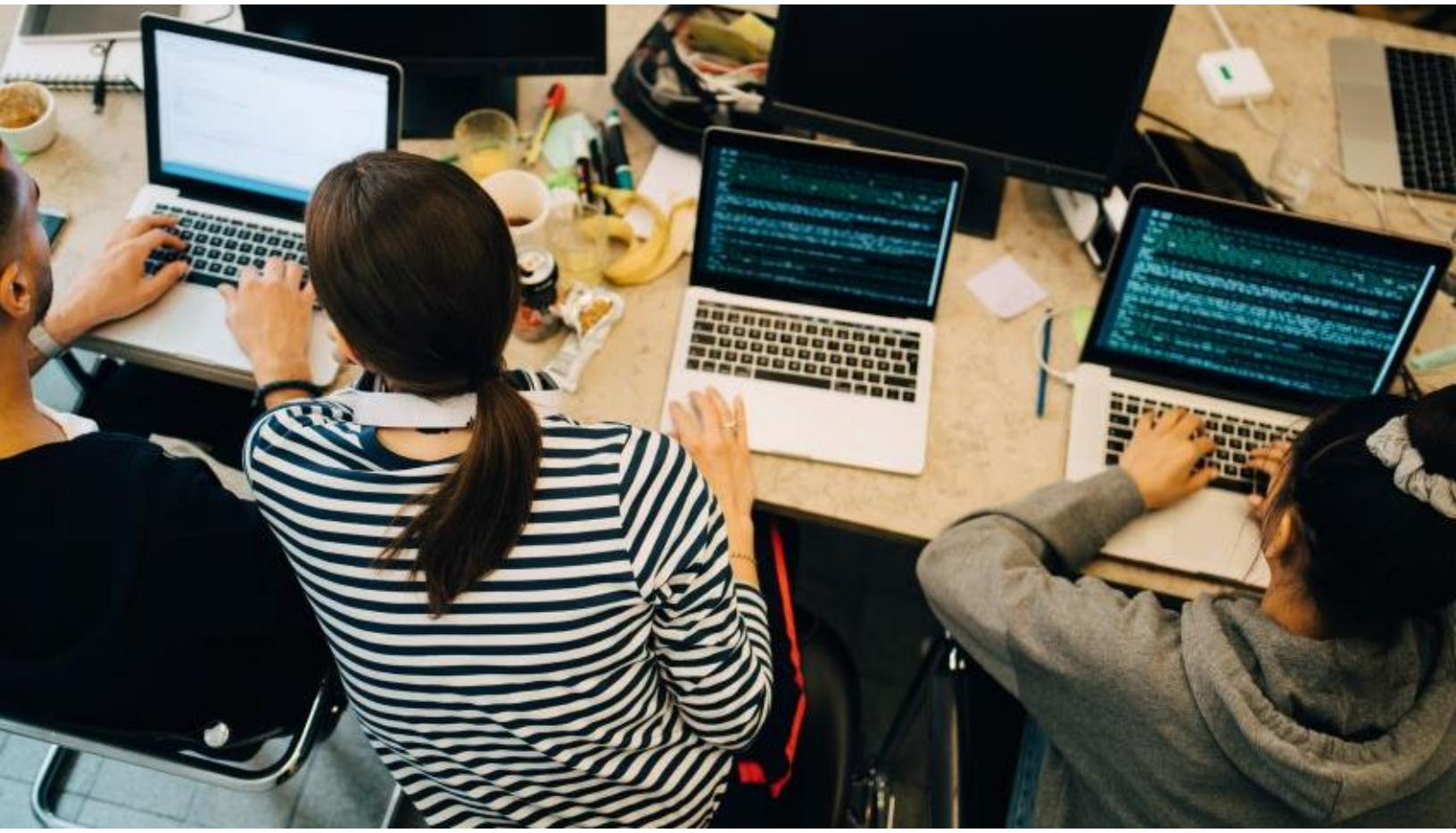
USAID FROM THE AMERICAN PEOPLE

UK International Development
Partnership | Progress | Prosperity

DAI
Shaping a more livable world.



CURRICULUM ASSESSMENT

Tertiary Cybersecurity Education in North Macedonia

This publication was produced by the Critical Infrastructure Digitalization and Resilience Program under Contract No. 7200AA21CA00015 at the request of the United States Agency for International Development (USAID). This document is made possible by the support of the American people through USAID. Its contents are the sole responsibility of the author or authors and do not necessarily reflect the views of USAID or the U.S. Government.

CURRICULUM ASSESSMENT

Tertiary Cybersecurity Education in North Macedonia

Program Title:	Critical Infrastructure Digitalization and Resilience Program
Sponsoring USAID Office:	USAID Bureau for Europe and Eurasia
Contract Number:	Cooperative Agreement No. 7200AA21CA00015
Contractor:	DAI Global, LLC
Date of Submission:	May 9, 2024
Author:	DAI Global, LLC and Florida International University

TABLE OF CONTENTS

PROGRAM BACKGROUND

The Critical Infrastructure Digitalization and Resilience (CIDR) program is a five-year initiative managed by DAI Global LLC on behalf of the U.S. Agency for International Development (USAID)'s Bureau for Europe and Eurasia. The CIDR program in North Macedonia (CIDR/North Macedonia) is tasked with enhancing the nation's cybersecurity capabilities and identifying the primary cybersecurity vulnerabilities within the country's critical infrastructure. To do this, CIDR/North Macedonia facilitates stakeholder collaboration, cyber policy formulation, cybersecurity workforce development, and information sharing.

In terms of cybersecurity workforce development in North Macedonia, CIDR has established a collaboration with several information and communication technologies (ICT) faculties in North Macedonia to identify the challenges and needs of tertiary ICT institutions. The tertiary ICT institutions were then surveyed and asked to describe their institutional approach to cybersecurity education and identify institutional cybersecurity needs and challenges. As a result of the survey, CIDR, in partnership with Florida International University (FIU), facilitated three (3) "training-of-trainers" (ToT) courses between September 2023 and March 2024. The topics of the courses were: IoT Security and Privacy, Cyber-Physical Systems Security of Critical Infrastructure, and Digital Forensics.

Each ToT course lasted six weeks and was concluded with an in-person workshop facilitated in Skopje, North Macedonia. The goal of the ToT courses was to introduce university professors to contemporary cybersecurity topics and practices. Moreover, ToT courses provided university professors with the learning material and resources, and the ability to gain hands-on experience and engage in practical learning. In total, courses facilitated by the CIDR program and FIU were attended by 49 university professors from 12 faculties in North Macedonia. After the completion of the ToT course, university professors are expected to have the knowledge, skills, and practical tools needed to implement and enrich their existing programs with cybersecurity-related topics. The fourth and last series of courses—Network Forensics—is scheduled for May 2024.

Besides establishing collaboration with ICT faculties in North Macedonia and facilitating cybersecurity courses, CIDR also published a report "Cyber Workforce—State of Play and Future Needs of Public Institutions in North Macedonia" in December 2023. This report summarized the results of the cybersecurity workforce survey sent out to 1,374 public institutions in North Macedonia. The sample included public institutions such as primary and secondary educational institutions and other public institutions that provide government services. This report found that: 1) the cybersecurity workforce in North Macedonia is increasing, and 2) the cybersecurity workforce in public institutions is diversifying; with future workforce leaning toward more technical and managerial cybersecurity roles. The results of this survey are reflective of regional trends and increasing demand for IT professionals.

CIDR is also tasked with assessing whether tertiary institutions in North Macedonia can satisfy market needs for qualified and knowledgeable cybersecurity professionals. In general, the demand for IT professionals is increasing in North Macedonia, and according to the State Statistical Office of North Macedonia, the number of employed ICT professionals increased almost twofold between 2018 and 2022. In 2022, more than 21,000 ICT professionals were active in the labor force in North Macedonia. This demand has direct implications for the demand for cybersecurity professionals; the demand for cybersecurity professionals will continue to increase toward a more diversified workforce as North

Macedonia follows the pathway toward European integration and becomes home to global ICT companies.

EUROPEAN CYBERSECURITY WORKFORCE

The European Union Agency for Cybersecurity (ENISA) is the European Union's agency dedicated to strengthening the cybersecurity efforts and capabilities of their Member States. Since ENISA was established in 2004, this agency has contributed to the European cyber policy, information sharing, the trustworthiness of ICT products, and the development of the European cybersecurity workforce. ENISA provides guidelines for national cybersecurity strategies, and it facilitates cooperation with Member States to promote knowledge sharing, capacity building, and awareness raising. Through its community engagement and cross-national collaboration, ENISA empowers communities, increases operational cooperation, and boosts the resilience of the Union's infrastructure to keep European citizens digitally secure. ENISA emphasizes the continuous process of collecting, analyzing, and sharing information and knowledge and it requires all Member States to share information within the EU cybersecurity ecosystem.

The European Union recognizes that the sophistication of cyberattacks, and increased use of internet technologies has created a greater need for cybersecurity professionals in Europe. Therefore, ENISA is an active participant in the development of the European cybersecurity workforce. ENISA supports the development of Member States' cybersecurity workforce by investing and building competencies and talents in cybersecurity at all levels, from the non-expert to the highly skilled professional. ENISA efforts are not only focused on Member States but also on making sure that other European countries possess the appropriate operational capacity to deal with the European cyber threat landscape. This has direct implications for countries like North Macedonia that are seeking full membership of the Union. For North Macedonia, the step toward European integration assumes that the country's cyber preparedness and cyber policy are aligned with the ENISA framework and strategies.

To further support the development of the European cybersecurity workforce, ENISA introduced the European Cybersecurity Skills Framework (ECSF) in 2022. This framework is a practical tool aimed at supporting Member States as they identify and articulate tasks, competencies, skills, and knowledge associated with the cybersecurity workforce. The ECSF framework ensures a common terminology and shared understanding between the demand (workplace, recruitment) and supply (qualification, training) of cybersecurity professionals across the EU. It provides a common understanding of the relevant cybersecurity roles, and it facilitates talent-sharing across Member States. The ECSF summarizes the cybersecurity-related roles into 12 profiles, which are individually analyzed into the details of their corresponding responsibilities, skills, and tasks. Cybersecurity roles identified by ENISA are: 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.

In the United States, cybersecurity workforce development is supported by the National Initiative for Cybersecurity Education (NICE) Framework. The cybersecurity roles outlined by the NICE Framework overlap with some of ENISA's cybersecurity roles, but the NICE Framework is considered more

comprehensive since it outlines specific knowledge, skills, and abilities for 52 cybersecurity work roles. These work roles are categorized into seven cybersecurity functions and specialty areas that range from analyzing cybersecurity information to governing organization cybersecurity policies. Another advantage of the NICE Framework is that it provides the number of job openings for each position and estimates future cybersecurity workforce needs. As one of the initial program's activities, CIDR, in partnership with FIU, facilitated a "NICE Framework Workshop in March 2023 in Skopje. The workshop was led by the Manager of the NICE Framework, Karen Wetzel, who visited North Macedonia to initiate the conversation with local stakeholders on the application of the NICE Framework to the developing cybersecurity workforce in North Macedonia.

RESEARCH METHODOLOGY

Florida International University (FIU) visited North Macedonia on several occasions between March of 2023 and March of 2024 at the request of CIDR/North Macedonia. During their visits, the FIU and CIDR/North Macedonia teams met with local stakeholders, relevant ministries, and tertiary institutions that offer ICT-related degrees. During the meetings with tertiary institutions, FIU discussed the status of cybersecurity education at their institutions and their efforts to provide cybersecurity courses. Between March of 2023 and March of 2024, Florida International University (FIU) traveled to North Macedonia on five different occasions to meet with local stakeholders, relevant ministries, and tertiary institutions that offer ICT-related degrees. During the meetings with tertiary institutions, FIU and CIDR/MKD discussed the status of cybersecurity education at their institutions and their efforts to provide cybersecurity courses. The meetings were also used to identify market gaps and institutional challenges. FIU and CIDR also met with universities that offer undergraduate and graduate degrees to discuss the state of cybersecurity education and students' pathways toward employment in the cybersecurity workforce. During the meetings, universities and their professors provided insight into their curriculums, teaching methods, and institutional needs.

In-person and online interviews with respective faculties were conducted to complement the desk analysis conducted by the Florida International University team. In a few cases, CIDR/North Macedonia and FIU asked faculties' deans to provide up-to-date curriculum information and confirm the information provided online. The graduation and enrollment numbers are obtained from the State Statistical Office of North Macedonia.

CURRICULUM ASSESSMENT

A curriculum review is a process of gathering and analyzing information to improve the learning experience and learning outcomes. A curriculum review analyzes the program's purpose, learning objectives, relevance of the material used, and the structure of the course. A curriculum review also examines the strengths and weaknesses of the curriculum, as well as the skills and knowledge students acquire as they pursue their degrees and specific job positions. Assessing the curriculum is the first step in ensuring that the educational program is aligned with university goals, government standards, and workforce needs.

The tertiary institutions in North Macedonia are the primary source of graduates who possess the skills and knowledge to enter the labor force. Therefore, the overreaching goal of this curriculum assessment is to provide a summary of current cybersecurity education at tertiary institutions in North Macedonia. The secondary goal of this curriculum assessment is to map out institutional challenges and needs of tertiary cybersecurity education in North Macedonia and assess whether tertiary institutions provide graduates with sufficient cybersecurity knowledge and skills. In this analysis, the authors reflect on ENISA's framework since this is the most fitting cybersecurity workforce framework for North Macedonia's path toward European integration.

In this review, we focus on two (2) undergraduate and four (4) graduate cybersecurity degrees and we assess their approach to cybersecurity education. In the case of North Macedonia, all existing cybersecurity degrees are accredited in public institutions; therefore, public universities are seen as leaders in cybersecurity education at the tertiary level. Private universities have made positive strides in recent years by including cybersecurity courses in their curriculums, but students who attend private universities are not likely candidates to enter the cybersecurity workforce.

This Curriculum Assessment is completed by the Jack D. Gordon Institute for Public Policy at Florida International University on behalf of the DAI Critical Infrastructure Digitalization and Resilience program in North Macedonia. Information and data used in this Assessment are publicly available data.

MAIN FINDINGS

- Out of twenty-one (21) ICT-related faculties in North Macedonia, two (2) faculties offer undergraduate cybersecurity-related degrees. Four (4) faculties, including a Military Academy, currently offer graduate cybersecurity-related degrees.
- Students in North Macedonia who pursue an undergraduate cybersecurity degree are only required to take a few introductory cybersecurity courses during their studies; more advanced courses are offered only as electives.
    - The curriculum for these degrees is not aligned with the cybersecurity roles outlined by the European Cybersecurity Skills Framework.
- Students in North Macedonia who pursue a master's degree in cybersecurity are required to take at least four (4) cybersecurity courses. These students can also take many advanced cybersecurity electives and gain a more comprehensive understanding of cybersecurity practices despite the shorter length of studies.
    - Graduate cybersecurity degrees prepare students for technical and managerial cybersecurity roles: Chief Information Security Officer (CISO), Cyber Threat Intelligence Specialist, and Digital Forensics Investigator.
- Two (2) faculties that offer an undergraduate cybersecurity degree require their students to take thematically similar introductory cybersecurity courses.
- Students who pursue a graduate degree are exposed to different materials and curricula.
    - Graduate-level cybersecurity coursework is thematically different; each faculty specializes in a different field of study.
- Cybersecurity education in North Macedonia at the tertiary level has made positive strides in recent years but it is still under development.
    - There aren't enough undergraduate cybersecurity degree programs.
    - Since cybersecurity degrees are exclusively offered by public universities, graduates from these institutions are likely to enter the cybersecurity workforce as knowledgeable and skilled professionals.

ICT WORKFORCE IN NORTH MACEDONIA

According to the State Statistical Office of North Macedonia, approximately 21,192 people were employed in the information and communication sector in 2022. [1]In terms of growth, the number of ICT employees increased by 63.1% between 2018 and 2022. [2] This growth uniquely characterizes the IT sector in North Macedonia, and this growth has a direct impact on the demand for cybersecurity professionals and the cybersecurity workforce. Currently, the Government in North Macedonia does not standardize or recognize cybersecurity professions and no assumptions can be drawn regarding the true size of the cybersecurity workforce in North Macedonia.

It can be assumed that the cybersecurity workforce proportionally increases as the ICT labor force increases. The recent CIDR report "Cyber Workforce — State of Play and Future Needs of Public Institutions in North Macedonia" highlighted that the cybersecurity workforce in North Macedonia is growing toward a more diverse and technically well-versed workforce. This survey also demonstrated that only larger governmental institutions employ cybersecurity professionals who have more advanced and technical roles. In light of that report, this curriculum review assesses whether the tertiary educational institutions in North Macedonia can provide a sufficient number of university graduates who are entering the cybersecurity workforce with the skills and knowledge needed for roles such as Network Specialist, Information System Manager, and Chief Information Officers.

Tertiary educational institutions are the primary source of ICT-skilled graduates but, like other nations around the world, North Macedonia produces an insufficient number of ICT graduates. North Macedonia, additionally, is suffering from a significant "brain drain," low living standard, and a competitive labor market. According to the State Statistical Office of the Republic of Macedonia, between 2018 and 2022, a total of 4,144 students in North Macedonia graduated with an undergraduate ICT-related degree. A master's degree in an ICT-related field was obtained by less than 200 students between 2018 and 2022. When it comes to cybersecurity graduates, according to the State Statistical Office of North Macedonia, approximately 100 students received an undergraduate cybersecurity degree between 2018 and 2022. The number of students who received a graduate cybersecurity degree is even lower, even though faculties tend to provide more versatile and shorter master's studies. This shortage of qualified cyber workforce candidates is noticeable for all cybersecurity roles and positions throughout North Macedonia; with public institutions suffering from the most pronounced labor shortage.

[1] https://www.stat.gov.mk/pdf/2023/2.1.23.05_mk.pdf

[2] https://www.stat.gov.mk/pdf/2019/2.1.19.06.pdf

ICT EDUCATION IN NORTH MACEDONIA

Before assessing the undergraduate and graduate cybersecurity degrees in North Macedonia, a brief overview of all ICT faculties is provided. CIDR, in partnership with FIU, has collaborated with representatives from most of these institutions and their role within the cybersecurity educational ecosystem cannot be disregarded. These universities have contributed to the various activities facilitated by CIDR and they have been active participants in ongoing efforts to enhance cybersecurity education in North Macedonia. These ICT faculties currently do not offer cybersecurity degrees, but they are integral pillars for the development of cybersecurity education as cybersecurity education in North Macedonia evolves regionally and other ICT faculties start including cybersecurity courses within their curriculums.

Several faculties that do not provide cybersecurity degrees have made individual efforts to provide short-term cybersecurity courses and training. For example, the Faculty of Economics (Ss. Cyril and Methodius) facilitated a summer cybersecurity boot camp in the summer of 2023. Additionally, AUE-FON American University, a private university that does not offer undergraduate or graduate cybersecurity degrees, has been offering summer cybersecurity boot camps for its students and outside community members in recent years. Professors from both faculties have attended cybersecurity training facilitated by CIDR and FIU. These seemingly minor efforts are a demonstration of the individual and collective effort of all tertiary institutions in North Macedonia that actively seek opportunities to introduce cybersecurity courses at their institutions.

Mapping the ICT faculties in North Macedonia and establishing collaboration with the ICT faculties laid the foundation for identifying faculties that provide undergraduate and graduate cybersecurity-related degrees. Currently, cybersecurity degrees are offered by four (4) public universities: the University of Cyril and Methodius, the Military Academy, the University of Goce Delcev, and St. Paul the Apostle University of Information Science and Technology. Two (2) universities—the University of Cyril and Methodius and St. Paul the Apostle University of Information Science and Technology—offer undergraduate cybersecurity degrees. These faculties also offer graduate cybersecurity degrees. The Military Academy and the University of Goce Delcev are associated faculties and they only offer graduate cybersecurity degrees. The Military Academy offers a specialistic cybersecurity degree that introduces its cadets to cyber warfare, international cyber law, and cyber defense.

PRIVATE ICT UNIVERSITIES IN NORTH MACEDONIA

UNDERGRADUATE ICT DEGREES AT PRIVATE UNIVERSITIES

In North Macedonia, there are a total of eight (8) private ICT universities. Those students who seek to attend a private university can pick from a total of six (6) 3-year programs and ten (10) 4-year programs. Private universities offer a variety of ICT-related degrees, such as computer science, software engineering, and computer engineering. Our analysis revealed that none of the private ICT universities offer a cybersecurity degree at either the undergraduate or graduate level. The list of all private ICT faculties and their degrees is listed in Appendix A.

While none of the private ICT universities offer a cybersecurity degree, some private ICT universities have included cybersecurity courses in the curricula. There are notable differences between ICT faculties and areas of study. For example, two (2) faculties out of eight (8) private faculties do not require their ICT students to take cybersecurity courses, nor do they offer cybersecurity electives. The remaining faculties either require their students to take a cybersecurity course or they offer cybersecurity courses as an elective. There are notable differences across faculties and areas of study.

When it comes to three-year studies, some private universities either require their undergraduate students to take a cybersecurity course or offer it as an elective. For example, two (2) out of six (6) faculties that offer three-year programs require their students to take cybersecurity courses during their studies. These courses are considered introductory courses that cover cybersecurity concepts and practices. The other four (4) faculties do not require their students to take a cybersecurity course, but they offer introductory cybersecurity courses as electives. These elective courses are introductory-level courses; the only three-year program that offers the more advanced elective Introduction to Software Security is American College University.

When it comes to four-year studies, private universities tend to require their students who pursue a four-year degree to take cybersecurity courses. Out of ten (10) four-year programs, seven (7) require their students to take a cybersecurity course. Most of these courses are foundational and introductory courses that are thematically close to the security of the computer and information systems and the objective of these courses is to introduce students to general cybersecurity security principles and practices. More advanced introductory courses, such as the Fundamentals of Software Security and Cryptography are only offered during the third year or fourth year as electives by two private faculties (American College University and Southeastern European University).

Most of the faculties require students to take cybersecurity courses later during their studies, either during a third year or a fourth year. Only two faculties—the Faculty of Computer Science and Information (American College) and the Faculty of Computer Science (International Slavic University)—require their students to take an introductory cybersecurity course during the second year. Introducing cybersecurity courses later in the studies has implications for students pursuing a three-year degree; these students, due to their shorter studies and graduation requirements have fewer opportunities to take cybersecurity electives. A similar pattern is seen within public universities, which often offer both three-year and four-year tracks.

GRADUATE ICT DEGREES AT PRIVATE UNIVERSITIES

In North Macedonia, there are a total of six (6) private ICT universities that offer graduate ICT degrees. Students who are attending a private university can pick from a total of nine (9) one-year programs and six (6) two-year programs. These degrees are mostly focused on data science, computer science, and software engineering. The European University and International Vizion University, under their Faculty of Computer Science, only offer undergraduate degrees and they are omitted from this analysis. Our analysis revealed that none of the private six (6) ICT universities offer a cybersecurity graduate degree. The list of all private ICT faculties and their degrees is listed in Appendix A.

As seen in Appendix A, private ICT universities predominately accredit longer, four-year undergraduate programs. Those who attend four-year ICT studies obtain an engineering degree, a prerequisite for many ICT entry-level positions. Higher attainment is also associated with higher specialization and better employment opportunities. In terms of cybersecurity education, those who pursue a four-year ICT degree are more likely to take mandatory cybersecurity courses or electives.

At the graduate level, on the other hand, private ICT universities predominately offer shorter studies and one-year programs. Shorter studies are seen as a pathway toward greater student retention and higher graduation rates since many ICT students halt their studies to enter the labor market. For those reasons, most of the private ICT faculties in North Macedonia have accredited one-year programs, which are more effective for those students who are already in the labor market. One-year programs, however, lack the structure and flexibility to allow students to explore cybersecurity electives.

None of the private faculties that offer one-year ICT-related graduate studies require their students to take cybersecurity courses. This is not surprising considering that curriculums of one-year studies tend to be more rigid and focused on the area of the study. This is true across all faculties and degrees since students who pursue a one-year master's ICT degree are only allowed a certain number of credits before moving on to their graduate thesis work. For those reasons, many faculties either limit the number of available electives or do not allow their students to take electives. For those one-year studies that offer cybersecurity electives, electives are often offered during the first semester since the second semester is usually reserved for research and graduate thesis. During the second semester, the students are expected to finalize their coursework without further exploration of electives.

Our analysis revealed that three (3) out of seven (6) private faculties that offer one-year master's degrees offer cybersecurity-related courses as an elective. For example, both the American College University and the University of Skopje offer Cryptography as an elective to students who are pursuing a one-year Software Engineering degree. There are differences between curricula because the structure and teaching capacity of the program dictate the number of available elective credits. These also dictate whether cybersecurity courses will be given as an elective each semester. For example, American College University offers Cryptography as an elective during both semesters, but the likelihood of a student taking that elective is lower since the students are allowed to pick only four (4) electives and are offered a total of fifteen (15) available electives. Those who pursue a one-year degree in Software Engineering at the University of Skopje have a higher likelihood of taking a cybersecurity elective, but they are only allowed to take it during the first semester.

The third faculty that offers cybersecurity-related electives to their students pursuing a one-year degree is the Faculty of Modern Sciences and Technologies (Southeastern European University). This elective is

relative to the field of study, but as with other faculties, the ratio of available electives to cybersecurity electives is similarly unfavorable toward cybersecurity electives. Under their one-year Data Science program, students are offered Information Retrieval as an elective during the first semester. During this semester the students are allowed to pick two (2) electives out of nine (9) available electives.

Our research revealed that three (3) out of six (6) private faculties offer two-year ICT degrees. There are notable differences across faculties. For example, under the Faculty of Modern Science and Technologies (Southeastern European University) all students who pursue a two-year master's degree are required to take a cybersecurity course during the first year of their studies. These students, regardless of their studies, are also allowed to take two (2) additional cybersecurity electives as a general elective during the first year. The other private university that offers two-year degrees—American College University— allows those who pursue a Software Engineering degree to take Cryptography as an elective during all semesters.

Private ICT universities are unlikely to require their graduate students to take a cybersecurity course; those that do require their students to take one (1) cybersecurity course. The exception to this pattern is American College University, which requires students who are pursuing a two-year master's degree in Management of Information Systems to take two (2) cybersecurity courses during their first year of studies. The students are required to take Information Systems Security during the first semester and Security and Ethics in ICT during the second semester. These students can also take more advanced electives such as Security Management, Cryptography, and Internet Security for Cloud.

Coincidently, universities that offer cybersecurity courses to students pursuing two-year ICT master's degrees are also the only ICT faculties that provide cybersecurity electives to their students pursuing a one-year degree (American College University, Southeastern European University, and University of Skopje). All other ICT faculties that only offer one-year degrees do not include cybersecurity courses in their curricula. This finding indicates that private ICT universities that, in general, dedicate more resources to their ICT programs are more likely to implement cybersecurity courses as either electives or required courses. This greater investment in ICT programs translates to more comprehensive learning that provides graduates who are well-versed in cybersecurity.

GENERAL FINDINGS

- None of eight (8) private ICT-related faculties in North Macedonia offer an undergraduate or graduate cybersecurity-related degree.
- None of eight (8) private ICT-related faculties in North Macedonia produce graduates whose abilities and knowledge align with cybersecurity roles defined by ENISA's framework.
- At the undergraduate level, almost all private ICT-related faculties in North Macedonia introduce either mandatory or elective cybersecurity courses.
    - While most of these courses are considered introductory courses, this is a significant improvement for faculties that historically did not offer cybersecurity courses.
- At the graduate- level, students pursuing a one-year degree are not likely to take a cybersecurity course.
    - Students pursuing a one-year master's degree are often required to take a cybersecurity course.
    - The number and the difficulty of cybersecurity courses are consistent across institutions.

- On both undergraduate and graduate levels, students pursuing shorter studies have fewer chances to interact with cybersecurity material.
    - These have a limited number of credits, and the emphasis is on the area of study.
- Courses that are considered "advanced cybersecurity electives" at private universities are often taken as introductory cybersecurity courses at public universities.
    - This demonstrates that, in terms of prestige and teaching capacities, cybersecurity education at private ICT universities is still lagging behind public ICT universities.

RECOMMENDATIONS

1. All private ICT faculties should consider implementing mandatory introductory cybersecurity courses for all students during first or second year of undergraduate studies.
    - Earlier introduction of the cybersecurity courses can reflect on the overall learning experience as students consider proper cybersecurity practices as they examine other courses and topics.
2. All private ICT faculties should consider replacing some of the general university-level electives (such as chemistry) with cybersecurity electives to allow students pursuing all ICT degrees to have continuous access to cybersecurity education.
    - Most ICT faculties allow students to take university-level electives that are not relevant to the field of study.
3. All private ICT faculties should consider implementing more advanced and relevant cybersecurity electives:
    - American College University under the Management of Information Systems program offers Fundamentals of Software Security. This elective is especially relevant to those students pursuing Software Engineering degrees; a degree offered by half of all ICT private universities in North Macedonia. Other universities should implement cybersecurity courses that are relevant to their students and their learning experience.
4. All private ICT faculties should consider evaluating whether they possess institutional and teaching capacities to implement undergraduate and graduate cybersecurity-related degrees.
    - Private universities, unlike public universities, have greater flexibility and their curriculums are subject to different accreditation procedures.
    - If there is no capacity for an accredited program, private faculties should engage in short-term courses and training.
        - For example, AUE-FON American University, a private university that does not offer cybersecurity degrees, has been offering a summer cybersecurity ThriveDX six-month boot camp for its students and outside community members for several years.

GRADUATE STUDIES

- All private ICT faculties should consider introducing cybersecurity elective courses to all one-year programs.
    - Currently, only three (3) out of six (6) one-year study programs offer cybersecurity electives, often under conditions that do not favor selecting cybersecurity electives. All

ICT faculties should allow students to take cybersecurity electives during the entirety of their studies.

- All private ICT faculties should consider introducing mandatory cybersecurity courses for all two-year degrees.
    - Currently, only some two-year programs require their students to take cybersecurity courses. All two-year degrees should implement mandatory cybersecurity courses that are relevant to their studies.
    - For example: Software Engineering students can take Software Security.
- All private ICT faculties should consider incentivizing students to conduct relative research and graduate thesis on cybersecurity.
    - Graduate students have a limited number of credits before moving on to the graduate thesis—the professors should encourage their students to focus their graduate work toward security practices and tools.

CONCLUSION

Private ICT universities in North Macedonia are unlikely to produce any cybersecurity professionals who can take on managerial, technical, or executive roles. None of eight (8) private ICT-related faculties in North Macedonia produce graduates whose abilities and knowledge align with cybersecurity roles defined by ENISA's framework. This is not surprising since none of the public faculties have a cybersecurity degree at either undergraduate or graduate level.

The current curriculums at private ICT faculties are unable to produce graduates with sufficient knowledge and skills to tackle organizational cybersecurity challenges and policies. However, the role of private universities in closing the demand for cybersecurity professionals is still significant. A handful of degrees that require students to take at least one (1) cybersecurity course and offer several other electives have a better foundation than other faculties to produce cybersecurity professionals and these degrees can be seen as pathways toward a cybersecurity profession and an entry-level cybersecurity role. Many private ICT faculties include networking and system administration in their curricula; thus, private universities can be seen as a source of entry-level cybersecurity professionals who can take on administrative roles with security in mind.

Several private universities advertise their programs as a pathway toward computer networks and cybersecurity-related employment in the ICT sector. Private ICT faculties also emphasize cybersecurity in their accreditation and the applicability of security and cryptography within the field of study. Most of these roles are synonyms for system and network administrators but also employees who can build upon their knowledge to accept more managerial and executive cybersecurity roles. From our analysis, it can be deduced that private ICT universities are adjusting their curriculums to meet the demands of their students and the labor market, but they still lack the dedication to implement an accredited cybersecurity program.

PUBLIC ICT UNIVERSITIES IN NORTH MACEDONIA

UNDERGRADUATE ICT DEGREES AT PUBLIC UNIVERSITIES

Public ICT universities in North Macedonia are organizationally larger than private universities and they offer a greater variety of undergraduate and graduate ICT degrees. Some of the ICT degrees offered by public ICT universities are computer science, computer science education, computer engineering, and electrical engineering. Public universities in North Macedonia also prescribe to a multidisciplinary approach that allows students to take electives from other areas of study. For those reasons, public universities offer a great number of subject-related and general electives that can be taken by students pursuing different degrees.

In North Macedonia, there are a total of seven (7) public ICT universities. These universities are further categorized into ICT faculties with some universities only housing one (1) ICT faculty under their organizational umbrella. For example, Mother Theresa University and State University of Tetovo, due to their location and size are associated with only one (1) ICT faculty. The St. Paul Apostle University of Information Technologies, on the other hand, is made up of five (5) ICT-related faculties. There are a total of fourteen (14) public ICT faculties in North Macedonia. The list of all public ICT universities and their respective faculties is provided in Appendix B.

There is a total of twelve (12) three-year programs and thirty-four (34) four-year studies offered under public ICT universities in North Macedonia. Our analysis revealed that two (2) public ICT universities offer an undergraduate degree in cybersecurity: Ss. Cyril and Methodius University and the University for Information Science & Technology St. Paul the Apostle. Both programs offer both three-year and four-year studies. Graduate cybersecurity degrees are offered by four (4) ICT universities, including these two universities. The list of all cybersecurity degrees is listed in Appendix C. The structure of cybersecurity degrees, learning objectives, and the curriculum are provided in the following section.

Similarly to private ICT universities, public ICT universities offer degrees in computer science, computer engineering, computer science education, application of information technologies, etc. Public ICT universities also predominately accredit longer ICT studies that emphasize the continuation of education and higher levels of educational attainment. Public universities support the continuation of education by implementing almost identical three-year and four-year programs, an approach that allows students to continue their education after obtaining a three-year degree. According to in-person interviews with faculties, the universities offer a greater number of four-year degrees because students often enroll in three-year studies in anticipation of reapplying for another year and continuing their education.

When it comes to three-year studies, similarly to the curricula of private universities, public ICT universities reserve the first two (2) years of the three-year ICT studies for general studies and foundational coursework. The third year is reserved for finalizing the required coursework and master's thesis. Due to their structure and shorter length, three-year ICT degree studies are unlikely to require their students to take a cybersecurity course. For example, out of public universities that offer three-year ICT degrees, Mother Theresa University, St. Kliment Ohridski University, and the University for Information Science & Technology St. Paul the Apostle do not require students pursuing a three-year degree to take a cybersecurity course. This is a surprising finding for the University for Information Science & Technology St. Paul the Apostle, which is one of two (2) public ICT universities that offers both undergraduate and graduate cybersecurity degrees. Even those students pursuing a three-year

Computer Networks and Security degree at this university are not required to take any cybersecurity courses; all cybersecurity mandatory courses are taken during the fourth year of the studies.

The only faculty that requires students who are pursuing a three-year degree to take cybersecurity courses is the Faculty of Information Science and Computer Engineering (Ss. Cyril and Methodius University). All students attending this faculty, regardless of their area of study or length of studies, are required to take at least one (1) cybersecurity course. At this faculty, students pursuing a three-year degree in Software Engineering and Information Systems, Computer Engineering, Computer Science, or Application of Information Technologies are required to take a mandatory course Computer Networks and Security during the third semester of their studies. These students are also allowed to take up to four (4) other electives during their last year of studies. The student can use those credits to take cybersecurity electives that are offered (Cybersecurity Fundamentals, Information Security, Cybersecurity, Network and Mobile Forensics, Digital Forensics, Ethical Hacking, Cryptography, and Software-Defined Security). Besides these four (4) ICT programs, no other three-year study programs require their students to take an introductory cybersecurity course.

Most of the three-year programs at public ICT universities offer cybersecurity courses as general electives to their students. Only one university does not offer cybersecurity electives to their students pursuing a three-year degree (Mother Theresa University). Under the University for Information Science & Technology St. Paul the Apostle structure, all cybersecurity courses are considered major electives and they can be taken by all undergraduate ICT degrees. The students who are pursuing a three-year ICT degree at this university can take electives: Network Security, Data Security and Privacy, Wireless Networks Security, Cryptography, and Cybersecurity. Depending on the degree, students can choose up to eight (8) major electives. Another smaller public ICT university— St. Kliment Ohridski University— allows its students who are pursuing a three-year degree in Computer Science to take a cybersecurity elective Cryptography and Information Security during the fifth semester of their studies.

Even though four-year ICT degrees are considered more versatile and multidisciplinary, there are small differences between three-year and four-year programs. Most of the four-year programs in North Macedonia build upon three-year programs to allow students who wish to extend their education and raise their level of specialization. When curriculums are compared, the only dissimilarities arise during the last year of studies for three-year studies that require students to complete their master's thesis. In terms of credits, three-year programs require their student to obtain 180 credits before graduating, and four-year programs require 240 credits. The difference in credits translates to ten (10) additional courses that can be taken during the fourth year. For some programs, that means providing additional cybersecurity courses to their students. For example, under the structure of the University for Information Science & Technology St. Paul the Apostle, students who attend four-year studies can take up to twelve (12) electives. Those who attend three-year studies can only take eight (8) electives during their studies. This significantly increases the chances that the students will choose one of five available cybersecurity electives.

The greatest difference between three-year and four-year programs and their approach to cybersecurity education is that even smaller faculties, such as the Faculty of Information Sciences (Mother Theresa University) and the Faculty of Natural Sciences and Mathematics (State University of Tetovo), require their students who are pursuing a four-year degree to take a cybersecurity course. At these universities, all students pursuing a four-year ICT degree, regardless of their degree, are required to

take a cybersecurity course. For example, those pursuing a Computer Science degree under the Faculty of Natural Sciences and Mathematics (State University of Tetovo) must take Coding and Cryptography during the eighth semester. The Faculty of Information Sciences (Mother Theresa University) requires all students to take two (2) cybersecurity courses: Introduction to Cryptography during the fifth semester and Computer Security during the 8th semester. This is a significant divergence from their three-year studies, Applied Programming; this is the only ICT program under this faculty that does not require students to take computer security courses.

When larger ICT public universities are considered, a similar pattern emerges. The University of Goce Delcev, under their Faculty of Computer Science, requires students who are pursuing a degree in Computer Science or Computer Engineering and Technologies to take Security of Computer Systems during the seventh semester. The Faculty of Computer Science (Ss. Kliment Ohridski University) requires those students who pursue a four-year Science and Communications Engineering degree to take Security of Computer Systems and Networks during the seventh semester. These students can take Cryptography and Information Security as an elective during the same semester. The second-largest ICT faculty in the country, the Faculty of Electrical Engineering and Information Technology (Ss. Cyril and Methodius University), also requires its students who pursue a four-year degree in Computer Technologies and Engineering to take Security and Protection of Computer Communication Systems and Networks during the sixth semester. These students can also take a university-level elective that is offered to all students—Network Forensics. The students who pursue a four-year degree in Telecommunication and Information Engineering at this faculty can also take the electives Network Forensics and Secure Communications during the seventh semester.

The largest ICT faculty in North Macedonia—the Faculty of Information Science and Computer Engineering (Ss. Cyril and Methodius)—in line with its three-year ICT studies, has the most comprehensive approach to cybersecurity education when compared to other ICT faculties in North Macedonia. All students pursuing a four-year degree, regardless of their area of study, are required to take an introductory cybersecurity course. The same course is taken by those pursuing a three-year degree. In terms of the structure, the differences between three-year and four-year degrees are minor, but significant. For example, those who pursue four-year degrees at the Faculty of Information Science and Computer Engineering have more chances to take cybersecurity electives than those pursuing three-year degrees. This faculty offers approximately 200 electives from a variety of subjects and these electives are listed under five (5) distinctive lists of electives. These electives are thematically tied to semesters and can only be taken during certain semesters. For example, cybersecurity electives are listed under two lists (F23L3S and F23L3W); electives that can be taken during the third or fourth year only. Cybersecurity electives from the F23L3S list (contains four cybersecurity electives) can be taken during the sixth and eighth semesters and electives from the FL3L3W list (contains three cybersecurity electives) can be taken during the fifth and seventh semesters only.

The University for Information Science & Technology St. Paul the Apostle, the only ICT-focused faculty in North Macedonia does not require the students pursuing a non-cybersecurity degree to take cybersecurity courses. This applies to all ICT faculties under this university. This is a surprising finding considering that the Faculty of Communication Networks and Security of this university offers undergraduate and graduate cybersecurity degrees. This is the only major public university in North Macedonia that does not require their four-year studies graduate to take a cybersecurity course even

though the university has the pre-established teaching capacity to administer cybersecurity to all students. Students pursuing a non-cybersecurity degree at the University for Information Science & Technology St. Paul the Apostle are allowed to take up to twelve (12) major electives and are allowed to pick from 75-80 available electives. Cybersecurity courses offered as electives to four-year studies are Network Security, Data Security and Privacy, Wireless Networks Security, Cryptography, and Cybersecurity. An exception to this is the four-year Digital Business Analytics degree; students pursuing this degree can take Legal Aspects of Computer Crime, Offensive Safety, and Cryptography. The first two classes are not available as electives for those pursuing a cyber degree or other ICT degrees. Offensive safety is more technically aligned with penetration testing and students need to have some foundational knowledge before engaging in examining offensive cybersecurity practices.

GRADUATE ICT DEGREES AT PUBLIC UNIVERSITIES

Public ICT universities offer significantly more graduate degrees than undergraduate degrees. Public ICT universities in North Macedonia offer a total of fifty-six (56) one-year ICT degrees and fourteen (14) two-year ICT degrees. Similarly to private ICT universities, public ICT universities mostly accredit shorter graduate-level studies which are anticipated to quickly prepare the students to enter the labor market with practical skills and knowledge. Shorter studies are also more likely to be attended by employed professionals who are seeking higher specialization and field-related knowledge. The greater versatility of ICT graduate degrees also translates to the availability of cybersecurity programs at the graduate level. Our analysis revealed that there are a total of four (4) public ICT universities that offer graduate cybersecurity-level degrees. These universities offer four (4) one-year and two (2) two-year cybersecurity study programs. The list of all cybersecurity degrees is listed in Appendix C.

When compared to private ICT universities, public ICT universities are more likely to require their students to take a cybersecurity course, regardless of the area of study or the length of their studies. The only exception is Mother Theresa University, which does not offer mandatory or elective cyber security courses. All other public ICT universities, including smaller public ICT faculties such as the Faculty of Natural Sciences and Mathematics (State University of Tetovo), require their students to take a cybersecurity course during the first semester of their studies, regardless of the length of their studies. Students pursuing a Computer Science Education degree are required to take Computer Security while those pursuing a Software and Application Engineering degree are required to take a more advanced course, Security of Web Applications. One of the ICT faculties that has a regional impact, the Faculty of Information and Communication Technologies (Ss. Kliment Ohridski University), requires those pursuing a two-year degree in Informatics and Computer Technology to take Cryptographic Algorithms and Parallel Processing during the second semester.

Larger universities, such as Ss. Cyril and Methodius University and the University of Goce Delcev include a greater number of cybersecurity courses and they often require the students pursuing other ICT-related degrees to take cybersecurity courses. More importantly, these universities introduce cybersecurity courses that are thematically relative to the study program. This comprehensive approach can be attributed to the argument that these universities have the capacity and resources to facilitate cybersecurity courses because these universities already offer cybersecurity-related degrees.

For example, the largest ICT faculty in North Macedonia, the Faculty of Information Science and Computer Engineering (Ss. Cyril and Methodius University) requires students who are pursuing a one-year and two-year Cloud Computing degree to take Security Challenges in Virtual Environments. Those who are pursuing a two-year degree are also required to take Cybersecurity during the first semester. Students who are pursuing a degree in Software for Embedded Systems are required to take Building IoT and IoT Security during the first semester of their studies. These students, like other ICT-degree-seeking students, are also allowed to take up to two (2) additional cybersecurity electives out of sixteen (16) available cybersecurity electives. The cybersecurity electives offered by the Ss. Cyril and Methodius University range from Cybersecurity Fundamentals and Mobile and Web Application Security to Cyber Threat Analysis.

Under the Faculty of Computer Science (University of Goce Delcev) students who are pursuing a one-year degree in Information Systems and Technologies are required to take Security of Information Systems during the second semester of their studies. Under this faculty, students who are also pursuing a degree in Software Engineering can take Software Security as an elective during the first semester of their studies. Those pursuing a degree in Robotics and Intelligent Systems can take Internet of Things with Security as an elective during the first semester.

There are five distinctive ICT faculties under the University for Information Science & Technology St. Paul the Apostle. Appendix B provides a list of all faculties and program studies under this university. Our analysis revealed that degrees offered under these faculties are specific to their area of study and that they do not include mandatory cybersecurity courses. The only exception is the cybersecurity program study Information and Network Security, Privacy and Data Protection, which requires students to take five (5) mandatory cybersecurity courses before moving on to the graduate thesis. Other ICT study programs allow students to take cybersecurity electives throughout the entirety of their studies, but they do not require students to take cybersecurity courses. The students who are pursuing any ICT-related degree at the University for Information Science & Technology St. Paul the Apostle are also allowed to pick up to five (5) additional electives. University-level electives offered to all ICT students are: Digital Forensics, Cryptography, Advanced Cryptography, Ethical Hacking, and Performance, Reliability, and Security of Databases.

GENERAL FINDINGS

- At the undergraduate level, almost all public ICT-related faculties in North Macedonia introduce mandatory cybersecurity courses.
    - The approach to cybersecurity significantly differs across study programs.
    - Students who are pursuing three-year ICT studies are not required to take cybersecurity courses; only four-year degrees require students to take introductory cybersecurity courses.
- Public ICT universities, when compared to private ICT universities, include more advanced undergraduate cybersecurity courses.
    - Universities that offer cybersecurity degrees provide the most versatile cybersecurity courses; they also offer the greatest number of cybersecurity electives.
- On both undergraduate and graduate levels, students pursuing shorter ICT studies have fewer chances to take a cybersecurity course.

- At the graduate level, almost all public ICT-related faculties in North Macedonia include more versatile and advanced cybersecurity courses.
    - Graduate study programs offer cybersecurity courses relative to the field of study (i.e. Software and Application Engineering degree requires students to take Security of Web Applications)
    - This is a significant divergence from undergraduate degrees that only include introductory cybersecurity courses.

RECOMMENDATIONS

1. All public ICT universities should consider assessing their current approach to cybersecurity education and its alignment with their studies.
    a. For example, the Faculty of Electrical Engineering and Information Technology (Ss Cyril and Methodius University) provides degrees focused on energy, automation, and computer engineering and it offers Network Forensics to all undergraduate degrees. This class is too advanced for students who do not take any introductory forensics courses since network and mobile forensics are more advanced than the classes on the general application of digital forensics.
    b. An example of alignment: State University of Tetovo requires their students who are pursuing a Software and Application Engineering degree to take Security of Web Applications.
2. All public ICT universities should consider implementing more advanced mandatory undergraduate cybersecurity courses.
    a. Currently, only foundational cybersecurity courses are required courses; all public universities should implement at least one (1) advanced cybersecurity course.
3. Faculties that offer undergraduate and graduate cybersecurity degrees should consider collaborating with other faculties that do not provide cybersecurity degrees.
    a. These faculties have the teaching capacities and resources to facilitate cybersecurity courses; they should be the facilitators of talent and resource sharing.
4. At the graduate level, public ICT universities should consider offering a greater number of one-year ICT programs that do not require students to take cybersecurity courses.
    a. ICT faculties should include mandatory cybersecurity courses for all one-year programs; these electives should be relevant to their field of study.

CONCLUSION

Public ICT universities in North Macedonia introduce students to computer systems, processes, data management, intelligent computer systems, programming, and networking. Almost all public ICT universities have accredited curriculums that include cybersecurity courses as either mandatory or elective courses. These courses range from introductory and theoretical courses to advanced courses with practical application. The most challenging courses are graduate level; these classes introduce students to digital forensics, software security, and Internet of Things security. Furthermore, most public ICT universities classify cybersecurity courses as general electives, which allows all ICT students to enroll in various cybersecurity courses throughout their studies.

Several public ICT universities advertise their curriculums and areas of study as a pathway toward the IT profession and cybersecurity-related employment in the ICT sector. Public ICT universities also emphasize cybersecurity in their accreditation; this includes universities that do not require their students to take cybersecurity courses. Because public ICT faculties include a variety of cybersecurity courses in their curriculum as either mandatory or elective courses, public ICT faculties are likely to produce cybersecurity professionals who can take on some cybersecurity roles. Most of these courses are closely related to information security and computer security; therefore, students who graduate with an ICT degree are qualified to take on roles such as: Network and IT Systems Manager or Information Security Administrator. These cybersecurity roles are not outlined by ENISA's framework, but they represent a significant proportion of the current cybersecurity workforce in North Macedonia.

Notably, the most significant contributors to the cybersecurity workforce in North Macedonia are universities that also offer cybersecurity degrees. These public universities allow all students pursuing ICT degrees to take cybersecurity courses that are either mandated or offered to students pursuing a cybersecurity degree. For those reasons, even those students who are not pursuing a cybersecurity-related degree at these ICT universities can graduate with sufficient knowledge and skills to enter the cybersecurity workforce. However, these students must be intentional in their studies to maximize the number of cybersecurity courses they take. Only those students who take multiple advanced cybersecurity courses such as Digital Forensics or Ethical Hacking can gain sufficient knowledge and skills enter to the cybersecurity workforce with ambitions to become Cybersecurity Risk Manager, Digital Forensics Investigator, or Penetration Tester.

CYBERSECURITY EDUCATION IN NORTH MACEDONIA

UNDERGRADUATE CYBERSECURITY CURRICULUMS

Two (2) ICT universities in North Macedonia offer undergraduate cybersecurity degrees:

1) Ss Cyril and Methodius University
    a. Internet, Networks, and Security (3 & 4 years)
2) The University of Information Science and Technology St. Paul the Apostle
    a. Communication Networks and Security (3 & 4 years)

The University of Information Science and Technology "St. Paul the Apostle

The students who are pursuing a Communication Networks and Security degree under the University of Information Science and Technology St. Paul the Apostle are expected to gain knowledge in computer networks, network security, wireless technology, and cryptography. The students attending this program learn about computer science, wireless communication, and network programming. The students are also expected to learn about computer networks, their organization, function, and methods of secure information transfer and security testing. At the end of the program, the students are expected to address the challenge of designing, setting up, and maintaining computer networks.

The University of Information Science and Technology St. Paul the Apostle promotes this degree as a pathway toward various job positions such as: "Cloud Application Developer, Java Developer, NET Developer, Security Analyst, Ethical Hacker, Chief Information Security Officer, Network Engineer, Network Technical Analyst, Network Infrastructure Analyst, Systems Administrator, Network and IT Systems Manager, Computer Software Engineer, Database Developer, Games Programmer."

It is unclear how the University for Information Science & Technology St. Paul the Apostle prepares its students for some of the cybersecurity roles listed above. For example, roles such as Security Analyst, Ethical Hacker, Chief Information Security Officer, and Network Infrastructure Analyst require students to take more advanced cybersecurity courses such as Penetration Testing and Cyber Threat Analysis. These roles, moreover, require continuous exposure to the practical application of the material, something that is absent from the faculty's curriculum.

The current curriculum of the program does not align with these roles for several reasons. Primarily, those who pursue a three-year Communication Networks and Security degree are not required to take any cyber security courses, yet they obtain a Bachelor of Engineering in Information Science and Technology in the field of Communication Networks and Security. It is unclear the level of expertise those who pursue a three-year degree obtain since these students are only allowed to take eight (8) major electives courses and up to three (3) cybersecurity electives throughout their studies. Moreover, the current curriculum does not include classes that will provide skills and knowledge to be employed in these roles. This is also true for those students who are pursuing a four-year degree; these students are only required to take Cryptography during the seventh semester and Cybersecurity during the eighth semester.

Some of the advanced cybersecurity courses that could prepare students for the roles above are offered as electives. Three (3) electives that are offered to students pursuing both three-year and four-year degrees in Communication Networks and Security are Network Security, Data Security and Privacy, and Wireless Network Security. Whether these individual courses are sufficient to prepare students to take on roles such as Network Specialist is unknown, especially since only those students who take all cybersecurity electives would gain a sufficient understanding of network security. Interestingly, other cybersecurity electives that could prepare students for these roles—such as Legal Aspects of Computer Crime or Offensive Safety— are only offered to those who pursue a four-year Digital Business Analytics degree. The course Offensive Safety is more technically advanced, and it requires students to have some foundational knowledge before engaging in examining offensive cybersecurity practices. This class, however, is not offered to those who are pursuing an undergraduate cybersecurity degree. Students who graduate with an undergraduate cybersecurity degree from the University for Information Science & Technology St. Paul the Apostle are likely to enter the labor force as Network and IT Systems Managers or Information Security Administrators.

Ss. Cyril and Methodius University

The Faculty of Computer Science and Engineering (Ss. Cyril and Methodius), on the other hand, has a more comprehensive approach to undergraduate cybersecurity education. Students pursuing both three-year and four-year studies are required to take at least two (2) cybersecurity during the first three years of their studies. Those who pursue a three-year degree in Internet, Networks, and Security are required to take Fundamentals of Cybersecurity during the second semester and Cybersecurity during the fifth semester. Those who pursue a four-year degree follow a similar curriculum, but they are also required to take Software-Defined Security during the sixth semester. This course is also offered as an elective to those who pursue three-year studies.

The introduction of cybersecurity courses earlier in the studies is a significant advantage of this cybersecurity degree. Earlier introduction of cybersecurity courses sparks greater interest in the topic, and it provides students with a security mindset as they take on other courses. Furthermore, introducing cybersecurity courses earlier is especially beneficial for students attending the Faculty of Computer Science and Engineering (Ss. Cyril and Methodius). Similarly to students pursuing other ICT degrees, those who are pursuing an undergraduate degree in cybersecurity at this faculty are only allowed to take cybersecurity electives during their third year and fourth year of studies. Early introduction of mandatory introductory cybersecurity courses, therefore, lays the foundation for cybersecurity electives that tend to be more advanced and technical. The electives that are offered during the third and fourth years are: Digital Forensics, Cryptography, Network and Mobile Forensics, and Ethical Hacking.

The Faculty of Computer Science and Engineering (Ss. Cyril and Methodius) advertises this program as a pathway toward job positions that oversee network and information infrastructure design and management. The students attending this program are expected to gain practical knowledge in the field of information security and protection from malicious attacks. The two introductory courses Fundamentals of Cybersecurity and CyberSecurity emphasize protection from malicious attacks and these courses provide a theoretical overview of cyber risks and cyberattacks. These courses also cover

forensics tools and ethical hacking, two courses that prepare students to take on more technical roles, such as Network Analyst and Cyber Threat Intelligence Specialist. Those students who additionally take Digital Forensics and Network and Mobile Forensics as electives would be the most fitting candidates to take more technical roles, such as Digital Forensics Investigator and Penetration Tester.

GENERAL FINDINGS

- Only the University for Information Science & Technology St. Paul the Apostle and Ss. Cyril and Methodius University offer undergraduate cybersecurity degrees.
- Students who graduate with an undergraduate cybersecurity degree from the University for Information Science & Technology St. Paul the Apostle are likely to enter the labor force as Network and IT Systems Managers or Information Security Administrators.
- Students who graduate with an Internet, Networks, and Security degree from Ss. Cyril and Methodius University are more prepared to take more technical roles:
    - Digital Forensics Investigator or Penetration Tester.
- Undergraduate cybersecurity education in North Macedonia remains underdeveloped, with both universities adopting a generalist and multidisciplinary approach.
    - Students who take only mandatory cybersecurity courses do not acquire sufficient skills and knowledge to acquire managerial or executive cybersecurity positions.
- Students who pursue three-year undergraduate cybersecurity degrees retain less knowledge and they have fewer opportunities to engage in learning.
    - In fact, those who are pursuing a three-year degree from the University for Information Science & Technology St. Paul the Apostle are not required to take a cybersecurity course during their studies yet after the completion of their studies they receive a Bachelor of Engineering in Information Science and Technology in the field of Communication Networks and Security.
- When the number of general electives is accounted for, cybersecurity electives represent a small percentage of electives at both universities.
    - Both universities offer many general electives; students who are pursuing a cybersecurity degree must be intentional when they pick electives if they wish to maximize their learning opportunities.
    - The University for Information Science & Technology St. Paul the Apostle's curriculum provides three (3) cybersecurity electives and eighty-seven (87) other general electives.
    - Ss Cyril and Methodius University's curriculum provides four (4) cybersecurity electives and ninety-eight (98) other general electives.

GRADUATE CYBERSECURITY CURRICULUMS

Four (4) ICT universities in North Macedonia offer graduate cybersecurity degrees:

1) Military Academy
    a. Cybersecurity and Digital Forensics (one year)
2) Ss Cyril and Methodius University

    a. Security, Cryptography, and Coding (one and two years)
    b. Internet Technologies and Cybersecurity (one year)
3) The University of Information Science and Technology St. Paul the Apostle
    a. Information and Network Security, Privacy, and Data Protection (two years)
4) University of Goce Delcev
    a. Computer Security and Digital Forensics (one year)

Military Academy

The Military Academy offers a specialistic cybersecurity degree that introduces its military cadets to cyber warfare, international cyber law, and cyber defense. This program is facilitated jointly with the University of Goce Delcev, but the program is exclusively open to students who are attending the Military Academy. The emphasis of the program is on digital forensics and the protection of military infrastructure from cyberattacks. Upon completion of the program, the students are expected to be able to deal with complex situations in the field of digital forensics. Students who graduate with a degree in Cybersecurity and Digital Forensics are expected to support cybersecurity operations of the Ministry of Interior, the Military, and the Ministry of Foreign Affairs.

The students who pursue a Cybersecurity and Digital Forensics degree from the Military Academy are required to take three (3) cybersecurity courses during the second semester of their studies. The first semester is reserved for more general courses and a research course. The required cybersecurity courses are: Information Communication Security, Digital Forensics, and International Relations and Legal Aspects of Cyber Security. The last course is International Relations and Legal Aspects of Cyber Security, which introduces students to the legal norms, principles, and standards related to cybersecurity, as well as the role of international organizations in the creation of legal regulations and policies related to cybersecurity.

The students who pursue Cybersecurity and Digital Forensics are also allowed to take one (1) additional elective during each semester. Under the structure of the Military Academy, all electives offered under this program are cybersecurity-related degrees; no other general electives are offered. This is a significant advantage of this program. During the first semester, the students choose between taking Cyber Security and Cyberspace or Biometrics and Cryptography. Under the military pretense, cyberspace is a space where doctrines, strategies, and operational requirements dictate state strategy. The students are expected to learn concepts of the integrated, controlled, and effective use of cyberspace during military operations. During the second semester, the students are allowed to pick between electives Vulnerability of Systems and Networks and Penetration Testing or Protection of Critical Information Infrastructure, two courses that prepare the students to engage in both offensive and defensive practices. Students who graduate with a Cybersecurity and Digital Forensics degree from the Military Academy can enter the workforce as Chief Information Security Officer (CISO), Cyber Legal, Policy & Compliance Officer, Digital Forensics Investigator, and Penetration Tester.

Ss Cyril and Methodius University

The Faculty of Computer Science and Engineering (Ss. Cyril and Methodius University) is the largest ICT faculty in North Macedonia. This faculty offers the greatest number of ICT-related degrees and is the

biggest contributor to the number of ICT graduates, including cybersecurity graduates. At the graduate level, the Faculty of Computer Science and Engineering (Ss. Cyril and Methodius University) offers a total of three (3) cybersecurity graduate degrees: Security, Cryptography, and Coding (1 & 2 years) and Internet Technologies and Cybersecurity (1 year).

Students who pursue the Security, Cryptography and Coding study program can choose between pursuing a one-year or two-year degree. Students who are pursuing a one-year degree in Security, Cryptography, and Coding are only required to take Applied Cryptography during the first semester and Advanced Information Security during the second semester before moving on to their graduate thesis. After completing these courses, the students are expected to know basic cryptographic principles and methods. The students are also expected to be able to practically use cryptographic algorithms. The second mandatory course Advanced Information Security introduces students to advanced authentication and authorization methods. The students taking this course are expected to understand access control and security models. The emphasis of this study program is on cryptography and advanced information security and students who attend this program are expected to be well-versed in cybersecurity practices and information security.

The current curriculum does not allow students, especially those pursuing a one-year degree, to further explore more advanced cybersecurity topics. Those pursuing a one-year degree are allowed to take all multidisciplinary university-level electives but are not allowed to take cybersecurity courses that are required under the one-year program. This has implications for students who wish to enroll in more advanced cybersecurity courses. For example, those who pursue a one-year degree are not allowed to take an introductory Digital Forensics course but are allowed to take more advanced electives such as Practical Application of Digital Forensics or Machine Learning Forensics. Without foundational knowledge, these students are unlikely to reach learning objectives and apply this knowledge in their professional setting. Students who graduate with a one-year degree in Security, Cryptography, and Coding are expected to be skilled and qualified for roles such as Information Security Manager.

Students who are pursuing a two-year degree are required to take the same courses as those students pursuing a one-year degree. Under the two-year program, these courses are a part of the second-year curriculum. Furthermore, those who attend two-year studies are expected to take four (4) additional cybersecurity courses during the first year of their studies (Computer Networks and Security, Information Security, Digital Forensics, and Cryptography). Due to the versatility of these classes, students who attend two-year studies are more likely to engage in more comprehensive learning than those attending one-year studies. Students who graduate with a two-year degree in Security, Cryptography, and Coding are expected to be skilled and qualified for roles more technical or high-level roles such as Information Security Manager, Chief Information Security Officer, and Digital Forensics Investigator.

Overall, the two-year Security, Cryptography, and Coding program is more advanced and comprehensive than the one-year program. Those who attend a two-year degree can take on various cybersecurity roles since these students get familiar with network architecture and protocols, as well as the principles and techniques needed for a digital forensic investigation during the first year of their studies. Students who attend a two-year program are more likely to gain hands-on experience while working with different forensic tools and different operating systems. Longer studies also allow students to take more cybersecurity electives. The one-year program, on the other hand, emphasizes information

security and secure communication networks. Students pursuing a one-year can only take two (2) cybersecurity electives. For those reasons, students who attend one-year and two-year programs are expected to achieve different learning objectives and enter the cybersecurity workforce with different skill sets.

When it comes to electives, both programs offer the same cybersecurity electives to their students. These electives are university-level electives that are also offered to other students who are not pursuing a cybersecurity degree. In total, there are fifteen (15) additional cybersecurity electives and two hundred (200) general electives. Depending on the program, students can take between 1-2 additional cybersecurity electives during their studies. Students attending two-year studies can be allowed to take four (4) additional electives. The cybersecurity electives range from Cryptographic Protocols, Network Security Analysis, and Cyber Security Incidents and Forensics to Machine Learning Forensics.

The third graduate cybersecurity degree offered by the Faculty of Computer Science and Engineering (Ss Cyril and Methodius University) is the one-year degree in Internet Technologies and Cybersecurity. This degree is more advanced than the other cybersecurity programs since it emphasizes analysis and response to cyber-attacks. The students who complete this program are expected to be familiar with standard technologies and threat detection methods. This program also introduces the students to the fundamental concepts and tools of modern cyber threat analysis. The second objective of this program is to introduce students to data privacy and information security. After completing this program, the students should understand the implementation of confidentiality, integrity, and authentication of information systems and system monitoring.

Students who pursue a degree in Internet Technologies and Cybersecurity are required to take Cyber Threat Analysis during the first semester of their studies and Cybersecurity and Privacy during the second semester of their studies. These two courses introduce students to standards of information securing and identification of cyber threats. There are no other mandatory cybersecurity courses, but students who pursue this degree are also allowed to take up to three (3) additional electives. Similarly to students pursuing other cybersecurity graduate programs under the Faculty of Computer Science and Engineering (Ss. Cyril and Methodius University), students in this program are offered an additional fifteen (15) cybersecurity electives. The electives are identical to those being offered to other programs but the most relevant electives to these studies are: Network Security Analysis, Cyber Security Incidents and Forensics, and Practical Application of Digital Forensics. Students who enroll in these courses during their studies are expected to gain further knowledge and practical application of digital forensics and threat analysis. Students who graduate with a degree in Internet Technologies and Cybersecurity are expected to be skilled and qualified for roles such as Cyber Threat Intelligence Specialist or Chief Information Security Officer.

The University of Information Science and Technology St. Paul the Apostle

The University for Information Science & Technology St. Paul the Apostle offers a two-year cybersecurity degree in Information and Network Security, Privacy, and Data Protection. The emphasis of the program is on information security, network security, and data protection. The students who complete this program are expected to know the principles of data protection, data processing security, networking monitoring, network security, and security of cloud protocols. Most of the mandatory

cybersecurity courses are closely related to the protection of data and information security; therefore, students who complete this program are expected to enter the cybersecurity workforce as qualified candidates for roles Data Administrator, Information Security Manager, and Chief Information Security Officer.

During the first year, the students are required to take Privacy of Data Processing, Threats to Information Systems, and Privacy and Data Protection. During the second year of their studies, the students are required to take Privacy of Electronic and Internet Communications and Performance, Reliability, and Security of Databases. These students can take up to five (5) electives throughout their studies. On the list of general university-level electives are a total of nineteen (19) electives, four (4) of these electives are cybersecurity electives (Cybersecurity, Offensive Safety, Digital Forensics, and Ethical Hacking.) All electives except Offensive Safety are general university-level electives that are offered to all ICT graduates. This is a technically advanced course that introduces students to hacking tools and penetration testing; advanced techniques that prepare students to be Network Analysts and Penetration Tester.

University of Goce Delcev

The Faculty of Computer Science (University of Goce Delcev) offers a one-year graduate degree in Computer Security and Digital Forensics. This is the second most comprehensive and advanced cybersecurity program in North Macedonia. The students who complete this program are expected to understand the legal aspects, the principles, techniques, and tools used in computer security and digital forensics. The students are also expected to learn techniques and tools used for the analysis of the security of web applications, and mobile devices. After completing the program, the students are expected to be familiar with the identification, acquisition, and preservation of digital evidence. They are also expected to be familiar with practical tools used in ethical hacking and penetration testing.

The students who are pursuing a one-year degree in Computer Security and Digital Forensics are required to take Cryptographic Algorithms and Protocols and Digital Forensics during the first semester of their studies. These courses cover a variety of topics, from advanced knowledge of cryptography and cryptographic algorithms to techniques of digital forensics. The students also learn to use most forensic tools and perform basic forensic analysis on Windows and Linux computer systems and Android mobile phones. During the second semester, the students are required to take Ethical Hacking and Penetration and Computer Network Security and Web Security. These are more advanced courses that focus on various hacking tools and the protection of the computer system from unauthorized access and cyberattacks.

The students pursuing a one-year graduate degree in Computer Security and Digital Forensics are also allowed to take three (3) additional electives during their studies. Because the number of available electives and their versatility are a significant advantage of this program, there is a high likelihood that students will pick cybersecurity electives. Most of the program's electives are cybersecurity electives; seven (7) out of ten (10) offered electives are cybersecurity electives. This favorable ratio urges students to take cybersecurity electives over general electives and further expand their knowledge on specific topics, such as Software Security, Mobile Security and Forensics, and Multimedia Forensics and Security, This program also excels in providing unique and contemporary cybersecurity courses such as Security

of Control Systems and IoT or Internet of Things with Security, areas that cover cybersecurity practices that are integral for the protection of critical infrastructure.

By offering versatile advanced cybersecurity courses, the Faculty of Computer Science (University of Goce Delcev) prepares its students for various technical and managerial cybersecurity job positions. The mandatory coursework prepares students to take on roles such as Digital Forensics Investigator and Penetration Tester. Depending on the electives they take, some students could take on more technical advanced roles, such as Network Forensics Analyst or Administrator of Security Controls. Students who graduate from this university obtain sufficient knowledge and skills to enter the cybersecurity workforce and lead organizational cybersecurity policies.

GENERAL FINDINGS

- Four (4) universities in North Macedonia offer graduate cybersecurity degrees.
    - Military Academy, Ss Cyril and Methodius University, University for Information Science & Technology St. Paul the Apostle, and University of Goce Delcev.
- Students who pursue a graduate cybersecurity degree in North Macedonia are well-versed in Digital Forensics and Information/Computer Security
- Students in North Macedonia who pursue a master's degree in cybersecurity are required to take at least four (4) cybersecurity courses.
    - The number of cybersecurity electives varies across faculties; most of these electives are considered advanced cybersecurity courses.
- Students who graduate with a graduate degree in cybersecurity are likely to possess specific skills and knowledge needed for executive and managerial roles.
    - Students who receive a graduate degree are prepared for roles: Chief Information Security Officer, Digital Forensics Investigator, and Penetration Tester.
    - Prospective job positions are dictated by the curricula.
- Graduate-level cybersecurity degrees in North Macedonia, when compared to undergraduate-level degrees, are more comprehensive and advanced. Graduate students are more likely to engage in various learning opportunities despite the shorter duration of their studies.
    - Graduate programs are more likely than undergraduate studies to produce highly qualified cybersecurity candidates.

RECOMMENDATIONS

UNDERGRADUATE CYBERSECURITY STUDIES

1. Currently, only two public faculties offer an undergraduate degree in cybersecurity. Other faculties, especially those who already have graduate-level programs, should need to assess their abilities and capacities to implement undergraduate cybersecurity programs.
    a. The emphasis is on the University of Goce Delcev and the Military Academy to implement undergraduate studies by relying on existing teaching capacity and resources.
2. The University of Information Science and Technology St. Paul the Apostle should consider revisiting their curriculum to include more mandatory cybersecurity courses, especially for those students pursuing a 3-year degree.
    a. These courses should be introduced during the first or second year.
3. The Faculty of Computer Science and Engineering (Ss. Cyril and Methodius) should consider revisiting their curriculum to include more advanced cybersecurity courses.
    a. Additional cybersecurity electives can replace general electives to increase the likelihood that the student will pick a cybersecurity elective.
    b. Examples: Digital Forensics Engineering, IoT Security, and Malware Reverse Engineering.
4. All ICT Faculties that offer undergraduate cybersecurity courses should include more advanced cybersecurity courses as electives.
    a. Currently, both faculties offer cybersecurity electives as subsections of general electives.
    b. Students are offered more than 100 general electives; some general electives (such as mathematics and chemistry) should be replaced with cybersecurity electives.
5. To encourage more students to pursue cybersecurity degrees, ICT faculties should expand their capacity to offer cybersecurity courses to all ICT undergraduate students.
    a. The faculties under the University of Information Science and Technology St. Paul the Apostle do not require their undergraduate students to take a cybersecurity course during their studies; this further discourages ICT students from taking more advanced cybersecurity electives, such as Network Security and Wireless Network Security.
6. Undergraduate studies should consider revisiting their curricula to include courses that prepare students for other cybersecurity roles.
    a. According to ENISA's framework, students who graduate with an undergraduate cybersecurity degree are qualified to become Cyber Threat Intelligence Specialists, Digital Forensics Investigators, and Penetration Testers.

GRADUATE CYBERSECURITY STUDIES

1. The University for Information Science & Technology St. Paul the Apostle should consider revisiting its curriculum to add more cybersecurity electives.
    a. Currently, this program offers four (4) cybersecurity electives; most of these courses are offered by other universities as well.
    b. Electives that could be added: Software Security, Advanced Information Security, and Network Security Analysis.
2. The Ss. Cyril and Methodius University should consider restructuring its curriculum to increase the opportunities for students to take cybersecurity electives.

    a. This university offers a significant number of cybersecurity electives, but these courses are just a fraction of more than 200 general electives.
    b. Students who pursue graduate cybersecurity degrees should be restricted from taking general electives that are not relative to their studies.
3. The Ss. Cyril and Methodius University should consider restructuring its one-year Security, Cryptography, and Coding program.
    a. This program is less comprehensive than other cybersecurity programs because students are only required to take two (2) cybersecurity courses.
    b. Some cybersecurity electives should be recategorized as mandatory courses.
4. The University of Goce Delcev as the university with the second most comprehensive cybersecurity curriculum, should assess its capacities to implement the two-year program.
    a. This university currently offers only one-year studies, but it has capacities to develop a longer program; this program should prepare students to take roles that have executive or managerial responsibilities.
5. The Military Academy should consider opening its academy to outside community members.
    a. North Macedonia suffers from low graduation rates of ICT graduates.
    b. Considering that Military Academy is one out of two universities that provides Digital Forensics courses, the Military Academy can be a significant contributor to the cybersecurity workforce by closing the demand for Digital Forensics Investigators.
6. All public ICT faculties that offer graduate cybersecurity degrees should assess their teaching capacity to promote talent and information sharing.
    a. Graduate cybersecurity programs are the most advanced and comprehensive cyber programs in North Macedonia.
    b. These programs should assess their ability to translate their courses to undergraduate cybersecurity programs; the priority should take more advanced cybersecurity courses that are not included in the undergraduate curriculum.
7. Undergraduate studies should consider revisiting their curricula to include courses that prepare students for more advanced and executive cybersecurity roles.
    a. According to ENISA's framework graduate cybersecurity programs in North Macedonia provide qualified Chief Information Security Officer (CISO), Cyber Legal, Policy & Compliance Officers, Cyber Threat Intelligence Specialists, Digital Forensics Investigators, and Penetration Testers.
    b. While graduate studies are significant contributors to the cybersecurity workforce, there is still a great need for other cybersecurity roles outlined by ENISA's framework: Cyber Incident Responder, Cybersecurity Architect, Cybersecurity Auditor, Cybersecurity Educator, Cybersecurity Implementer, Cybersecurity Researcher, and Cybersecurity Risk Manager.