DJM-CYBER: A Joint Master in Advanced Cybersecurity

Yianna Danidou*
y.danidou@euc.ac.cy
European University Cyprus
Nicosia, Cyprus

Sara Ricci
ricci@vut.cz
Brno University of Technology
Brno, Czech Republic

Antonio Skarmeta
skarmeta@um.es
Universidad de Murcia
Murcia, Spain

Imre Lendak
Eötvös Loránd University (ELTE)
Budapest, Hungary
lendak@inf.elte.hu

Jiri Hosek
hosek@vut.cz
Brno University of Technology
Brno, Czech Republic

Stefano Zanero
stefano.zanero@polimi.it
Politecnico di Milano
Milano, Italy

ABSTRACT

Various publicly available studies show that millions of cybersecurity experts are missing worldwide. One possible way to tackle the workforce gap is with tailored higher education programmes. The goal of this paper is to present the relevant projects and frameworks of the European Union which can guide the development of novel cybersecurity education offerings. We describe the most relevant and freely available tools and test them in the development of a joint Master study programme to be offered by a consortium of five European universities. We show that these tools allow educators and study programme developers to map their outputs to the European Cybersecurity Framework developed by the ENISA and other similar frameworks. We complete our work with a detailed analysis of a joint cybersecurity master programme consisting of four innovative and distinctly different tracks.

CCS CONCEPTS

• Social and professional topics → Model curricula; **• Applied computing → Education**; **• Human-centered computing → Human computer interaction (HCI)**.

KEYWORDS

cybersecurity education, joint master programme, cybersecurity roles, cybersecurity profiles, ENISA ECSF, NICE Framework

ACM Reference Format:
Yianna Danidou, Sara Ricci, Antonio Skarmeta, Imre Lendak, Jiri Hosek, and Stefano Zanero. 2023. DJM-CYBER: A Joint Master in Advanced Cybersecurity. In *The 18th International Conference on Availability, Reliability and Security (ARES 2023), August 29–September 01, 2023, Benevento, Italy*. ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3600160.3605002

1 INTRODUCTION

In today's digital landscape, cybersecurity has emerged as a critical and pressing topic, given the growing reliance of public and private organisations as well as individuals on technology for their day-to-day operations and communication. However, the demand for cybersecurity expertise often surpasses the availability of skilled professionals who can implement and maintain effective cybersecurity measures. As a result, this skill gap poses vulnerabilities and risks, with potential consequences for individuals, businesses, and even nations.

Europe has been particularly affected by the shortage of cybersecurity experts, as the demand for these skills has increased rapidly in recent years, leading to a significant skills gap in the field. The complex and ever-evolving nature of cybersecurity necessitates ongoing training and education, making it challenging to identify, address, and update the required security skills [1, 2]. To address this issue, companies, governments, and academia have defined cybersecurity profiles and related skills in an ad-hoc manner, resulting in diverse definitions for the same requirements. Therefore, there is a need to standardize these profiles and skills to align with the European perspective, in order to develop more efficient training programs that can meet the current and future training needs. A notable outcome of these efforts is the European Union Agency for Cybersecurity's (ENISA) European Cybersecurity Skills Framework (ECSF) [6], which has successfully redefined and consolidated cybersecurity profiles into 12 comprehensive profiles that encompass all necessary current skills, with provisions for future skill updates.

The shortage of cybersecurity experts continues to be a persistent challenge, and the demand is expected to surpass the supply in the foreseeable future. This underscores the ongoing need for sustained investment in education and training programs, as well as the promotion of cybersecurity as a viable and rewarding career path to attract more talent to the field. Across Europe, there are several initiatives that emphasize the importance of cybersecurity from an early age, aiming to generate increased interest among young people in pursuing a career in cybersecurity in the future [3]. Providing comprehensive and engaging guidance to teachers at the basic education levels is crucial, with content that not only fosters curiosity and interest in the cybersecurity field but also raises awareness about cybersecurity and underscores the demand for experts in this sector.

2 IMPACT OF THE PROGRAMME

In response to the skills gap, European governments and businesses are investing in education and training programs to cultivate the next generation of experts. One such European investment is the Erasmus Mundus initiative which leads to Higher Education institutions (HEIs) to collaborate and jointly offer specialized Master-level study programs. Erasmus Mundus Joint Master (EMJM) projects

ARES 2023, August 29–September 01, 2023, Benevento, Italy
© 2023 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-0772-8/23/08.
https://doi.org/10.1145/3600160.3605002

can receive EU funding and be implemented by mature consortia in a single stage, or consortia can be set up with the Erasmus Mundus Design Measures lump-sum funding instrument of the EU. The Designing a Joint Master in Cybersecurity (DJM-CYBER) was an EMDM project which aimed to design and develop a Joint Master in Advanced Cybersecurity programme. In order to ensure the effectiveness and relevance of the proposed curriculum, the consortium prioritized academic education to match the profiles identified in ENISA's ECSF and the NIST NICE Competencies framework.

The design and eventual establishment of the Joint Master's in Advanced Cybersecurity can have a significant impact by enhancing education and training by providing a comprehensive and specialised curriculum, interdisciplinary, cutting-edge research and practical training; creating a pool of diverse and highly skilled professionals, while attracting top talents from across Europe and beyond; improving cybersecurity practices and standards raising the overall cybersecurity posture in Europe; fostering collaborative research and innovation among students, faculty, and researchers from different countries and institutions, leading to the exchange of ideas, novel research findings, and innovative solutions; strengthening the European cybersecurity ecosystem by facilitating partnerships between academia, industry, and government, leading to increased collaboration, information sharing, and joint initiatives in cybersecurity research, development, and policy-making; and addressing the skills gap in the field by producing highly trained graduates with specialized expertise. Graduates of the program would possess advanced qualifications recognized across Europe, making them highly competitive in the job market and capable of meeting the increasing demand for skilled cybersecurity experts.

3 CYBERSECURITY ROLES AND PROFILES

In this section, we briefly review the NIST NICE Competencies framework and the ENISA European Cybersecurity Skills Framework Role Profiles (ECSF). The consortium has aligned the curriculum of the (future) Joint Master's Programme with both taxonomies to ensure that graduates will possess the necessary knowledge, skills and abilities that are in current demand in the cybersecurity workforce as well as in the future, making them more competitive and relevant in the job market, and helping to close the skills gap.

3.1 NIST NICE work roles

The National Initiative for Cybersecurity Education (NICE) is a United States partnership between government, academia and the private sector led by the National Institute of Standards and Technology (NIST). It supports cybersecurity training and education providers by developing taxonomies, standards, and best practices. Among the created standards, the NICE Framework [12] provides a detailed description of 1) work roles, 2) knowledge, skills, and abilities (KSAs), and 3) tasks of aforementioned work roles. Accordingly, this framework identifies which knowledge and skills are required by particular work roles available in the cybersecurity job market.

3.2 ENISA Cybersecurity Skills Framework - ECSF

The ENISA European Cybersecurity Skills Framework (ECSF) [6] is the result of the joint efforts of ENISA and the ENISA ad-hoc working group on cybersecurity skills framework. The ECSF aims to create "a common understanding of the relevant roles, competencies, skills and knowledge in order to facilitate cybersecurity skills recognition and to support the design of cybersecurity-related training programs". The framework summarizes all cybersecurity-related roles into 12 profiles, with clearly outlined related key tasks, skills, knowledge, and competencies. It is important to notice that the ECSF counts a total of 84 key skills and 69 key knowledge areas defined. This list of key skills and knowledge create a common taxonomy for academia, i.e., they specify which knowledge are needed to be taught. The 12 ECSF profiles are as follows: Chief Information Security Officer (CISO), Cyber Incident Responder, Cyber Legal, Policy & Compliance Officer, Cyber Threat Intelligence Specialist, Cybersecurity Architect, Cybersecurity Auditor, Cybersecurity Educator, Cybersecurity Implementer, Cybersecurity Researcher, Cybersecurity Risk Manager, Digital Forensics Investigator, and Penetration Tester.

4 RELATED CYBERSECURITY EDUCATION PROJECTS

Several cybersecurity frameworks have been developed over the last five years (2017- 2022), aimed at providing suitable reference structures for different purposes: academic education, professional training, and scientific and technological research. We mention in particular the following frameworks, due to the broadness of their scope and the well-established international institutions that produced them:

- The Cybersecurity Curricular Guidelines (CSEC) [7]
- The Cybersecurity Workforce Framework (CWF) [12]
- The European Cybersecurity Taxonomy (JRC) [11]
- The Cybersecurity Body of Knowledge (CyBOK) [13]
- The European Cybersecurity Education and Professional Training Minimum Reference Curriculum (ECSO) [16]

Our consortium was composed of partners involved in two (over four) pilot projects namely CyberSec4Europe and SPARTA, which were chosen to address the Horizon 2020 Cybersecurity call and are part of the European Cybersecurity Competence Network which aims to strengthen and sustain Europe's cybersecurity competence where the pilots collaboratively share their achievements and results. Moreover, two members of our partnership are part of the Cybersecurity Skills Alliance – A New Vision for Europe (REWIRE) ERASMUS+ Sector Skills Alliance (SSA) project, which "aims to provide concrete recommendations and solutions that would lead to the reduction of skill gaps between industry requirements and sectoral training provision and contribute to support growth, innovation and competitiveness in the field of Cybersecurity" [14].

4.1 SPARTA - Curricula Designer

SPARTA is a project which created a long-lasting community capable of collaboration to define, develop, share, and evolve solutions that will help practitioners prevent cybercrime and enhance cybersecurity. SPARTA Deliverable D9.2 [8] contains the description of the methodology for designing higher education study programs and professional training courses, specifically recommends that a Master's degree should have at least 40 % of practical lectures.

Within the SPARTA project, a novel free web application, namely the Cybersecurity Curricula Designer [9], was developed. This app can be used to design cybersecurity curricula that reflect the needs of particular work positions. The application uses the SPARTA framework that is derived from the NIST NICE framework. In particular, through the insertion mechanism, the generated curricula can be analyzed and mapped to the NICE NIST work roles.

Moreover, the application was extended to work with the key skills of the ENISA framework and, therefore, maps the added curriculum to the ENISA framework [10].

4.2 REWIRE - Cybersecurity Profiler

Within the analysis of the ENISA ECSF framework, the REWIRE project found that the ENISA key skills and knowledge describing the profiles are uniquely phrased [5]. Moreover, this list requires technical knowledge and can be demanding to be managed for non-experts of the sector. A way to overcome this issue is to group the key knowledge and skills that represent the exact same concepts but phrased in different ways. Accordingly, a total of 31 groups were identified and used as back-end of the developed user-friendly REWIRE web applications, i.e. the Cybersecurity Profiler [5] and Cybersecurity Job Ads analyzer [15].

The REWIRE Cybersecurity Profiler is an open-source, freely available, dynamic web application which allows the design and the analysis of curricula. In particular, the Cybersecurity Profiler 1) maps existing curricula, trainings, and certifications to the ENISA profiles, 2) identifies which courses, trainings, and certifications are recommended for a certain profile, and 3) allows designing a study program, training, or certification scheme and seeing to which profile is more related. This application is an extention of the SPARTA Curricula Designer of which it shares the main features. While the Curricula Designer is intended only for curricula, the Cybersecurity Profiler also incorporates the design of professional training and certification schemes. In the Cybersecurity Profiler, the curricula are mapped to the ENISA profile through the 31 REWIRE group. For instance, the following groups/skills belong to the Cybersecurity Architect profile: "Collaborate and Communicate", "Data Privacy", "Data Security", "Enterprise Architecture and Infrastructure Design", "Information Security Controls Assessment", "Law, Policy, and Ethics", "Operating Systems", "Risk Management", "Software Development", "Technology Fluency", and "Workforce Management". We refer to [5] for more details.

4.3 CyberSec4Europe

One of the central aspects of the CyberSec4Europe cybersecurity pilot project was the identification of an education and assessment framework described in [4], which aims to support continuing education and lifelong training. The aim of the framework is not to produce all possible content required to implement educational and training programmes, but instead to define guidelines and tools that support the design of capability building instruments, open to external sources and third-party material outside the consortium, which in particular contain guidelines and methodologies to ensure adequate quality standards. This includes the identification of cybersecurity knowledge units and curricula, the specification of learning objectives and competences required to develop and enhance cybersecurity skills for different profiles and roles, the development of training and awareness to achieve such objectives and competences, together with activities to apply and test such competencies. Cybersecurity is among the fastest moving fields in today's digital world, which means that education programmes must be continuously updated with state-of-the-art research and innovation knowledge to keep them up-to-date and relevant. For this purpose, and as a forward-thinking tool for the CyberSec4Europe framework, the project has provided community-emergent suggestions on how to incorporate research and demonstrators (from CyberSec4Europe) into future educational offers. Moreover, we explain how non-traditional education formats such as cyber ranges, serious games and MOOCs can be used to offer suitable cybersecurity learning experiences.

Overall, the CyberSec4Europe provides an overview over most of the education and training activities which include curated summaries of key contributions, including translations from this framework to the European Cybersecurity Education and Professional Training Minimum Reference Curriculum (ECSO) occupations and skills standard, guidelines to develop Security Serious Games (SSG) and other gamification approaches to education, studies on job profiles of long prevalence in the cybersecurity field (border control), and incidence of current research initiatives into the knowledge areas defined in our framework.

5 JOINT PROGRAMME DEVELOPMENT

In the development of DJM-CYBER study program we made the following steps:

1. *An analysis of existing cybersecurity-oriented ERASMUS Mundus programmes.* We analysed 5 existing ERASMUS Mundus study programmes in cybersecurity considering the following aspects: 1) Selection of candidates, 2) Number of ECTS, 3) Programme duration, 4) Tuition fees and scholarships, 5) Summer schools and internships, 6) Involved countries, and others.
2. *Comparison and solution proposal.* The analysis is then followed by a comparison of the collected data where our proposed solutions are justified.
3. Usage of existing international and European level recommendations. In order to strengthen our proposal, documents on curricula recommendations were analysed.
4. *Usage of existing tools*, namely SPARTA Curricula Designer and REWIRE Cybersecurity Profiler. Both applications were used in the selection of the courses to make our proposal fit the desired NICE work roles and ENISA profiles.
5. *Structure of the proposed study programme.* At last, we propose our study program's structure.

5.1 Analysis of Existing Programmes and Comparison

We identified 5 masters currently being implemented at the European level: 1. Master‘s Programme in Security and Cloud Computing (SECCLO), 2. European Master In Law, Data and Artificial Intelligence (EMILDAI), 3. Cyberspace Behavior and E-therapy (CBE), 4. Cyberus Erasmus Mundus Master in Cybersecurity (CYBERUS),

Table 1: Comparison of existing cybersecurity ERASMUS Mundus study programmes with our proposal, i.e., DJM-CYBER. "S/W" states for Summer or Winter.

	SECCLO	**EMILDAI**	**CBE**	**CYBERUS**	**IMSISS**	**DJM-CYBER**
♯ Universities	6	4	3	3	4	5
♯ Mobility	2	2 or 3	3	3	3	2 or 3
♯ Tracks	6	4	2	2	8	4
Faculties	Engineering and Computer Science	Law and Computer Science	Psychology	Engineering and Computer Science	Social and Political Science	Engineering and Computer Science
Topics	Cloud computing, information security	Law, computing	Human behaviour background, exact sciences, engineering background	IoT cybersecurity, software cybersecurity	Intelligence, peace-building and terrorism, causes of conflicts	9 ENISA profiles
Internship	Yes (5 ECTS)	Yes (Elective)	Yes	Yes	Yes (only for selected students)	Yes (Elective)
♯ S/W School	1	3	1	1	4	1

5. International Master Security, Intelligence & Strategic Studies (IMSISS).

Table 1 shows a comparison of the five masters and our proposal. Unluckily, the analysis pointed out that there is no common strategy in the structure of these joint masters. For example, the involved faculties and topics can be either technical or humanistic. SECCLO, EMILDAI, and CYBERUS are of particular interest since we are going to propose more “technical” topics due to our expertise. However, it is important to notice that our study programme will focus on the multidisciplinarity of cybersecurity. In fact, DJM-CYBER proposes 4 tracks, and the students will receive a double degree title, more specifically 4 different double degree programmes are accredited by a consortium consisting of five universities.

The number of visited universities will be either 2 or 3 in each proposed track. We would like to minimize the number of mobilities of the students that need to adapt to the new university environment and country. We seek to achieve internationalization of their knowledge and language not only related to the cybersecurity study. However, each student should have the possibility to follow the track that he/she likes the most, and therefore, the option of 3 visited universities is required for students who already studied a bachelor’s degree in one of the involved partner countries.

Moreover, each existing study programme presents a different number of involved universities. In some cases, they have involved associated partners which either manage the summer/winter school or participate in the thesis development. The number of tracks is also varied. SECCLO study programme is the closest one due to the number of involved universities. Following the existing proposal, DJM-CYBER takes two years for a total of 120 ECTS. This allows students to have a possible access to future Ph.D. study programme without a need for any additional study. Moreover, each semester will count 30 ECTS as in all analysed programmes.

The number credits assigned to the MSc thesis is 30 ECTS. The thesis is an important component of the study programme which is compulsory in all analyzed joint masters. We also seek to give to students the possibility to work independently while supervised by an expert in the field. Most of the existing programmes assign the entire last semester to the thesis preparation. Note that there is no common strategy for the number of visited universities whereas an internship is always included.

5.2 DJM-CYBER Development and Structure

Our study programme DJM-CYBER consists of 4 different tracks that cover 4 main cybersecurity areas:

(1) **Track 1.** Cybersecurity Design and Development,
(2) **Track 2.** Infrastructure Security and Resilience,
(3) **Track 3.** Security and Cyber Intelligence,
(4) **Track 4.** Cybersecurity Operations and Management.

All the tracks have the same strategy as shown in 1. Two universities of the consortium are responsible for every track. It is planned that students will attend courses for a complete year in one university. This permits a better cultural acquaintance and academic involvement of the student in the hosting country. Moreover, each student should have the possibility to access the desired track not depending on the country that he/she studied. For instance, students who have a bachelor’s degree from either the Czech Republic or Cyprus can anyway select Track 1 with the limitation that Semester 4, the thesis development, will be done in collaboration between one of the two HEIs involved in the current track and with one of the other partner HEIs.

Our master follows the ENISA recommendations, and each track is designed to cover 2 ENISA profiles allowing a clear path from academia to work positions. Moreover, a natural continuation is to become a Cybersecurity Researcher in all cases. The connection between academia and profiles is achieved by selecting courses of each partner with the ENISA key skills and knowledge described in the considered profile. Moreover, the NIST NICE work roles related to the track are also provided.

Each track was designed using both the Curricula Designer and the Cybersecurity Profiler applications allowing, respectively, the mapping to NIST NICE framework and ENISA ECSF frameworks.

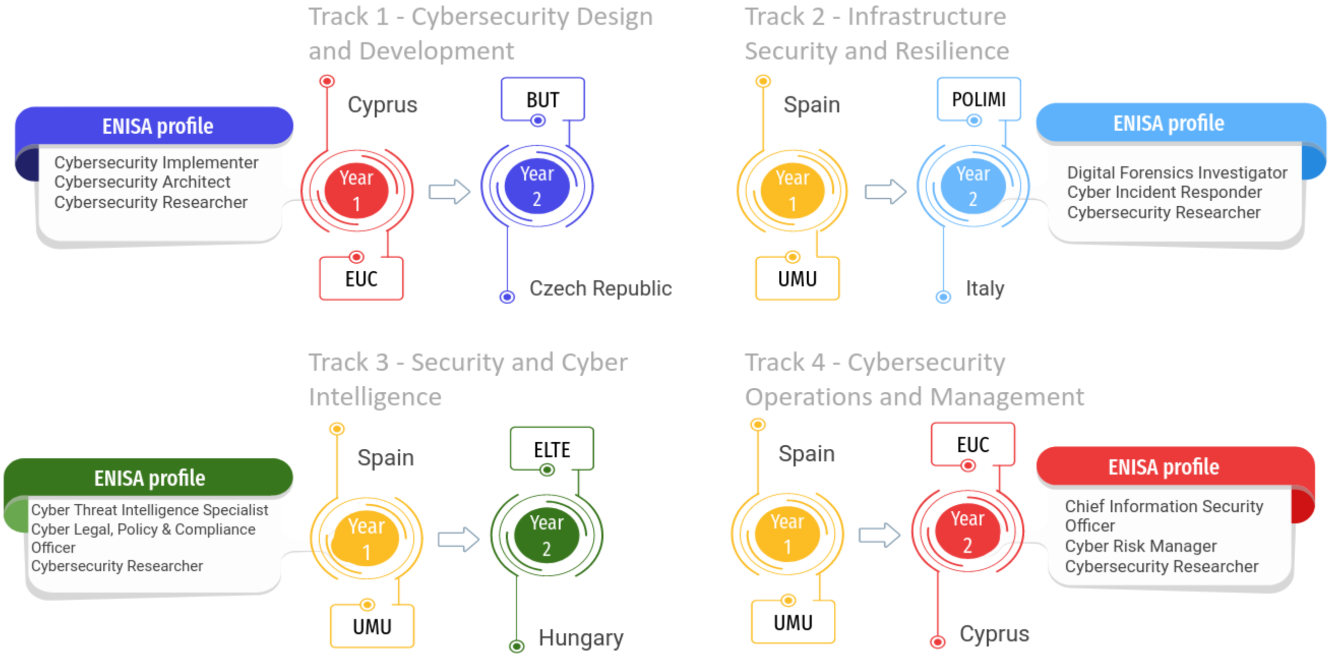
Track 1 - Cybersecurity Design and Development
Cyprus
BUT
Year 1
Year 2
EUC
Czech Republic
ENISA profile
Cybersecurity Implementer
Cybersecurity Architect
Cybersecurity Researcher
Track 2 - Infrastructure Security and Resilience
Spain
POLIMI
Year 1
Year 2
UMU
Italy
ENISA profile
Digital Forensics Investigator
Cyber Incident Responder
Cybersecurity Researcher
Track 3 - Security and Cyber Intelligence
Spain
ELTE
Year 1
Year 2
UMU
Hungary
ENISA profile
Cyber Threat Intelligence Specialist
Cyber Legal, Policy & Compliance Officer
Cybersecurity Researcher
Track 4 - Cybersecurity Operations and Management
Spain
EUC
Year 1
Year 2
UMU
Cyprus
ENISA profile
Chief Information Security Officer
Cyber Risk Manager
Cybersecurity Researcher

Figure 1: Structure of DJM-CYBER study program. Credits for the template to Slidesgo and Freepik.

In case of Track 1, at first we focus on courses covering those REWIRE skills that the Cybersecurity Architect and Cybersecurity Implementer profiles have in common, i.e., "Data Security", "Enterprise Architecture and Infrastructure Design", "Information Security Controls Assessment", "Operating Systems", and "Software Development". For instance, "Enterprise Architecture and Infrastructure Design" is covered in "Cybersecurity Architecture and Operations" (EUC) and "Mobile Network Communication Systems" (BUT) subjects. Then we tried to reach out the remaining skills. The main REWIRE skills, allowing the correlation between courses and ENISA profiles, of each subject are listed below in the tracks descriptions. We refer to Sections 4.1 and 4.2 for more details on the tools.

Accordingly, our DJM-CYBER master provides graduates with a wide range of career opportunities in various sectors, such as government, finance, healthcare, SMEs and technology industry. Graduates will be well-prepared for at least the following roles: Cybersecurity Implementer; Cybersecurity Architect; Cybersecurity Researcher; Digital Forensics Investigator; Cyber Incident Responder; Cyber Threat Intelligence Specialist; Cyber Legal, Policy & Compliance Officer; Chief Information Security Officer and Cybersecurity Risk Manager.

We recognize the importance of specialization in a master degree and, therefore, elective courses are provided whenever possible. However, a strong background is also vital to cover the profile skills and knowledge. Accordingly, elective courses can be added to the track after the basic knowledge is achieved. Following the need for integration each university provides elective language courses. Internships and summer schools are not mandatory in this program. Both summer schools and internships are beneficial for students, thus they will be incorporated in the future either by partners of the project or by associated partners. Summer schools will be available at the end of every academy year and internships during the second year of study.

Track 1. *Cybersecurity Design and Development.* This track is jointly provided by the European University Cyprus (EUC) and Brno University of Technology (BUT) universities. In the first year, students enrich their knowledge in cybersecurity governance, ethical hacking, and data protection. In the second year, cryptography, IoT, and networks are the main focus of this track. The courses are interconnected over the years. For instance, following “Data Privacy in the Era of Data Mining and AI“ course, the student will be introduced to data privacy from a legal and economic point of view whereas with “Modern Cryptography“ and “Parallel Data Processing“ courses they will study the same topic in cryptography- and machine learning-oriented way. Figure 2 shows the level of multidisciplinarity in Track 1. The SPARTA Curricula Designer was deployed in the analysis. At last, Track 1 passes the SPARTA practical lecture limit with a 64% score.

Semester 1 (EUC, 30 ECTS) consists of three compulsory courses:

- Introduction to Cybersecurity (Comp., 10 ECTS) Main skill(s) acquired: Data Security.
- Cybersecurity Policy, Governance, Law and Compliance (Comp., 10 ECTS). Main skill(s) acquired: Policy Development, and Law, Policy, and Ethics skills.
- Communications and Network Security (Comp., 10 ECTS) Main skill(s) acquired: Information Systems and Network Security and Threat Analysis.

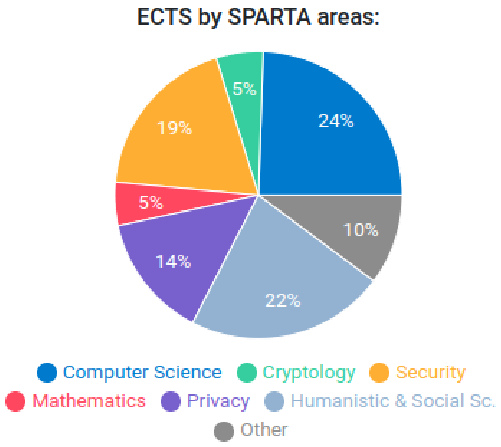

Figure 2: Curricula Designer analysis of Track 1.

Semester 2 (EUC, 30 ECTS) includes two compulsory courses (20 ECTS) and one elective course (10 ECTS) to choose among three possibilities:

- Cybersecurity Architecture and Operations (Comp., 10 ECTS). Main skill(s) acquired: Risk Management, Testing and Evaluation, Incident Management, Enterprise Architecture and Infrastructure Design, and Data Security.
- Ethical Hacking and Penetration Testing (Comp., 10 ECTS). Main skill(s) acquired: Testing and Evaluation, and Law, Policy, and Ethics.
- Data Privacy in the Era of Data Mining and AI (Elect., 10 ECTS) This course has as main key skills: Data Privacy, Data Security, and Data Analysis.
- Cybersecurity Risk Analysis and Management (Elect., 10 ECTS) Main skill(s) acquired: Risk Management, and Testing and Evaluation.
- Incident Response and Forensic Analysis (Elect., 10 ECTS) Main skill(s) acquired: Incident Management, and Digital Forensics.

Semester 3 (BUT, 30 ECTS) consists of five compulsory courses (25 ECTS) and one elective course (5 ECTS) to choose among three possibilities:

- Mobile Network Communication Systems (Comp., 6 ECTS). Main skill(s) acquired: Information Systems and Network Security, Enterprise Architecture and Infrastructure Design, and Network Management.
- Foundation of Cryptography (Comp., 6 ECTS). Main skill(s) acquired: Data Security, Information Systems and Network Security, and Collaborate and Communicate.
- Modern Cryptography (Comp., 6 ECTS). Main skill(s) acquired: Data Security, Data Privacy, Software Development, Problem solving and Critical Thinking.
- Parallel Data Processing (Comp., 6 ECTS). Main skill(s) acquired: Data Analysis, Software Development, and Information Systems and Network Security.
- Semestral Thesis (Comp., 1 ECTS). Main skill(s) acquired: Software Development, Problem solving and Critical Thinking, and Technology Fluency.
- Data Structures and Algorithms (Elect. 5 ECTS). Main skill(s) acquired: Data Analysis, and Software Development.
- Modern Network Technologies (Elect., 5 ECTS). Main skill(s) acquired: Information Systems and Network Security, and Network Management.
- Optical Networks (Elect., 5 ECTS). Main skill(s) acquired: Information Systems and Network Security, and Network Management.

Semester 4 (BUT, 30 ECTS): Diploma Thesis (Comp., 30 ECTS). Main skill(s) acquired: Software Development, Problem solving and Critical Thinking, and Technology Fluency.

Track 2. *Infrastructure Security and Resilience.* This track is jointly implemented by the University of Murcia (UMU) and Politecnico di Milano (POLIMI). In the first year, students enrich their knowledge in cybersecurity law and management, security, privacy, ethical hacking and malware technologies. In the second year, students get acquainted with data science, neural networks and deep learning, cybercrime and computer ethics. Figure 3 shows the multidisciplinarity assessment of Track 2 measured in the SPARTA Curricula Designer. Track 2 also passes the SPARTA limit of practical lecture achieving a 79% of them.

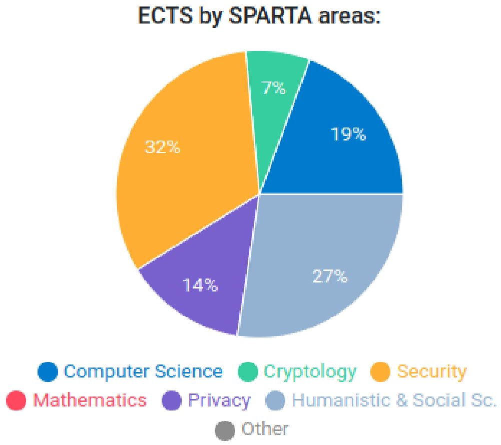

Figure 3: Curricula Designer analysis of Track 2.

Semester 1 consists of 6 mandatory courses (UMU, 30 ECTS):

- Ethical Hacking (Comp., 6 ECTS). Main skill(s) acquired: Threat Analysis, and Law, Policy, and Ethics.
- Techniques for the Management of the Cybersecurity (Comp., 6 ECTS). Main skill(s) acquired: Information Systems and Network Security, Business Continuity, Identity Management, and Risk Management.
- CyberDefense (Comp., 6 ECTS). Main skill(s) acquired: Information Systems and Network Security, Enterprise Architecture and Infrastructure Design, and Incident Management.

- Cybersecurity and Communications (Comp., 6 ECTS). Main skill(s) acquired: Information Systems and Network Security, Incident Management, and Network Management.
- Cryptography (Comp., 3 ECTS). Main skill(s) acquired: Data Security.
- Innovation and Entrepreneurship Seminar (Comp., 3 ECTS). Main skill(s) acquired: Problem solving and Critical Thinking, and Technology Fluency.

Semester 2 consists of five mandatory course and four elective courses to choose from (UMU, 30 ECTS) :

- CyberSecurity Lab (Comp., 6 ECTS). Main skill(s) acquired: Problem solving and Critical Thinking, and Incident Management.
- 5G and IoT and Cyber-physical systems security (Elect., 6 ECTS). Main skill(s) acquired: Network Management, and Physical Device Security.
- Software Security & Secure Software lifecycle (Comp., 3 ECTS). Main skill(s) acquired: Software Development, Incident Management, and Data Security.
- AAI Authentication and Authorization Infrastructures (Comp., 3 ECTS). Main skill(s) acquired: Identity Management, and Enterprise Architecture and Infrastructure Design.
- Advanced Techniques in Cyber Intelligence (Elect., 6 ECTS). Main skill(s) acquired: Intelligence Analysis.
- Cybersecurity and Law (Comp., 3 ECTS). Main skill(s) acquired: Data Privacy, Enterprise Architecture and Infrastructure Design.
- Distributed Systems Security (Elect., 3 ECTS). Main skill(s) acquired: Information Security Controls Assessment.
- Hardware Security (Elect., 3 ECTS). Main skill(s) acquired: Information Security Controls Assessment and Data Security.
- Malware & Attack Technologies (Comp., 3 ECTS). Main skill(s) acquired: Testing and Evaluation.

Semester 3 consists of 2 mandatory courses and 6 elective courses to choose from (POLIMI, 30 ECTS):

- Offensive and Defensive Cybersecurity (Comp., 5 ECTS). Main skill(s) acquired: Information Systems and Network Security.
- Data Science and Security for Mobility (Elect., 10 ECTS). Main skill(s) acquired: Information Systems and Network Security, and Physical Device Security.
- Resilience of Critical Infrastructures (Elect., 5 ECTS). Main skill(s) acquired: Enterprise Architecture and Infrastructure Design.
- Cryptography and Architectures for Computer Security (Elect., 5 ECTS). Main skill(s) acquired: Data Security, and Enterprise Architecture and Infrastructure Design.
- Digital Forensics and Cybercrime (Comp., 5 ECTS). Main skill(s) acquired: Digital Forensics.
- Safety in Automation Systems (Elect., 5 ECTS). Main skill(s) acquired: Threat Analysis.
- Computer Ethics (Elect., 5 ECTS). Main skill(s) acquired: Law, Policy, and Ethics.
- Artificial Neural Networks and Deep Learning (Elect., 5 ECTS). Main skill(s) acquired: Data Analysis.

Semester 4 (POLIMI, 30 ECTS): Thesis consultation (Comp., 30 ECTS). Main skill(s) acquired: Software Development, Problem solving and Critical Thinking, and Technology Fluency.

Track 3. *Security and Cyber Intelligence.* This track is jointly provided by the University of Murcia, Spain (UMU) and Eötvös Loránd University, Hungary (ELTE). In the first year, students enrich their knowledge in cybersecurity law and management, security, privacy, ethical hacking and malware technologies. In the second year, students focus on advanced cryptography, the security aspects of Machine Learning/Artificial Intelligence (ML/AI), open-source data analysis technologies and stream mining, thereby acquiring a breadth of knowledge in various relevant topics in cybersecurity and a more focused skillset in security data analytics necessary for at least the following ENISA ECSF roles: Cyber Threat Intelligence Specialist; Cyber Legal, Policy & Compliance Office; and Cybersecurity Architect. 4 shows the multidisciplinarity score of Track 3 measured with the SPARTA Curricula Designer. Track 3 also passes the SPARTA limit of practical lectures achieving a 77% score.

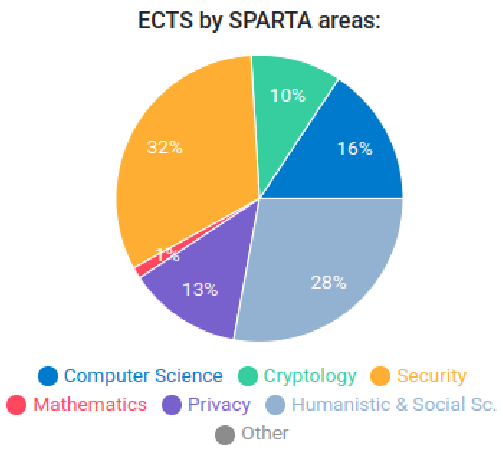

Figure 4: Curricula Designer analysis of Track 3.

Semester 1 consists of 6 mandatory courses (UMU, 30 ECTS):

- Ethical Hacking (Comp., 6 ECTS). Main skill(s) acquired: Threat Analysis, and Law, Policy, and Ethics.
- Techniques for the Management of the Cybersecurity (Comp., 6 ECTS). Main skill(s) acquired: Information Systems and Network Security, Business Continuity, Identity Management, and Risk Management.
- CyberDefense (Comp., 6 ECTS). Main skill(s) acquired: Information Systems and Network Security, Enterprise Architecture and Infrastructure Design, and Incident Management.
- Cybersecurity and Communications (Comp., 6 ECTS). Main skill(s) acquired: Information Systems and Network Security, Incident Management, and Network Management.
- Cryptography (Comp., 3 ECTS). Main skill(s) acquired: Data Security.
- Innovation and Entrepreneurship Seminar (Comp., 3 ECTS). Main skill(s) acquired: Problem solving and Critical Thinking, and Technology Fluency.

Semester 2 consists of five mandatory courses and four elective courses to choose from (UMU, 30 ECTS):

- CyberSecurity Lab (Comp., 6 ECTS). Main skill(s) acquired: Problem solving and Critical Thinking, and Incident Management.
- 5G and IoT and Cyber-physical systems security (Elect., 6 ECTS). Main skill(s) acquired: Network Management, and Physical Device Security.
- Software Security & Secure Software lifecycle (Comp., 3 ECTS). Main skill(s) acquired: Software Development, Incident Management, and Data Security.
- AAI Authentication and Authorization Infrastructures (Comp., 3 ECTS). Main skill(s) acquired: Identity Management, and Enterprise Architecture and Infrastructure Design.
- Advanced Techniques in Cyber Intelligence (Elect., 6 ECTS). Main skill(s) acquired: Intelligence Analysis.
- Cybersecurity and Law (Comp., 3 ECTS). Main skill(s) acquired: Data Privacy, Enterprise Architecture and Infrastructure Design.
- Advanced aspects of Cybersecurity Management (Elect., 3 ECTS). Main skill(s) acquired: Business continuity, Threat Analysis, and Intelligence Analysis.
- Human Factors and Privacy & Online Rights (Elect., 3 ECTS). Main skill(s) acquired: Law, Policy, and Ethics.
- Malware & Attack Technologies (Comp., 3 ECTS). Main skill(s) acquired: Testing and Evaluation.

Semester 3 consists of one compulsory course and 6 elective courses to choose from (ELTE, 30 ECTS):

- Cyber Security Lab II (Comp., 6 ECTS). Main skill(s) acquired: Threat Analysis, and Intelligence Analysis.
- Data Science Lab II (Opt., 6 ECTS).Main skill(s) acquired: Data Science and Analytics, Information and Knowledge Management, Documentation Production.
- Advanced cryptography (Elect., 6 ECTS). Main skill(s) acquired: Data Security.
- Data Security (Elect., 6 ECTS). Main skill(s) acquired: Data Security, Data Privacy, Data Science and Analytics, and Intelligence Analysis.
- Introduction to Data Science (Elect., 6 ECTS). Main skill(s) acquired: Data Science and Analytics
- Open-source technologies for real-time data analytics (Elect., 6 ECTS). Main skill(s) acquired: Enterprise Architecture and Infrastructure Design, Technology Fluency, Technology Trend Monitoring.
- Stream mining (Elect., 6 ECTS). Main skill(s) acquired: Threat Analysis, and Intelligence Analysis.

Semester 4 (ELTE, 30 ECTS): Thesis Consultation (Comp., 30 ECTS). Main skill(s) acquired: Software Development, Problem solving and Critical Thinking, and Technology Fluency.

Track 4. *Cybersecurity Operations and Management.* This track is jointly implemented by the University of Murcia, Spain (UMU) and the European University Cyprus (EUC). In the first year, students enrich their knowledge in cybersecurity law and management, security, privacy, ethical hacking and malware technologies. In the second year, students deepen their knowledge in various aspects of cybersecurity (management, policy, law, or architecture). 5 shows the multidisciplinarity assessment of Track 4 measured in the SPARTA Curricula Designer. Track 4 also passes the SPARTA limit of practical lecture achieving a 55% score.

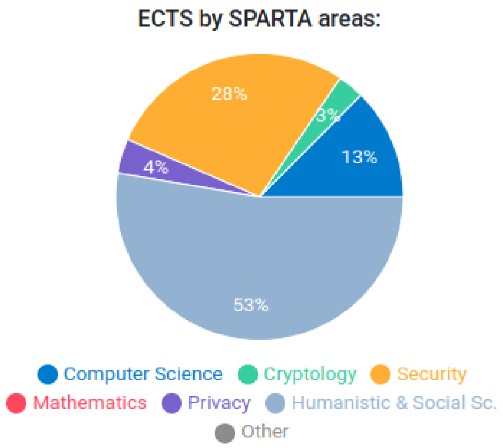

Figure 5: Curricula Designer analysis of Track 4.

Semester 1 consists of 6 mandatory courses (UMU, 30 ECTS):

- Ethical Hacking (Comp., 6 ECTS). Main skill(s) acquired: Threat Analysis, and Law, Policy, and Ethics.
- Techniques for the Management of the Cybersecurity (Comp., 6 ECTS). Main skill(s) acquired: Information Systems and Network Security, Business Continuity, Identity Management, and Risk Management.
- CyberDefense (Comp., 6 ECTS). Main skill(s) acquired: Information Systems and Network Security, Enterprise Architecture and Infrastructure Design, and Incident Management.
- Cybersecurity and Communications (Comp., 6 ECTS). Main skill(s) acquired: Information Systems and Network Security, Incident Management, and Network Management.
- Cryptography (Comp., 3 ECTS). Main skill(s) acquired: Data Security.
- Innovation and Entrepreneurship Seminar (Comp., 3 ECTS). Main skill(s) acquired: Problem solving and Critical Thinking, and Technology Fluency.

Semester 2 consists of one mandatory course and 10 elective courses to choose from (UMU, 30 ECTS):

- CyberSecurity Lab (Comp., 6 ECTS). Main skill(s) acquired: Problem solving and Critical Thinking, and Incident Management.
- 5G and IoT and Cyber-physical systems security (Elect., 6 ECTS). Main skill(s) acquired: Network Management, and Physical Device Security.
- Software Security & Secure Software lifecycle (Comp., 3 ECTS). Main skill(s) acquired: Software Development, Incident Management, and Data Security.
- AAI Authentication and Authorization Infrastructures (Comp., 3 ECTS). Main skill(s) acquired: Identity Management, and Enterprise Architecture and Infrastructure Design.

- Advanced Techniques in Cyber Intelligence (Elect., 6 ECTS). Main skill(s) acquired: Intelligence Analysis.
- Cybersecurity and Law (Comp., 3 ECTS). Main skill(s) acquired: Data Privacy, Enterprise Architecture and Infrastructure Design.
- Advanced aspects of Cybersecurity Management (Elect., 3 ECTS). Main skill(s) acquired: Business continuity, Threat Analysis, and Intelligence Analysis
- Distributed Systems Security (Elect., 3 ECTS). Main skill(s) acquired: Information Security Controls Assessment.
- Hardware Security (Elect., 3 ECTS). Main skill(s) acquired: Information Security Controls Assessment and Data Security.
- Human Factors and Privacy & Online Rights (Elect., 3 ECTS). Main skill(s) acquired: Law, Policy, and Ethics.
- Malware & Attack Technologies (Elect., 3 ECTS). Main skill(s) acquired: Testing and Evaluation.

Semester 3 consists of three mandatory courses (EUC, 30 ECTS):

- Cybersecurity Architecture & Operations (Comp., 10 ECTS). Main skill(s) acquired: Risk Management, Testing and Evaluation, Incident Management, Enterprise Architecture and Infrastructure Design, and Data Security.
- Cybersecurity Policy, Governance, Law and Compliance (Comp., 10 ECTS). Main skill(s) acquired: Policy Development, and Law, Policy, and Ethics skills.
- Cybersecurity Risk Analysis and Management (Comp., 10 ECTS). Main skill(s) acquired: Risk Management, and Testing and Evaluation.

Semester 4 (EUC, 30 ECTS): Thesis (Comp., 30 ECTS). Main skill(s) acquired: Software Development, Problem solving and Critical Thinking, and Technology Fluency.

6 CONCLUSIONS

It is a well-known fact that the worldwide workforce gap in cybersecurity is measured in millions of missing experts. Tackling this challenge is not an easy task. One significant aspect of the mixture of approaches are highly tailored, novel study programmes offered either by single universities or joint programmes provided by higher education consortia consisting of multiple universities and/or colleges. Ensuring that any new study programme will meet the requirements of the job market is itself a daunting task, which is fortunately made easier via publicly available skills frameworks like the ENISA's European Cybersecurity Framework (ECSF) or the National Institute of Science and Technology's (NIST) NICE Competencies Framework.

The goal of this paper was to describe a methodology allowing single universities or higher education consortia to select the best freely available tools which might aid them in the design and continuous development of novel cybersecurity study programmes. We described the most relevant EU-level projects and the valuable tools developed by them. We also touched the most relevant skills frameworks, namely by describing the above-mentioned ECSF and NICE CF. Finally, we utilized the presented set of tools and frameworks to design and assess a joint master-level study programme developed by a consortium of five European universities and structured into four markedly different study tracks. We measured the coverage of the most relevant skills and scored the tracks' practicality.

Our proposal provides a clear and recognized ecosystem consisting of tools and framework for the development of cybersecurity competencies and skills, ensuring that graduates are well-equipped to meet the demands of the cybersecurity workforce in Europe and beyond. It also provide a common language and reference point for employers, educators, and students, facilitating communication, standardization, and consistency in cybersecurity education and training across Europe.

ACKNOWLEDGMENTS

The following funding sources are gratefully acknowledged: the ERASMUS+ Erasmus Mundus Design Measures (EMDM) programme of the European Union (grant 1701-EPP-1-2020-1-LT-EPPKA2-SSA-B 'DJM-CYBER'), the ERASMUS+ Sector Skills Alliance (SSA) programme of the European Union (grant 621701-EPP-1-2020-1-LT-EPPKA2-SSA-B 'REWIRE'), and Project no. TKP2021-NVA-29 which has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund, financed under the TKP2021-NVA funding scheme.

REFERENCES

[1] Borka Jerman Blažič. 2021. The cybersecurity labour shortage in Europe: Moving to a new concept for education and training. *Technology in Society* 67 (2021), 101769. https://doi.org/10.1016/j.techsoc.2021.101769

[2] Sergey Bratus, Iván Arce, Michael E. Locasto, and Stefano Zanero. 2014. Why Offensive Security Needs Engineering Textbooks: Or, How to Avoid a Replay of "Crypto Wars" in Security Research. *login Usenix Mag.* 39, 4 (2014). https://www.usenix.org/publications/login/august14/bratus

[3] CONCORDIA. 2022. Teach-the-Teachers in high-school. Methodology and Guidelines. (2022). https://www.concordia-h2020.eu/wp-content/uploads/2022/11/Teach-the-TeachersMethodology-for-publication.pdf

[4] CyberSec4Europe. 2023. Final Educational and Assessment Framework (CyberSec4Europe). https://cybersec4europe.eu/wp-content/uploads/2022/07/D6.6-Final-Educational-and-Assessment-Framework_submitted.pdf

[5] Petr Dzurenda and Sara Ricci. 2022. R3.4.1 Mapping the framework to existing courses and schemes. https://rewireproject.eu/wp-content/uploads/2023/03/REWIRE_R3.4.1_Deliverable-v8-Final-EC-Check.pdf

[6] ENISA. 2022. European Cybersecurity Skills Framework Role Profiles. https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

[7] CSEC2017 Joint Task Force. 2017. Cybersecurity Curricula 2017 — Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Retrieved from Association for Computing Machinery: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf.

[8] Jan Hajny. 2020. D9.2 Curricula descriptions. https://www.sparta.eu/assets/deliverables/SPARTA-D9.2-Curricula-descriptions-PU-M18.pdf

[9] Jan Hajny, Sara Ricci, Edmundas Piesarskas, and Marek Sikora. 2021. Cybersecurity Curricula Designer. In *Proceedings of the 16th International Conference on Availability, Reliability and Security* (Vienna, Austria) *(ARES 21)*. Association for Computing Machinery, New York, NY, USA, Article 144, 7 pages. https://doi.org/10.1145/3465481.3469183

[10] Jan Hajny, Marek Sikora, Athanasios Vasileios Grammatopoulos, and Fabio Di Franco. 2022. Adding European Cybersecurity Skills Framework into Curricula Designer. In *Proceedings of the 17th International Conference on Availability, Reliability and Security* (Vienna, Austria) *(ARES '22)*. Association for Computing Machinery, New York, NY, USA, Article 82, 6 pages. https://doi.org/10.1145/3538969.3543799

[11] Igor Nai Fovino, Ricardo Neisse, Juan Hernandez Ramos, Nicoleta Polemi, Gian-Luca Ruzzante, Markus Figwer, and Alessandro Lazari. 2019. A Proposal for a European Cybersecurity Taxonomy. Retrieved from EUROPA - European Union website, the official EU website: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf.

[12] Rodney Petersen, Danielle Santos, Matthew C. Smith, Karen A. Wetzel, and Greg Witte. 2020. NIST Special Publication 800-181 Revision 1: Workforce Framework for Cybersecurity (NICE Framework). available online at https://nvlpubs.nist.gov/

nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf. https://doi.org/10.6028/NIST.SP.800-181r1

[13] Awais Rashid, Howard Chivers, George Danezis, Emil C. Lupu, and Andrew Martin. 2019. CyBOK — The Cyber Security Body of Knowledge — Version 1.0. Retrieved from CyBOK: https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf.

[14] REWIRE. 2020. Cybersecurity Skills Alliance – A New Vision for Europe (REWIRE). https://rewireproject.eu/

[15] Sara Ricci, Marek Sikora, Simon Parker, Imre Lendak, Yianna Danidou, Argyro Chatzopoulou, Remi Badonnel, and Donatas Alksnys. 2022. Job Adverts Analyzer for Cybersecurity Skills Needs Evaluation. In *Proceedings of the 17th International Conference on Availability, Reliability and Security* (Vienna, Austria) *(ARES '22)*. Association for Computing Machinery, New York, NY, USA, Article 84, 10 pages. https://doi.org/10.1145/3538969.3543821

[16] WG5 PAPER - European Cybersecurity Education and Professional Training Minimum Reference Curriculum - SWG 5.2. 2021. European Cybersecurity Education and Professional Training Minimum Reference Curriculum - SWG 5.2. Retrieved from European Cyber Security Organisation (ECSO): https://www.ecs-org.eu/documents/publications/61967913d3f81.pdf.

Received 2 May 2023; accepted 14 June 2023