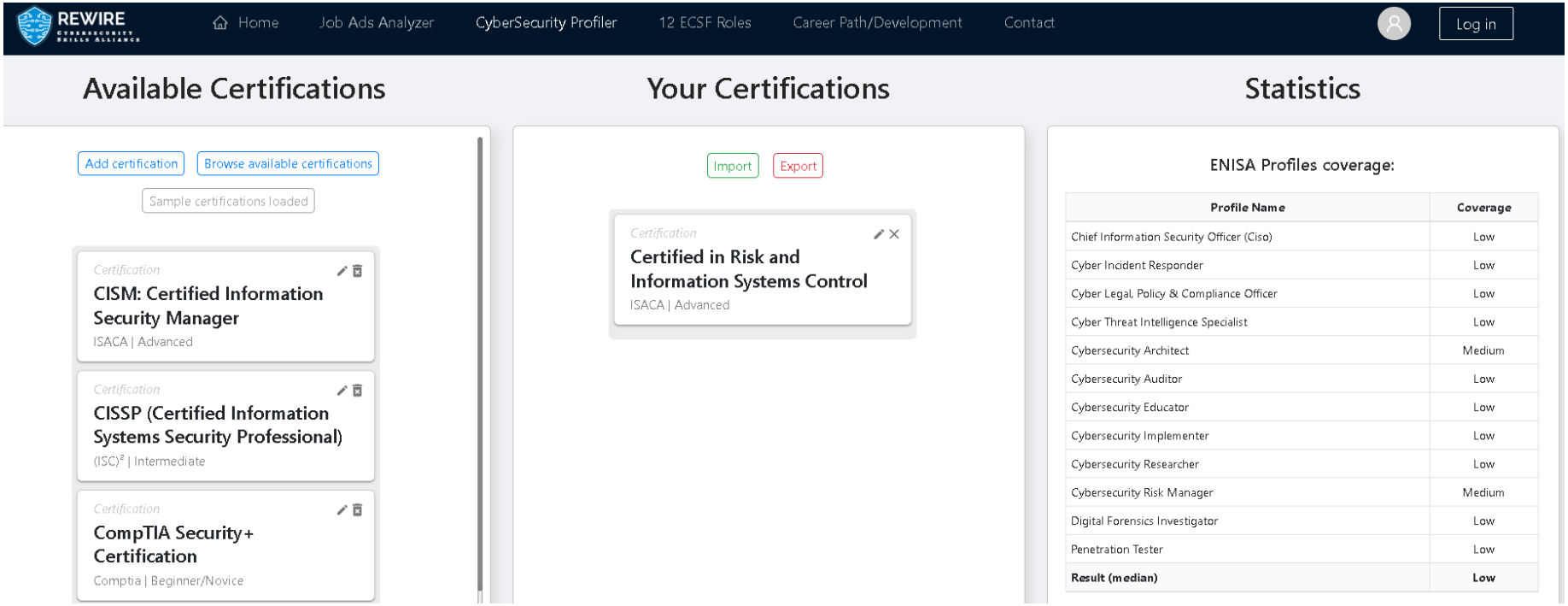
Co-funded by the European Union

Based on these skills and knowledge groups, the REWIRE project also assessed the extent to which each of the 12 ENISA role profiles are aligned with the over 85 European university curricula, 59 professional trainings and 15 certification schemes identified and analysed. This is reflected in the REWIRE **CyberSecurity Profiler** tool Statistics, that provide an overview of how different cybersecurity study options can prepare one for a specific ENISA job profile or another, including what required skill groups are covered and which ones are missing, as exemplified in the image below.



Other functionalities of the REWIRE CyberSecurity Profiler further allow one to browse and asses how taking specific Certifications or Trainings would get them ready for the 12 cybersecurity roles in ENISA Competence Framework, as exemplified in the image below.

Co-funded by the European Union

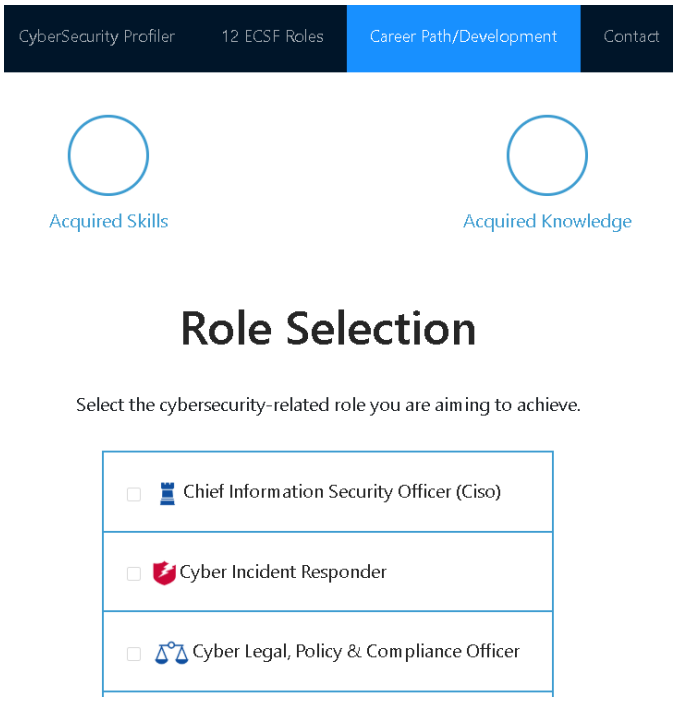


Co-funded by the European Union

Moreover, the REWIRE project carried out a stakeholders' survey on what are the best European Higher Education programmes in cybersecurity from the perspective of the relevance and transferability of the skills and competences they develop. The findings indicate an overall ranking having Estonia in top, followed by Luxembourg, Belgium, Austria, Portugal, Spain and Poland. The slight differences between them along relevance and transferability criteria are reflected in the table below extracted from the REWIRE Fiche IV on best practices in cybersecurity higher education programmes in Europe.

Country	Relevance		Transferability	
	Average	Mode	Average	Mode
Belgium	3.67	4	3.75	3
Poland	3.25	3	3.50	3
Portugal	3.50	3	3.75	4
Spain	3.58	4	3.33	3
Luxembourg	3.92	4	3.75	4
Estonia	3.92	5	3.83	5
Austria	3.67	4	3.67	4

The REWIRE tool for Career Path Development charting allows one to start by choosing a desired role from the 12 key ones, then select the required skills and knowledge for that role that one already has, to then get a summary of the skills and knowledge still needed and guidance on available study options.

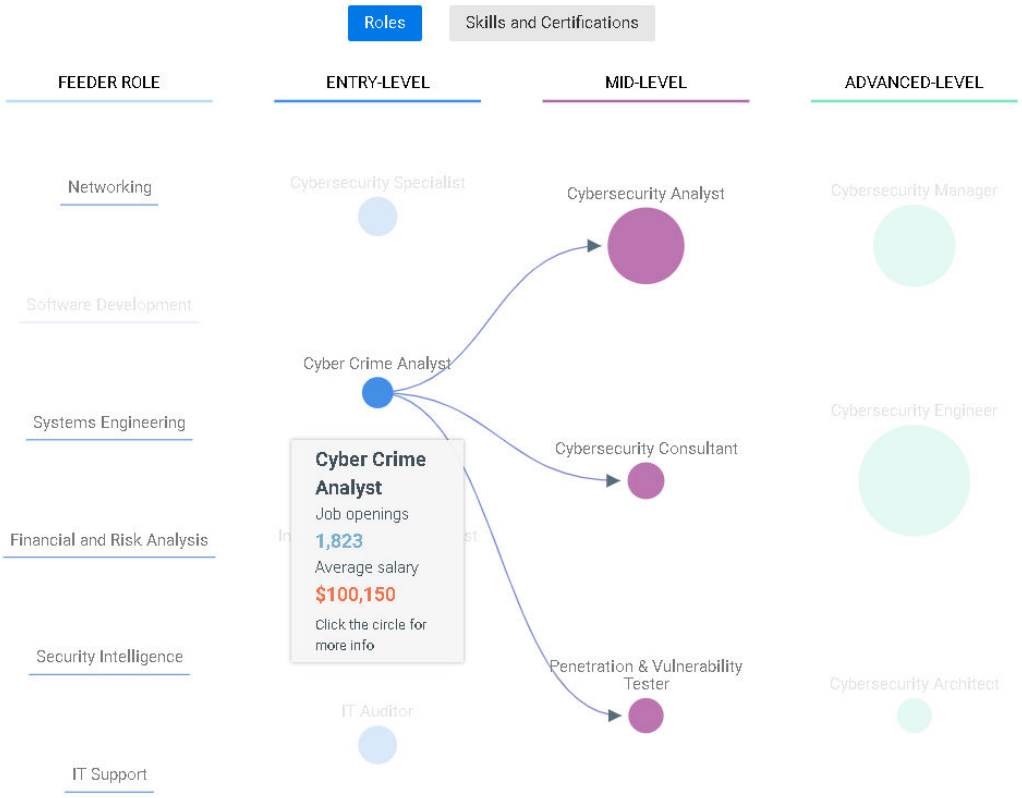


Co-funded by the European Union

4.2 Tools focused on the American context

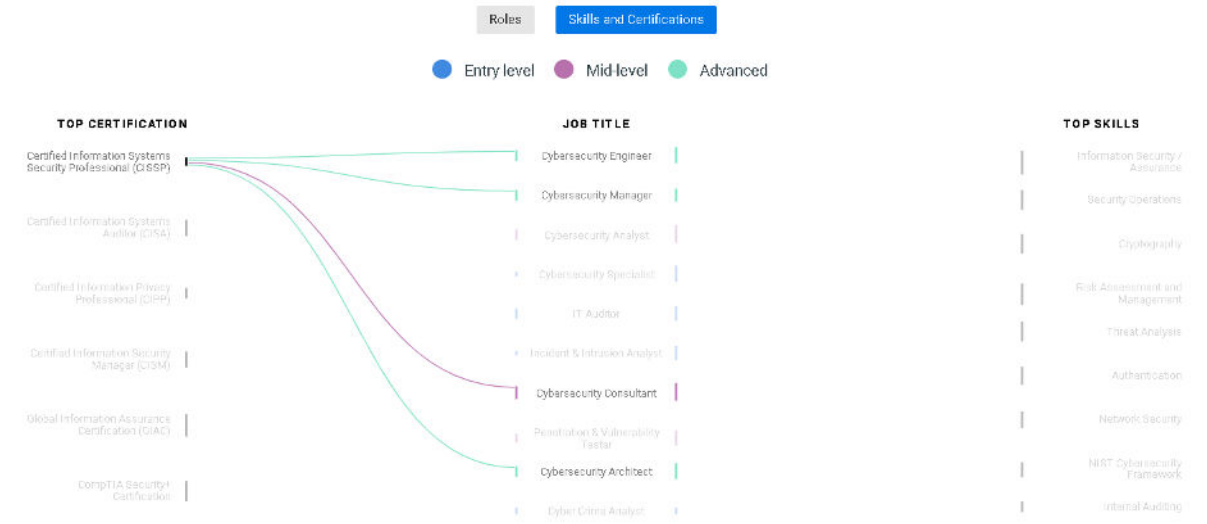
The **CyberSeek Platform** developed in partnership with the US National Initiative for Cybersecurity Education (NICE) also offers a very useful **Career Pathway tool**. This allows students, educators, guidance and career counselors, parents, to identify the skills and educational credentials needed to enter and develop a career in cybersecurity; the courses that could help in this sense; how entry-, mid- and advanced- level roles are interconnected to allow for career progression and charting of pathways.

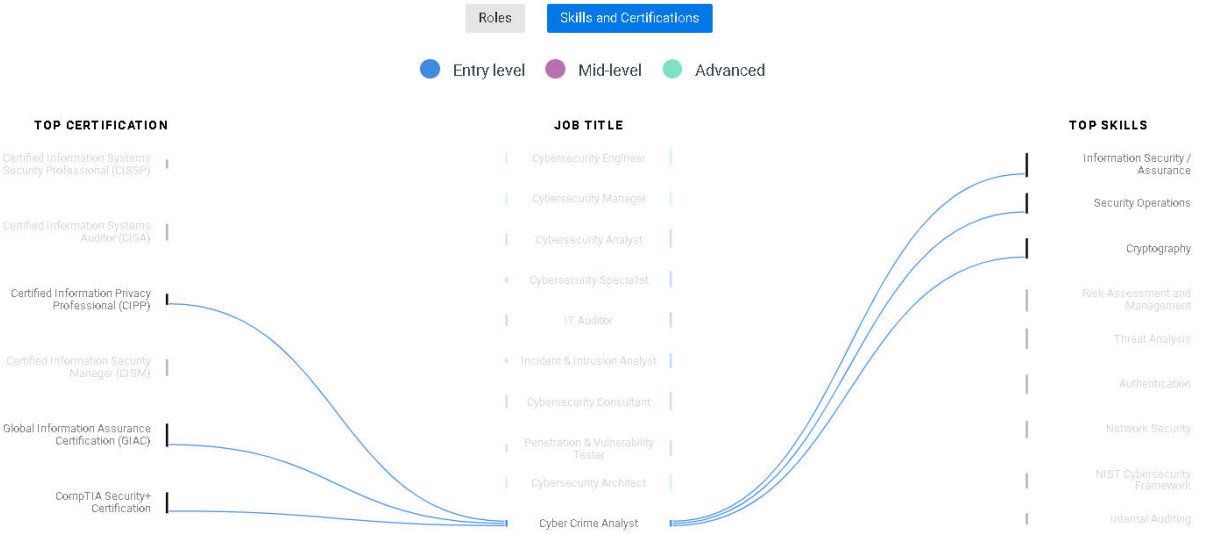
Career pathways can be explored from two different perspectives – starting from the Roles desired, or from the Skills & Certifications one has. Taking the Roles perspective, users can navigate between the different levels based on each area of specialization and get interactive information about career pathways towards key roles within cybersecurity, common transition opportunities between them, the skillsets associated with each role, as well as information about salary levels and jobs opportunities. See example below.



Co-funded by the European Union

Taking Skills & Certifications perspective, the user can see the relationships between the different certifications and role profiles through the skills they provide and require, respectively. As examplified below, one can find out what specific job / role profiles can be aimed at as a Certified Information Systems Security Professional (CISSP), or the main skills required to work as a Cybercrime Analyst and specific certifications that provide them.

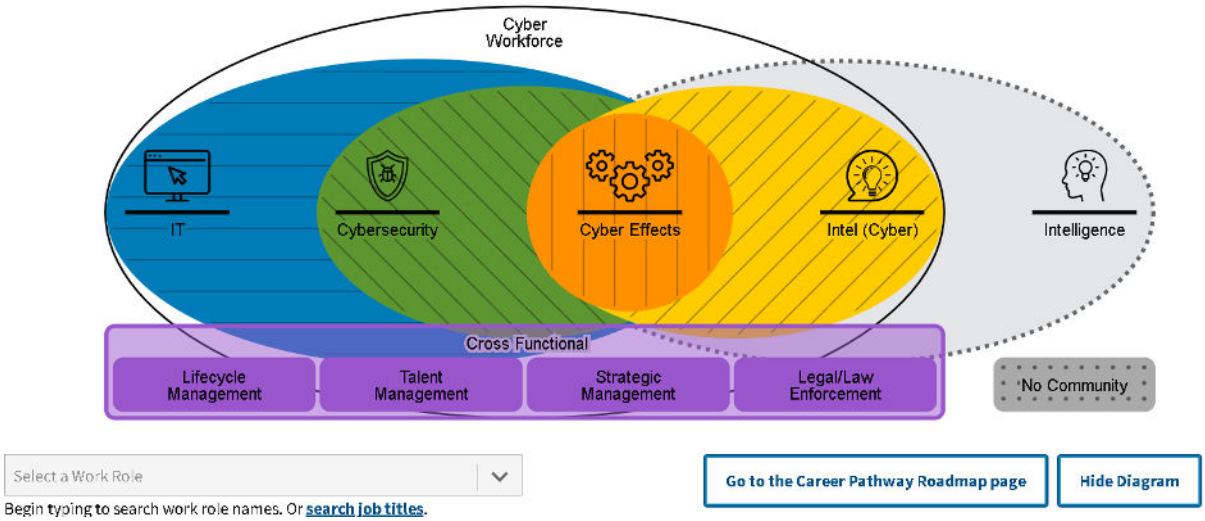




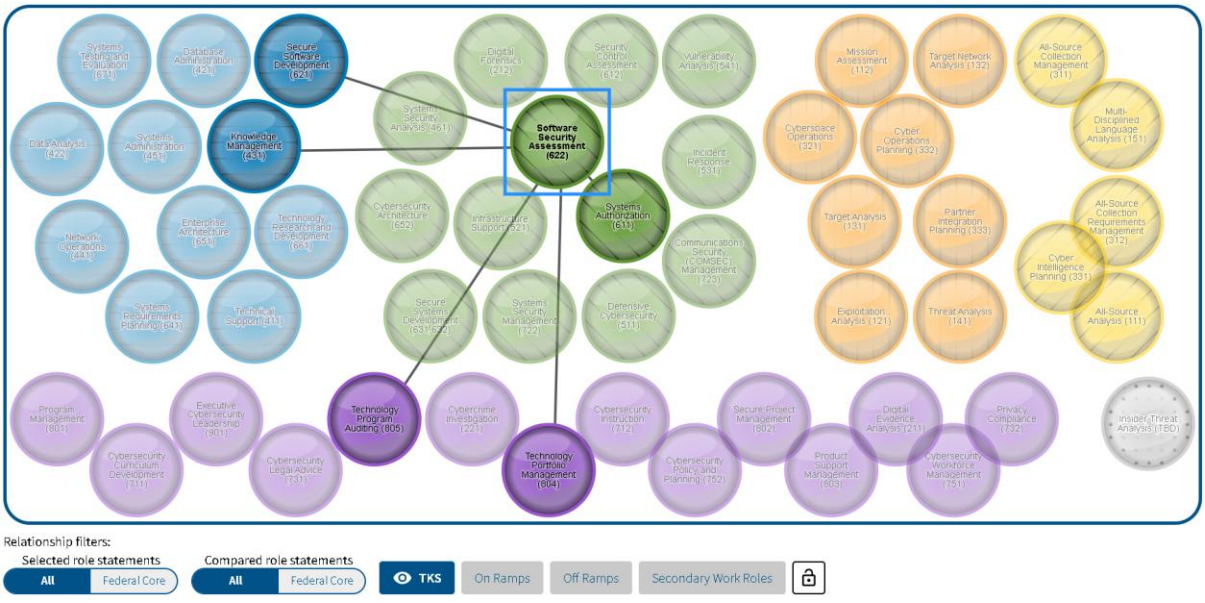
The **Cyber Career Pathways Tool** developed by the National Initiative for Cybersecurity Careers and Studies (NICCS) presents another way to explore job / role profiles as per the NICE Workforce Framework for Cybersecurity. This tool

Co-funded by the European Union

groups the cybersecurity workforce along 5 different, but complementary, skill communities and highights the main attributes of each of the 52 work roles as per the NICE Framework. As exemplified below, the tool also helps visualise the Cybersecurity skill community within the wider Cyber Workforce group, that also includes the Cyber effects skill, and functionally involves Talent Management and Strategic Management.



The tool allows users to navigate between all the different roles, for example Software Security Assessment, and see them in this overall context of skill sets and roles interplay, allowing also comparison with other roles when clicking on it.



Co-funded by the European Union

4.3 Others

The Coursera Cybersecurity Career Roadmap offers a structured guide to pathways for career development in cybersecurity, detailing essential roles and skills needed to progress from an entry-level position to senior leadership. It includes a job leveling matrix to help one understand their current standing and potential career trajectory.

There are also other Coursera resources available to help one develop cybersecurity career paths. For example, this article that outlines five common career paths within cybersecurity, providing insights into the skills and certifications needed for each path. It also offers practical advice on how to get started and make a cybersecurity career.

Coursera also offers a variety of cybersecurity courses, some of which are EU recognized. For example, 12 professional certificates from Google and IBM available on Coursera have received European Credit Transfer and Accumulation System (ECTS) credit recommendations. This means that these certificates can be recognized and transferred as university credits across 49 member nations in the Bologna Process and European Higher Education Area.

There are also other tools allowing one to explore cybersecurity jobs and chart career pathways, like the **Dutch Career Navigator in Safety and Security** provided by Security Delta (HSD) Cluster in the Netherlands. This covers a board range of 42 different job profiles in safety and security, both in the cyber and physical space (e.g. Police expert, Fire brigade officer, Fraud examiner).

Moreover, the **ICT Skills Framework of Singapore** and career maps navigation tool addresses 104 job roles in ICT along 7 track (one of them Cybersecurity) and 32 subtracks (7 of which Cybersecurity related), allowing for a user-friendly and integrated approach for ICT career planning and training.

Co-funded by the European Union

5. CYBERSECURITY PROFESSIONALS IN PRACTICE

Maltese role models

Christopher CUTAJAR - Principal Information Security Engineer

My journey started when at a young age when I got interested in how computers work and started building computers. I started learning computer software and the principles of coding at secondary school. While cybersecurity wasn't even mentioned at school, reading about hackers breaching organizations was something I was always fascinated by. My first encounter with security measures was when a couple of friends and I wanted to install a game on a couple of computers in the school's lab to play against each other. However, we were blocked by a domain policy that disabled USB ports. Bypassing USB access restriction became an obsession which we never managed to but it made us enrol in a summer course on ethical hacking.

After that, I continued my studies at the University of Malta enrolling in BSc Computing Science. To my disappointment, the course only had one cybersecurity module related to cryptography. Meanwhile, I kept learning and reading more about technical areas of cyber security and the different hacking techniques used by malicious users to infiltrate companies. Ghost in Wires by Kevin Mitnick was also one of the books that inspired my interest and passion for the area.

After graduating, I started working full-time as an application developer at RS2 Software PLC, a software house in the payment industry. After a couple of months, an opportunity came within the InfoSec team, and I joined the team as an InfoSec Analyst. During that time, I started a long-distance MSc in Information Security at Royal Holloway, University of London. Working full-

Co-funded by the European Union

time while studying part-time wasn't easy. Loads of sleepless nights but I was enjoying it. This also came with a lot of benefits, as I was able to implement what I was learning during my studies in practice. Apart from the technical side of cyber security, the full-time role introduced me to the governance side of cyber security.

Over the years, my role changed and after 4 years I was heading the Information Security team. During the same period, I also managed to get the Certified Infomation Security Professional (CISSP) certification. In 2019, I joined the InfoSec team at Elastic a search AI company as one of their Senior Security Engineers. The Security Engineering team is responsible for deploying and managing InfoSec's infrastructure and tools. Elastic is a fully distributed company where traditional networks don't exist. While such an environment has its challenges, this makes the job much more interesting. I must say that being part of world-class humble security professionals makes it a little easier. Over the years I've been invited to showcase our teams' work at various conferences such as RSA, ArgoCon, and meetups organized by the Maltese National Coordination Centre (NCC-MT).

Cybersecurity is a very fast-paced industry where one needs to keep abreast of new technologies and learn different areas. Every day is a school day, if you're not learning, you aren't progressing.

Dr. Jennifer BELLIZZI – DevSecOps

I began my academic journey with a Bachelor's degree in Computer Science and Artificial Intelligence at the University of Malta, which provided me with a solid foundation in software development. Following my undergraduate studies, I worked as a software developer in the R&D team of a financial services provider. Information security and technology misuse had always interested me, but working in the industry gave me practical experience in software

Co-funded by the European Union

engineering, and I witnessed firsthand the challenges of operating in a high-security environment and the importance of implementing information security best practices. Having witnessed the importance of cybersecurity in the industry, I decided to pursue a Master's degree in Cybersecurity, allowing me to deepen my knowledge in the field. This led to roles in Information Security and Security Engineering, where I focused both information security certification and implementing security controls to ensure system integrity and service continuity. I then had the opportunity to pursue a PhD in Digital Forensics while working as a Research Supporting Officer at the University of Malta, thus combining academic research with practical applications in incident response. This progression led to my current role as a DevSecOps engineer with an international company, where I integrate security practices into development and operational processes, ensuring security is embedded throughout our services and systems.

Prof. Dr. André XUEREB – Chief Security Officer & Academic

As a professor at the University of Malta, when speaking to prospective students I often tell them that there are many paths open to them: academia, private companies, and policy. I chose to take all three paths simultaneously! First and foremost, I am a professor of physics at the University of Malta, where my specialisation is quantum mechanics. Much of my work is very theoretical and "far fetched," in the sense that it consists of answering interesting questions, but perhaps not directly contributing to the creation of new technologies. More recently I started working in a particular area of quantum mechanics called quantum communication, which provides us with a means for building communication systems that are not susceptible to any of the well-known attacks that could compromise all our present-day communication systems, particularly with the advent of quantum computers. I now run a small enterprise, Merqury Cybersecurity Limited, which helps to bridge the gap between this technology

Co-funded by the European Union

and its users. We hope that, with our technologies, your data – as it is being processed by governments, hospitals banks – will be secure now and in the future. I also mentioned that I work in policy. Since 2021 I have had the honour and privilege to be Malta's Ambassador for Digital Affairs, where I am often called upon to contribute to policy discussions or otherwise give input on all manner of digital topics, including cybersecurity and artificial intelligence.

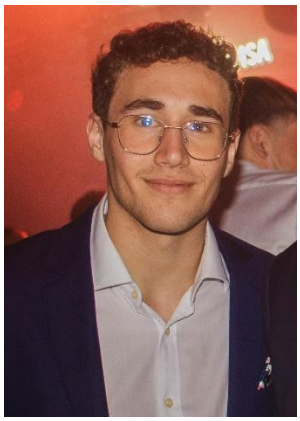
Diane ABELA - Chief Information Security Officer

Diane works for a London-based health technology supplier for the NHS, where she currently leads both the information security and the data protection functions of the business. She also sits on the board as a non-executive director of a highly regulated financial services organisation in Malta. Diane has over 9 years of experience safeguarding millions of records of personally identifiable data and quickly building high-impact, lean teams for fast growing, regulated tech companies. After graduating with a B.Sc degree in ICT from the University of Malta, Diane started off her career as an IT consultant at a big-four audit firm, where she discovered her passion for risk-based implementation of controls. She then moved on to do a Masters in IT management and Organisational Change at Lancaster University, focusing her dissertation on digital transformation in large healthcare organisations. Upon coming back to Malta, Diane joined a large group of companies as their first information security officer where she was tasked with building an information security program to govern the various organisations within the group. Here she learned the importance of adapting your information security program to industry, risk appetite and company strategy. At her next role within a listed technology organisation in the online gambling industry, Diane built her first information security function from the ground up, taking the business on a journey of maturity over the span of 4+ years. Diane left her role as Director of Information Security, to then moved to London where she has been working at residing for over 2 and a half years.

Co-funded by the European Union

Diane is a mentor and a vocal advocate for inclusivity in the workplace, with a focus on the importance of gender equality and equity in the information security space, leading Diversity, Equity, Inclusion and Belonging initiatives in current and previous companies.

Ganni GALEA CURMI - Cybersecurity Engineer



My journey into cybersecurity began during my teenage years when I stumbled upon an online Ethical Hacking course. That initial spark of curiosity quickly grew into a passion for all things tech and security. It set me on a path of continuous learning—one opportunity led to another, deepening my skills and interest in the field. From early on in my career I've realised the importance of combining practical experience with theoretical knowledge.

I began my career as a Trainee at PwC, gaining experience in both the Internal Tech and the Cybersecurity Team. Later, I had the privilege of studying abroad at Sapienza Università di Roma for a Bachelor of Science in Applied Computer Science and Artificial Intelligence, focusing on Artificial Intelligence and Network Security. Through an Erasmus exchange at the University of Oslo, I further specialised in topics like Ethical Hacking and Network Security. Alongside my studies, I've worked on projects like developing a honeypot system to analyse local botnet activities and building a machine-learning-based brand imitation detection tool, which evolved from my undergraduate thesis into a product under development at PwC Malta.

For aspiring cybersecurity professionals, my advice would be to utilise the wealth of resources available today. Platforms like TryHackMe, HackTheBox, and even YouTube offer affordable or free ways to build foundational skills. Above all, the key traits for succeeding in this field are curiosity and persistence—cybersecurity challenges often require a deep dive into nuanced problems, and the ability to "try harder" will take you far.

Austrian role models

Dr. Dr. Florian Skopik – Academic & Cyber auditor

Florian Skopik is Head of the Cyber Security Research Program at the Austrian Technology Institute. He is also a court certified expert which means that he is authorized to give advisory opinions on legal questions concerning IT security and data security at court. He is further appointed auditor for operators of essential services, and ISO27001 ISMS Lead Auditor.

Florian spent 15+ years in cyber security research, before, and partly in parallel, he worked another 15 years for numerous SMEs as a firmware developer. His main interests are centered on critical infrastructure protection, anomaly detection, and incident response. He published more than 150 scientific conference papers and journal articles and holds 75 industry relevant security certifications, including CISSP, CISM, CRISC, CCNP Security, GPEN, GCIH, GCTI, etc.

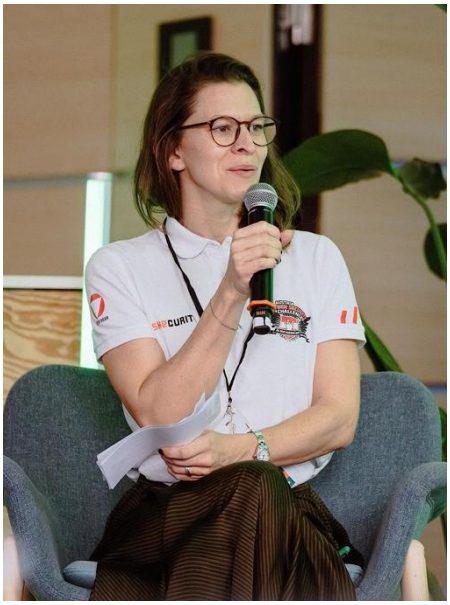
Florian completed his academic education at TU Wien, where he earned his PhD in the field of computer science. In addition to his studies in Austria, he further enhanced his expertise by obtaining a professional degree in Advanced Computer Security from Stanford University in 2017.

Moreover, Florian is member of various conference program committees, editorial boards and standardization groups. He frequently serves as reviewer for numerous high-profile journals.

One key piece of advice Florian would like to give to aspiring cybersecurity professionals is to understand how incredibly fast-paced this industry is. Standards that seem fundamental today may be outdated in just a few years. New security solutions emerge every few months to address threats that did not even exist before, while new malware appears every few weeks and vulnerabilities surface virtually every day — each requiring immediate attention. Staying ahead in cybersecurity requires continuous learning and adaptability; there is no time to become complacent.

At the same time, for those truly passionate about the field, cybersecurity is not just financially rewarding, but also deeply fulfilling on a personal level. It is a profession where boredom is never an option, where you can grow every single day, and where your skills actively contribute to a safer digital world.

Stephanie Jakoubi – Managing Director



Stephanie Jakoubi is part of the Management Board and head of the Strategic Partnership Management and Communication team at an Austrian research center for information and IT security, SBA Research.

After graduating with a B.Sc in Software Engineering at the Hagenberg Campus FH Upper Austria she started her career at the company in project management and applied research, primarily in the area of security awareness. Furthermore, she also led and co-founded several educational programs in the field of IT security. She then decided to complete a Masters program in Information Security Management again at the FH Upper Austria. Afterwards she took over as head of the Strategic Partnership Management department at the same company as before. She then moved on to her current position where she works closely with company partners and increasingly develops into an interface between industry, research and funding bodies.

Stephanie is also a board member of numerous associations and initiatives that deal with cyber security. There she is the security, education or female voice at the table. She is especially committed to empowering women in IT and cyber security. The lighthouse initiatives are shedigital (https://shedigital.at) including the "the IT-day" where 240 female IT experts visited 170 high school classes all over Austria to talk about the power and possibilities of IT. Furthermore she is the force and founder behind shecurity (https://www.linkedin.com/company/shecurity-women-in-security/) a community of female security experts and a female hacker training (https://verbotengut.at/allgemein/hackerinnen-training/).

Co-funded by the European Union

She is also involved in the area of security awareness for children.

Associated Professor Sujoy Sinha Roy, Ph.D.

Dr. Sujoy Sinha Roy is an Associate Professor at TU Graz, specializing in secure and efficient cryptographic algorithms on hardware and software platforms. He is known for his work in post-quantum cryptography (SABER KEM design, efficient software and hardware implementations, and side-channel security assessment) and Fully Homomorphic Encryption (FHE design, hardware acceleration, and application). Dr. Sinha Roy earned his PhD in 2017 from KU Leuven, receiving the IBM Innovation Award for his thesis. Before TU Graz, he was an assistant professor at the University of Birmingham. He obtained his habilitation in January 2024.

Co-funded by the European Union

Ukrainian role models

Dr. Oleksii BARANOVSKYI

An accomplished cyber security expert with an impressive background in both academia and industry, Dr. Baranovskyi began his career as a security analyst at a software product company before transitioning into the banking and financial industry. He then went on to work for a professional cyber security services company and academic institutions, honing his skills along the way. Dr. Baranovskyi holds certifications from recognized international organizations such as (ISC)2, ISACA and others, and is a certified trainer in cyber security with expertise in CISSP, CISM, CEH, and more.

Dr. Baranovskyi has received numerous accolades for his work in cyber security, including recognition from the National Security Council of Ukraine, the State Telecommunication Service, and the Head of Cyberpolice for his contributions to the development of cyberpolice and national cybersecurity capabilities.

His research interests lie in forensic investigations, particularly in hybrid and cloud environments, APT-attack analysis, anomaly detection, and threat hunting. In recognition of his scientific contributions, he was awarded the President of Ukraine award for young scientists in 2018. Oleksii has also lent his expertise to several international projects, serving as a subject matter expert for organizations such as OSCE, USAID, and CRDF Global from 2015-2023.

Co-funded by the European Union

Anastasiia KONOPLOVA

Ms. Konoplova, CISA, CRISC, CDPSE is a highly accomplished entrepreneur, IT auditor, analyst, trainer, and speaker with extensive experience in governance, compliance, risk management, IT consulting, and cybersecurity. As the CEO and owner of LLC UAG since 2017, she has led the company in providing assurance and consulting services to commercial banks and enterprises, focusing on information security, IT systems management, and risk governance.

Anastasiia's expertise spans over two decades, beginning with her work as the Head of Analysis and IT Department at an audit firm, where she controlled financial statements, managed office technology, and provided technical support for audit activities. She later became the Deputy Director General of AF Union Aud Group Ltd, where she managed advice and assurance projects in the areas of IT, information security, credit risk, operational risk, and due diligence for Ukrainian banks and enterprises.

In addition to her corporate leadership, Anastasiia served as the President of ISACA Kyiv Chapter from 2018 to 2020. During her tenure, she achieved a 26% growth in chapter membership and improved membership renewal rates. She also facilitated the implementation of the ISACA Affiliation Agreement and oversaw the localization and distribution of key ISACA resources such as the COBIT 2019 Framework and its associated toolkits and guides. Her efforts significantly advanced the adoption of governance and management frameworks in Ukraine.

As a trainer and advocate, Anastasiia is certified in CISA, CRISC, and CDPSE, accredited by APMG as a certifications trainer and she has delivered numerous

Co-funded by the European Union

training sessions to help professionals excel in IT auditing, risk management, and information security. She is also an accomplished author and speaker, having participated in and contributed to over 50 international conferences. Anastasiia holds a master's degree in economics, specializing in economic cybernetics, and a strong professional background in cybersecurity and risk management. Her dedication to improving information security extends to her consultancy work for banks such as ProCredit Bank Ukraine and DV Bank, where she conducted audits and provided actionable recommendations to enhance cybersecurity frameworks.

Under her leadership, LLC UAG has remained at the forefront of IT risk consulting, helping businesses navigate the complexities of modern business environment, including cybersecurity challenges. Anastasiia's commitment to fostering innovation and excellence in the information services industry has solidified her reputation as a leading expert and thought leader.

More about her professional activity:

Profile: https://www.linkedin.com/in/anastasiia-konoplova-9342b57b/
Public activity: https://www.slideshare.net/AnastasiiaKonoplova
Blog: https://www.facebook.com/llcuag
Reputation: https://ec.europa.eu/futurium/en/Women4Cyber
Certifications: https://www.credly.com/users/anastasiia-konoplova

Dr. Yegor AUSHEV

Dr. Aushev is a distinguished "white hacker" and cybersecurity expert, renowned for his innovative contributions to the tech and information services industry. He is the CEO of CyberUnitTech and Co-Founder of Cyber School Ukraine and Hacken, where he leads

efforts to strengthen digital security across private enterprises, government institutions, and critical infrastructure.

With over 11 years of experience in cybersecurity, Yegor has popularized the concept of engaging ethical hackers to identify and mitigate vulnerabilities in various systems. His groundbreaking work includes the development of platforms that connect businesses with ethical hackers who are rewarded for identifying system weaknesses. His company, Hacken, launched a cryptocurrency-funded platform, creating a global ecosystem of ethical hackers.

Yegor holds a Ph.D. in High Energy Physics from the National Technical University of Ukraine 'Kyiv Polytechnic Institute' and has previously conducted research at Fermilab and DESY, specializing in data analysis. He is also an alumnus of the Ukrainian School of Political Studies, where he gained insights into legislative reforms and governance.

A prolific author, Yegor has co-authored several international publications on Ukraine’s legislative reforms in cybersecurity and has represented his expertise at over 50 international conferences. Notably, on February 24, 2022, he spearheaded the mobilization of over 1,000 cybersecurity experts to bolster Ukraine's digital defense during the critical early hours of Russia's invasion.
Yegor's entrepreneurial achievements are backed by his strong expertise in business strategy, blockchain, and education. His innovative solutions and strategic vision have cemented his reputation as a Ukrainian leader in cybersecurity.

Co-funded by the European Union

Greek role models

Dr. Dimitris GRITZALIS

Dr Dimitris Gritzalis is Professor of ICT Security at the Department of Computer Science of the Athens University of Economics and Business (AUEB). He is also Chairman of the University Research Centre, Director of the Information Security and Critical Infrastructure Protection (INFOSEC) Laboratory (www.infsec.aueb.gr) and Director of the Master's Programme in Information Systems. Prof. Gritzalis holds a B.Sc. (Mathematics, Univ. of Patras, Greece), an M.Sc. (Computer Science, City University of New York, USA) and a Ph.D. (Critical Information Systems Security, Univ. of the Aegean, Greece).

He has served as Associate Commissioner of the Greek Data Protection Commission, President of the Greek Computer Society and Chairman of Digital Aid S.A. He has provided expert services to several international organisations, including the Council of Europe, CEN, the EU Joint Research Centre and EUROPOL. He has also worked as an evaluator for the Framework Programmes funded by the European Commission.

His current research interests include security and privacy in online social networks, digital forensics, critical infrastructure protection, hacking and hacktivism, and civil rights in cyberspace. His publication record includes 10 books and more than 160 papers published in peer-reviewed journals and international scientific conferences, with proceedings published by international publishers.

Dr. Christos XENAKIS

Prof. Christos Xenakis received his B.Sc. degree in Computer Science in 1993 and his M.Sc. degree in Telecommunications and Computer Networks in 1996, both from the Department of Computer Science. degree in Telecommunications and Computer Networks in 1996, both from the Department of Department of

Co-funded by the European Union

Computer Science and Telecommunications, University of Athens, Greece. In 2004 he received his D. degree from the University of Athens (Department of Computer Science and Telecommunications). From 1998 to 2001 he worked in a Greek telecommunications systems development company, where he was involved in the design and development of involved in the design and development of advanced telecommunications subsystems. From 1996 - 2007 he was a member of the Communication Networks Laboratory of the University of University of Athens.

Since 2007 he is a member of the faculty of the Department of Digital Systems of the University of Piraeus, Greece, where he is currently a Professor, a member of the Systems Security Laboratory and the Director of the Laboratory and Director of the Postgraduate Course in Digital Systems Security. He has participated in numerous projects carried out in the framework of EU programmes (ACTS, ESPRIT, IST, AAL, DGHOME, Marie Curie, Horizon2020) as well as national programmes (Greek). He is the project leader of the CUREX, SECONDO, INCOGNITO and SealedGRID projects, funded by Horizon2020, while he was the project manager of the ReCRED project funded by Horizon 2020 and Technical Manager of the UINFC2 project funded by DGHOME/ISEC. He is also a member of the Steering Committee of the European Cyber Security Challenge (ECSC) and leader of the Hellenic Cyber Security Team.

He is a member of the editorial board of three Thomson Reuters indexed journals: a) Computers & Security Journal, published by Elsevier, b) Computer Communications Journal, also published by Elsevier, and c) IET Information Security from the Institute of Engineering and Technology. His research interests are in the area of systems, networks and application security, networks and applications security. He has authored more than 90 papers in peer-reviewed journals and international journals and international conferences.

Co-funded by the European Union

German role models

Dr. Stefan Steiger – Information Security Specialist

I have always been interested in IT security and still remember pinging friends on IRC (Internet Relay Chat) after school. That was my first encounter with (D)DoS attacks. Initially, however, I didn't pursue a technical career path as I was more interested in politics. During my time at university, I focused on security policy and when the Stuxnet computer worm became known, my interests converged. As a result, I wrote my graduation thesis on cyber security and then went on to do my doctorate with a comparative study on German and British cyber security policy.

During my academic employment, I also worked on various interdisciplinary projects that dealt, for example, with the analysis of political cyber attacks. At the same time, I had the opportunity to improve my technical knowledge through practical work at the university's computing center and by attending IT security courses in the field of computer science at Heidelberg University.

I now work as part of a team that improves information security at universities in the state of Baden-Württemberg. My tasks include planning and implementing vulnerability scans as well as consulting academic institutions in setting up effective information security management systems. I also regularly offer courses on international cyber security politics as an associate lecturer at the University of Heidelberg.

Co-funded by the European Union

6. COUNTRY SPECIFIC CYBERSECURITY OPPORTUNITIES

6.1 GERMANY

6.1.1 Cybersecurity sector situation and general work opportunities

In Germany, there is a high demand for cyber security specialists in different sectors such as finance (e.g. ING), transportation (e.g. DB), telecommunications (e.g. Telekom), health (e.g. hospitals), consulting (e.g. PwC), public sector (e.g. BND, BSI, Bundeswehr) etc.

There are different ways to enter the cyber security profession; the most common way is to go to university and enroll in a cyber security programme; especially in academia in Germany there are several different programmes and options to choose from (study at university, study at university of applied sciences, dual study programmes), which are described in more detail in the next chapter, but there are also opportunities for apprenticeships and training

However, there is no single path to cybersecurity - there are several different options and possibilities.

The following list does not claim to be exhaustive and is intended to provide an initial overview of the opportunities and pathways that could be a helpful gateway to a career in cyber security.

6.1.2 Study programs, trainings, certifications, online/offline courses

Study programs

University

<u>Bachelor (B.Sc.) Cybersecurity</u>

The study program is derived from a general curriculum in computer science but offers specific cybersecurity related courses.

Three universities offering this program are:

Co-funded by the European Union

- University of Bonn (https://www.informatik.uni-bonn.de/de/studium/bachelor/cyber-security-bsc)
- Saarland University (https://www.uni-saarland.de/studium/angebot/bachelor/cybersecurity.html)
- Ruhr University Bochum (https://studienangebot.ruhr-uni-bochum.de/de/it-sicherheit-informationstechnik/bachelor-1-fach)

Master (M.Sc.) Cybersecurity

After completing a general computer science (or related) degree, it is possible to specialize in cybersecurity with a master's degree offered at e.g. these three universities:

- University of Bonn (https://www.uni-bonn.de/de/studium/studienangebot/studiengaenge-a-z/cyber-security-msc)
- Technical University of Darmstadt (https://www.tu-darmstadt.de/studieren/studieninteressierte/studienangebot_studiengaenge/studiengang_341504.de.jsp)
- Saarland University (https://www.uni-saarland.de/studium/angebot/master/cybersecurity.html)
- University of Bundeswehr Munich: https://www.unibw.de/inf/studium/studiengang-cyber-sicherheit

Master (M.Sc.) IT-Security

- Ruhr University Bochum: IT Security Networks and Systems (https://informatik.rub.de/studium/its/msc-n/)
- Ruhr University Bochum: IT Security (https://studienangebot.ruhr-uni-bochum.de/de/it-sicherheit-informationstechnik/master-1-fach)
- Ruhr University Bochum: Applied IT Security https://studienangebot.ruhr-uni-bochum.de/de/applied-it-security/master-1-fach

Co-funded by the European Union

- Lübeck University: https://www.uni-luebeck.de/studium/studiengaenge/it-sicherheit/master/profil.html

Bachelor (B.Sc.) Computer Science (with possible specialisation in cybersecurity)

Usually, computer science studies at German universities offer the opportunity to specialize further after the third semester. The curriculum can then be adjusted to incorporate more cybersecurity related courses.

A list with the referring study programs can be found here: https://www.studis-online.de/studium/informatik/studiengaenge/?hsart=uni&abschluss=bachelor

University of Applied Sciences

The German 'Hochschule' (equals University of Applied Sciences) has the benefit of a more practice-oriented curriculum. Project based learning is the focus of most courses.

Bachelor (B.Sc.) Cybersecurity

Nine schools offering this course are:

- Hochschule Mannheim: https://www.hs-mannheim.de/csb.html
- Deggendorf Institute of Technology: https://www.th-deg.de/cy-b
- Technische Hochschule Ingolstadt: https://www.thi.de/informatik/studiengaenge/cybersicherheit-bsc/
- Fachhochschule des Mittelstands: https://www.fh-mittelstand.de/studiengang/cyber-computer-security/vollzeit/
- Hochschule für Technik und Wirtschaft Berlin: https://cyber-security-business.htw-berlin.de
- IU Hochschule: https://www.iu.de/bachelor/cyber-security/
- FOM Hochschule: https://www.fom.de/de/hochschulbereiche/it-management/cyber-security-ba.html?locations=55594

Co-funded by the European Union

- HS Furtwangen: https://www.hs-furtwangen.de/zukunft-studieren/studiengaenge/it-sicherheit-und-cyber-security-bachelor
- Hochschule Bonn-Rhein-Sieg: https://www.h-brs.de/de/inf/studienangebot/bachelor/cybersecurity-und-privacy

Bachelor (B. Sc.) IT Security

- Berliner Hochschule für Technik: https://www.bht-berlin.de/b-its-o
- Technische Hochschule Brandenburg: https://informatik.th-brandenburg.de/studium/bachelorstudiengaenge/it-sicherheit/
- Wilhelm Büchner Hochschule: https://www.wb-fernstudium.de/kursseite/bachelor-studiengang-it-sicherheit-bsc.html?srsltid=AfmBOopbrkoR9ANyBjKEoL6hRc6jOcEh-_rdss5QtmKoFLxv7Jj4jNjX
- Hochschule Esslingen: https://www.hs-esslingen.de/fileadmin/media/Fakultaeten/Studiengangflyer/Flyer_Bachelor_IT-Sicherheit_studieren.pdf?utm_source=StudyCheck&utm_campaign=StudyCheck&utm_medium=Premiumprofil-Studiengang&utm_term=IT-Sicherheit-B.Eng.-31101
- Leibnitz FH: https://leibniz-fh.de/studiengaenge/it-security/
- oncampus GmbH: https://lernen.oncampus.de/course/view.php?id=892
- Technische Hochschule Lübeck: https://www.th-luebeck.de/studium/studienangebot/studiengaenge/it-sicherheit-online-bsc/uebersicht/
- Technische Hochschule Würzburg-Schweinfurt: https://fiw.thws.de/studienangebot/bachelor-informationssicherheit/
- Hochschule Stralsund: https://www.hochschule-stralsund.de/host/fakultaeten/elektrotechnik-und-informatik/studienangebot/it-sicherheit-und-mobile-systeme/
- Ostfalia Hochschule für angewandte Wissenschaft: https://www.ostfalia.de/cms/de/i/studium-vfh---online/studiengaenge-00001/it-sicherheit-b.-sc./

Co-funded by the European Union

Bachelor (B. Sc.) Applied computer science

Similar to the bachelor's degree in computer science at universities, the general curriculum of applied computer science can also be adjusted to incorporate specialised courses in cybersecurity. More information about specific study programmes can be found here: https://www.studis-online.de/studium/angewandte-informatik/fh/

Master (M.Sc. / M.Eng.) Cybersecurity

Building on a previous degree in cyber security or a related degree programme at a university of applied sciences, a master's degree can be chosen.

Four universities of applied sciences offer this program are:

- Deggendorf Institute of Technology: https://www.th-deg.de/de/weiterbildung/master/cyber-security
- Fachhochschule des Mittelstands: https://www.fh-mittelstand.de/studiengang/cyber-security/berufsbegleitendes-studium/
- IU: https://www.iu.de/master/cyber-security/
- Hochschule für angewandtes Management Ismaning: https://www.fham.de/studiengaenge/master/cyber-security/

Bachelor (B.Sc.) Digital Forensics

It is a special curriculum in which students learn to investigate "cybercrime scenes" in order to identify the perpetrators behind cyberattacks. More information about specific study programmes can be found here: https://www.studis-online.de/studium/it-forensik-cybercrime/

Co-funded by the European Union

6.1.3 Other trainings

Dual Study Programme Cybersecurity

Dual Study programmes consist of two phases: A study phase at the respective university of applied sciences and a practice phase at the company where you will work and gain practical experiences additionally to your studies.

Interested students have to apply at a company which enrols them at a university for applied sciences. For example, there are 103 companies partnering with DHBW Mannheim (Duales Studium) https://studyup.mannheim.dhbw.de/unternehmenssuche

Further possibilities for a Duales Studium can be found here: https://www.ausbildung.de/berufe/duales-studium-it-security/stellen/#tab-bar-anchor

There are also possibilities to accomplish a Duales Studium at a Federal Office such as the BSI (https://www.bsi.bund.de/DE/Karriere/Einstieg/Studium-und-Ausbildung/Studiengang-DACS/studiengang-dacs.html), the BND (https://www.bnd.bund.de/DE/Karriere/Ausbildung_Studium/Duales_Studium/Cyber/dual_node_cyber.html) or at state offices such as in Baden-Württemberg (https://www.cybersicherheit-bw.de/duales-studium-bei-der-csbw) Digital Administration and Cyber Security

Apprenticeships (should equal trainings)

There are not too many possibilities for a cybersecurity apprenticeship in Germany at first hand, but there are possibilities to get there without studies. You can for example accomplish an apprenticeship as an IT Specialist (Fachinformatiker) and do some further specializations in order to become a cybersecurity specialist. If you are further interested in the apprenticeship as an IT specialist you can get further information here: https://web.arbeitsagentur.de/berufenet/beruf/7847

Co-funded by the European Union

However, there is for example the opportunity for an apprenticeship at the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik BSI)

https://www.bsi.bund.de/DE/Karriere/Einstieg/Studium-und-Ausbildung/Ausbildung-in-der-IT/it-ausbildung-im-bsi_node.html

Certifications (online / offline courses)

There are several courses offering further training in cyber security in Germany, here are just some examples:

- Cyber Security Advisor (IHK Webinar): https://www.ihk.de/rhein-neckar/system/veranstaltungssuche/vstdetail-antrago/5232590/95046?terminId=95046
- IT basic protection consultant (IHK course online/offline): https://www.ihk.de/rhein-neckar/system/veranstaltungssuche/vstdetail-antrago/5232590/94019?terminId=94019
- IT security coordinator (IHK Webinar): https://www.ihk.de/rhein-neckar/system/veranstaltungssuche/vstdetail-antrago/5232590/85533?terminId=85533
- IT security management (IHK course online/offline): https://www.ihk.de/rhein-neckar/system/veranstaltungssuche/vstdetail-antrago/5232590/92546?terminId=92546
- Data protection officer (IHK Webinar): https://www.ihk.de/rhein-neckar/system/veranstaltungssuche/vstdetail-antrago/5232590/92246?terminId=92246
- CompTIA Security+ certificate (Online): https://www.comptia.org/de/zertifizierungen/security
- IT Security certificate program DHBW (offline): https://www.wissenschaftliche-weiterbildung.dhbw.de/it-security
- There are several offers by TÜV Akademie:

Co-funded by the European Union

- Certified Ethical Hacker (online/offline): https://akademie.tuv.com/weiterbildungen/certified-ethical-hacker-ceh-intensiv-seminar-3155681
- Certified Cybersecurity Technician (online): https://akademie.tuv.com/weiterbildungen/certified-cybersecurity-technician-cct-16020924
- Certified Network Defender (online): https://akademie.tuv.com/weiterbildungen/certified-network-defender-cnd-v2-ilearn-14821812
- IT basic protection consultant (online): https://akademie.tuv.com/weiterbildungen/it-grundschutz-berater-16913139
- Cybersecurity incident – first response (online): https://akademie.tuv.com/weiterbildungen/cybersecurity-incident-first-response-2961818
- Check Point Certified Security Administrator (online/offline): https://akademie.tuv.com/weiterbildungen/check-point-certified-security-administrator-r81x-ccsa-14822654
- Further offers by TÜV Akademie: https://akademie.tuv.com/themen/it-informationsmanagement/cybersecurity

- Further course offers for additional training can be looked up at the BSI webpage:https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/Personenzertifizierung-IT-Grundschutzberater/Schulungen-zum-IT-Grundschutz-Praktiker-und-IT-Grundschutzberater/schulungen-zum-it-grundschutz-praktiker-und-it-grundschutzberater.html

6.1.3 Funding support opportunities to undertake cybersecurity studies, trainings, certifications

Co-funded by the European Union

- courses by IHK or TÜV are most of the time paid by your company
- apprenticeships and trainings are usually also paid, as well as Duales Studium
- there are some scholarships for study programs in cyber security e.g. at German Bundeswehr: https://www.bundeswehrkarriere.de/stipendium-im-masterstudiengang-cyber-sicherheit-376; https://karriere.bund.de/arbeiten-bei-uns/stellenangebote/stipendium-fuer-den-masterstudiengang-cyber-sicherheit-2026/22953616;
- at BKA (Bachelor's program scholarship) https://www.karriere.bka.de/Karriereportal/DE/Jobs/BerufeBeimBKA/ItNachwuchsfoerderung/itNachwuchsfoerderung_artikel.html
- ISACA (Master's program scholarship) https://www.isaca.de/sheatisaca/programm3.html
- e-fellows scholarship also for the IT sector: https://www.e-fellows.net/events/it-stipendium
- Further scholarships for university programmed in the STEM sector can be found here: https://www.komm-mach-mint.de/studentinnen/stipendien

There are also 13 general scholarship organizations funding your general studies at university, more information can be found here: https://www.bmbf.de/bmbf/de/bildung/begabtenfoerderung/die-begabtenfoerderungswerke/die-begabtenfoerderungswerke_node.html

Co-funded by the European Union

6.2 AUSTRIA

6.2.1 Cybersecurity sector situation and general work opportunities

The cybersecurity market in Austria has demonstrated significant growth in recent years, with revenues expected to reach €542.50 million in 2025. It is driven by a strong focus on data privacy, a robust technology infrastructure, and increasing investments in cyber resilience.

The rapid digital transformation across industries, alongside a significant rise in cyber threats (particularly ransomware, phishing, scam, DDoS attacks, etc.), has accelerated the need for cybersecurity solutions in Austria. There is a growing demand for advanced security solutions and cyber expertise across both public and private sectors.

Austria has a well-developed public cybersecurity ecosystem with national institutions managing threat intelligence, cyber defense, and policy enforcement. Some of the key actors include:

- **Federal Chancellery – Cybersecurity**. Manages strategic coordination in cybersecurity within the federal public administration in Austria, as well as European and international cooperation.
- **Strategic Network and Information Systems Security Office (NIS Office).** Ensures compliance with the NIS Directive and the Network and Information Systems Security Act (NIS Act).
- **Government Computer Emergency Response Team – GovCERT Austria**. Responds to and prevents security incidents relating to information and communications technology (ICT) in cooperation with CERT.at.
- **National Computer Emergency Response Team – CERT.at**. Serves as the primary contact point for cybersecurity incidents and coordinating threat intelligence.
- **Criminal Intelligence Service Austria – Cybercrime Competence Centre (C4).** Responsible for cybercrime investigations and digital forensics.

Co-funded by the European Union

- **State Security and Intelligence Directorate (DSN) – Cyber Security Centre (CSC).** Focuses on incidents relating to state security, in particular the critical infrastructure and constitutional institutions.
- **Federal Ministry of the Interior Department IV/10 Network and Information Systems Security.** The operational NIS authority ensures cybersecurity compliance for essential service operators, digital service providers, and public institutions.
- **Austrian Energy CERT (AEC)**. The sector-specific CERT for energy infrastructure, providing cybersecurity coordination for the electricity and gas industries.
- **Austrian HealthCERT (AHC)**. The sector-specific CERT for healthcare institutions, handling security incidents and supporting technical risk management.
- **Federal Ministry of Defence (BMLV).** Leads Austria's cyber defense strategy, securing military ICT systems and defending against cyberattacks targeting national sovereignty.
- **Federal Ministry for European and International Affairs (BMEIA).** Manages cyber diplomacy, developing Austria's international cybersecurity policies and engagement within the United Nations and EU.

These institutions actively invest in cybersecurity measures, research, and workforce development. They provide career opportunities in cyber defense, digital forensics, compliance, and policy development, reflecting Austria's increasing investment in national cyber resilience.

The private sector, businesses, and critical infrastructure operators in Austria have also significantly increased their cybersecurity budgets, driven by regulatory requirements and growing cyber risks. Many companies, especially those in critical infrastructure sectors (finance, energy, healthcare, manufacturing, and telecommunications), have implemented Security Operations Centers (SOC), Endpoint Detection and Response (EDR), Information Security Management Systems (ISMS)

Co-funded by the European Union

and Security Information and Event Management (SIEM) solutions, requiring trained cybersecurity professionals to manage and operate these technologies.

Furthermore, the NIS2 Directive, Digital Operational Resilience Act (DORA), and other legal regulations have forced more companies to adopt stronger cybersecurity frameworks, leading to a growing demand for risk management and regulatory compliance professionals.

For those seeking career opportunities in cybersecurity, Austria offers a dynamic job market, strong institutional support, and significant private sector investment. The demand for experts in threat intelligence, incident response, risk management, and regulatory compliance is expected to continue growing in the coming years, making cybersecurity one of the most promising career fields in Austria.

6.2.2 Study programs, trainings, certifications, online/offline courses

Austria offers a comprehensive array of study programs, training courses, and certifications in cybersecurity, catering to both academic and professional development. Below is an overview of some of the notable opportunities available within the country.

Vienna University of Technology (TU Wien) is Austria's largest university in the field of engineering and natural sciences. The Bachelor's Programme in Informatics at the Vienna University of Technology provides a comprehensive education in computer science, covering programming, databases, networks, algorithms, and software engineering, with a strong emphasis on mathematical and theoretical foundations. The Cybersecurity specialization equips students with skills to detect cyberattacks, conduct security testing, and develop secure systems. Core subjects include operating systems, distributed systems, logic and reasoning in computer science, and artificial intelligence, while electives focus on cryptography, security engineering, privacy-enhancing technologies, and others. Graduates can pursue careers as Security Architects, Cyber Vulnerability Analysts, Risk Analysts, Data Security Expert, and Security Consultants in the rapidly growing field of cybersecurity. More details can be found here.

Co-funded by the European Union

Graz University of Technology (TU Graz) conducts teaching and research in the field of engineering and technical natural sciences. The Bachelor's Degree Programme in Computer Science at Graz University of Technology provides a comprehensive foundation in computer technologies, software engineering, and information security, preparing students for diverse career opportunities in IT and research. The program offers specialization options in security, software engineering, data science, machine learning, or computer vision, emphasizing both theoretical knowledge and hands-on experience. Students gain expertise in IT security, cryptography, and secure system design, making them well-equipped for roles as IT specialists, data scientists, researchers, and software developers. More details about the programme can be found here.

The MSc in Software Engineering and Internet Computing at Vienna University of Technology (TU Wien) focuses on software development for distributed systems, mobile computing, internet security, and e-commerce technologies. The program covers key areas such as software engineering, system architecture, networking, privacy, and others. Students can specialize in Security and Privacy, gaining expertise in system security, network security, cryptography, and formal security methods. Graduates acquire strong skills in software design, risk management, and cybersecurity, preparing them for careers in IT security, software architecture, research, and consulting. The program offers international exchange opportunities, research involvement, and a pathway to doctoral studies. More details are available here.

The University of Innsbruck, as the largest research and educational institution in Western Austria, also offers specific training in ICT security. The Master's Programme in Computer Science at the University of Innsbruck provides an advanced education in computation, interaction of software and hardware in distributed systems, digital system optimization, and other areas. Students can specialize in Logic and Learning, Secure and Distributed Computing, or Perception, Interaction, and Robotics, developing skills in problem-solving, systematization, and independent research. The

program includes elective modules in information security and network security, equipping students with expertise in cryptography, secure and distributed computing, robotics, etc. Graduates are prepared for research and development roles in academia, industry, and cybersecurity-focused careers. More details are available on the programme's website.

TÜV AUSTRIA Academy offers specialized training and certification programs, equipping people with the skills to protect industrial and production systems from cyber threats:

- **Certified OT Security Practitioner (COSP).** Focuses on securing production systems, understanding vulnerabilities, and recognizing cyber threats in industrial environments with long update cycles.
- **Certified OT Security Technical Expert (COSTE).** Provides in-depth technical security knowledge, covering attack campaigns, threat detection, and protective measures for technicians and engineers, among others.
- **Certified OT Security Manager (COSM).** Prepares participants to identify threats, enhance security levels, and implement long-term risk management strategies, with a focus on process management and organizational security.

More details are available on the official website.

CIS - Certification & Information Security Services GmbH is an Austrian certification body specializing in information security, data protection, cloud computing, IT services, data center management, and business continuity management. The organization is federally accredited by Akkreditierung Austria, which operates under the Federal Ministry of Labour and Economy (BMAW). It also has the internationally recognized accreditation by APMG.

CIS organizes education and training programs, offering a wide range of courses and seminars that equip individuals with the necessary expertise in cybersecurity, data protection, and IT governance. It also provides corporate and professional certifications. For instance, CIS Personal Certificates for ISO 27001 (an international information security standard) are officially recognized, offering professionals a

valuable credential in the field of information security. More details about the personal certification can be found here.

6.2.3 Funding support opportunities to undertake cybersecurity studies, trainings, certifications

Austria offers a variety of scholarships and financial aid programs to support students at different stages of their academic journey in different fields, including cybersecurity. These funding opportunities are available to Austrian students as well as international students, depending on eligibility criteria. Scholarships in Austria are designed to recognize academic excellence, support research projects, facilitate international mobility, and assist students facing financial constraints.

Different types of scholarships in Austria include:

1. Merit-based scholarship (Leistungsstipendium). Merit-based scholarships are awarded to students who demonstrate outstanding academic performance. These scholarships are granted by higher education institutions based on predefined criteria set by each institution. Students can apply through their faculty or the administration of their educational institution. The funding amount varies depending on academic achievements and available budget allocations.

2. Research and project scholarship (Förderungsstipendium). This scholarship is intended for students with exceptional academic records who are conducting scientific research projects as part of their diploma, master's, or doctoral studies. It provides financial assistance for the completion of dissertations, theses, or creative projects. The application process and award decisions are managed by the university's faculty or research department.

3. Study abroad scholarship (Auslandsstipendium). Students enrolled in Austrian universities who undertake a temporary study program abroad, including in the field of cybersecurity, may be eligible for financial aid for a maximum period of 20 months. To qualify, students must already be receiving regular study grants

Co-funded by the European Union

(Studienbeihilfe) while studying in Austria. The application must be submitted within three months after the completion of the study period abroad.

4. Graduation scholarship (Studienabschluss-Stipendium). This scholarship is designed for working students who decide to leave their jobs in order to focus on completing their studies. Eligible students must be in the final phase of their degree and must not have reached the age of 41 years at the time of application. This funding helps students successfully finish their studies without financial burdens.

5. Student aid after self-support scholarship (Studienbeihilfe nach Selbsterhalt). The student aid after self-support scholarship is intended for students who have been financially independent before or during their studies. To qualify, students must have earned at least €11,000 per year for four years before applying (parental income is not considered when determining eligibility).

6. Funding opportunities for apprentices. Austria offers financial support not only for students but also for apprentices. Beyond the apprentice salary provided by training companies, apprentices can apply for various federal and state-level grants to help cover expenses such as living costs, travel to training centers, accommodation, and further education opportunities. More information about support and funding for apprentices can be found here.

7. Funding opportunities for international students and researchers. Depending on your country of origin and specific area of study, various institutions — including the OeAD, foundations, and other funding organizations — offer a wide range of scholarship programs. Some universities, like TU Graz, offer scholarships specifically to pursue a career in cybersecurity. A comprehensive overview of available funding options can be found on grants.at, Austria's largest database for scholarships and research funding across all academic disciplines.

Further information about these additional scholarship opportunities in Austria is available here and here.

Co-funded by the European Union

6.2.4 Other supporting organisations

Austria has a robust cybersecurity ecosystem supported by government institutions, private sector initiatives, and non-profit organizations. These stakeholders play a crucial role in providing information, organizing events, facilitating internships, and offering support to strengthen the cybersecurity sector. Below is an overview of key organizations and initiatives fostering cybersecurity careers and professional development in Austria.

Cybersecurity networks and initiatives in Austria include the following:

National Coordination Center for Cybersecurity (NCC Austria). The National Coordination Center for Cybersecurity (NCC Austria) serves as a central hub for cybersecurity initiatives, supporting Austria's cybersecurity strategy and fostering collaboration between industry, academia, and government. It provides access to networks, funding opportunities, and knowledge-sharing platforms that help professionals and organizations navigate the cybersecurity landscape.

European Digital Innovation Hubs (EDIH) in Austria. The European Digital Innovation Hubs (EDIHs) support the application of artificial intelligence, cybersecurity, high-performance computing, and other digital technologies. These hubs operate on both regional and European levels, facilitating digital transformation efforts. Austria has four EDIHs, each with a specific focus:

- **Applied-CPS** – specializes in Applied Cyber-Physical Systems.
- **Crowd in Motion** – focuses on crowd technology and motion data science for tourism, sports, and public organizations.
- **EDIH innovATE** – supports digital innovation in agrifood, timber, and energy sectors.
- **AI5production** – facilitates AI-driven digital transformation of SMEs towards Industry 5.0 production processes.

Co-funded by the European Union

These hubs provide consulting, training, and innovation support, complementing Austria's national cybersecurity network.

Cyber Security Platform (CSP). The Cyber Security Platform (CSP) is Austria's primary cooperation platform for public-private partnerships in cybersecurity. It brings together government agencies, critical infrastructure operators, and private companies to develop recommendations for cybersecurity. The platform holds meetings one to two times per year and operates working groups focusing on various cybersecurity challenges. The Federal Chancellery of Austria (BKA) oversees CSP activities.

KIRAS Security Research Map. The KIRAS Security Research Map includes over 500 registered institutions involved in security research, including cybersecurity. This initiative helps organizations find suitable partners for cybersecurity research and development.

Women4Cyber Austria. Women4Cyber is an initiative dedicated to increasing female participation in the cybersecurity sector. The network supports women through mentorship programs, workshops, and training sessions aimed at building skills and professional confidence in cybersecurity. Women4Cyber Austria actively promotes diversity and inclusion, ensuring more women enter and succeed in the cybersecurity field.

Competence Center for Safe Austria (KSÖ). The center works to improve Austria's overall security through collaboration among citizens, law enforcement, policymakers, media, academia, and businesses. The organization runs various cybersecurity awareness campaigns and educational initiatives.

Austrian Digital Skills Initiative. The initiative is supported by four federal ministries and promotes digital literacy in society, administration, education, and the workforce. It offers free workshops on topics such as digital security, e-government services, and artificial intelligence, ensuring Austria remains at the forefront of digital skills development.

Austrian Trust Circle (ATC). The Austrian Trust Circle (ATC) is a national initiative for knowledge exchange on ICT security and security incidents. It primarily focuses on critical infrastructure sectors and public administration, ensuring a secure and coordinated response to cybersecurity threats. The ATC is a joint initiative between CERT.at and the Austrian Federal Chancellery.

Cyber Security Austria (CSA). Cyber Security Austria (CSA) is an independent non-profit association addressing IT and cybersecurity challenges for Austria's critical and strategic infrastructures. CSA actively engages in publications, lectures, and research projects, enhancing cybersecurity awareness and knowledge-sharing.

CERT Association Austria. The CERT Association Austria is a cooperation between Austrian Computer Emergency Response Teams (CERTs), as well as GovCERT Austria, which supports cybersecurity efforts for public administration. The initiative ensures that cybersecurity risks are managed effectively through information sharing and resource optimization.

IT-Security Experts Group. The IT-Security Experts Group is a national association of IT security service providers and consultants, promoting high-quality cybersecurity solutions and standardized processes for businesses and institutions in Austria.

More information about these and other initiatives can be found here:

- NCC Austria - Overview of networks and initiatives dealing with cybersecurity in Austria.
- Federal Chancellery of Austria - Cybersecurity Activities and Initiatives.
- Austrian Federal Chancellery and the A-SIT Center for Secure Information Technology-Austria - Advice and awareness-raising in the ICT sector.

A number of organizations and companies in Austria offer internship programs for students and young professionals looking to gain practical experience in cybersecurity. Below are some examples of such **internship opportunities**:

Co-funded by the European Union

KPMG Austria – Technical cybersecurity consulting internship. KPMG Austria offers an internship in technical cybersecurity consulting starting from January 2026, providing students with hands-on experience in penetration testing, incident response, security architecture, and vulnerability management. The program is available in Linz, Graz, and Vienna, with a possible full-time job offer upon completion. Students are expected to have basic IT security knowledge and programming skills.

SBA Research – security consulting & penetration testing internship. SBA Research, one of Austria's largest cybersecurity research and consulting centers, offers a cybersecurity internship in Vienna focused on secure software development, penetration testing, and security operations. Candidates should have a background in IT security, programming, and network infrastructure. The internship currently lasts up to six months, with an option for permanent employment afterward. In addition to exciting internship opportunities, SBA research organizes regular Security Meetups, the SBA Live Academy, the "Zukunft Denken" – Podcast and the sec4dev Conference talks. You can learn more about these and other activities **here.**

Deloitte Austria – cybersecurity internship. This internship at Deloitte Cyber Risk Advisory offers opportunities in IT security consulting, identity and access management, data protection, GDPR compliance, and penetration testing. Interns engage in real-world security projects for clients, supporting cloud security and network security implementations.

In addition to cybersecurity networks, initiatives and internship opportunities, inspiring cybersecurity enthusiasts can also showcase and enhance their skills by participating in the Austria Cybersecurity Challenge (ACSC). It is Austria's first initiative dedicated to identifying and recruiting emerging cybersecurity talent, supported by the Federal Chancellery of Austria and organized by the Cyber Security Austria (CSA) Association in collaboration with the Austrian Federal Ministry of the Interior and the Austrian Federal Ministry of Defence.

Co-funded by the European Union

6.3 GREECE

6.3.1 Cybersecurity sector situation and general work opportunities

Greece has seen a surge in demand for cybersecurity professionals as digital transformation accelerates across industries such as finance, healthcare, telecommunications and energy. With the implementation of the EU's General Data Protection Regulation (GDPR) and an increase in sophisticated cyberattacks, ranging from phishing scams to advanced persistent threats (APTs), organisations in Greece are prioritising cybersecurity investments to protect sensitive data. Industries such as finance, healthcare, shipping, and energy are particularly vulnerable due to their critical infrastructure. This has led to a growing demand for skilled cybersecurity professionals capable of addressing these challenges.

The cybersecurity field in Greece offers diverse roles such as cybersecurity analysts, penetration testers, security engineers and IT risk managers. These roles are particularly prevalent in Athens and Thessaloniki, where technology hubs are expanding. Job postings on platforms such as LinkedIn and Glassdoor highlight positions that require expertise in threat analysis, incident response and security architecture.

The Greek cybersecurity market is expected to grow at a compound annual growth rate (CAGR) of 7.7% from 2022 to 2027.[11] This growth is driven by the rising number of IoT devices and cloud-based services, which present both opportunities and vulnerabilities. Mordor Intelligence (2023)[1] underscores the significant investments in cybersecurity infrastructure and solutions by private and public sectors.

The market landscape is distinguished by a moderate degree of competition, with leading entities investing in product development and strategic

[11] https://www.mordorintelligence.com/industry-reports/greece-cybersecurity-market

Co-funded by the European Union

partnerships in order to reinforce their market position. The advent of the global pandemic has precipitated a rapid acceleration in the digital transformation of enterprise security, with a concomitant shift in focus towards cloud and virtualised infrastructure. The expansion of internet access across urban, suburban, and rural households in Greece offers substantial growth prospects for the cybersecurity sector. Moreover, the rising uptake of digital payment instruments and the growth of online payment solutions are also contributing to an expansion in the market. Joint initiatives between governmental bodies and global technology leaders such as Cisco and ISACA are aimed at enhancing Greece's cybersecurity infrastructure and promoting awareness and educational programmes in this area.[12]

6.3.2 Study programs, trainings, certifications, online/offline courses

Undergraduate Programs

American College of Greece (ACG): ACG's BSc in Cybersecurity and Networks program[13] integrates practical training with a strong theoretical foundation. Students gain skills in areas like network security, cryptography, and ethical hacking, preparing them for certifications such as CompTIA Security+ and Certified Ethical Hacker (CEH).

Metropolitan College: The BSc (Hons) Cyber Security and Networks program[14] is offered in collaboration with UK universities, ensuring international academic standards. The program includes modules like Cloud Security, Malware Analysis, and Cybercrime Investigations.

---

[12] https://www.mordorintelligence.com/industry-reports/greece-cybersecurity-market/market-size

[13] https://www.acg.edu/undergraduate/undergraduate-programs/school-of-liberal-arts-sciences/liberal-arts-sciences-majors/cybersecurity-and-networks/

[14] https://www.mitropolitiko.edu.gr/en/programmes-of-study/faculty-of-computing/bsc-hons-cyber-security-and-networks/

Co-funded by the European Union

Postgraduate Programs

Mediterranean College MSc in Cyber Security[15]: This program offers advanced training in enterprise security, digital forensics, and risk management. The curriculum incorporates case studies and hands-on lab sessions using real-world cybersecurity tools like SIEM and intrusion detection systems.

International Hellenic University (IHU): The MSc in Cybersecurity[16] emphasizes practical application, with students engaging in projects that address real-world cybersecurity challenges. The program's partnerships with industry leaders provide internship opportunities for hands-on learning.

6.3.3 Funding support opportunities to undertake cybersecurity studies, trainings, certifications

A small number of scholarships are available from academic institutions in Greece. The American College of Greece[17] offers scholarships like the OTE Group Expendable Scholarship, targeting students pursuing careers in IT and cybersecurity. These scholarships cover partial tuition fees based on academic merit and financial need. Mediterranean College[18] provides scholarships covering up to 50% of tuition for its MSc programs, especially targeting professionals who wish to advance their cybersecurity expertise.

Additional, the Greek government[19] supports cybersecurity education through initiatives like the Digital Greece program, which aims to upskill the workforce in ICT fields. Subsidies are available for professionals enrolling in certified training programs.

---

[15] https://www.medcollege.edu.gr/en/courses/msc-cyber-security/
[16] https://st.ihu.gr/studies/postgraduate/cybersecurity
[17] https://www.acg.edu/current-students/financial-assistance/undergraduate-financial-assistance/scholarships-for-entering-students/
[18] https://www.medcollege.edu.gr/en/study-in-mc/admissions/fees-funding-scholarships/
[19] https://digital-skills-jobs.europa.eu/en/latest/briefs/greece-snapshot-digital-skills

6.3.4 Other supporting organisations

European Union Agency for Cybersecurity (ENISA): Based in Athens, ENISA acts as a hub for cybersecurity expertise in Europe. The agency organizes the annual Cybersecurity Skills Conference and provides reports, tools, and guidelines to improve skills across the sector. ENISA also offers internship programs for students interested in cybersecurity policy and operations.

Hellenic Police Cyber Crime Division: This specialized unit combats cybercrime in Greece and offers collaborations with academic institutions to train students in forensic analysis and cyber investigations. They frequently host awareness campaigns and events to educate the public about cybersecurity threats.

Microsoft Greece: Microsoft's initiatives, such as the Microsoft Learn platform, provide free resources on cybersecurity fundamentals and advanced topics. Additionally, Microsoft organizes events like the Azure Security Bootcamp to familiarize students and professionals with cloud security best practices.

Cisco Networking Academy: Cisco's programs in Greece focus on training the next generation of cybersecurity professionals. Through partnerships with universities, they deliver courses that prepare students for globally recognized certifications. Cisco also runs hackathons and workshops for hands-on practice.

National Cybersecurity Authority (NCSA): The NCSA promotes public-private partnerships to foster innovation in cybersecurity. It supports startups by providing funding, mentorship, and networking opportunities. The NCC also collaborates with universities to align academic curricula with industry needs.

Co-funded by the European Union

6.4 UKRAINE

6.4.1 Cybersecurity sector situation and general work opportunities

According to Statista's projections, the cybersecurity industry is expected to grow by a substantial 8.54% annually between 2024 and 2029, reaching a market volume of US$208.80 million by 2029. Key areas driving this growth include AI, machine learning, and blockchain, with high-demand sectors such as finance, healthcare, and government. Professional certifications like CISSP, CEH, and CCSP can significantly enhance career opportunities in the field.

The Ukrainian cybersecurity market consists of 67 local companies, with 67% headquartered in Ukraine but maintaining foreign offices, while 33% are foreign companies with offices in Ukraine. Of these market players, 59% are small to medium-sized businesses, and 8% are large local companies. The private sector dominates, comprising 98% of the market, with 88% privately owned and 10% publicly traded. Notably, 90% of public companies in the sector are foreign entities, including Deloitte, Ernst & Young, KPMG, and PWC. The top three services offered by cybersecurity companies include security audits and IT system testing, compliance with international standards, and penetration testing. Remote work opportunities are increasing, with high availability across various job platforms.

Top cybersecurity employers in Ukraine include Hacken, Iterasec, Berezha Security Group, Apriorit, TechMagic, and Infopulse. These companies are highly regarded for their expertise and cutting-edge solutions in the cybersecurity realm. Networking and continuous learning are crucial for landing jobs in this thriving sector. Startups are widely regarded as engines of growth, driving employment, innovation, and competitiveness while contributing to economic development. Startups in the cybersecurity sector add a crucial dimension: they enhance the overall level of cybersecurity and provide empoyment. Notable examples include CyberUnit, UnderDefence, Divoro,

Co-funded by the European Union

10Guards, Berezha Security Group, Cyberlands, and CyberLabs (SET University).

According to cybersecurity indexes rankings, Ukraine presents the following NSCI fulfilment percentages:

- 10th National Cyber Security Index (81 %)
- 78th Global Cybersecurity Index (66 %)
- 46th E-Government Development Index (80 %)
  43rd Network Readiness Index (55 %)

Ukraine brings significant value in terms of talent, entering 2023 with a rapidly expanding IT market that includes over **240,000 tech specialists[20].** Ongoing cyberattacks from Russia have provided these professionals with unparalleled experience and knowledge, which will serve as a critical asset for Ukraine in the years ahead. There is a notable emphasis on harnessing AI technologies and building a robust cybersecurity ecosystem, creating abundant career opportunities within the field. To sustain their growth, Ukrainian cybersecurity companies need access to a skilled talent pool. However, they face fierce competition from both domestic and international companies for top professionals, which can limit their growth potential.

However, the shortage of skilled professionals remains one of the most pressing challenges for the global cybersecurity community. Despite the industry's growth, the ongoing Russian aggression has resulted in a brain drain, with many skilled cybersecurity professionals leaving Ukraine. This has made recruiting and retaining top talent more challenging for Ukrainian companies, potentially slowing the industry's development. Addressing this talent shortage while promoting greater inclusivity is essential to building a stronger, more resilient cybersecurity ecosystem.

[20] Cyber/nnov8, Building Tech of Tomorrow, 2023

Co-funded by the European Union

In the European Union alone, the gap is estimated to range between **260,000 and 560,000 cyber professionals[21].** One significant aspect of the cybersecurity talent gap is the low participation of women and the underrepresentation of minority groups. Currently, women account for only **24% of cybersecurity professionals** worldwide. Ukraine faces a similar challenge, grappling with its own gender gap in the field[22].

The average salary for a Cybersecurity Analyst in Ukraine is $51,750 per year. Entry-level positions (Junior Level) start at $31,050 - $41,400, while experienced professionals (Senior Level) can earn up to $62,100 - $93,150. Core skills include Security Analysis, Incident Response, and Threat Detection. Trending skills are Cloud Security and Zero Trust, while emerging skills focus on AI Security and Quantum Security. A whopping 68% of job postings on popular portals like Work.ua, Jooble, and Robota.ua list specific technical skills as requirements[23].

The **Cybersecurity Strategy of Ukraine (2021)** outlines critical goals and tasks, grouped into three overarching strategic priorities: deterrence (focused on preventing cyber threats), cyber resilience (emphasizing the ability to withstand and recover from cyber incidents), and promoting collaboration among key stakeholders. Current requirements for technical, operational, and organisational measures have faced criticism for being overly complex, rigid, and adopting a one-size-fits-all approach. As a response, Ukraine's updated basic cybersecurity requirements are anticipated to align more closely with global best practices in cybersecurity risk management. Specifically, these updates are expected to incorporate methodologies from the NIST Cybersecurity Framework 2.0.

[21] https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy
[22] https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx?la=en&hash=4C3B33AABFBEAFDDA211856CB274EBDDF9DBEB38
[23] https://jobicy.com/salaries/ua/cybersecurity-analyst

Co-funded by the European Union

Traditionally regarded as the domain of military or special agencies, national defence is now, after 2022, approached as a whole-of-nation endeavour. The full-scale Russian invasion has catalyzed an unprecedented level of **private sector engagement in national defence**. Thousands of private individuals and organisations have actively supported Ukraine's efforts to counter Russian aggression, significantly shaping the potential evolution of public-private collaboration in cybersecurity. Civilians with an interest in contributing to national defence through cybersecurity can participate in voluntary, pro-bono cyber defence activities during peacetime and serve in specialized cyberwar defence units during wartime or emergencies. However, there are significant challenges in determining the formats for involving individuals and private entities.

Ukraine seeks to develop versatile mechanisms to leverage the expertise of individual professionals and private entities in its cyber defence initiatives. The **Ukrainian cybersecurity community** was among the first to join the defense efforts during the aggression. Initiatives like the **IT Army**, launched by the Ministry of Defense, and multiple cyber defense groups continue to play a pivotal role. Given the importance of involving civil society in developing Ukraine's cybersecurity sector for Ukraine, it is anticipated that legal mechanisms will soon be developed to establish a robust framework for diverse models of public-private collaboration in cybersecurity.

In parallel, the Government of Ukraine (GoU) is actively fostering the growth of local cybersecurity products and services while encouraging innovation in the sector. Ukraine has already introduced a special legal regime, **"DIIA CITY,"** to support the development of the IT industry, including the cybersecurity domain. Other notable initiatives include cybersecurity innovation clusters like **BRAVE1**, an accelerator program by the Ministry of Defence of Ukraine, and the annual **National Defence Hackathon.** Additionally, Ukraine continues to invest in its cybersecurity education system, creating favourable opportunities for young professionals and supporting

Co-funded by the European Union

workforce development. These efforts are expected to raise public awareness and enhance overall cybersecurity culture among Ukrainian citizens[24].

6.4.2 Study programs, trainings, certifications, online/offline courses

Ukraine offers significant opportunities for enhancing vocational education and training (VET) in cybersecurity, which is particularly relevant for students in vocational schools such as nursing, electrical work, and aviation technologies. This potential is driven by **several key factors:** Ukraine is a leader in the cyber warfare arena, and there are promising opportunities to develop bachelor's and master's degree programs in cybersecurity through partnerships with both private enterprises and government entities. Over the past two years, Ukrainian institutions have significantly improved their cyber education capabilities by bringing in instructors from top industry firms and governmental organizations. As educational programs in cybersecurity continue to grow, more vocational schools are incorporating cybersecurity-related courses into their curricula. Additionally, many of these institutions are hosting Capture the Flag competitions to spark greater interest among students in the field.

The need for cybersecurity skills is especially urgent in infrastructure sectors such as energy, banking, and fintech. This guidance aims to equip vocational school students with the necessary knowledge and skills in cybersecurity, ensuring they are prepared for the evolving demands of their respective fields.

In Ukraine a young person may enroll in cybersecurity after grade 9 in a college (VET) under the specialty "125 Cybersecurity". The form of study is full-time, lasting 3 years and 10 months. The educational degree awarded is a professional junior bachelor. You can enroll in a college based on an interview and a motivational letter. The admission process will begin with the registration of applicants' electronic cabinets in the summer of the admission year. Up to

[24] https://practiceguides.chambers.com/practice-guides/cybersecurity-2024/ukraine/trends-and-developments

Co-funded by the European Union

10 schools offer this speciality, they may be found at such aggregator websites as: https://www.education.ua/colleges/kiberbezpeka-ta-zakhyst-informatsii/ Then, after grade 11, it is possible to enrol in the same specialty "125 Cybersecurity" in either full-time or part-time study formats to the HEIs. To enter a university, you will need the results of external independent evaluation (EIE)/Unified National Testing (UNT) and a motivational letter. The admission process will start with the registration of applicants' electronic cabinets in the summer of the admission year. The duration of study depends on the chosen degree: Bachelor - 4 years (3 years and 10 months), Master - 5 years (4 years and 10 months). The specialty 125 "Cybersecurity and Information Protection" in Ukraine belongs to the field of knowledge 12 "Information Technology". This specialty trains professionals who are skilled in programming, encrypting data, detecting potential threats, preventing cyber attacks, developing information protection strategies, administering and updating network systems, investigating digital intrusions, and mitigating the consequences of hacker attacks.

There are more than 60 institutions offering cybersecurity as a specialisation, they mostly may be found at such consultancy websites as: https://osvita.ua/vnz/guide/search-17-0-0-42-0.html This list represents only state funded institutions. In 2024, the state allocated 1,457 budget places for the preparation of bachelors in specialty 125 "Cybersecurity and Information Protection". To be eligible for state-funded education, your competitive score must be above 130, which is above minimum.

There are also other such nation-wide initiatives as a **governmental initiative** on cybersecurity education for wider audience. The Ministry of Digital Transformation, together with the Office of the Prosecutor General, have created three educational series, which discuss cybersecurity and types of internet fraud (https://osvita.diia.gov.ua/catalog/topic/cyber-security , it uses an approach of educational series of short movies). The series can be viewed on the Diia.Education website: "Cyber Hygiene: How to Protect Yourself

Co-funded by the European Union

from Phishing"; "Cyber Hygiene for Youth"; "Basic Knowledge of Cyber Hygiene". The project was created with the support of the USAID project "Cybersecurity for Ukraine's Critical Infrastructure."

The nationwide information and educational campaign to raise the awareness level of the Ukrainian population regarding cyber threats and the basic rules of cyber hygiene is being implemented by the U.S. Civilian Research and Development Foundation (CRDF Global) in Ukraine, supported by the U.S. State Department and facilitated by the National Cybersecurity Coordination Center at the National Security and Defense Council of Ukraine and the Ministry of Education and Science of Ukraine, as well as with the informational support of "All-Ukrainian School Online," NGO "Osvitoria," and "Kyiv Digital." The initiator and organizer of the campaign is the U.S. Civilian Research and Development Foundation in Ukraine (CRDF Global in Ukraine) with support from the U.S. State Department. The goal of the campaign is to increase the overall level of citizens' awareness about online threats and to teach the basics of cyber hygiene. The program materials will be useful for teenagers, adults, and the elderly. This campaign is a continuation of the first successful wave, which lasted from September 2022 to September 2023. It is continuously being improved, adapting to new threats and engaging new users to create a safe online space in Ukraine. Participants of the campaign will be able to familiarize themselves with simple and understandable cybersecurity rules, and also test their knowledge through an interactive game: this can be done via the provided link (https://game.shotam.info/pravyla-kiberbezpeky/).

There is also **a number of international projects**, e.g. Google's platform on Internet safety for children (https://mon.gov.ua/news/google-predstavyv-v-ukraini-platformu-bezpeka-ditei-v-interneti); Encycled Erasmus+; Cyberteens, etc. The goal of the CyberTeens project is to raise the awareness of teenagers about cybersecurity through an educational online platform, which will facilitate their protection in the digital space from social and digital threats, cyberbullying, and provide the corresponding psychological support.

Co-funded by the European Union

6.4.3 Funding support opportunities to undertake cybersecurity studies, trainings, certifications

Except governmental scholarships, Ukraine offers several funding opportunities for individuals seeking to pursue studies, training, and certifications in cybersecurity. Here are some notable programs:

- **Google Cybersecurity Scholarships**

In May 2023, Google announced the provision of 5,000 scholarships for Ukrainians to enroll in cybersecurity courses. This initiative aims to enhance the nation's cyber defense capabilities amid ongoing cyber threats.

- **SET University Scholarships**

SET University offers scholarships for its programs, targeting representatives of the Armed Forces, National Guard, children of combatants, Ukrainian women aspiring to enter the IT field, and migrants from conflict zones. These scholarships cover the full cost of education, promoting inclusivity in the cybersecurity sector. https://www.setuniversity.edu.ua/grants/

- **EC-Council Cybersecurity Scholarships**

The EC-Council has pledged $7 million towards cybersecurity education, aiming to certify approximately 20,000 cyber professionals globally. Ukrainian aspirants can apply for these scholarships to obtain certifications such as the Certified Cybersecurity Technician (C|CT). EC-Council Campaigns

- **USAID and Cisco Partnership**

In December 2023, USAID and Cisco partnered to support education and cybersecurity in Ukraine. Cisco is equipping five instructional labs at Ukrainian universities with state-of-the-art telecommunications equipment to train a new cadre of cybersecurity experts. USAID

- **CRDF Global Cybersecurity Grants**

CRDF Global offers grants aimed at strengthening cybersecurity in Ukrainian governmental institutions and critical infrastructure. While primarily targeting

Co-funded by the European Union

organizations, these grants contribute to the broader cybersecurity ecosystem, indirectly supporting educational and training initiatives. CRDF Global
These programs reflect a concerted effort by both international and local organizations to bolster Ukraine's cybersecurity workforce through education and training support.

6.4.4 Other supporting organisations

Below is the list and descriptions of some key stakeholders supporting cybersecurity careers and sector development in Ukraine:

- **SET University**: to promote cybersecurity education and career development offers scholarships and MicroMasters programs, specialized courses, and workshops designed to educate individuals and SMBs on cybersecurity threats and defenses. SET University
- **BRAVE1**: A defense-tech cluster accelerating cybersecurity innovation and startups, supported by Ukraine's Ministry of Defense (mentoring, funding, and resources, competitions and hackathons). BRAVE1
- **Women4Cyber Ukraine**: Focuses on increasing the participation of women in cybersecurity through training, mentorship, and advocacy. Women4Cyber Ukraine
- **Lviv IT Cluster**: Actively supports cybersecurity companies and facilitates collaboration on R&D and education initiatives (collaboration with local universities, resources for joint R&D projects, events to connect students and professionals.
- **Kharkiv IT Cluster**: Provides a platform for industry players to foster innovation and organize market-oriented events (training sessions, networking opportunities for students and professionals). Kharkiv IT Cluster
- **Ukrainian Cyber Alliance**: A volunteer-driven organization engaged in cybersecurity defense and advocacy (pro-bono training for volunteers, educates the public). Ukrainian Cyber Alliance

Co-funded by the European Union

- **UACS (Ukrainian Association of Cyber Security)** provides specialized training programs for cybersecurity professionals, offers internationally recognized cybersecurity certifications, organizes industry events, runs awareness campaigns and educational initiatives.
- **Non-profit organizations** play a crucial role in improving education quality in this sector. For example, the U.S. Civilian Research & Development Foundation (CRDF Global) promotes safety and innovation by hosting cybersecurity-themed hackathons for students. Additionally, the International Foundation for Electoral Systems conducted cyber hygiene training in Kyiv to address critical issues in democracy, governance, and elections.
- The **IT Army** is a collective of international and Ukrainian volunteer hackers collaborating with officials from Ukraine's Ministry of Defene. Organized through a Telegram channel, the IT Army identifies new Russian targets for volunteers to attack, focusing on disrupting Russian infrastructure and websites.

Before 2022 Ukraine had a rich network of foreign partners (both governments and companies) who were able to provide training and assistance, including remote monitoring and mitigation. Tech companies provided invaluable assistance; some still continue doing so. Currently many partnerships are suspended or broken.

Co-funded by the European Union

6.5 MALTA

6.5.1 Cybersecurity sector situation and general work opportunities

The cybersecurity professional community in Malta revolves around Malta Information Technology Agency (MITA) that, as also indicated in the National Cybersecurity Strategy 2023-2026[25], continues to serve as the national contact point in the field by hosting the National Cybersecurity Coordination Centre. MITA also acts as the Maltese Government Computer Security Incident Response Team (govmt-CSIRT), engaging in fora, agreeing and coordinating on cybersecurity incident response at local and international levels.

In line with the current strategy, a National Cyber Security Response Centre was also established, as well as a National Cyber Security Committee, composed of diverse national stakeholders in cyber security. Together with a network of Security Operations Centres (SOCs), these are the key means to facilitating the coordinated conduct of cybersecurity efforts in Malta.

The MITA National Cybersecurity Coordination Centre further fosters a Community of relevant stakeholders from the private and public sectors, academia and research, aimed at growing the Maltese cybersecurity field. This Community is open for all individual professionals and entities interested in cybersecurity, with membership structured along the following 6 domains: academia, research and innovation; industrial or product development; training and education; security management and operations; formal and technical standardization and specifications; law, regulations and ethics. As of end of 2024, the Community was composed of over 700 individuals and 85 entities, with 17% of them being women and 25% affiliated with an entity. The most

[25] https://economy.gov.mt/wp-content/uploads/2023/05/National-Cyber-security-2023-2026.pdf

Co-funded by the European Union

prominent expertise of these individuals and entities being Security Management & Operations[26].

The significant role that regulated industries like financial services, i-gaming, aviation and education services have in the Maltese economy, further raises Malta's demand for cybersecurity specialists to protect the sensitive financial and personal data that these industries work with. According to latest data from sectoral regulators, there are over 1,000 closely regulated companies in Malta. Moreover, Malta's ICT sector (handling information and communications, including computer and network hardware, as well as connected software) includes over 300 companies and represents over 10% of the Gross Domestic Product (GDP), one of the highest proportions in the EU[27].

6.5.2 Study programs, trainings, certifications, online/offline courses

A number of cybersecurity related education and training opportunities are available in Malta, including:

The **Master's Programme in Cybersecurity of the University of Malta** Faculty of ICT, aimed at providing both theoretical knowledge and practical skills in cybersecurity by exposing students to topics ranging from ethical hacking, network security, cloud security, digital forensics and incident response, to AI in data security, management and legal aspects. With a view to facilitate its uptake also by people already working, the lectures and labs are planned to be delivered on a part-time blended basis, involving a mix of in-person, online and asynchronous learning. This Master's Programme is designed with practitioners in mind, involving hands-on practical sessions and industry placements, with learning outcomes that prepares students to further specialise in cybersecurity roles. For more information see here and here.

[26] Malta NCC presentation at CyberBreakfast event organised in December 2024
[27] https://businessnow.mt/ict-sector-makes-up-10-3-of-maltas-economy-most-in-eu/

The **Malta College of Arts Science and Technology (MCAST)** Institute of ICT also offers a **Bachelor of Science (Honours) in Cybersecurity**. This is a 3-year degree programme that covers topics like open source operating systems, network security, database programming, digital forensics, and offensive security. The work-based and research components of this programme allow students to gain sufficient hands-on experience to swiftly and effectively pursue careers in the cybersecurity sector. Read more here and here.

Besides other ICT security related courses, like ITNET-506-1806 Network Security and ITSFT-506-2012 Securing Applications, MCAST also offers opportunities for cybersecurity related learning outside of the classroom, like the Hackspace initiative.

It is also important to highlight that all MCAST degrees are have an internship component, with a minimum of 1096 hours of credited work based learning. Read more here.

Another higher education organisation in Malta, STC is offering both a **Bachelor of Science (Honours) in Cybersecurity** and a **Masters of Science in Cybersecurity**. Additionally the American University of Malta is also offering a **Masters of Science in Cybersecurity**.

In parallel, **Domain Academy Malta**, in collaboration with University of Derby and Pearson UK, offers an **online top-up course** to those holding a foundation degree in a Computing subject or international equivalent qualification, leading **to a Computing and Information Technologies BSc Degree** with components related to Cybersecurity and Ethical Hacking. This course offers the flexibility of three annual intakes and study at one's own pace, fully online. For more details see here.

The **Cybersecurity Skilling Programme run by the National Cybersecurity Coordination Centre** within Malta Information Technology Agency (MITA) also offers individuals a range of upskilling opportunities in

cybersecurity. Different specialised and generic training opportunities have been offered during different time windows between 2023-2025. The first type of training offered has been for the Security Operations Centre (SOC) Analyst role, but other courses are coming too. With entry requirements of just a minimum MQF Level 3 qualification in any discipline and minimum 1-year experience in an IT role, this training is for anyone looking to discover a new domain or simply to upskill oneself in the area of cybersecurity. It offers a blended learning approach that supports theoretical concepts with hands-on sessions, as well as one-to-one interaction opportunities with the trainers. As this Programme is fully funded by the Recovery and Resilience Facility fund, part of the NextGenerationEU Programme, the training is offered free of charge to the selected participants. For more information see here and here.

Moreover, Learnkey is also offering a **Certificate in IT Security (Cyber Security)** at EQF Level 3.

Furthermore, PwC Academy offers **various courses towards technical certification**, with further detail on these available here.

6.5.3 Funding support opportunities to undertake cybersecurity studies, trainings, certifications

Besides certain trainings being directly EU funded, the Maltese Government also offers a number of scholarship and educational tax credit schemes that may be applicable to Cybersecurity related studies. These are typically provided through key stakeholders like:

- Malta Digital Innovation Authority (MDIA) Pathfinder Digital Scholarship grants, as explained here
- Ministry of Education offering the Endeavour and Tertiary Education Scholarship schemes explained here
- Malta Enterprise managed Get Qualified and Higher Educational Qualifications schemes, that offer a tax credit of up to 70% of eligible

Co-funded by the European Union

costs to students successfully completing certification, diploma, degree or post-graduate degree courses. For more details see here and here.

6.5.4 Other supporting organisations

There are many other key stakeholders supporting cybersecurity careers and sector development in Malta – for example in terms of information, industry networking and informative events, facilitation of internships, entrepreneurship support. For example,

- Malta Information and Technology Agency (MITA), that also runs an annual ICT Summer Traineeship Scheme that matches ICT and ICT related students and employers of all sectors. Read more here.
- The Malta Digital Innovation Hub that offers digital entrepreneurship support services, a High-Tech Workspace for technical "Test before Invest" support, advanced digital skills development through short-term training courses, an apprenticeship programme and a train-the-trainer programme, digital innovation ecosystem networking and collaboration facilitation through events and other initiatives. Read more here.
- Tech.MT - a public-private partnership created by the Government of Malta and the Malta Chamber of Commerce, Enterprise and Industry, is not just supporting tech companies based in Malta, but also puts youth at its governing table to ensure its vision is aligned with students' education aspirations related to tech. Tech.MT is also a licensed educational institutions having implemented a number of initiatives related to cybersecurity too. Read more here and here.
- eSkills Malta Foundation - a National Coalition of various Government, industry and education representatives contributing to the increase in digital skills and the development of the IT profession. Read more here.
- Malta Communications Authority includes in its remit eCommerce and an extensive range of digital services, covering these from legislative framework setting, compliance monitoring and stakeholder engagement perspectives. Read more here.

Co-funded by the European Union

- Malta IT Law Association provides a specialized forum where legal developments within the ICT sector can be studied, discussed and championed with the aim to assist local technological empowerment through technology neutral legal frameworks. Read more here.
- Silicon Valletta is an association set up by Malta based tech entrepreneurs wanting to accelerate Malta's attractiveness & strengthen knowledge sharing within Maltese startup community. They do this through a number of events and activities, mentorship, investor groups and support for our members' community. Read more here.
- Microsoft Malta Hub aimed at facilitating IT entrepreneurs along their journey and to be a leader in technology skills development for all ages. Read more about their cybersecurity and other initiatives here and here.

Co-funded by the European Union

7. SPECIFIC OPPORTUNITIES FOR GIRLS

Women are still relatively rare in the field of cybersecurity, although a female perspective could lead to improved problem-solving. Nevertheless, increasing awareness of the benefits of promoting gender equality and diversity for improving team creativity and performance, hence to higher resilience against cyber threats, led to various educational and career guidance opportunities specifically for girls.

The European Cyber Security Organisation (ECSO) set-up a dedicated Women4Cyber foundation that offers webinars and in-person events, a mentorship program, scholarships and catalogue of women role models in European cybersecurity. Organisational Chapters are active in all EnCycled partner countries, except in Malta as yet.

The Women in Cybersecurity (WiCyS) organisation, although US based, is active worldwide offering a wide range of training and mentorship programs, scholarships, challenges, networking events and student chapters. Microsoft is currently also supporting the expansion of their student chapters in 12 European countries.

The SHECURITY initiative of Security Business Austria SBA Research intends to reach girls and women interested in IT security, offering regular and free training sessions that provide a unique opportunity to dive into the world of digital defence and offense. Their Hackerinnen-Training offers hacker training aiming to increase the proportion of women in the industry in the future.

The 2-3 hours training sessions cover a range of topics, from the basics of hacking, web security, Linux shell, binary exploitation, crypto basics, network security, to forensics and penetration testing. The sessions are mostly hybrid and include lectures, group problem-solving and practice.

The SBA also offers regular "Let's hack together" practice sessions and socializing events.

Co-funded by the European Union

The Austrian INDUCE project also investigates broader access and expansion of cyber exercises to new target groups by adopting a diversity approach. Through the development of diverse-sensitive cyber scenarios and competence-building actions, in the long term, this project aims to contribute to the empowerment of diverse target groups to act in digital society.

The UK Unlock Cyber – Opening Futures in Cybersecurity initiative also has dedicated events and resources for engaging girls. Moreover, the SEIDEA cybersecurity career development platform with a community of over 8000 Black, Asian and minority ethnic women offers training courses, bootcamps and educational podcasts.

CTF Tech, a woman-led Estonian startup that brings young people to cyber security through gamified training and competitions like Capture The Flag events, also has a dedicated Girls' Cyber Academy for the age group of 14-22.

Further information and resources for empowering women in cybersecurity is also available in the Women's Guide to Cybersecurity: Training & Career Paths

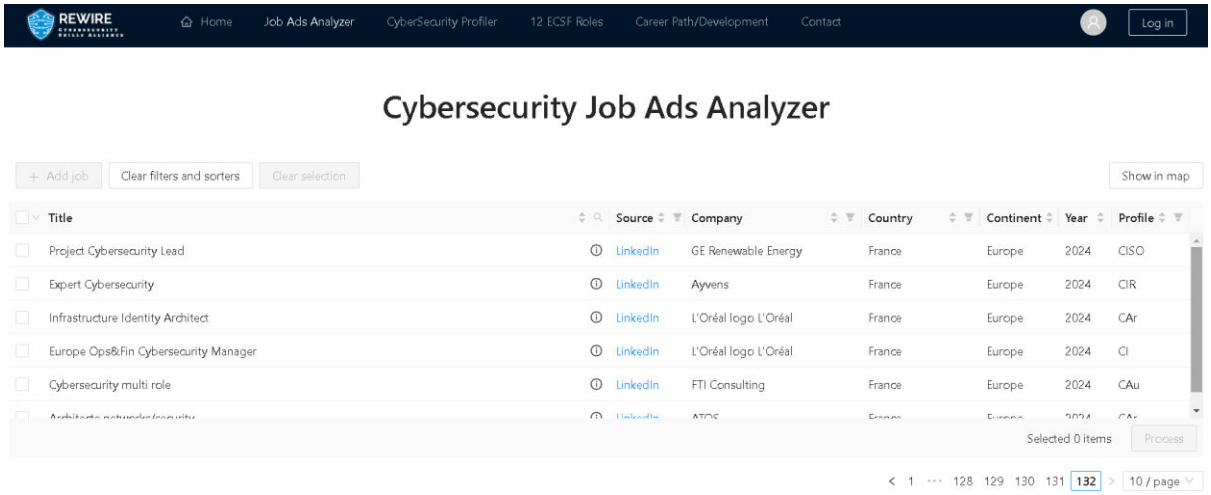
Co-funded by the European Union

8. OTHER RELEVANT EUROPEAN TOOLS AND INITIATIVES FACILITATING CYBERSECURITY STUDIES AND CAREERS

There are numerous other tools and initiatives that can help facilitating cybersecurity studies and careers in Europe.

8.1 REWIRE Job Analyzer

Part of the EU funded Cybersecurity Skills Alliance REWIRE project and the developed CyberABILITY Platform, there is also offered a Cybersecurity Jobs Analyzer tool. This provides not just a searchable database of job opportunities, but also very interesting statistics of the most sought-out skills and ENISA European Cybersecurity Competence Framework job / role profiles.



8.2 REWIRE Cyber Range

Co-funded by the European Union

The REWIRE project also developed a Cyber Range platform providing machine, container and network virtualization with an option to use public cloud infrastructure, orchestration capabilities for scenario provisioning and manual, semi-automated or automated scenario execution (including traffic generator, attack generator, event detector tools), as well as scenario packaging ability enabling standardized scenario building and exchange. Other useful information and user guides on this Cyber Range can be found here.

8.3 EU Talent Pool

Given the talent shortages in a number of European economic sectors, including in cybersecurity, the EU is currently piloting an EU Talent Pool initiative aimed at bringing together European employers with skilled 3rd country nationals jobseekers. Currently the pilot is open to persons fleeing the war in Ukraine and allowed to work in the EU under temporary protection, and operational in only a few EU Member States (e.g. Finland, Lithuania, Poland, Slovakia, Czechia, Italy, Spain and Cyprus).

Through the EU Talent Pool Pilot, Ukrainians with EU temporary protection status can create their CV and show their skills to over 5,000 employers validated and registered with the European Employment Services EURES.

8.4 EURES portal

Ofcourse, the EURES employment support services are also available to all EU citizens and employers. There are almost 4 million job vacancies currently listed on the EURES portal and employers can search for candidates through the EURES CV database. Moreover, about 1,000 EURES advisers working in the EURES Member and Partner organisations all over the EU and EEA countries, are providing support prior, during and after the recruitment process.

8.5 Digital Skills and Jobs Platform

Co-funded by the European Union

The Digital Skills and Jobs Platform is an initiative by the European Commission designed to address the digital skills gap in Europe. It serves as a comprehensive resource for individuals and organizations looking to improve their digital competencies. The Platform offers a wide range of training courses, online learning paths, and Massive Open Online Courses (MOOCs) to help users enhance their digital skills, from basic to advanced levels. Some examples of what it currently offers:

- Career Development - guidance on career paths, employability trends, and job opportunities across Europe, helping individuals to navigate the digital job market.
- Funding and Support opportunities, like grants and financial instruments available at both European and national levels to support digital skills development.
- Community and Networking, as users can join a collaborative community to network, share best practices, access expert advice and resources.
- Insights and Resources on various EU and national initiatives, research-based facts and figures, and best practices in the digital skills area.

8.6 EIT Digital

EIT Digital aims to drive Europe's digital transformation and innovation focuses on fostering digital technologies as well entrepreneurial talent with the aim to drive economic growth and improve quality of life by linking education, research and business. They focus on nurturing digital talent in Europe by providing education and training programs, including support for innovation and entrepreneurship. The overall focus is on giving people the skills, support and collaboration networks they need to succeed in the digital economy, being committed to ensuring that digital technologies are used to tackle societal challenges and improve the quality of life in Europe.

Co-funded by the European Union

EIT Digital also has specific educational offering in cybersecurity, ranging from cybersecurity essentials to specialised education programmes in Cybersecurity and Robotics. The latter focus on the design and delivery of two double-degree Master's programmes and self-standing learning modules in these two key digital technologies. These Master School programs are open to applicants with either a Bachelor of Science degree or who are in their final year of study in Computer Science, information systems, mathematics or electrical engineering.

8.7 Ukrainian Attestation Scheme of cybersecurity skills

The launch of Ukraine's first **Qualification Center for Information Technology and Cybersecurity** in June 2024 represents a pivotal step forward in the Ukraine's efforts to formalize and enhance its cybersecurity workforce. This initiative introduces a structured system for verifying and certifying the skills of cybersecurity professionals, aligning their capabilities with the rapidly evolving demands of digital market and national security objectives.

The primary goal of this new center is to establish a contemporary system for professional certification in cybersecurity, helping bridge the gap between current skills and industry requirements. By setting **standards for knowledge, skills, and competencies**, the center aims to foster a more capable and systematic cybersecurity labor market. Support from international partners has been instrumental in equipping the center with advanced tools and software, reinforcing its capacity to provide high-quality certification.

Currently, the center offers certification for two key roles: "Information Systems Security Developer" and "Network and Systems Security Administrator." These certifications are not only a testament to an individual's expertise but also contribute to elevating the standard of cybersecurity professionals across Ukraine. Future expansions are anticipated to include additional qualifications, addressing both management and technical aspects

Co-funded by the European Union

of cybersecurity, which are essential for professionals working in public institutions and critical infrastructure sectors.

In developing these standards, the Qualification Center has drawn from internationally recognized frameworks (**ECSF**[28] and Workforce Framework for Cybersecurity/**NICE Framework**[29]), **adapting** them to the unique challenges faced by Ukraine's cybersecurity landscape. This approach not only raises the professional caliber of cybersecurity specialists within the country but also prepares them to meet the challenges of an increasingly interconnected and risk-laden cyber world.

Ukraine's new certification system for cybersecurity professionals provides a structured pathway for individuals to achieve recognized expertise. By formalizing and validating the skills and competencies of its cybersecurity workforce, Ukraine is building a stronger, more resilient defense against cyber threats, safeguarding both its digital infrastructure and its broader national interests.

[28] https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework
[29] https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

Co-funded by the European Union

9. SOME SECTOR SPECIFIC CYBERSECURITY CHALLENGES AND OPPORTUNITIES RELEVANT TO VET

This section briefly presents the main challenges and opportunities related to cybersecurity in a number of vocational occupations and sectors, like healthcare, education, construction and buildings operation, energy, transportation, agro-food. The objective is to provide Vocational Education and Training (VET) students, teachers, career counsellors with a general overview of these sectors' current situation vis-à-vis cybersecurity, highlighting the importance of raising awareness and training on this topic even for future personnel in these sectors that will not be directly involved in cybersecurity. For example, doctors, nurses, carers, teachers, architects, electricians, technicians, drivers, pilots, hospitality workers, etc.

9.1 HEALTHCARE

The healthcare sector is a critical component of society, responsible for safeguarding the health and well-being of individuals. However, the increasing reliance on digital technologies has exposed the sector to a myriad of cybersecurity challenges, from phishing and malware attacks to data breaches and insider threats[30]. Nevertheless, emerging technologies, better human-computer and inter-personal interaction approaches also create opportunities for healthcare organizations to enhance their cybersecurity posture to protect sensitive patient data and ensure the continuity of critical healthcare services. For example, by leveraging AI, interoperable systems, better employee training and collaboration with cyber experts, implementing advanced security measures and adhering to regulatory standards

First, it is imperative to properly understand the faced cybersecurity challenges. **Data breaches** and **service provision disruption** are the

[30] https://www.scarlettcybersecurity.com/top-10-healthcare-cybersecurity-challenges-problems-and-issues

Co-funded by the European Union

biggest concerns for healthcare organizations, as they store highly sensitive personal information and provide vital services. Unauthorized access to patient data can lead to identity theft, financial fraud, and loss of patient trust, while inability to provide medical care can lead to deaths and significant socio-economic repercussions.

Historically, the healthcare sector been less prepared for cyber risks, further compounding the issue. Many healthcare organizations rely on **outdated technology and legacy systems** that lack modern security features. These systems are more susceptible to cyberattacks, as they may not receive regular security updates or patches. Healthcare professionals should be aware that upgrading to more secure and interoperable systems is crucial for enhancing cybersecurity, and advocate for the adoption of modern technologies to improve patient care and data security. For example, interoperable electronic health record (EHR) systems have enhanced security features and support team-based collaboration, which can not only reduce the risk of data breaches but also streamline clinical workflows and improve patient care.

Healthcare professionals should also be aware of the main ways in which cyberattacks are performed, and how can they contribute to their mitigation.

- **Phishing Attacks**, that are a very prevalent threat in the healthcare sector. Cybercriminals often send deceptive emails to healthcare workers, posing as legitimate entities such as government health agencies or insurance providers. These emails aim to trick recipients into revealing personal information or login details, leading to unauthorized access to sensitive data. Healthcare professionals must be vigilant and cautious when handling emails and messages to avoid falling victim to phishing scams. They must prioritize data security and follow protocols to protect patient information.
- **Malware Attacks**, including from spyware, adware and viruses, also pose a significant threat to healthcare systems. Malware can infiltrate networks, computers, and other connected systems, causing data

Co-funded by the European Union

breaches and disrupting healthcare services. Trojan horse malware, that is disguised as a harmless software to gain access to sensitive information, is particularly dangerous. Healthcare professionals need to have their devices equipped with up-to-date antivirus software and should not download suspicious files.

- **Ransomware Attacks** involve encrypting a healthcare organization's data and demanding a ransom for its release. These attacks can cripple healthcare services, as organizations cannot afford to lose access to critical patient data and systems. The healthcare sector's reliance on legacy systems and outdated technology makes it particularly vulnerable to ransomware attacks. The antidote is for health workers to follow best practices in data backup and recovery.
- **Insider Threats**, whether accidental (like an employee falling prey to a phishing attack) or intentional (as employees with access to sensitive data misusing their privileges), can lead to data breaches or other security incidents. Ensuring robust access controls and monitoring healthcare employees activities are essential to mitigating the risk of insider threats. Healthcare professionals should be aware of such threats and report any suspicious activities.

The **two-pronged propagation of cyberattacks,** both **via technology and human behaviour**, should be also reflected in the cybersecurity improvement measures. And as healthcare is a human intensive sector, **enhancing employee training and awareness is crucial**. Investing in cybersecurity training and awareness programs for healthcare employees can help mitigate the risk of phishing attacks and insider threats. Educating staff on best practices for data security and recognizing potential threats is essential for maintaining a secure healthcare environment.

Improvements on the technology side need to be also adopted and implemented, with the healthcare professionals needing to be key advocates and supporters in this sense, and follow best practices for data security. Like,

Co-funded by the European Union

- **Implementing advanced security measures**, such a multi-factor authentication, encryption and intrusion detection systems, can significantly reduce the risk of cyberattacks.

- **Adoption of interoperable electronic health record (EHR) systems** with enhanced security and team-based collaboration features, can not only reduce the risk of data breaches but also streamline clinical workflows and improve patient care.

- **Leveraging AI**-powered tools that can detect and respond to cyber threats in real-time, identify vulnerabilities and automate security processes, while also upholding ethical responsibility, data security and standards of patient care[31].

Healthcare staff need to also be aware and supportive of the importance of

- **regulatory compliance and adherence to industry standards** for data security, privacy and interoperability, like for example the US Health Insurance Portability and Accountability Act (HIPAA).

- **collaboration with cybersecurity experts** who can provide access to specialized knowledge, resources and technologies needed to address emerging cyber threats effectively for effective data security and patient care.

Given the huge role that human behaviour has on cybersecurity, there is also a significant opportunity for reverse **collaboration with psychologists, sociologists, mental, emotional and social care workers**. This could lead not just to better resistance, resilience and faster recovery from cyberattacks, but also to less attacks and exposure to insider threats.

31 https://kpmg.com/xx/en/our-insights/ai-and-technology/cybersecurity-considerations-healthcare-sector-insights.html

Co-funded by the European Union

9.2 BUILT ENVIRONMENT

Cyber-physical systems improve the management of connected building assets for both new and existing projects. Digital security is critical to prevent disruptions and increase resilience. The construction and infrastructure (C&I) sector is expected to grow through 2022, supporting national growth plans and driving investment in healthcare, public safety, and other infrastructure. The pandemic has accelerated the shift from traditional IT plans to digital plans, requiring a cybersecurity approach that focuses on data, not just perimeter security. In the age of ransomware, maintaining the integrity and availability of advanced analytics (AA) and artificial intelligence (AI) is essential. Key operators must protect their process knowledge to maintain a competitive edge, and data governance must prioritize classification and security[32].

This section briefly presents the main challenges and opportunities related to cybersecurity in the Architecture, Engineering, Construction, and Operation of buildings and infrastructure (AECO) sector.[33]

The following challenges should be considered:

- **Rapid digitisation**: As the construction sector rapidly adopts digital tools and technologies, it introduces potential vulnerabilities if not adequately protected. Outdated systems and software, not designed for modern cybersecurity threats, can pose significant risks. These systems may lack encryption, strong authentication and regular security patches, making them vulnerable to exploitation. For example, management systems that rely on

[32] Building cybersecurity in the construction industry - #1 Construction Prediction 2022 https://www.deloitte.com/ce/en/industries/industrial-construction/perspectives/ce-building-cybersecurity-in-the-construction-industry.html

[33] Getting Concrete about Cyber: Mitigating Risks for Construction - By Kelly Butler, Cyber Practice Leader, Marsh Specialty, 03/12/2023 https://www.marsh.com/en-gb/industries/construction/insights/getting-concrete-about-cyber-mitigating-risks-for-construction.html

Co-funded by the European Union

outdated Windows servers or unpatched software can be targeted by ransomware or other malware.

- **Autonomous machines**: The use of autonomous machinery, drones and robots, as well as the integration of Internet of Things (IoT) devices and the adoption of smart sensors and management systems in buildings, can cause physical and operational disruptions, such as the shutdown of critical structures, the manipulation of access controls and the disruption of energy management systems.

- **Collaborative projects**: Construction projects often involve multiple subcontractors and vendors with varying levels of cybersecurity practices, each of which adds potential entry points for cyberattacks. Managing and securing third-party access is complex, especially in shared environments.

- Lack of cybersecurity awareness in facility management: Facility managers and construction crews often have limited cybersecurity training, making them less aware of potential security threats and more prone to human error. Security protocols are often applied inconsistently.

- **Regulatory compliance and data privacy concerns**: Compliance with various regulations, such as GDPR in Europe or data protection laws in other regions, can be challenging due to the diverse types of data collected in smart buildings, such as tenant activity, occupancy, and CCTV footage.

- **Physical and Digital Convergence**: Combining physical security (e.g. access control) with IT networks poses unique cybersecurity challenges. An attack on a digital network can directly affect physical security, and vice versa.

- **Transient workforce**: The reliance on temporary and subcontracted labour can make it difficult to ensure consistent cybersecurity practices.

It is crucial to be aware of the potential risks in order to enhance resilience in this business area. It is therefore important to develop a strategy to reduce

Co-funded by the European Union

the impact of cyberattacks. The following section outlines some fundamental attitudes that can be adopted to mitigate risks in the build environment:

- **Adopting security principles by design**: Security by design principles encourage the incorporation of cybersecurity measures at all stages of development, from initial design to system implementation and operation. This approach helps build resilience from the start.

- **Blockchain technology for data management**: Blockchain can enhance the integrity and security of data in building management systems by creating immutable records of access, maintenance, and control activities[34].

- **Enhanced IoT and device management**: Implementing robust IoT device management practices, including firmware updates, access controls, and vulnerability management, can significantly reduce cyber risks.

- Improved cybersecurity protocols: Investing in robust cybersecurity measures can mitigate risks and protect sensitive data.

- **Integration of physical and cybersecurity measures**: Implementing solutions that integrate physical and cybersecurity measures helps to protect the building holistically. Combining physical and digital access point monitoring on a single platform can improve incident response.

- **Investment in AI and automation related to cybersecurity**: AI-driven cybersecurity tools can automate threat detection and response in real-time, which is especially valuable in large facilities with extensive digital and physical infrastructure. Through AI, it is possible to detect anomalous behaviour

[34] Blockchain Opportunities and Issues in the Built Environment: Perspectives on Trust, Transparency and Cybersecurity, Chapter, First Online: 3/12/2021, pp 569–588. https://www.researchgate.net/publication/356758000_Blockchain_Opportunities_and_Issues_in_the_Built_Environment_Perspectives_on_Trust_Transparency_and_Cybersecurity

Co-funded by the European Union

patterns in IoT devices, allowing for early detection and proactive response to potential breaches, even with limited human oversight.

- **Development of industry-specific cybersecurity standards and frameworks**, like those established for IT (e.g. NIST and ISO), can provide tailored guidelines that address the unique requirements of the built environment. Ensuring compliance with these standards can significantly enhance the fundamental security posture of buildings. Furthermore, the creation of a cybersecurity framework specifically for the building management industry can delineate best practices for network segmentation, access control, and incident response, thus fortifying the sector's overall cybersecurity resilience.

- **Cyber insurance**: Increasing the adoption of cyber insurance can help manage the financial impact of cyber incidents.

- **Cybersecurity Awareness and Training for Facility Management Teams**: Educating employees and subcontractors on cybersecurity best practices can strengthen the overall security posture by reducing human error, increasing surveillance, and improving adherence to security protocol. For example, regular training on phishing detection, password management, and incident response can help facility staff better protect building systems from cyber threats.

As buildings become increasingly intelligent and more interconnected, cybersecurity becomes a fundamental aspect of physical security. The implementation of advanced cybersecurity practices and their integration into all aspects of building management provides protection and competitive advantages as tenants and businesses prioritize secure environments.

9.3 ENERGY

The energy sector faces various cybersecurity challenges that pose risks to individual companies, national security, and public safety. These challenges

Co-funded by the European Union

arise from the unique structure of energy infrastructure, characterized by a reliance on **Operational Technology (OT)** systems, increased interconnectivity with **Information Technology (IT)** networks, and the heightened interest of nation-state actors in targeting critical infrastructure.

A significant cybersecurity challenge in the energy sector is the **vulnerability of OT systems**. These systems, including **Supervisory Control and Data Acquisition (SCADA)** systems, are essential for monitoring and controlling energy production and distribution. However, they were initially designed to focus on reliability and efficiency rather than security. This legacy design makes them more susceptible to cyber threats, as they lack many protections in modern IT systems. For instance, OT systems often operate without built-in encryption or authentication mechanisms, leaving critical processes and equipment open to manipulation by malicious actors.

Further complicating cybersecurity efforts is the **convergence of IT and OT networks**. While integrating these networks offers operational benefits, it also creates new vulnerabilities. As energy companies connect OT to IT systems for improved data analysis and operational insights, they unintentionally increase the attack surface available to cybercriminals. A vulnerability in an IT system can now provide a gateway to the OT environment, exposing critical infrastructure to cyber threats and increasing the likelihood of attacks with potentially devastating consequences.

The energy sector has also become a prime target for **ransomware attacks**. Cybercriminals recognize the high value of uninterrupted service in the energy sector and exploit this need by employing ransomware to extort money from companies. By encrypting essential data or compromising control systems, attackers can disrupt energy services, pressuring companies into paying ransoms to restore operations quickly. In recent years, high-profile ransomware incidents have underscored the urgent need for robust defenses against such threats, as these attacks' financial and operational impacts are immense.

Co-funded by the European Union

Another cybersecurity challenge is the **complex supply chain dependencies** within the energy sector. Energy providers rely on suppliers and third-party vendors for everything from hardware components to software solutions. Each vendor presents a potential vulnerability, as a breach at any point in the supply chain can lead to widespread consequences across the entire network. Attackers increasingly target supply chains, exploiting these third-party connections to access sensitive energy systems and data. This interdependency magnifies the challenge, as energy companies must implement stringent security measures within their own networks and across their supply chain partners.

Regulatory compliance is yet another challenge for energy companies. As cybersecurity threats evolve, regulatory standards and requirements often change rapidly. Energy companies operate in multiple jurisdictions, each with cybersecurity regulations, making compliance complex and costly. This regulatory landscape creates a significant challenge, as companies must ensure their systems meet all necessary security standards while remaining agile enough to adapt to new or updated requirements.

Legacy systems that remain in use across many energy providers add to the complexity. These systems, though reliable, lack modern cybersecurity features, making them especially vulnerable to cyberattacks. Replacing or updating these systems can be prohibitively expensive, leading many companies to maintain them despite the security risks. Attackers often exploit these outdated systems, knowing they are more susceptible to unauthorized access and manipulation.

Moreover, energy infrastructure has increasingly become a target for **nation-states and cyberterrorists** who view the sector as critical to national stability. Disrupting energy systems can have widespread effects on a country's economy, public health, and security. These cyber threats are sophisticated, often involving advanced tactics that are difficult to detect and mitigate. The energy sector must prepare for such targeted attacks, which aim not only to

Co-funded by the European Union

disrupt operations but to send a political message or create strategic advantage.

Finally, **insider threats** remain a constant concern in the energy sector. Employees, contractors, or other insiders who access critical systems can unintentionally or intentionally compromise security. Disgruntled employees or those whom malicious actors may manipulate have the potential to cause significant harm, from data breaches to operational sabotage. Given the sensitive nature of energy systems, managing insider risk is essential, yet it remains a challenging aspect of cybersecurity for energy providers.

In conclusion, the energy sector's cybersecurity challenges are multifaceted and require a robust, coordinated response. From securing OT systems and managing IT-OT convergence to addressing supply chain vulnerabilities and staying compliant with evolving regulations, energy companies must adopt a proactive approach to cybersecurity. The sector's critical role in maintaining public safety and national security underscores the importance of building resilient infrastructure capable of withstanding and recovering from cyber threats. Addressing these challenges will require investment in technology, employee training, and cross-industry collaboration to build a resilient and secure energy landscape for the future.

9.4 TRANSPORTATION

In recent decades, there has been a rapid increase in the use of Internet of Things (IoT) systems, either for vehicle monitoring and traffic regulation (e.g. urban transport) or for freight transport and the protection of vulnerable products and the safe delivery of shipments. In this digitally enriched environment, there is a large volume of information that is recorded and utilized for the management of transport and transportation services. This extensive digital data movement system is vulnerable to technical failures and malicious acts. There is a need to protect information movement and IoT

Co-funded by the European Union

automation systems for transport and transportation and this is a subject that should be taught together with training on the use of smart IoT systems.

9.5 AGRO-FOOD

In the Agri-Food sector, there is an immediate and urgent need for the implementation of the "Green Transition" policy. Part of this policy is the implementation of smart farming systems that mostly concern the use of Internet of Things (IoT) digital sensor systems.

In addition to the safe and reliable transfer of data recorded with IoT digital sensors, there is also the issue of data preservation, when these are part of a closed information system and there is a question of intellectual property of the data and metadata produced by their processing (e.g. cultivation care based on smart farming data).

There is therefore a need for the education of agricultural economic actors (producers, farmers, processing professionals, traders, etc.) to be trained in the safe use of digital systems in agri-food.

9.6 EDUCATION

The education sector has become an increasingly attractive target for cybercriminals due to its extensive digital infrastructure, valuable data repositories, and often limited cybersecurity resources. Schools, universities, and vocational education and training (VET) institutions handle vast amounts of sensitive student and staff data, research materials, and financial records, making them prime targets for cyber threats such as ransomware, phishing, DDoS-attacks, and data breaches. As digital learning platforms and cloud-based technologies become integral to education, the attack surface continues to expand, increasing cybersecurity risks.

Recent studies indicate a sharp rise in cyber threats targeting educational institutions. The education sector ranks fifth globally in terms of cybercrime incidents, with malware and phishing attacks being some of the most common threats. This data

Co-funded by the European Union

demonstrates that cybersecurity is no longer an optional consideration for educational institutions — it is a critical necessity for safeguarding students, staff, and learning environments.

Key cybersecurity challenges and threats in education include the following:

1. **Data privacy and protection of personal information.** Educational institutions collect personal student and staff data, financial records, and academic research, making them attractive to intellectual property thieves, identity thieves, and ransomware operators. However, many institutions lack cybersecurity awareness, secure access controls, and data backup strategies, leaving them vulnerable to data breaches and financial fraud. Compliance with data protection laws such as the EU's GDPR is essential but often challenging due to limited resources and cybersecurity expertise in educational institutions.

2. **Phishing and social engineering attacks.** Phishing remains one of the most significant threats to the education sector, often targeting teachers, students, and administrators with deceptive emails to steal credentials, deploy malware, or manipulate users into revealing confidential information. Since teachers and students may lack cybersecurity awareness training, they are particularly vulnerable to these attacks, increasing their susceptibility to credential theft and account takeovers. Raising awareness and incorporating cybersecurity education into educational institutions' curricula can help mitigate these risks.

3. **Ransomware: a persistent and costly threat.** Ransomware has become a major cybersecurity crisis for educational institutions, causing financial losses, data encryption, and operational disruptions. Ransomware attacks have surged, affecting 79% of higher education institutions and 80% of lower education providers in 2023. These attacks typically involve encrypting institutional data and demanding a ransom for its release, causing costly downtime and potential data loss. Malware threats, adware, and spam are also prevalent. Schools and universities, often operating with outdated security measures and limited IT budgets, are particularly vulnerable, making it

Co-funded by the European Union

essential to implement strong endpoint protection, network segmentation, and staff training to mitigate these risks.

4. **Limited cybersecurity budgets and outdated infrastructure.** Many educational institutions, especially schools and vocational training centers, operate with limited IT budgets and may lack a sufficient amount of dedicated cybersecurity professionals. Research shows that only a fraction of higher education institutions have a structured cybersecurity strategy in place. Such conditions lead to outdated software, weak access controls, and insufficient network security measures, making them relatively easy targets for cybercriminals. Educational institutions must prioritize basic cybersecurity measures, such as regular software updates, secure authentication protocols, and staff training to improve security resilience.

5. **Vulnerabilities in online learning platforms and EdTech tools.** With the rise of e-learning platforms, virtual classrooms, and digital assessment tools, educational institutions increasingly rely on third-party technology providers. Many of these platforms collect and process vast amounts of student data, yet they may lack strong security features or compliance with data protection regulations. Cybercriminals can exploit software vulnerabilities to gain unauthorized access, disrupt online learning, or launch denial-of-service (DDoS) attacks to disable platforms during exams or key learning sessions. Educational institutions must implement strategies for mitigating cyber threats in EdTech.

6. **DDoS-attacks disrupting learning environments.** DDoS attacks, which flood university and school networks with excessive traffic, have increased in frequency, disproportionately targeting the educational sector. They have the potential to disrupt school operations, affecting online learning, communication between educators and learners, and online exams.

7. **Risks from bring your own device (BYOD) policies.** The increasing use of personal devices (laptops, tablets, smartphones) for education creates security risks, including unauthorized access, malware infections, and unsafe

Co-funded by the European Union

applications. Many institutions do not have strong BYOD policies, leading to inconsistent security configurations across student and faculty devices. Establishing a clear policy for BYOD usage is a complex yet essential task for educational institutions. It requires them to define which sensitive information must be protected, determine which teachers or students should have access to it, and ensure that all students and personnel are properly educated on the policy.

8. **Emerging threats of AI-assisted cheating and deepfakes.** Many universities are struggling to detect and prevent AI-assisted cheating, leading to increased concerns about exam integrity and digital verification. Hence, special measures should be adopted to ensure the ethical use of AI in education (and some educational institutions already offer guidance on the use of AI in teaching and learning). Furthermore, as AI tools become more advanced, cybercriminals exploit AI-driven methods to compromise educational integrity and security. Deepfake technology may be used to create inappropriate images or impersonate faculty members and students, posing a risk for bullying, fraud and academic dishonesty.

Despite these challenges, the education sector has opportunities to improve cybersecurity and resilience by implementing measures, such as:

1. **Cybersecurity training for educators and students.** Mandatory cybersecurity awareness programs for teachers, students, and administrative staff can reduce phishing, ransomware, and data breach risks. Cyber hygiene training and security workshops can help build a culture of cybersecurity within educational institutions.
2. **Integrating cybersecurity training into educational curricula**. Educational institutions should integrate basic cybersecurity education into curricula, preparing students for digital work environments.
3. **Strengthening cybersecurity policies.** Educational institutions should establish clear security policies, conduct regular risk assessments, and invest in cybersecurity infrastructure to protect digital learning environments.

Co-funded by the European Union

4. **Implementing essential and advanced cybersecurity measures**. To protect educational institutions from cyber threats, both essential and advanced security measures must be implemented. Essential protections include firewalls, endpoint security, cloud protection, and multi-factor authentication to prevent unauthorized access. Regular vulnerability assessments could help identify security gaps. For stronger defenses, institutions should consider adopting zero trust architecture (ZTA), which continuously verifies all users and devices, along with network segmentation, AI-powered threat detection, Security Information and Event Management (SIEM) systems, among others, for real-time monitoring and response. A layered security approach would ensure greater resilience against cyber risks.
5. **Improving digital resilience through public-private partnerships**. Collaborations with cybersecurity firms, EdTech companies, and government agencies could help enhance security protocols, provide cybersecurity training, and implement secure learning technologies.

As educational institutions continue to embrace digital tools, they must prioritize cybersecurity to protect data, ensure safe learning environments, and prevent financial losses. The rise in ransomware, phishing, DDoS attacks, and data breaches underscores the urgent need for enhanced security measures, cybersecurity education, and investment in modern IT infrastructure. A proactive approach to cybersecurity will safeguard the future of digital learning and prevent educational institutions from becoming easy targets for cybercriminals.

Co-funded by the European Union

10. SPECIFIC GUIDANCE FOR THE SCHOOL COMMUNITY

Recognition and promotion of a career in cybersecurity as a very relevant career choice start with the teaching and showcasing of good cyber hygiene and cybersecurity practices, of building and demonstrating educational systems and environment were cyber risks awareness, readiness and resilience are key.

There are three main axes in the use of digital online technology in educational environments. Corresponding are the categories of cybersecurity threats in education:

- Teachers: secure management of digital systems and applications in school life and formal education
- Students: informal education, secure information and secure interaction on social networks
- Parents and responsible shaping of the digital environment in family life

Besides the above, the promotion and pursuit of cybersecurity education by students should be not just about protecting oneself and his / her own family, but also about being able to protect a future work environment and others in the community.

The insufficient general awareness about cybersecurity career potential, the skills gaps and workforce shortages, as well as the low level of diversity in today's cybersecurity sector, require some changes in the way the teachers and other school staff engage with the students on cybersecurity topics.

10.1 New ways to preparing the future cybersecurity professionals

Various school teachers and staff, but especially those involved in ICT and computing studies, as well as those in civic studies, personal, social and career development, are recommended[35] to adopt a new approach towards

[35] REWIRE Cybersecurity Skills Alliance: A New Vision for Europe – Policy Recommendations

Co-funded by the European Union

cybersecurity, one that positions it as a valuable and attractive career, accessible to people of all genders, with diverse competences and educational backgrounds. Such positioning needs to be done both vis-à-vis students and towards their parents. For example, by:

- Integrating cybersecurity awareness and fundamental principles into non-technical training and educational programs at all levels and types of education, starting as early as possible.
- Using learning materials and teaching methods that are free from gender stereotypes and bias, by encouraging a diverse range of perspectives and experiences to appeal and engage a broader range of students.
- Make cybersecurity practical and engaging, including through hands-on workshops and simulations, escape games, industry study visits, summer camps, hackathons and Capture-the-Flag competitions.
- Highlighting the importance of diverse competences and skill sets in cybersecurity, emphasizing that diverse teams are more effective at addressing complex security challenges.
- Emphasizing not just technical and computing skills, but also transferable skills like critical-thinking, options analysis, problem-solving, team work.
- Demonstrating how cybersecurity can solve societal problems, highlighting the ultimate role and impact of the cybersecurity workforce rather than the specific ways in which each and every of the different specialists do their work. Getting students (especially girls) interested in the "why", would make them more willing to pursue "what" is needed to enter cybersecurity.
- Addressing gender stereotypes that women and girls are not interested in cybersecurity, by introducing female professionals as role models and by actively seeking the perspectives and perceptions of girl students on cybersecurity topics.

Co-funded by the European Union

- Partnering up with cybersecurity companies and organizations that are committed to diversity and gender inclusion to contribute to formal and non-formal education activities,
- Inviting various cybersecurity professionals to speak with students and parents about their educational background and contributions to cyber work, to provide mentoring and internship guidance to interested students.
- Highlighting the economic advantages of choosing studies towards a career in cybersecurity, especially in the context of the increasing shortage of professionals in the field.

10.2 The school community

In the school community environment, there is intense information flow, as part of formal education. Some of the basic functions in a modern school environment are:

- Use of digital applications,
- Research in sources and resources,
- Registration and use of a digital communication platform

For the safe operation of the above and the safe transfer of information in cyberspace, the role of educational staff is crucial. Any school should have at least a Cybersecurity Officer who knows all the functions of school life and can identify threats, risks and gaps in cybersecurity issues in the circulation of educational information. Accordingly, he/she suggests and helps with the utilization of filters and security applications in cyberspace. The role of such Cybersecurity Officer would include the following tasks:

- Malware protection settings and applications
- Creating security filters for access to inappropriate content
- Informing and educating students on cybersecurity issues
- Raising awareness and guiding parents on safe internet browsing issues

Co-funded by the European Union

10.3 Students and access to sources and applications

Young people and students are considered the most vulnerable group of users of digital applications. For this reason, education, in a broader approach, should also include guiding students in the safe use and navigation of the internet. In the school and personal lives of students there is intense interaction, either as part of research in sources and resources of informal or non-formal education, or as a free interaction with social media. In all the above cases, it is necessary to have a network of protection for young people and students in the use of digital applications. Therefore, cybersecurity applications should be integrated into the curricula. Teaching cybersecurity issues as a separate subject will be the task of specialist teachers who will be aware of the needs of students, the school environment and the communication of information on the Internet.

10.4 The role of parents

In the time of family life and free time, the personal and social networking of young people develops. Here, the threats of cyberspace are greater because there is no structured use of the internet. If we consider that the school community includes students, teachers and parents, it is easy to conclude that parents should align themselves with the security policies and practices implemented by the school, as well as with the new vision of working in cybersecurity.

A strong role for both the Cybersecurity Officer and other education staff emerges here, not just for informing and guiding parents on how to organize a network of safe browsing at home, but also in reshaping their attitudes to increase familial support and encouragement toward female and students with diverse abilities participation in cybersecurity.

In summary, parents need guidance on the following topics:

- Safety in searching for sources and information; recognizing fake news

Co-funded by the European Union

- Safety against seduction attempts on social networks
- Protection from bullying on social media

In addition to the above, parents should be informed by school teachers on how to recognize changes in their children's behaviors that may be due to unorthodox and misuse of the internet. This observation of children's behavior can be lifesaving for children and prevent situations due to threats from cyberspace.

Co-funded by the European Union