29-04-2025

Deliverable D1.1:
Master's in Cyber Security: Curriculum Design

Deliverable D1.1

Contractual Date:	31-08-2024
Actual Date:	29-04-2025
Grant Agreement No.:	101123118
Work Package:	WP1
Task Item:	D1.1
Lead Partner:	ELTE

Authors: Viktoria Villanyi (ELTE), Antonio Faonio (EURECOM), Bruno Crispo(UNITN), Darius-Vasile Bufnea(UBB), Mohamed Sabt(UR), Florian Hahn(UT), Seppo Virtanen (UTU),

Abstract

Report on the design phase of the curriculum of the master's programme in Cybersecurity. The report describes the labour market needs analysis carried out by the consortium and presents the final curriculum of the master's programme. The Curriculum of the Master's programme is designed on the analysis of the existing literature linked to the needs of the European labour market in digital skills and in the broad field of Cybersecurity. ELTE leads a consortium of 7 higher education Institutions from 6 different countries.

The activities leading to these results has received funding from the European Community's DIGITAL Programme under Grant Agreement No. 101123118 (SPECTRO).

Versioning and contribution history

Version	Date	Authors	Notes
0.1	07/06/2024	Viktoria Villanyi (ELTE)	First version.
0.2	07/06/2024	Antonio Faonio (EURECOM)	Provided information about EURECOM's curriculum
0.3	07/06/2024	Bruno Crispo (UNITN)	Provided information about UNITN's curriculum
0.4	07/06/2024	Darius-Vasile Bufnea (UBB)	Provided information about UBB's curriculum
0.5	07/06/2024	Mohamed Sabt (UR)	Provided information about UR's curriculum
0.6	07/06/2024	Florian Hahn (UT)	Provided information about UT's curriculum
0.7	07/06/2024	Seppo Virtanen (UTU)	Provided information about UTU's curriculum
0.8	09/07/2024	Viktoria Villanyi (ELTE)	Revised details on master programmes.
0.9	19/07/2024	Viktoria Villanyi (ELTE)	Labour market analysis updated
0.10	25/07/2024	Seppo Virtanen (UTU)	Labour market analysis updated (UTU)
0.11	29/07/2024	Darius-Vasile Bufnea (UBB)	Labour market analysis updated (UBB)
0.12	29/07/20024	Florian Hahn (UT)	Labour market analysis updated (UT)
0.13	31/07/2024	Bruno Crispo (UNITN)	UNITN's curriculum updated
0.14	28/08/2024	Andrea Biancini (EITD)	Final version formatting.
0.15	25/11/2024	Viktoria Villanyi (ELTE)	Small modifications and updates.
0.16	28/03/2025	Viktoria Villanyi (ELTE)	Small modifications and updates.

Table of Contents

1 Labour market analysis

1.1 Introduction

Ensuring the security of IT infrastructure is becoming increasingly challenging. We are fully connected in the online space, and the shift to remote work during the pandemic has moved many of our activities online. Our everyday lives are heavily impacted by online services. While we consider security measures against various adversaries, we must also protect our systems from innocent human errors.

One notable example of IT outage occurred on July 19, 2024, when Crowdstrike, a well-established cybersecurity company with a 24% market share in endpoint-protection market, and close ties to Microsoft, released an update containing a bug. This mistake led to a global IT outage on an unprecedented scale, affecting airports, banks, hospitals, and causing widespread disruption and financial losses. Even this incident that involves major cybersecurity companies highlights the critical importance of the field of cybersecurity.

The first part of our labour market analysis of the field of Cybersecurity based on the European Cybersecurity Skills Framework [1], researched and documented by European Union Agency for Cybersecurity (ENISA). The main purpose of the European Cybersecurity Skills Framework research was to create a common understanding between individuals, employers and providers of learning programs across EU Member States. This makes it a valuable tool to bridge the gap between the cybersecurity professional workplace and learning environments.

1.2 Cybersecurity workforce

The cybersecurity workforce is reaching an all-time high with an estimated 5.5 million professionals already employed worldwide. However, there is still a global shortage of 3.9 million workers in this field [2]. ISC2 estimates an 8.7% increase year over year and nearly 440,000 new jobs. The gap between the number of workers needed and the number available has continued to grow, with a 12.6% increase year over year. According to an assessment by the International Information System Security Certification Consortium [3], Europe faces a deficit of over 347,000 cybersecurity professionals.

1.3 Diversity

The cybersecurity workforce faces a significant diversity challenge. Women constitute only 24% of the global cyber security workforce [3]. Among OECD countries, some like Israel (53%), Norway (31%), Canada (28%), and Sweden (27%) have a higher percentage of women among ICT graduates, while others like France (17%)have a lower percentage, partly due to the small proportion of women trained in the information and communication technology field overall[2].

Our EITD's historical data on diversity is slightly better. The percentage of the female students in our EITD Cyber Security Programme (predecessor of SPECTRO Cyber Security Programme) was 26% in cohort 2023 and 33% in cohort 2022.

1.4 The typical cybersecurity professional role profiles

ENISA defined the following 12 typical cybersecurity professional role profiles [1]:

1. Chief Information Security Officer (CISO)
2. Cyber Incident Responder
3. Cyber Legal, Policy & Compliance Officer
4. Cyber Threat Intelligence Specialist
5. Cybersecurity Architect
6. Cybersecurity Auditor
7. Cybersecurity Educator
8. Cybersecurity Implementer
9. Cybersecurity Researcher
10. Cybersecurity Risk Manager
11. Digital Forensics Investigator
12. Penetration Tester

These profiles provide a common understanding of the main cybersecurity missions, tasks, and skills needed in a professional cybersecurity context, making it the perfect reference for profiling skills and knowledge needed by cybersecurity professionals. The needed skills and sets of knowledge for different profiles can be very distinct. The field of cybersecurity need professionals with diverse background and different skill sets, who should acquire the necessary knowledge along their study or training programmes.

1.5 General knowledge required by cybersecurity professionals

In the same study [1], ENISA collected a list of essential knowledge required to perform work functions and duties for the profiles. According to the study, most of the cybersecurity professional role profile need the following knowledge:

1. Cybersecurity-related certifications
2. Cybersecurity controls and solutions
3. Cybersecurity standards, methodologies, and frameworks
4. Computer network security
5. Cyber threats
6. Cybersecurity recommendations and best practices
7. Cybersecurity-related laws, regulations, and legislations
8. Operating systems security
9. Computer systems vulnerabilities
10. Cybersecurity attack procedures
11. Computer programming
12. Cybersecurity-related technologies
13. Legal, regulatory, and legislative compliance requirements, recommendations, and best practices

During the first year of the SPECTRO programme, our students obtain solid knowledge of all these covered by our common core courses, or they have already acquired this knowledge during their Computer Science BSc program (e.g., computer programming). In the second year, we focus on more specialized, advanced technical topics based on the current work environment requirements and the interest of our MSc students. We are keep updating and improving our programme based on the new results and challenges from IT word.

1.6 The required skill set for cybersecurity professional roles

The required skill set for the 12 typical cybersecurity professional role profiles was defined by ENISA [1]. Here is a collection of skills that are demanded by more than one profile, with the exact number of profiles needing each skill indicated in parentheses:

1. Communicate, present and report to relevant stakeholders (8)
2. Identify and solve cybersecurity-related issues (5)
3. Collaborate with other team members and colleagues (4)
4. Decompose and analyse systems to identify weaknesses and ineffective controls (3)
5. Collect, analyse and correlate cyber threat information originating from multiple sources (2)
6. Communicate, coordinate and cooperate with internal and external stakeholders (2)
7. Conduct technical analysis and reporting (2)
8. Decompose and analyse systems to develop security and privacy requirements and identify effective solutions (2)
9. Motivate and encourage people (2)

It is evident that soft skills related to the cybersecurity profession are increasingly important. Our education model emphasizes activities that support the development of soft skills next to the development of hard skills, such as the Kick-Off event, and I&E-related courses (30 ECTS). The SPECTRO education programme focuses on developing the necessary basic and the competitive advanced technical skills by offering a 90 ECTS technical part of the education programme. Our Cyber Security MSc programme offers 7 different advanced technical specializations. Online certification programmes for professionals will also be offered contribute to the participants' life learning journey of studying. Our programme is upskilling and reskilling the workforce in the EU.

1.7 Skill gaps (technical skills)

In the Cybersecurity Workforce Study [3], many organizations reported skills gaps. These are the most common (technical) skill gaps in the field of cybersecurity nowadays according to the study:

- 1. Cloud computing security,
- 2. AI/ML and
- 3. Zero Trust implementation.

Historically, cloud computing security was the most common area where the organization reported a skills gap.

In 2023, for the first time, AI/ML skills were among the top five in terms of demand. The previous year, AI/ML skills were among the least significant, but they are becoming increasingly important and soon critical.

The organization also has a shortage of cybersecurity staff needed to prevent and troubleshoot security issues.

Other identified technical skills gaps include penetration testing, application security, digital forensics and incident response, risk assessment, analysis and management, security engineering, threat intelligence analysis, and malware research/analysis.

1.8 Local labour market analysis and new specializations

Our Cyber Security Consortium consists of seven partner institutes. Based on the results of literature review on Cyber Security and labour market analyses, the partners have developed an up-to-date Cyber Security Programme with new and revised exit year specializations. In the following subsections, the partners explain the reasons of these changes.

1.8.1 Babeș-Bolyai University (UBB), Software Security

The Faculty of Mathematics and Computer Science of the Babeș-Bolyai University (UBB) is in contact with several dozen companies, mostly from the IT&C field. These companies vary in type, ranging from small startups and SMEs to large multinational corporations. The collaboration with these companies takes various forms: they offer internship positions to Babeș-Bolyai students, provide private scholarships, and their representatives are invited to deliver guest lectures to students, among other activities.

The UBB Computer Science Department also maintains periodic contact with these companies, either through their representatives at invited lectures or through regular meetings at various events such as Internship Workshop Day, Graduation Day or the Student Scientific Communications Session (SCCSS).

In the context of this project, these companies were invited to respond to a questionnaire whose primary goal was to assess the need for cybersecurity education both in general society and specifically within these companies. Additionally, it aimed to determine the competencies required of graduates and to shape the curriculum for such programs based on specific industry and societal needs.

The Faculty of Mathematics and Computer Science received 26 responses to this questionnaire at the time of completing this report, including responses from strategic partners such as Computacenter, NTT Data, Bitdefender, and Siemens. It is noteworthy that Computacenter and NTT Data support various educational programs within the faculty, with Computacenter even providing a support fund for private scholarships for cybersecurity students. Additionally, Bitdefender, a major player in the IT&C sector specializing in cybersecurity, has pledged to support UBB's cybersecurity master's program from the first SPECTRO cohort with an optional course on Extended Detection and Response.

From all the companies that responded to the questionnaire, 100% of the respondents consider that, given the current state of Internet development and the information society, as well as the current geopolitical context, cybersecurity and cybersecurity education are extremely important for any company, institution, organization, and for society in general. Approximately two-thirds of the respondents (65.4%) consider that cybersecurity education should take place at the master's level, while approximately one-third of the respondents (34.6%) believe that cybersecurity education should occur at the undergraduate level. A vast majority of respondents (96.2%) considered that software security should be the main focus of these studies, while only 3.8% of respondents felt that such studies should focus on hardware security. Additionally, considering the expertise of the faculty at Babeș-Bolyai University, a focus on software cybersecurity for such a master's program is a natural choice.

The companies surveyed were asked to identify essential knowledge, skills, and capabilities for graduates of cybersecurity educational programs. The key competencies highlighted include understanding main cyber threats, implementing security programs, and knowledge of common attack patterns and countermeasures. Graduates should have strong foundations in cybersecurity fundamentals, network security, cryptography, risk management, compliance, and emerging

technologies. Essential skills include technical proficiency, analytical skills, programming, communication, and problem-solving. They should also be adept in information security principles, security policies, network architectures, secure software development, and regulatory issues. Practical abilities such as conducting risk assessments, incident response, penetration testing, and forensic analysis are critical. Additionally, graduates should be familiar with operating systems, network protocols, security tools, and frameworks. Understanding the legal, regulatory, and compliance landscape, such as GDPR is also crucial. The emphasis on software cybersecurity education reflects the industry's need for well-rounded professionals capable of addressing various cyber threats and implementing comprehensive security measures.

Most respondents confirmed that they had faced cybersecurity incidents or problems, with a vast majority of them (88%) willing to hire cybersecurity specialists in the future. They deal with social engineering attacks (e.g., phishing), technology-based threats (e.g., DoS attacks), and user errors. The shortage of cybersecurity specialists exacerbates these issues. Companies are tasked with implementing security measures with minimal impact on productivity, addressing threats such as phishing, LoTL attacks, and cryptojacking, and conducting vulnerability assessments. Securing internal networks through independent penetration testing and managing application access are also critical. Other concerns include navigating complex security standards, cloud and IoT security, and compliance with frameworks like NIST2. Companies often encounter vulnerabilities in third-party libraries and must update these to prevent exploitation. They also face challenges in system integrations, protecting core data, and ensuring safe technology use while meeting customer expectations. Ultimately, securing enough cybersecurity professionals is essential to effectively address these needs.

Among the advantages of hiring cybersecurity specialists in the future, the companies that responded to the questionnaire highlighted that cybersecurity is increasingly critical due to the interconnected nature of software systems, with failures potentially halting their operations. Cybersecurity is becoming one of the most crucial aspects in technology and business continuity. Experienced specialists are needed to bring expertise in the complex field of cybersecurity, enabling them to implement robust measures that protect companies' infrastructure and applications. This approach helps in identifying and mitigating threats, ensuring compliance with industry standards and regulatory requirements such as GDPR for example. Additionally, cybersecurity specialists can tailor security solutions to an organization’s specific needs, enhance data handling practices, and raise security awareness internally. Ultimately, expanding the team with skilled cybersecurity graduates not only safeguards operations but also creates opportunities for increased revenue by offering advanced cybersecurity solutions to other businesses.

1.8.2 University of Turku (UTU), Security Technologies and Intelligence specialization

Based on the market research and analysis, the specialisation offered by the University of Turku (UTU) was revised to "Security Technologies and Intelligence".

A stakeholder study was made in Finland during spring 2024 jointly by the leading Finnish universities offering cyber security education. The study was led by UTU. The stakeholders (companies and organizations in the cyber security field or in need of cyber security professionals) were asked to rate their skill needs in the JRC Cybersecurity Taxonomy [5] topics currently and in the near future. In addition to JRC taxonomy items, also the skill need for artificial intelligence and machine learning in the cyber security context was added as a topic in the survey due to their current disruptive effect across the ICT field.
Altogether 61 companies and organizations answered the survey and further details were received through interviews of respondents that indicated there willingness in the survey to participate in interviews.
Altogether 12 interviews were made among the different companies and stakeholders. The 61 respondents consisted of both national and international companies and organizations but with the respondents representing the stakeholders' Finnish branches in the case of international companies and organizations.

The analysis of the survey results revealed that artificial intelligence and machine learning in the cyber security context, data security and privacy and software and hardware security engineering were among the top three skill needs for the future among the respondents. The analysis made based on these results and all the more detailed results obtained in the Finnish market survey were used as a key input in the spring 2024 cyber security curriculum design for SPECTRO at UTU, resulting in a revised focus in the specialisation.

The revised (new) Security Technologies and Intelligence specialisation at UTU focuses on researching pre-emptive, reactive and analytical security technologies to protect systems from cyber threats and malicious exploitation attempts in the era of artificial intelligence and machine learning. The compulsory studies are on intelligent technologies for protecting systems and networks (firewalls and intrusion prevention), ethical hacking (penetration testing) and analysing digital traces of malicious activity (digital forensics). The revised specialisation reflects very well the analysis results of the market research performed in Finland in spring 2024.

The revised specialisation gives its students profound and substantial education and expertise in the field. Optional studies selected personally for each student build a special individual cyber

security expertise profile. The curriculum consists of both theoretical and hands-on study modules. Also, a large group project module called 'Capstone project' can be included in the studies. The graduates of the revised specialisation will have a strong technological, theoretical and practical understanding of security technologies for protecting systems and environments against cyber threats. With these new skills and knowledge, graduates can proceed to building a successful career in securing and protecting the ICT intensive industry. The graduate's unique expertise profile may lead to a career title of, for example, one of the following: Cyber Security Analyst, Penetration and Vulnerability Tester, Cyber Security Consultant, Cyber Security Manager, Network Security Specialist, Cyber Security Entrepreneur, System / Network Administrator, Business Information Security Officer, Chief Information Officer, Chief Information Security Officer, Head of Corporate IT.

1.9 Other new specializations

1.9.1 University of Twente (UT), Circular Security

The Twente University Centre for Cybersecurity Research (TUCCR) is a public-private partnership between the University of Twente and its partners from industry with the goal to create innovation in form of technology, tools and knowledge making an impact on today's digital society. One key aspect towards a positive change is the education of the next generation of cybersecurity professionals. As reflected by the diversity of our industry partners[1] ranging from the banking sector and governmental institutions over classical ICT companies towards cybersecurity experts, the knowledge required from our graduates at University of Twente is just as diverse. Inspired by the research areas identified for TUCCR with our industry partners, we leverage SPECTRO to take the next step and align also our educational programme with these areas.

The specialisation in Circular Security covers the complete range of steps necessary to develop secure solutions for the real world: starting from the analysis of known cyber-harm, -attacks and -vulnerabilities and their proper modelling, to the engineering of targeted protection, mitigation, detection, and response solutions, all the way to their implementation and extensive testing. For each of these steps, we acknowledge the importance of the socio-economic context and the involved human factor, which can be part of the problem and part of the solution at the same time.

1.9.2 Eötvös Loránd University (ELTE), Quantum-resistant specialization

The European Commission encourages member states to develop a comprehensive strategy for the adoption of post-quantum cryptography to ensure a coordinated and synchronized transition among the different Member States and their public sectors [4].

[1] https://www.utwente.nl/en/digital-society/research/Cybersecurity_tuccr/people/partners/

US National Institute of Standards and Technology (NIST) has launched initiatives to standardize a new type of cryptography called quantum-resistant cryptography. NIST has selected four algorithm for standardization (2022) that can withstand attacks from both classical and quantum computers. It is critical to prepare now to migrate to the new standards as soon as possible, protect privacy and provide security in the near future.

The new Quantum-resistant Cryptography specialization will prepare our students for the challenges of the time when quantum computers become a reality, and the widely used old public key algorithms will be insecure and breakable in polynomial time. We should start using quantum-resistant algorithms even before the appearance of quantum computers. We have already entered the period of "harvest now, decrypt later," also known as "store now, decrypt later," when we will be able to run quantum algorithms.

1.10 Literature used for the labour market analysis

1. European Cybersecurity Skills Framework (ECSF): https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework
2. OECD (2024), Building a Skilled Cyber Security Workforce in Europe: Insights from France, Germany and Poland, OECD Skills Studies, OECD Publishing, Paris, https://doi.org/10.1787/3673cd60-en.
3. ISC2, 2023 Cybersecurity Workforce Study (2023), https://www.isc2.org/Research
4. Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography: https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography
5. Nai Fovino, I., Neisse, R., Hernandez Ramos, J., Polemi, N., Ruzzante, G., Figwer, M., & Lazari, A. A Proposal for a European Cybersecurity Taxonomy. In EUR 29868 EN. Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-11603-5, doi:10.2760/106002, JRC118089.
https://op.europa.eu/en/publication-detail/-/publication/a1fcc114-01eb-11ea-8c1f-01aa75ed71a1/language-en

2 Curriculum design

2.1 Programme objectives

The Cyber Security program (previously known as Security and Privacy) is a Masters level program within the EIT Digital Master School. The Master School is a highly prestigious ICT engineering education provider on advanced level with a business minor focused on Innovation and Entrepreneurship (I&E). These students will be an elite group of forthcoming ICT professionals. The unique features of this advanced level education are:

- A standardized I&E minor.
- Personal industrial relationships for the students, including industrial mentors and internships.
- Thematic area grounding and utilization of resources from EIT Digital innovation activities.
- Utilization of EIT Digital co-location center (CLC) resources.
- Inter disciplinary and inter node teambuilding events**.**

2.2 Structure

The Cyber Security program (120 ECTS) is a comprehensive combination of an I&E Minor (30 ECTS), a Technical Major (90 ECTS):

- 20-30 ECTS mandatory courses ('common base')
- 30-40 ECTS elective and specialized courses ('specialisation')
- 30 ECTS master's thesis project.

Typically, during the entry year, students have to take 36 ECTS for the technical major and 24 ECTS for the minor in Innovation & Entrepreneurship whereas during the second year, they have to take 24 ECTS for the technical major, 6 ECTS for the minor and 30 ECTS for the master's thesis project. The Innovation & Entrepreneurship minor (30 ECTS) includes the mandatory Summer School (4 ECTS).
All Master School education will be held in English and all partner universities are assumed to use ECTS units.

Upon fulfilment of all degree requirements, students receive two degrees. Students also receive an EIT Label Certificate endorsed by the EIT and issued by EIT Digital.

2.3 Learning objective

The learning objectives of the Cyber Security Master are that a graduate:

- Understanding the concepts and technologies for achieving confidentiality, integrity, authenticity, and privacy protection for information processed across networks.

- Mastering the key principles underlying a constructive approach to secure systems, including threat characterization and subversion; confinement; fundamental abstractions, principles, and mechanisms; and life-cycle assurance.

- Being able to apply fundamental Information Systems Security Engineering principles and processes, as applied to the stages a life-cycle model in the context of a defence-in-depth protection strategy

- Recognizing potential vulnerabilities in networked systems by studying methods to obtain information about remote networks and how to exploit or subvert systems on that network.

- Being able to use current tools and techniques for assessing network attacks and vulnerability and for systematically reducing vulnerabilities and mitigating risks.

- Ability to examine security engineering concepts and practices from a system lifecycle perspective based on a "systems thinking" approach that supports assessment of system security behaviours based on dependencies, interactions, and emergent properties of system components in the context of functionality, scalability, interoperability, and maintainability.

- Competences in communication, knowledge integration, open innovation and technology management from the viewpoints of both business and technology.

- Business skills to understand and execute a business development process, and have insight in legal and societal aspects of security and privacy.

Those outcomes of the Cyber Security major will be combined with the I&E minor to enable graduated students to create or get involved in start-up companies, and lead innovation in existing

companies developing the data value chain and monetize data. In summary, create a new corpse of professionals for a career in a highly innovative area of Cyber Security. The learning objectives of the Cyber Security Master are that a graduate:

- Understanding the concepts and technologies for achieving confidentiality, integrity, authenticity, and privacy protection for information processed across networks.

- Mastering the key principles underlying a constructive approach to secure systems, including threat characterization and subversion; confinement; fundamental abstractions, principles, and mechanisms; and life-cycle assurance.

- Being able to apply fundamental Information Systems Security Engineering principles and processes, as applied to the stages a life-cycle model in the context of a defence-in-depth protection strategy

- Recognizing potential vulnerabilities in networked systems by studying methods to obtain information about remote networks and how to exploit or subvert systems on that network.

- Being able to use current tools and techniques for assessing network attacks and vulnerability and for systematically reducing vulnerabilities and mitigating risks.

- Ability to examine security engineering concepts and practices from a system lifecycle perspective based on a "systems thinking" approach that supports assessment of system security behaviours based on dependencies, interactions, and emergent properties of system components in the context of functionality, scalability, interoperability, and maintainability.

- Competences in communication, knowledge integration, open innovation and technology management from the viewpoints of both business and technology.

- Business skills to understand and execute a business development process, and have insight in legal and societal aspects of security and privacy.

Those outcomes of the Cyber Security major will be combined with the I&E minor to enable graduated students to create or get involved in start-up companies, and lead innovation in existing

companies developing the data value chain and monetize data. In summary, create a new corpse of professionals for a career in a highly innovative area of Cyber Security.

3 Admission Criteria for the CSES programme

To qualify for admission, applicants need to have a complete and suitable Bachelor's degree in the relevant field of studies and demonstrate proof of English language proficiency.

3.1 Bachelor's degree

Applicants must have completed a Bachelor's degree encompassing a minimum of 180 ECTS credits or equivalent academic qualifications from an internationally recognized university. Students in their final year of undergraduate education may also apply and if qualified, receive a conditional acceptance. They must include a written statement from the degree administration office (or equivalent department), confirming that they are enrolled in the final year of their education and giving their expected completion date - which should be before the start of the Master's programme.

3.2 Relevant field of studies

The Cybersecurity Master's programme is 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
- Electrical Engineering

Applicants with reasonable knowledge of the fundamentals of computing and information sciences and technologies may also be considered. In some circumstances, relevant work experience may compensate for a lack of relevant degree.

3.3 Proof of English language proficiency

All programmes are taught in English. As a result, applicants must provide proof of their English language proficiency. This is generally verified through an internationally recognized test such as TOEFL or IELTS. Most TOEFL and IELTS tests results are only valid for 2 years from the test date.

3.3.1 General language requirements

IELTS Academic test (www.ielts.org) An overall band score of at least 6.5, with no section lower than 6.0, is required. IELTS-tests are verified online by the Admissions office, submitting a photocopy of your test together with your application documents is therefore sufficient.
TOEFL Internet-based test, iBT (www.toefl.org) A total score of at least 92 with a minimum for each section of at least 21 and for writing section 22 is required.

3.3.2 English test proficiency waiver

English proficiency tests are waived for applicants who have completed a degree instructed in English at a university that is physically located in one of the following countries: USA, Canada, UK, Ireland, Australia or New Zealand.

3.3.3 University-specific language tests and exemptions

Find out more about the University-specific language tests and exemptions here: https://masterschool.eitdigital.eu/admissions/university-specific-language-tests-and-exemptions

3.4 Application necessary documents

To apply to the two SPECTRO Master's programme, candidates are required to upload into the application portal the following documentation:

- **Degree Certificate/Diploma** in its original language and translated into English (If your university does not provide this service, the translation has to be done by an authorised translator and his/her credentials, signature and stamps must be visible in the translated document). In case of ongoing studies, a statement certifying that you are in the final year of your studies. The statement must be written by the degree administration office (or equivalent department) confirming that you are enrolled on the final year of your education and giving your expected completion date.
- **Official and stamped transcript of records in original language and translated into English.** All courses taken must be included. Please scan the front and back of every document- all stamps and signatures must be fully visible.

- **Proof of English proficiency.** The requirement of English proficiency will vary depending on the higher education institution/country selected by the applicant. Please refer to EITD Master School website 'Admissions' tab for more information.
- **Curriculum Vitae** including details on your academic and professional career.
- **A letter of motivation** (maximum 3 pages) to prove the innovative potential of the applicant and their need for financial support. In this letter applicants will be required to discuss and/or propose an entrepreneurial idea and to explain their financial situation and need for financial support.
- **Supporting documents regarding the applicant's financial situation** (e.g. credit report).
- **An official ID**, such as passport or National ID.
- **Optional:** Document stating the GPA or the Relative Ranking, a 2-minute video to accompany your motivation letter.

3.5 Selection process

The application and selection process is coordinated from Sweden by the KTH Admissions Office and the EIT Digital Master School Office. They determining whether candidates fulfil the specific admission requirements for their technical major, and ranking the applicants is performed by the Selection Committee which is composed of academics involved in the programme at partner universities.
The ranking is based on a total evaluation of the following criteria:

- Suitability of acquired bachelor degree for intended study program
- Academic excellence (quality and recognition of home university, study success)
- Entrepreneurial excellence
- Innovative potential

Selected applicants are offered a study track based on preference and availability. If an applicant cannot be offered a seat in the preferred study track, an alternative track will be offered.
The application portal for admissions opens in November each year. There are three admission batches:

- The first deadline closes around mid-February. (Period 1)
- The second batch opens immediately after and closes around mid-April. (Period 2)
- The third batch opens immediately after Period 2 and closes at the end of May -or early June- (Period 3)

Students have the possibility to choose three options for their Entry university and three options for their Exit university, indicating the order of preference for each.

The universities selected as the first preference are involved in the evaluations.
In some cases, the application is evaluated by the next university chosen by the student according to their order of preference. These cases include:

- Insufficient evaluation (below the required threshold) by the selected university;
- Lack of admission requirements for the specific local program;
- Entry-Exit combination involving two universities from the same country.

If any of the evaluating coordinators (either from the entry or exit university) rejects an applicant, we ask for a third or even fourth opinion from the coordinators of the universities ranked second or third on the applicant's preference list. If any of them accept the applicant, that university will be designated as the assigned entry or exit university.

The final score assigned to the student is an average of the evaluations from the assigned Entry and Exit universities, based on the criteria described above.

During the selection process, the CSES Program Lead assigns the applications to evaluate to each Local Lead, indicating the deadline by which the evaluations must be submitted.

3.6 Scholarships

3.6.1 Financial support to EU students

SPECTRO provides eligible students the financial support to take part to the education programmes and offers scholarship programmes to promote diversity in terms of gender, age, social and economic background. SPECTRO's scholarships allow the greatest number to have access to high-quality education in digital areas and increase diversity among students and future digital experts. The students awarded a scholarship will be financially supported during their two years of studies in one of the double-degree in Masters' programmes offered by SPECTRO.

The number of scholarships awarded to students will be limited by the project's available budget. For the entire duration of the project, a maximum of €1,850,000 is allocated for financial support to third parties. Within this budget, the consortium will strive to provide financial support to at least 150 EU students, as indicated in KPI14.

All details about the Cascade funding call are available on the Funding and Tender portal of the European Commission: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/myarea/projects/cascade-funding-details/details/10469/43152860/101123118

3.6.2 Types of scholarships available

Three types of scholarships are available:

- scholarship of excellence, including a full tuition fee waivers and a monthly allowance,
- full tuition fee waivers,
- half tuition fee waivers.

The monthly allowance will be weighted based on the country correction coefficient (CCCs) of the country where a student is studying. Thus, the monthly allowance provided to a student it can vary between the first and second year of studies.

3.6.3 How to apply

To apply to a SPECTRO scholarship, candidates must enrol into one of SPECTRO two master's programmes. Enrolment is done via a single application portal. When enrolling to one of the two master's programmes, applicants are given the opportunity to select 3 options as Entry University and 3 options as Exit University with order of priority. It gives students a wider choice: applicants who would not be accepted to their preferred education institution might still be accepted by another education institution. At the same time, as the capacity of each education institution is limited, the multiple-option offer ensures that a high number of applications is processed.

To apply to the two SPECTRO Master's programme, candidates are required to upload into the application portal the following documentation:

- **Degree Certificate/Diploma** in its original language and translated into English (If your university does not provide this service, the translation has to be done by an authorised translator and his/her credentials, signature and stamps must be visible in the translated document). In case of ongoing studies, a statement certifying that you are in the final year of your studies. The statement must be written by the degree administration office (or equivalent department) confirming that you are enrolled on the final year of your education and giving your expected completion date.
- **Official and stamped transcript of records in original language and translated into English.** All courses taken must be included. Please scan the front and back of every document- all stamps and signatures must be fully visible.
- **Proof of English proficiency.** The requirement of English proficiency will vary depending on the higher education institution/country selected by the applicant. Please refer to EITD Master School website 'Admissions' tab for more information.
- **Curriculum Vitae** including details on your academic and professional career.
- **A letter of motivation** (maximum 3 pages) to prove the innovative potential of the applicant and their need for financial support. In this letter applicants will be required to discuss and/or propose an entrepreneurial idea and to explain their financial situation and need for financial support.
- **Supporting documents regarding the applicant's financial situation** (e.g. credit report).
- **An official ID**, such as passport or National ID.
- The allocation of scholarships will be done at the end of the selection process and before sending the letter of acceptance.

3.6.4 Eligibility requirements

SPECTRO scholarships are available to nationals of one of the eligible countries:

- EU Member States (including overseas countries and territories (OCTs))

- Listed EEA countries and countries associated to the Digital Europe Programme (associated countries) or countries which are in ongoing negotiations for an association agreement and where the agreement enters into force before grant signature

Only students enrolled and accepted in one of SPECTRO Masters' programme are eligible to financial support. When receiving their letter of acceptance and study offer, students will be notified of their scholarship allocation.

3.6.5 Selection criteria

The scholarships will award applicants based on merit. To quantify merit, a merit score (on a scale from 1 to 5, with 5 being the maximum) will be given to each applicant accepted to one of the master's programmes. Three elements will be considered in assigning a merit score:

- previous academic and professional experience of an applicant,
- curriculum vitae, and
- letter of motivation, which also includes the motivation for an applicant to receive financial support.

The initial merit score value will be an average of the two merit scores assigned by the two Local Programme Coordinators accepting an applicant (the Local Coordinator at the Entry University and the Local Coordinator at the Exit University). The merit scores assigned by Local Programme Coordinators will be reviewed by Programme Leaders to ensure uniformity between the scores given by Local Programme Coordinators from different universities and different countries. A final meeting including the Programme Leaders, all Local Programme Coordinators and the Quality Assurance Manager of the SPECTRO project will be set at the end of each Recruitment Period to agree and deliberate on the final merit score of each applicant.

3.6.6 Promotion of diversity

The SPECTRO scholarship programme will thrive to promote diversity and inclusion through its scholarship opportunities:

- Priority will be given to female applicants from any EU country or EU-associated country. The scholarship programme for women will aim increase female participation in master's programmes in Cybersecurity and Robotics.
- Priority will be given to applicants from RIS countries - included in the EIT Regional Innovation Scheme (RIS). The scholarship programme for participants from RIS countries is aimed to support the participation of students from countries with moderate or modest innovation score and with lower gross domestic product. Countries eligible to take part to the RIS include 1) EU members states, 2) Horizon Europe associated countries, and 3) outermost regions such as Guadeloupe, and Réunion (France), the Azores and Madeira (Portugal), and the Canary Islands (Spain).

3.6.7 Payment arrangements

The scholarship is reflected as a discount in the tuition fee. The candidates are informed of the net amount of the tuition fee, after deducting the applicable amount of the scholarship.

- half tuition fee waivers: the nominal value of the granted scholarship is of 2,500EUR per year
- full tuition fee waivers: the nominal value of the granted scholarship is of 5,000EUR per year
- scholarship of excellence, including a full tuition fee waivers and a monthly allowance: the nominal value of the granted scholarship is of 5,000EUR plus a monthly allowance of 900 EUR weighted based on the country correction coefficient (CCCs) of the country where a student is studying.

The students awarded a scholarship will be financially supported **during their two years of studies**.

3.6.8 Number of scholarships available

Scholarships are allocated on a rolling basis. The exact distribution of scholarships of each type in each scholarship programme will be decided by the SPECTRO consortium before the closing of each recruitment campaign and will be based on criteria defined in the project and aimed at sustaining enrolments to both master programs and at reaching all project KPIs.
The exact number of scholarships available will be updated for each cycle on the Funding and Tender portal of the European Commission: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/myarea/projects/cascade-funding-details/details/10469/43152860/101123118

3.7 How to apply – useful links

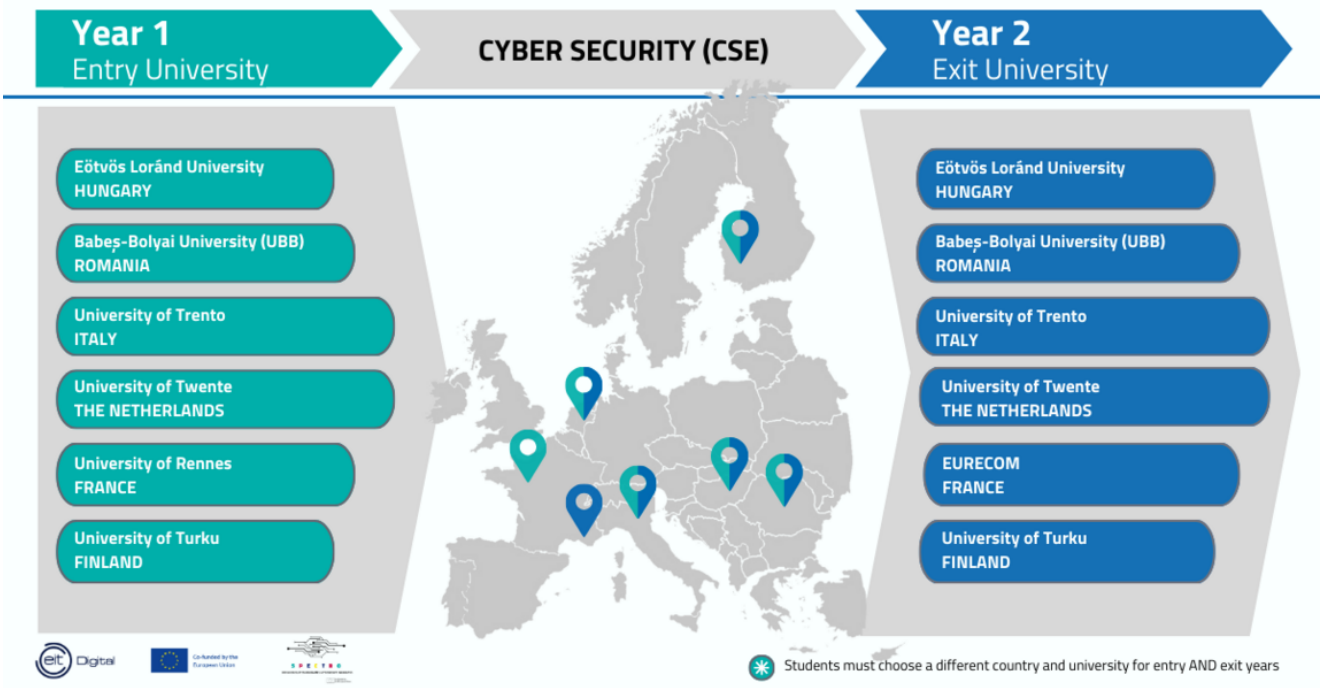
CSES Master's webpage: https://masterschool.eitdigital.eu/cyber-security
Enrollment to the CSES Master's programme is managed through the EIT Digital Master School Application portal: https://academy.eitdigital.eu/SITE/PRIVATE/GO/login.aspx
To apply to a SPECTRO scholarship, candidates must enroll into one of SPECTRO two master's programmes via the EIT Digital Master School Application portal.

Main information and updates about scholarships are published on the following reference:
EU Funding & Tenders Portal – call for proposal - Recruitment cycle cohort – SPECTRO
https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/calls-for-proposals
https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/competitive-calls-cs/10362 (cohort 2025)

Project SPECTRO - official web site
https://www.eitdigital.eu/eu-collaborations/spectro/

Project SPECTRO – Self-standing modules learning platform
https://eit.icarus.education/spectro/

4 Partners in the Consortium



- Eötvös Loránd University, ELTE, Hungary
- Babeș-Bolyai University, UBB, Romania
- University of Trento, UNITN, Italy
- Universiteit Twente, UT, The Netherlands
- University of Turku, UTU, Finland
- University Rennes, UR, France
- EURECOM, EUR, France

All involved University Parties are recognized degree awarding institutions. An EIT Digital technical major + I&E minor leads, upon successful completion, to two officially recognized Master of Science Degrees (120 ECTS) issued by the entry university and the exit university. A double degree will be awarded. The students are also awarded an EIT Label Certificate issued by EIT Digital. The Certificate is based on the two degrees issued by the partner institutions and summarizes the EIT label and EIT Digital Master School specific characteristics of the education.

Program details (modules, courses) and individual grades/marks are described in the Degree Certificates/Official transcripts. Exceptions to this rule of awarding double degrees are not possible unless specifically confirmed by written agreement between the Parties and must be communicated to the affected students in a timely manner.

4.1 Responsabilities of the partners

The following universities provide a first year:

- Eötvös Loránd University, ELTE, Hungary
- University Rennes, UR, France
- Babeș-Bolyai University, UBB, Romania
- University of Trento, UNITN, Italy
- Universiteit Twente, UT, The Netherlands
- University of Turku, UTU, Finland

The following parties provide an exit year and every exit University is supposed to define its own unique specialisation:

- Eötvös Loránd University, ELTE, Hungary
- EURECOM, EUR, France
- Babeș-Bolyai University, UBB, Romania
- University of Trento, UNITN, Italy
- Universiteit Twente, UT, The Netherlands
- University of Turku, UTU, Finland

4.2 Technical core (common base for the first year)

The courses offered in the Cyber Security programme give a common background at the Entry institutions, while the Exit points are specialised on specific topics.

Computer Security:

Definitions of basic security terms, Security Goals (CIA), Risks, Vulnerabilities, Attacks, Basic Cryptography and Cryptography Protocols (e.g., Kerberos, SSL), Threats in IT systems (Malware, targeted attacks, ...), Security Mechanisms (Authentication, Access Control, Network Security FW IDS, Browser, Email), Physical Security Example Literature: Ross Anderson: Introduction to Computer Security, William Stallings: Computer Security – Principles and Practice.

Network Security:

Firewalls, IDS (signature-, anomaly-based), IPsec (IKE), Malware, Remote Attacks, Protocol Attacks (ARP, DNS, Routing, ICMP), Non-IP Network Security (SS7, layer 2), Mobile Networks (WLAN). Example Literature: William Stallings: Network Security – Principles and Practice.

System security:

Overflows Attacks, Language-level security, Application-level security, Webbased Attacks (OWASP), Formal verification, Sandboxing, Isolation. Example Literature: Gary McGraw: Software Security Library.

Information Security Management:

Security policies. Roles. Classifications. Assets and threats. Risk, vulnerability, control, attack, damage. Risk analysis. Methods/tools for risk analysis. CERTs. Risk assessment and risk management. Code of Practise for Information Security (BS7799). Evaluation of information security, like ITSEC and the Common Criteria. Security plan, attack trees, business continuity planning/incident recovery. Legal issues: patents and copyright.

Cryptography:

Advanced Cryptography, Cryptoanalysis, Randomness, Adversary Models, Zero- Knowledge, SideChannel Attacks. Example Literature: Henk van Tilborg: Fundamentals of Cryptology, Stallings: Cryptography & Network Security – Principle and Practice.

Privacy:

Privacy, Data Protection, Legal Basis, Privacy Enhancing Technologies, Privacy by Design, Privacy Assessment, Location Privacy.

The above common technical content is delivered through different sets of mandatory and elective courses at the entry universities.

4.3 Specialisation courses (second year)

Technical specialisations offered by the Exit Universities in the second year of the programme, alongside with the I&E courses, are:

ELTE: Advanced Cryptography

The specialisation focuses on the general ideas, techniques and methods of applied cryptography as well as on the theoretical background and solid knowledge, putting security in a wider context. Security and privacy are considered both from the technological and from the economical point of view, which supports decisions in many practical cases. Applied cryptography serves as a base for most of the secure IT-systems (e.g. in Future Media and Content Delivery, Smart Spaces, Digital cities, Health and ICT-Mediated Human Activity, and Enabling the Internet of the Future).

ELTE: Quantum-resistant Cryptography

The specialisation focuses on the general ideas, techniques and methods of security in the coming era of quantum technology. The theoretical background gives a solid understanding of cryptographic aspects and supports technological and economical decisions on security. In order to maintain security and privacy of IT systems (e.g. in Future Media and Content Delivery, Smart Spaces, Digital cities, Health and ICT-Mediated Human Activity, and Enabling the Internet of the Future) when quantum devices are around, new physical communication layers, novel computational architecture and cryptographic protocols may be used. Quantum-resistant cryptography serves as a base to understanding and overcoming these challenges.

EURECOM: Big Data Security

EURECOM is offering a specialisation in Big Data Security that aims at providing a solid knowledge of security in cloud computing and networking combined with practical design and management skills. The students learn how to identify threats, vulnerabilities and privacy problems in networks and cloud systems including the Internet of Things. They learn to integrate security solutions to a

cloud computing platform and explore methods for holding cloud stakeholders accountable for the privacy and confidentiality of data in cloud systems.

The curriculum has a hands-on approach that combines laboratory work with classroom education, makes use of high-profile industry speakers to introduce the latest technologies, and includes a supervised semester-long team project on a topic of industrial relevance. One focus area is communication and organizational skills together with project planning and implementation competencies. A mandatory management course fosters an entrepreneurial mindset, and the elective courses enable students to further explore data science or networking.

UBB: Software Security

This master's programme offers a multiple perspective on the field of cyber security, addressing issues related to its various components: operating system security, network security, organisation and business process security, with a strong emphasis in the second year on the security of the software itself.

The courses in the 2nd year will have a strong focus on knowledge about 'Software Security', which is also the specialisation of the exit year. Students will be able to take courses like: Advanced Software Security, Securing Mobile and IoT Software, Program Analysis for Software Security, and Cloud Application and Infrastructure Security. These courses will address advanced topics such as: software quality models, security as a quality factor in software, security analysis and verification of software, design of security checking tools, cloud and mobile application security. The overall goal of this specialisation is for students to understand the secure by design principles and assess different software security issues, in order to learn how to detect security vulnerabilities as soon as possible in the development cycle and to develop a more secure software from design to implementation. Also, a new course on XDR (Extended Detection and Response) is offered in cooperation with an industry partner, students having the opportunity to learn how to technically address security incidents.

The programme also has a strong emphasis on practical knowledge in the field of cyber security, the curricula being discussed with a number of companies that offer services and solutions in this field. Some of the students' activities, such as the internship or the thematic projects, can be carried out in partnership with the partner companies/industry in the field. The latter have a strong local presence, the city of Cluj-Napoca, Romania, being known as a strong development hub in the field of IT&C.

UNITN: System Security

In recent years, the most popular computing and communications platforms have changed dramatically from old desktops and personal computers to a myriad of new devices, often embedded and personal usually interconnected using several communications technologies. Such novel platforms have pervaded all economic sectors, also those traditionally relying on analog technology. This revolution has touched private, business and governmental domains (e.g., industry 4.0, smart-homes, critical infrastructures, automotive, smart cities, etc.). This in turn has created entire new ecosystems that include technical, social and economic factors.

The specialisation System Security focuses on addressing security and privacy for these new ecosystems trying a holistic approach that does not focus only on technical issues. Of course, it covers the technological aspects such as investigating and experimenting new class of threats and vulnerabilities, developing new technology to establish trust, designing novel way to authenticate users and machines. But it covers also, methodology to assess and enhance the security of the software development process and the economic aspects that are crucial to understand attackers, their motivations and to design effective defence strategies

UT: Circular Security

With the transformation into a digital society, our world is relying more and more on interconnected ICT systems. Despite this increasing dependency on computer systems, cybersecurity is still often an afterthought and only considered at the end of the development process or even later during deployment; think about IoT devices that are installed in isolated networks or zero-day exploits that are patched in live systems.

It is common practice to offer only time-limited support after release and end-of-life products do not receive further (security) updates. This planned obsolescence does not only lead to wasteful consumption of resources but also exposes computer networks with outdated systems to significant security risks.

Contradicting this practice, the adoption of computer systems into long-living facilities such as power-plants or cars leads to the new challenge of secure systems that stand the test of time. Notably, many risks for such systems are not solely of technical nature. Thus, we address the challenge of circular security from the technical perspective and complement it with socio-economic context.

Our specialisation looks at the many risks in the above-mentioned setting and provides mitigations that can be used already at the beginning of the design-phase. Additionally students get introduced to approaches for subsequent monitoring of live systems, while taking into account the specific requirements and the impact of various risks over the system's complete lifecycle.

UTU: Security Technologies and Intelligence

The Security Technologies and Intelligence specialisation focuses on researching pre-emptive, reactive and analytical security technologies to protect systems from cyber threats and malicious exploitation attempts in the era of artificial intelligence and machine learning. The compulsory studies are on intelligent technologies for protecting systems and networks (firewalls and intrusion prevention), ethical hacking (penetration testing) and analyzing digital traces of malicious activity (digital forensics).
The specialisation gives its students profound and substantial education and expertise in the field. Optional studies selected personally for each student build a special individual information security expertise profile. The curriculum consists of both theoretical and hands-on study modules. Also a large group project module called 'Capstone project' can be included in the studies.
The graduates of this specialisation will have strong technological, theoretical and practical understanding in security technologies for protecting systems and environments against cyber threats. With these new skills and knowledge, graduates can proceed to building a successful career in securing and protecting the ICT intensive industry. The graduate's unique expertise profile may lead to a career title of, for example, one of the following: Cyber Security Analyst, Penetration and Vulnerability Tester, Cyber Security Consultant, Cyber Security Manager, Network Security Specialist, Cyber Security Entrepreneur, System / Network Administrator, Business Information Security Officer, Chief Information Officer, Chief Information Security Officer, Head of Corporate IT.

4.4 Specific admission requirements

In order to be admitted students have to meet the admission requirements (e.g. grade point average, graduation session) of each partner University they apply to. The ineligibility of the students with respect to the admission requirements of one of the chosen Universities may limit their mobility options. These additional admission criteria must be specified clearly on the webpage of the concerned EIT Digital Master programme.

The specific admission requirements for the Cyber Security education are: A B.Sc. degree in electrical engineering/ electronics, computer engineering, computer science or information

technology or applied mathematics is required. The studies should include at least 60 ECTS courses in computer science, computer architecture, or programming, and mathematics including calculus, algebra and mathematical statistics.

4.5 Degrees

The general degrees and legal frameworks for the EIT Digital partner universities are as follows:

- **Finland** UTU: Diplomi-insinööri, Diplomingenjör, Master of Science (Technology), Decree of the Council of State on University Degrees (1136/2009)
- **France** EUR and UR: DIPLÔME NATIONAL DE MASTER EN SCIENCES, TECHNOLOGIES, SANTÉ, MENTION INFORMATIQUE, PARCOURS SÉCURITÉ NUMÉRIQUE (Master of Science in Digital Security)
- **Italy** UNITN: Laurea Magistrale in Informatica - classe LM-18 (Master of Science in Computer Science) D.M. 270 dated 22 October 2004
- **The Netherlands** The Netherlands UT: Master of Science in Computer Science, Croho, 60300, 31-07-2014
- **Hungary** ELTE: "Master Degree" or "Magister" (abbreviated as MSc) (Section 52. Act. 5) and legal framework Act CCIV of 2011 On National Higher Education, National Assembly
- **Romania** UBB: SECURITATE CIBERNETICĂ. MASTER (CYBER SECURITY. MASTER'S DEGREE), HG 356/2023

4.6 Local programmes

The specific local master programs used for local implementation of this Cyber Security education are given below:

- **UTU:** Master's Degree Programme in Information and Communication Technology
- **UBB:** Cyber Security Master's Degree
- **EUR and UR:** M.Sc. in Digital Security
- **UT:** M.Sc. Computer Science
- **UNITN:** M.Sc. in Computer Science
- **ELTE**: M.Sc. in Computer Science

All local programs are nationally accredited.

4.7 Grading systems

The involved Partner Universities use national grading systems.

4.8 Guidelines

4.8.1 Guidelines for handling delays

The local guidelines of the partner which is responsible when a delay occurs and the general guidelines of the Master School Office shall be used to handle delays. In case of conflict, the corresponding guideline of the Master School Office shall be applied.

4.8.2 Guidelines for issuing Double Degrees

The local guidelines of both the Entry and the Exit University or Institution together with the general guidelines of the Master School Office are taken into account when issuing the Double Degree. Any potentially conflicting guidelines shall not be applied to the disadvantage of the degree candidate. In case of conflict the guidelines of the Master School Office concerning the specific matter shall be applied.

4.9 Conclusions

The field of cybersecurity is rapidly developing, with increasing challenges given by our growing dependence on the digital infrastructure. Despite significant growth in the cybersecurity workforce, the skills gaps persist and grow in many areas. This field still faces diversity challenges, women are underrepresented globally. Targeted education, upskilling, and continuous adaptation of cybersecurity programs are essential. Our approach is to align the curriculum with current and predicted market needs.

This deliverable provides a labor market analysis for cybersecurity and presents an updated curriculum for our Cyber Security MSc Programme based on the analysis.

5 Annex 1 – List of the courses for each Entry and Exit program

5.1 ELTE

5.1.1 Entry year (60 ECTS)

5.1.1.1 First semester (28 ECTS)

Compulsory Technical Courses (18 ECTS)	ECTS
▪ Research Methodology	5
▪ Symmetric Key Cryptography	4
▪ Introduction to Offensive Security I.	4
▪ Privacy-enhancing Technologies	4
▪ Introductory Mathematics for Cybersecurity Specialisation	1

Compulsory I&E Courses (10 ECTS)	ECTS
▪ I&E Basic	6
▪ Business Development Lab I.	4

5.1.1.2 Second semester (32 ECTS)

Compulsory Technical Courses (18 ECTS)	ECTS
▪ Design and Analysis of Algorithms	4
▪ Public Key Cryptography	4
▪ Introduction to Data Security	4
▪ Advanced Software Technology	4
▪ Network Security	2

Compulsory I&E Courses (14 ECTS)	ECTS
▪ Innosocial Aspects of the Entrepreneurship	6
▪ Thematic Innovation & Entrepreneurship project/Summer school	4
▪ Business Development Lab II	4

5.1.2 Exit year (60 ECTS)

5.1.2.1 *First semester* (30 ECTS)

Advanced Cryptography

Compulsory Technical Courses (24 ECTS)	ECTS
• Secure Multiparty Computation	4
• Zero-knowledge proofs and application	4
• Penetration testing	6
• Cryptographic Protocols	6
• Provably Secure Modular Design of Cryptographic Protocols	4

Compulsory I&E Course (6 ECTS)	ECTS
• I&E Study	6

Quantum-resistant Cryptography

Compulsory Technical Courses (24 ECTS)	ECTS
• Introduction to Quantum Information	4
• Post-quantum Cryptography	4
• Penetration testing	6
• Cryptographic Protocols	6
• Provably Secure Modular Design of Cryptographic Protocols	4
Compulsory I&E Course (6 ECTS)	ECTS
• I&E Study	6

5.1.2.2 *Second semester* (30 ECTS)

Compulsory Technical Course (30 ECTS)

- Master's thesis (includes internship) (30 ECTS)

5.2 EURECOM

5.2.1 Exit year (60 ECTS)

5.2.1.1 *First semester* (30 ECTS)

Big Data Security

First Semester (30 ECTS)

Compulsory Technical Courses (5 ECTS)	ECTS
• Security and Privacy for Big Data and Cloud	2.5
• Multiparty Computation and Blockchains	2.5
• Mobile Systems and Smartphone Security	5

Other Compulsory Courses (9 ECTS)	ECTS
Compulsory Semester Project (8 ECTS)	8
Compulsory Languages (1 ECTS)	1

Compulsory I&E Course (6 ECTS)

- Fundamental in Innovation and Entrepreneurship 6

Elective courses (10 ECTS) ECTS

- Machine Learning and Intelligent Systems 5
- Distributed Systems and Cloud Computing 5
- Quantum Information Science 2.5
- Digital Image Processing 2.5
- System and Network Security 5
- Mobile Communication Systems 5

5.2.1.2 *Second semester* (30 ECTS)

Compulsory Course (30 ECTS)

- Master's thesis (includes internship) 30

Additional Information:

A Research Methodology course is integrated into the Compulsory Semester Project (8 ECTS) course.

Elective courses are chosen individually by each student when their personal study plan is created, ensuring that the total number of credits in each academic year is 60 ECTS. The students can take more than 60 ECTS, and there is no fee for taking additional credits.

3.3 UBB

3.3.1 Entry year (60 ECTS)

3.3.1.1 First semester (30 ECTS)

Compulsory Technical Courses (17 ECTS) ECTS

- Cryptography 7
- Quality Aspects of Security in Software Testing 6
- Computer Ethics and Academic Integrity (equivalent to Research Methodology course) 4

Compulsory I&E Course (8 ECTS) ECTS

- Digital Economy Principles - I&E basics 8

Elective courses in I&E (5 ECTS) - see further information about elective courses in section 3.3.1.2

3.3.1.1. Second semester (30 ECTS)

Compulsory Technical Courses (12 ECTS) ECTS

- Web and Internet Security 6

- Security Audit and Risk Management 6

Compulsory I&E Courses (11 ECTS) ECTS
- Innovation Management - I&E Business Dev Lab 7
- Thematic Project with Innovation Challenge - EIT Digital Summer School 4

Elective courses in Cybersecurity (7 ECTS) - see further information about elective courses in section 3.3.1.2

3.3.1.2. Elective courses

Elective courses in I&E (5 ECTS) ECTS
- Agile Project Management (semester 1) 5
- Strategic Business Process Automation (semester 1) 5
- Business Forecasting and Predictive Modelling (semester 1) 5

Elective Courses in Cybersecurity (7 ECTS) ECTS
- Network Security and Administration (semester 2) *7*
- Blockchain Security (semester 2) 7
- Complex Networks in Security (semester 2) 7
- Quantum Cryptography (semester 2) 7

3.3.2. Exit year (60 ECTS)

3.3.2.1. First semester (30 ECTS)

Software Security

Compulsory Technical Courses (24 ECTS) ECTS
- Advanced Software Security 6
- Securing Mobile and IoT Software 6
- Program Analysis for Software Security 6
- Cloud Application and Infrastructure Security 6

Compulsory I&E Course (6 ECTS) ECTS
- Entrepreneurship in IT - I&E Study 6

Facultative courses - see further information about other courses in section 3.3.2.3

3.3.2.2. Second semester (30 ECTS)

Compulsory Courses (30 ECTS) ECTS
- Internship in Specialisation 20
- Project in Cybersecurity 6
- Elaboration of the Dissertation Thesis 4

3.3.2.3. Other courses

UBB is offering an additional course for Cybersecurity master's students, which grants extra credits. This is an optional course, and students can choose whether or not to enrol, with extra credits awarded upon completion. There is no fee for taking this course or receiving the corresponding credits.

Facultative Course	ECTS
• Extended Detection and Response (exit year, semester 1)	5

Additional Information:

A Research Methodology (or have research methodology topics in a) course at master's level is mandatory. This is a requirement imposed by the Romanian Agency for Quality Assurance in Higher Education. In our curricula this is the course titled: "Computer Ethics and Academic Integrity".

Elective courses are chosen individually by each student when their personal study plan is created, ensuring that the total number of credits in each academic year is 60 ECTS. The students can take more than 60 ECTS, and there is no fee for taking additional credits.

5.4 UR

5.4.1 Entry year (60 ECTS)

5.4.1.1 *First semester* (30 ECTS)

Compulsory Technical Courses (20 ECTS)	ECTS
• Basic Cryptography	5
• Low-Level Programming	5
• System Security	5
• Network Security	5

Compulsory I&E Courses (10 ECTS)	ECTS
• Innovation and entrepreneurship	5
• Business Development Laboratory 1	5

5.4.1.2 *Second semester* (30 ECTS)

Compulsory Technical Courses (20 ECTS)	ECTS
• Research Project (equivalent to Research Methodology)	5
• Privacy	5
• System Security	5
• Software Exploitation	5

Compulsory I&E Courses (10 ECTS)	ECTS
• Business Development Laboratory 1	5
• Knowledge and Intangible Assets Management	5

Additional information

At the University of Rennes, the Summer School is integrated into the programme's second year. As the SPECTRO programme is delivered exclusively during the first year at Rennes, the ECTS from the Summer School are awarded to students upon completion of the second year, counting towards coursework completed at partner institutions abroad.

5.5 UNITN

5.5.1 Entry year (60 ECTS)

5.5.1.1 *First semester (30 ECTS)*

Compulsory Technical Courses (12 ECTS)	ECTS
• Introduction to Computer and Network Security	6
• Applied Cryptography	6
• Security Testing	6
• Privacy and IPR	6

Compulsory I&E Courses (6 ECTS)	ECTS
• Innovation and Entrepreneurship Basics (Economics and Management)	6

Elective Courses (12 ECTS)	ECTS
• Machine Learning	6
• Embedded software for the Internet of things	6
• Security Experiments: attacks and defenses.	12
• Ethics for computer science and engineering	6
• Advance Programming of Cryptographic Methods	6
• Multimedia Data Security	6

5.5.1.2 *Second semester (30 ECTS)*

Compulsory Technical Courses (12 ECTS)	ECTS
• Cyber Security Risk Assessment	6
• Network Security	6

Compulsory I&E Courses (18 ECTS)	ECTS
• Business Development Lab	9
• ICT Innovation (includes the Summer School)	9

5.5.2 EXIT year (60 ECTS)

5.5.2.1 *First semester* (30 ECTS)

System Security

Elective Technical Courses (24 ECTS)	ECTS
• Multimedia Data Security	6
• Security Testing	6
• Privacy and Intellectual Property Rights	6
• Network Intrusion and Anomaly Detection with Machine Learning	6
• Advance Programming	6
• Security experiments: attacks and defenses	12
• Applied Cryptography	6
• Embedded Software for the Internet of Things	6
• Project course	6
• Machine learning	6
• Research Project	12
• High-Performance Computing for Data Science	*6*

Compulsory I&E Course (6 ECTS)	ECTS
• Innovation and Entrepreneurship Studies in ICT (Includes the summer school)	6

5.5.2.2 *Second semester* (30 ECTS)

Compulsory Courses (30 ECTS)	ECTS
Internship	6
Master's thesis	24

Additional information
A Research Methodology course is not mandatory at UNITN.
Elective courses are chosen individually for each student when their personal study plan is created, ensuring that the total number of credits in each academic year is 60 ECTS. The students can take more than 60 ECTS, and there is no fee for taking additional credits.

5.6 UT

5.6.1 Entry year (60 ECTS)

5.6.1.1 *First semester (30 ECTS recommended)*

Compulsory Technical Courses (15 ECTS)	ECTS
• Cyber Risk Management	5

- Security and Cryptography 5
- Software Security 5

Compulsory I&E Courses (15 ECTS) ECTS
- I&E Basics: Innovation Management for EIT 5
- Business Development Lab I 5
- Computer Ethics 5

Elective courses in Major Subject and I&E (see further information about elective courses in section 3.5.1.3)

5.6.1.2 *Second semester (30 ECTS recommended)*

Compulsory Technical Major Courses (10 ECTS) *ECTS*
- Internet Security 5
- System Security 5

Compulsory I&E Courses (9 ECTS) ECTS
- Business Development Lab II 5
- I&E for Venture Creation (includes a Summer School) 4

Elective courses in Major Subject and I&E (see further information about elective courses in section 3.5.1.3)

5.6.1.3 *Elective courses*

At least 11 ECTS of elective courses must be taken during the entry year. Elective courses can be taken in both the first and the second semester based on the student's personal study plan made together with the study plan advisor. It is recommended that the study plan is balanced between semesters (that is, that the semesters will include about 30 ECTS each). The following list contains a selection of recommended elective courses, however, based on individual interests, students can choose other offered by the computer-science department.

List of recommended elective courses (choose at least 11 ECTS) ECTS
- Basic Machine Learning (semester 1) 5
- Introduction to Biometrics (semester 1) 5
- Privacy-Enhancing Technologies Bootcamp (semester 1) 5
- I&E: Brand Management (semester 1) 5
- I&E Empirical Methods for Designers (semester 1) 5
- I&E: Smart Industry (semester 1) 5
- Automated Vulnerability Research and Mitigation (semester 2) 5
- Software Testing and Reverse Engineering (semester 2) 5
- Blockchain & Distributed Ledger Tech (semester 2) 5
- Cyber Data Analytics (semester 2) 5
- E-Law (semester 2) 5
- Security Services for the Internet of Things (semester 2) 5

5.6.2 Exit year (60 ECTS)

5.6.2.1 *First semester (30 ECTS recommended)*

Circular Security

Compulsory I&E Courses (15 ECTS)	ECTS
• Computer Ethics	5
• I&E Study	6
• Research Topics EIT	4

Elective courses in Major Subject (see further information about elective courses in section 5.6.2.3)

5.6.2.2 *Second semester*

Compulsory Technical Major Course (30 ECTS)	ECTS
• Master thesis (includes the internship)	30

Elective courses in Major Subject (see further information about elective courses in section 5.6.2.3)

5.6.2.3 *Elective courses*

At least 15 ECTS of elective courses must be taken during the exit year. Elective courses can be taken in both the first and the second semester based on the student's personal study plan made together with the study plan advisor. It is recommended that the study plan is balanced between semesters (that is, that the semesters will include about 30 ECTS each). Since students are expected to work on their final degree project in the second semester, the following list of recommended elective courses only contains courses offered in the first semester. However, based on individual interests, students can choose other courses.

List of recommended elective courses (choose at least 15 ECTS)		ECTS
• Secure Data Management	(semester 1)	5
• Secure Cloud Computing	(semester 1)	5
• Cloud Networking	(semester 1)	5
• Advanced Networking	(semester 1)	5
• Empirical Security Analysis & Engineering	(semester 1)	5
• Introduction to Biometrics	(semester 1)	5
• Cyber Risk Management	(semester 1)	5
• Design of Software Architectures	(semester 1)	5
• Machine Learning 1	(semester 1)	5
• Internet of Things	(semester 1)	5
• Quantum Information	(semester 1)	5

Additional information

A Research Methodology course at master's level is not mandatory. However, SPECTRO exit year students have the compulsory study unit "Research Topics EIT" which must be taken before they can start their master thesis. In this

study unit students are asked to plan their master thesis, which includes the definition of concrete research questions and a methodology how these questions will be answered.

Elective courses are chosen individually by each student when their personal study plan is created, ensuring that the total number of credits in each academic year is at least 60 ECTS. Students can take more than 60 ECTS, and there is no fee for taking additional credits.

5.7 UTU

5.7.1 Entry year (60 ECTS)

5.7.1.1 *First semester (31 ECTS recommended)*

Compulsory Technical Courses (16 ECTS)	ECTS
• System and Application Security	5
• Management of Information System Security	6
• Foundations of Cryptography	5

Compulsory I&E Courses (5 ECTS)	ECTS
• Introduction to Innovation and Business	5

Elective courses in Major Subject and I&E (see further information about elective courses in section 3.6.1.3)

5.7.1.2 *Second semester (29 ECTS recommended)*

Compulsory Technical Courses (15 ECTS)	ECTS
• Network Infrastructure Technologies and Security	5
• Human Element in Information Security	5
• Cryptography I	5

Compulsory I&E Courses (14 ECTS)	ECTS
• Lean Digital Business Design	10
• Summer School	4

Elective courses in Major Subject and I&E (see further information about elective courses in section 3.6.1.3)

5.7.1.3 *Elective courses*

At least 10 ECTS of elective courses must be taken during the entry year. Elective courses can be taken in both the first and the second semester based on the student's personal study plan made together with the study plan advisor. It is recommended that the study plan is balanced between semesters (that is, that the semesters will include about 30 ECTS each). Further details:

• The elective courses must contain at least 5 ECTS of I&E courses from this list:	ECTS
○ Knowledge and Innovation Management (semester 1)	5

- Enterprise Architecture (semester 2) 6
- Digital Business (semester 2) 3
- Digital Business Models (semester 2) 3

- Other elective studies (typically in the major subject) are chosen individually for each student from the selection of annually available qualifying courses in the personal study plan so that the entry year total is 60 ECTS. With the minimum amount of I&E studies, this means one additional elective course of 5 ECTS.

5.7.2 Exit year (60 ECTS)

Specialisation: Security Technologies and Intelligence

5.7.2.1 *First semester (30 ECTS Recommended)*

Compulsory Technical Courses (15 ECTS)	ECTS
• Firewall and IPS Technology	5
• Ethical Hacking	5
• Digital Forensics	5

Compulsory I&E Course (6 ECTS)	ECTS
• I&E Study	6

Elective courses in Major Subject (see further information about elective courses in section 3.6.2.3)

5.7.2.2 *Second semester (30 ECTS Recommended)*

Compulsory Technical Course (30 ECTS)	ECTS
• Master's Thesis in Technology (includes internship)	30

Elective courses in Major Subject (see further information about elective courses in section 3.6.2.3)

5.7.2.3 *Elective courses*

At least 9 ECTS of elective courses must be taken during the exit year. Elective courses can be taken in both the first and the second semester based on the student's personal study plan made together with the study plan advisor. It is recommended that the study plan is balanced between semesters (that is, that the semesters will include about 30 ECTS each).

The exit year elective courses are chosen individually for each student when their personal study plan is made so that the exit year total is 60 ECTS. They can be chosen from the list below or from other qualifying courses available annually.

List of recommended elective courses (choose at least 9 ECTS)	ECTS
• Privacy and Security for Software Systems (Semester 1)	5
• Security Engineering (Semester 1)	5
• Algebraic Structures in Cryptography (Semester 1)	5

- Protocol Processing and Security (Semester 1 or Semester 2) 5
- Capstone Project (Semester 1 or Semester 2) 10
- Seminar 1 (TurkuSec meetings) (Semester 1 or Semester 2) 1-5
- Communication Technologies and Security in IoT (Semester 2) 5
- Cryptography II (Semester 2) 5

Additional information

A Research Methodology course is not mandatory (by law) in Finland. In the SPECTRO curriculum, research methodology education is integrated into the following courses in the entry year: System and Application Security, Network Infrastructure Technologies and Security; and into the following courses in the exit year: Firewall and IPS Technology, Digital Forensics, Master's thesis.

Students can take more than 60 ECTS, and there is no additional fee for taking more than 60 ECTS.

References

[SPECTRO] http://eitdigital.eu/spectro/

Glossary

Community	A group of users, organised with a common purpose, and jointly granted access to resources. It may act as the interface between individual users and the resources. (see also [WISE-SCI])
EIT	European Institute of Innovation and Technology
KIC	Knowledge and Innovation Community
GDPR	General Data Protection Regulation
R&S	Research and scholarship