SPARTA

D9.3

Training Evaluation Pilot

Project number	830892
Project acronym	SPARTA
Project title	Strategic programs for advanced research and technology in Europe
Start date of the project	1st February, 2019
Duration	36 months
Programme	H2020-SU-ICT-2018-2020

Deliverable type	Demonstrator
Deliverable reference number	SU-ICT-03-830892 / D9.3 / V1.0
Work package contributing to the deliverable	WP9
Due date	January 2021 – M24
Actual submission date	29th January, 2021

Responsible organisation	PPBW
Editor	Klaudia Kaczmarek
Dissemination level	PU
Revision	V1.0

Abstract	The document contains a short description of the methodology used for evaluating higher education training pilots taking place at participating universities, both from students' and administrators' perspectives. The evaluation results should serve to support good practice for universities planning to develop their own study programs in cybersecurity. The document also includes high-level recommendations towards improvements in the training.
Keywords	Training, study programs, education, evaluation, recommendations.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892.

Editor

Klaudia Kaczmarek (PPBW)

Contributors (ordered according to beneficiary numbers)

Klaudia Kaczmarek, Steven Ormston, Bartosz Kożuch, Rashel Talukder (PPBW)

Reviewers (ordered according to beneficiary numbers)

Adam Kozakiewicz (NASK)

Nelson Escravana (INOV)

Executive Summary

Many reports consistently document the today's dramatic cybersecurity skills gap and scarcity of professionals with adequate qualification. One solution to this problem is to enhance cybersecurity education and training so that more experts in cybersecurity can fill the lacks. To face such challenge, we analysed the curricula currently offered at various European Universities which are SPARTA project partners as the starting points to improve existing curricula for bachelor degrees and master degrees in computer security.

Starting from the skills framework development model developed in T9.1, this report established a set of curricula recommendations, aiming at helping academic institutions with define which 'competencies' are missing from the learning paths that will enable students to fill three entry-level roles: **Technical Support Specialist, Cyber Defense Incident Responder** and **Cyber Defense Forensics Analyst.**

Thus, this report was prepared on the basis of an analysis of data from two questionnaires - the first aimed at the administration teams of the institutions, the second targeting the students completing the relevant courses. The surveys can be easily re-used to provide clarity on the topics covered in other courses, and to make similar assessments as to whether those courses follow the best practices highlighted in the SPARTA Cybersecurity Skills Framework. Nevertheless, it is worth the consideration conducting qualitative interviews after the initial courses are finished in order to better prepare future SPARTA Cybersecurity Framework programs.

The programs offered at the universities participating in WP9 were considered as pilots. Therefore, the evaluation confirmed which universities are following the SPARTA recommendations and also highlighted all gaps between their current approach and the best practices included in D9.2. Furthermore, by also gathering data directly from students, the team compared the results between the parties and highlighted where perceptions differ.

Finally, by collecting the recommendations provided by administrators, students and authors of the report, the document aims at improving the process of creating new cybersecurity study programs that take place at involved universities in the form of hands-on training. Furthermore, the report allows designing future programs, according to certain rules and standardized approaches reflecting actual requirements of particular cybersecurity positions.

Table of Content

List of Figures

List of Tables

Chapter 1 Introduction

1.1 Purpose of the Document

The main purpose of this document is to provide the recommendations for universities, so that they have a good-practice example of study plans suitable for the cybersecurity study programs.

Within the document, all the information captured through the two surveys is summarized and presented. The goal was to provide clear visualizations of the results - mapping the materials to the previously delivered reports D9.1 and D9.2 whenever possible. We consider that the recommendations presented can be used by other institutions to create their own cybersecurity study programs that suit their particular needs. Likewise, the survey used to engage the students could be distributed to capture the feelings of pupils currently engaged in academic study and those who have recently finished cybersecurity programs.

What needs to be underlined, due to the COVID-19 pandemic delaying the roll-out of professional courses, and the feasibility of official pilot programs being sanctioned in academic institutions, the WP9 team of the SPARTA project decided it was not possible to wait for professional certificate and academic pilot programs to start. After consideration of current conditions, the WP9 team decided upon a new approach to the deliverable and worked only with academic institutions in the project that are currently following – in the most part – the curricula recommendations of SPARTA, outlined in Deliverable 9.2 (D9.2). The short time schedule and the focus on ongoing and pioneering programs, resulted in resignation from the initially envisioned research methods (in-depth interviews and focus groups) in favor of survey research.

1.2 Methodology

While based on the ongoing courses at the partner universities, the main outcome of Deliverable 9.3 - The Training Evaluation Pilot – summarises the two key activities that took place in parallel in November 2020.

To map the current situation across the academic institutions, the SPARTA team implemented two questionnaires – for the Higher Education Program Administrators [1] and Students [2]. Launching such surveys was interesting as they provide information on what to improve; while delivering a methodological framework that can be used for the evaluation of programs in subsequent surveys. Thus, the team intended to use a ‘reusable template’ that, with minimum alterations, can be leveraged to capture and highlight similar information from other universities and course providers.

Moreover, the methodology focuses on the use of previously delivered results within WP9. One of which was the SPARTA Cybersecurity Skills Framework (CSF). The first important concept of the CSF is that it maps the Knowledge, Skills and Abilities (KSAs) grouping the Competencies into Work Roles. The SPARTA CSF was delivered in D9.1 in January 2020 and is currently approved by the EC and publicly available on the project website [3]. It is important to note that the SPARTA CSF is one of the first attempts to use an EU-wide cybersecurity education and training framework.

The SPARTA CSF is based on the structure of the NICE Framework, and takes into account the following considerations:

- **52 Work Roles** are the most general groupings of cybersecurity and related work, which include a list of attributes in the form of knowledge, skills, abilities (KSAs) and tasks required to perform these roles.
- **“Knowledge, Skills, and Abilities (KSAs)** are the attributes required to perform work roles and are generally demonstrated through relevant experience, education, or training” [4].
- **Tasks** are specifically defined pieces of work that, combined with other identified **Tasks**, make up the work in a specific specialty area or work role.

The second important input to the training evaluation pilot are the results of the D9.2 – SPARTA Curricula Description, which was delivered in July 2020 as a public report.

1.3 EUSurvey Tool

The EUSurvey Tool was used to conduct the training evaluation pilot. EUSurvey is the European Commission's official multilingual online survey management tool that can also be used free of charge by all European citizens. It facilitates the creation and publication of globally accessible forms, such as user satisfaction surveys, public consultations or registration forms.

EUSurvey provides a wide variety of elements used in forms, ranging from the simple (e.g. text questions and multiple-choice questions) to the advanced (e.g. editable spreadsheets and multimedia elements). It boasts a broad range of further features such as customizable forms, dependent questions, scheduled publishing, a user interface, online security, advanced privacy through anonymous form, invitations sent directly from the application, customization of the look and feel, saving of draft contributions, offline answering, enhanced contrast, uploading of supporting files and collaborative editing. Results can be displayed as histograms, percentages or in full detail and can be exported to standard spreadsheet formats for further analysis in statistical applications. They can also be published on a dedicated webpage within the application.

EUSurvey is freely available for public and private use at https://ec.europa.eu/eusurvey/ in 23 official EU languages. It is accessible by EU Login, the European Commission's authentication service.

This web application for online survey is developed and maintained by DG DIGIT, the Directorate-General for Informatics of the European Commission, within ISA program, which promotes interoperability solutions for European public administrations.

Chapter 2 Training Evaluation Pilot

2.1 Purpose

2.1.1 Questionnaire 1 - for Higher Education Program Administrators

The purpose of this questionnaire was to gain an understanding of the current programs covered by the universities that are dedicated to cybersecurity and to ascertain whether they align to the SPARTA guidelines/best practices detailed in D9.2. For the applicable programs, the goal was to capture the opinion of the universities covering SPARTA's Cybersecurity Skills Framework topics in their programs and to uncover the delivery ratio between theory and practical teachings. Moreover, the team wanted to gain the opinions of course providers on the competencies and knowledge areas they intend to transfer to students sitting the programs.

Higher Education Program Administrators answered five questions, which also included supporting questions. The analysis of the following questions allowed the development of the most important recommendations toward improvements in the trainings. All questions were compared with the students' answers - six of them were basic questions and the rest included also supporting questions

2.1.2 Questionnaire 2 - for Students

The purpose of this questionnaire was to capture the opinions of students participating in the programs provided at the university. The goals range from establishing whether the students feel the current delivery method provides the appropriate balance of practical-based vs theory-based learnings - to various matters connected to the skills and knowledge areas; including:

- The roles that they would like to start following qualification (if applicable).
- The (SPARTA) skills they believe the program provides.
- The knowledge areas they believe they will attain through the program.
- The improvements that can be gained through changes to the program structure.

2.2 Data analysis

2.2.1 Respondents structure and quantity

The questionnaires were conducted in the period from 7th November till 30th November, 2020 among 11 Higher Education Program Administrators (universities) participating in the SPARTA project which provide in total 17 programs dedicated to cybersecurity, covering SPARTA's Cybersecurity Skills Framework topics and a total of 78 students from 9 SPARTA project universities. The detailed information on survey respondents can be found in Table 1.

Table 1: Universities that participated in the questionnaires.

No.	Name of the university	Higher Education Program Administrators	Students
1	Brno University of Technology (BUT, Czech Republic)	yes	yes
2	Polytechnic Institute of Paris, Telecom SudParis (IMT, France)	yes	yes
3	Technical University of Munich (Germany)	no	yes
4	University of Bonn (UBO, Germany)	yes	yes
5	University of Milan (Italy)	yes	no
6	University of Molise (Italy)	yes	yes
7	University of Roma Tor Vergata (the CNIT Unit, Italy)	yes	yes
8	Sapienza University of Rome (Italy)	yes	yes
9	Kaunas University of Technology (KTU, Lithuania)	yes	yes
10	Mykolas Romeris University (MRU, Lithuania)	yes	yes
11	Vilnius Gediminas Technical University (Lithuania)	yes	no
12	Universidade de Lisboa (Portugal)	yes	no

Most of the students participating in the survey were from the Czech Republic (26 people, 33% of all), with a high representation of students from Italy (17 people, 21%) and Lithuania (16 people, 20%). The overall information on participants locations can be found in Figure 1.

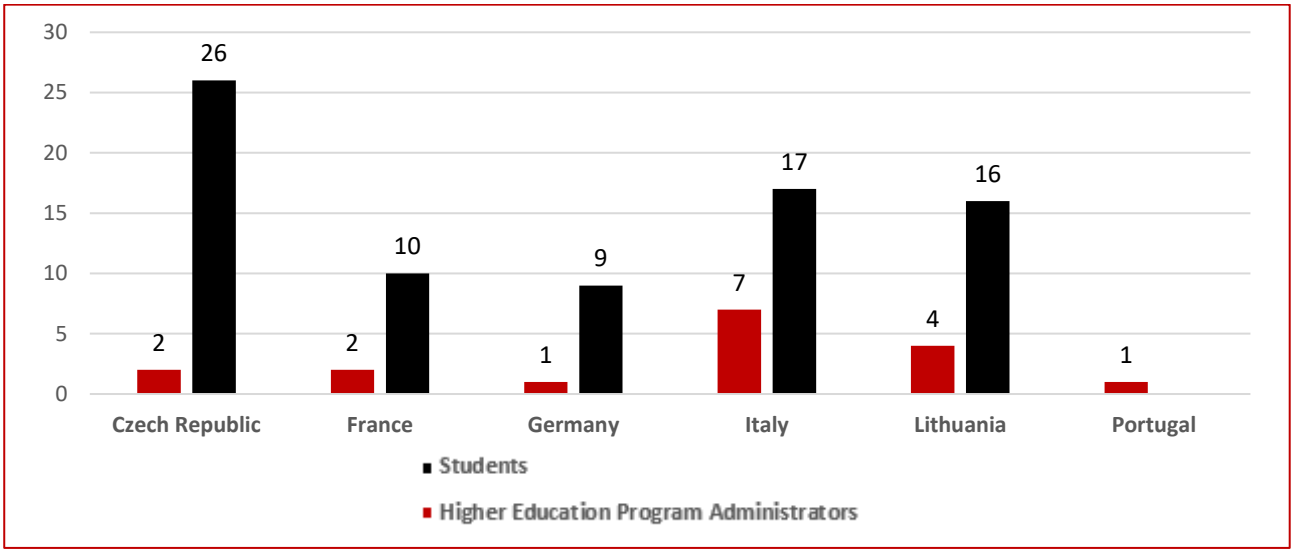


Figure 1: Analysis of university locations.

2.2.2 Cybersecurity programs offered at the SPARTA participating universities

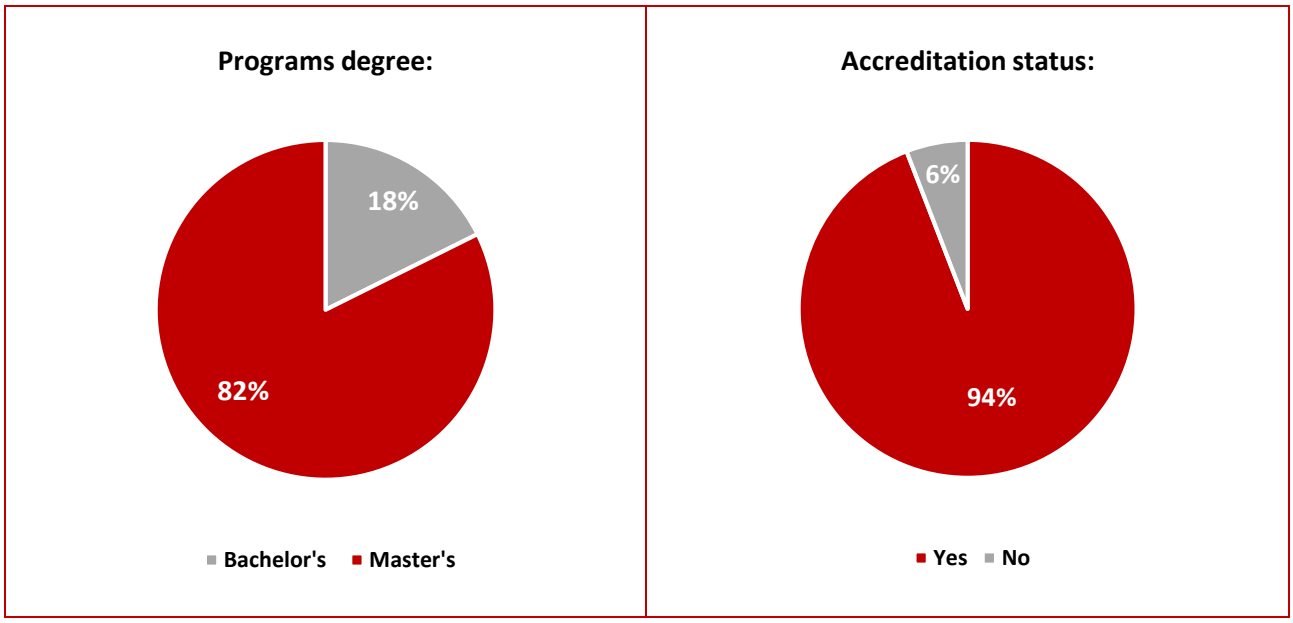


Figure 2: Cybersecurity programs degree (left side) and accreditation (right side) – Administrators' answers.

The answers provided by the Administrators' allowed identifying the following programs dedicated to cybersecurity:

- Computer Security;
- Cryptography;
- Cybersecurity;
- Cybersecurity Management;
- Cyberspace Law;
- Information Security;
- Information Systems;
- Information Technology Security;
- Malware Analysis;
- Networks and Systems Security;
- Privacy;
- Software System Security;
- Web Application Security.

Most of the programs (14 answers, 82% of all) were at the master's level, with only 18% (3 answers) accounting for bachelor's programs. Moreover, 94% (16 answers) of responders indicated the programs were officially accredited at the university. One of the Cybersecurity track (shared by two programs: Computer Engineering and Internet Engineering) at University of Roma Tor Vergata is not officially accredited at the university. The information on cybersecurity programs degree and accreditation (Administrators' answers) can be found in Figure 2.

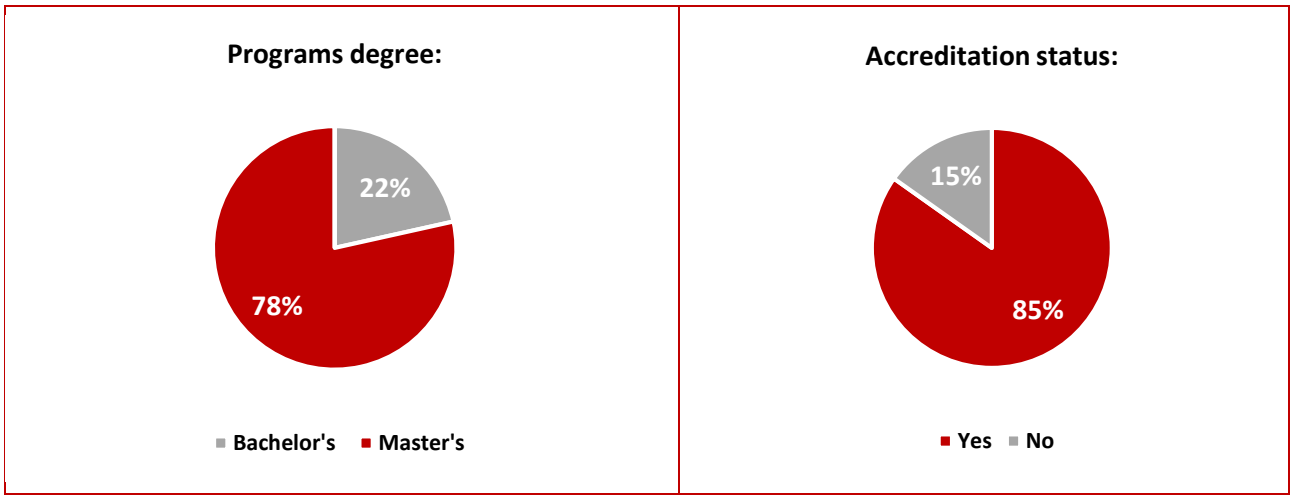


Figure 3: Cybersecurity programs degree (left side) and accreditation (right side) – students answers.

The Administrators answers go in line with the answers provided by the students. Most of them (62 cases, 78% of all respondents) are studying at the master's level and only 22% (17 cases) indicated bachelor's programs as their education level. Moreover, 85% (67 answers) of respondents indicated the programs they attend as officially accredited at the university. The information on cybersecurity programs degree and accreditation (students answers) can be found in Figure 3.

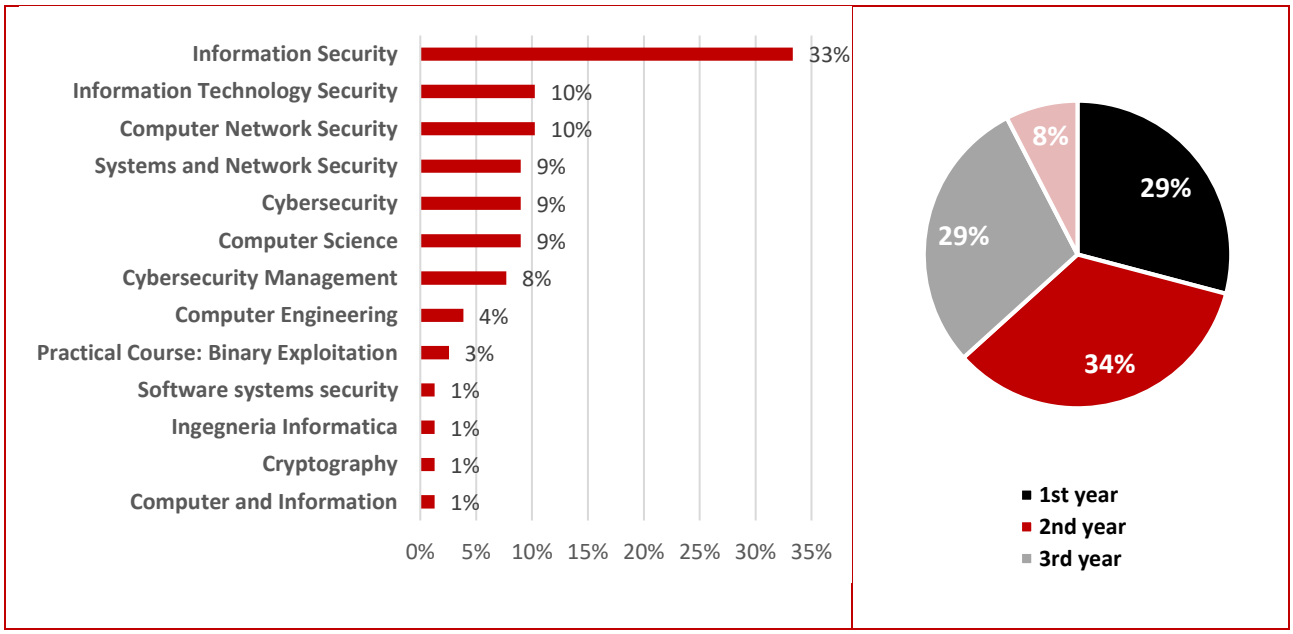


Figure 4: Programs attended by students and their level of education.

The mostly attended program identified through students questionnaire was Information Security (26 answers, 33% of all responses). Other mentioned programs included mostly Information Technology Security and Computer Network Security (8 answers, 10%), Systems and Network Security, Cybersecurity and Computer Science (7 answers, 9%) and Cybersecurity Management (6 answers, 8%). Most of the students (27 cases, 34% of all respondents) were on their 2nd year of studies, with 29% (23 cases) on 1st and 3rd years of studies. Figure 4 presents the list of programs attended by students and their level of education.

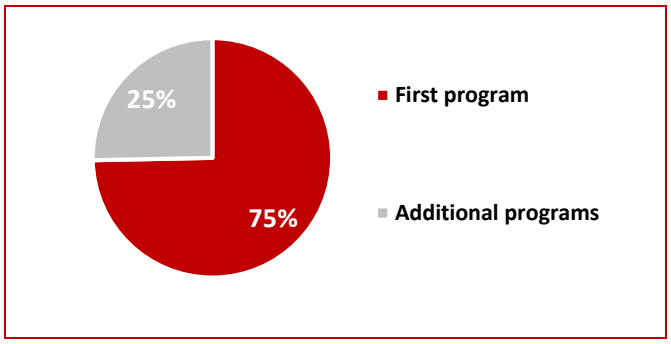


Figure 5: Students experience with other programs.

In order to deepen the results, several additional questions were asked, related to previous experience and training. As presented in Figure 5, for the vast number of students (59 answers, 75% of all respondents), the program dedicated to cybersecurity indicated in the first question is the first one they have studied. Just 25% of the students (20 cases) completed other programs in other countries and universities.

The students that have already participated in additional cybersecurity courses, indicated the following programs, countries and universities:

- Bachelor of Computer Applications (India),
- Computer Science at University of Bologna (Italy),
- Bachelor's in Computer Engineering (Italy),
- Mechanical Engineering (Germany),
- Business Informatics at Vilnius University (Lithuania),
- Bachelor's degree in Information systems at Kaunas University of Technology (Lithuania),
- Information technology Engineering at Kaunas University of Technology (Lithuania),
- Software Systems in Kaunas University of Technology (Lithuania),
- Software Systems (Lithuania),
- Computer Science (Finland),
- Bachelor of Science in Computer Science (Germany),
- First year of Master's in Computer Science (France).

2.2.3 Practical and theory-based training ratio

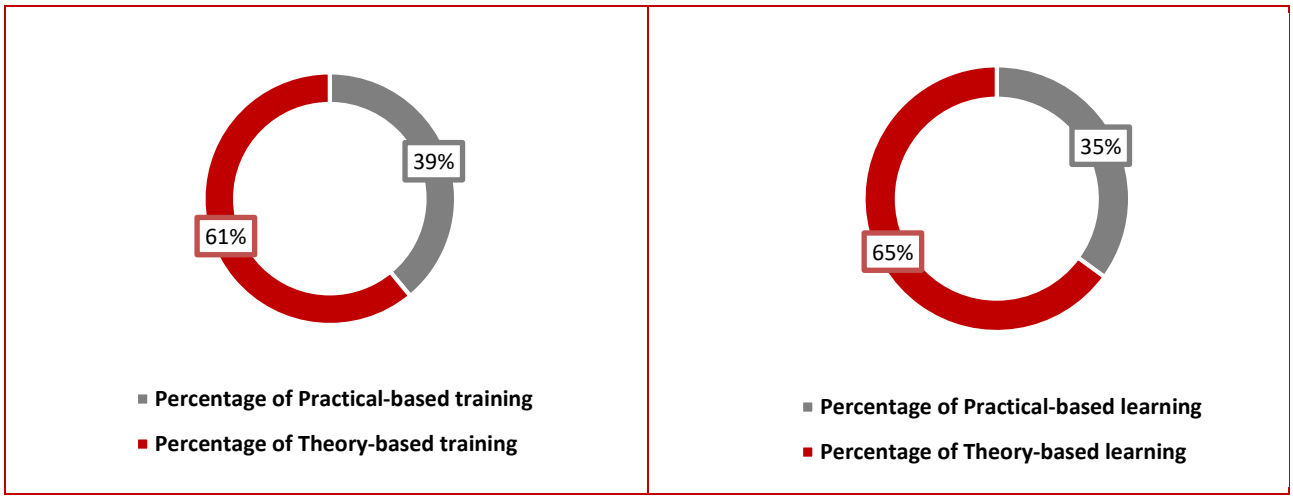


Figure 6: Practical and theory-based training ratio among Administrators' (left side) and students (right side).

The Higher Education Program Administrators and students were separately asked to estimate the ratio between theory and practice in the programs they are currently leading/attending. The average counted for both these groups of respondents shows in Figure 6 that both groups are quite compatible in their ratings, which reflects in stating that over 60% of the programs is theory based, with less than 40% focused on practice. It is important to notice that by 'practical parts of the program' we mean practice-based learning as well as practical learning in an academic setting.

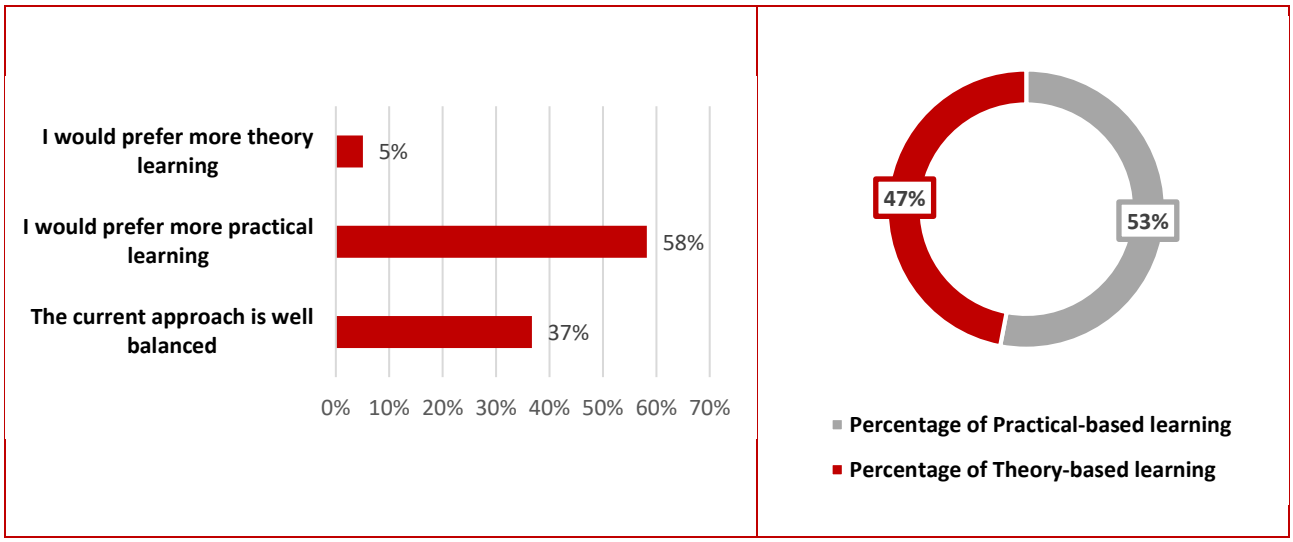
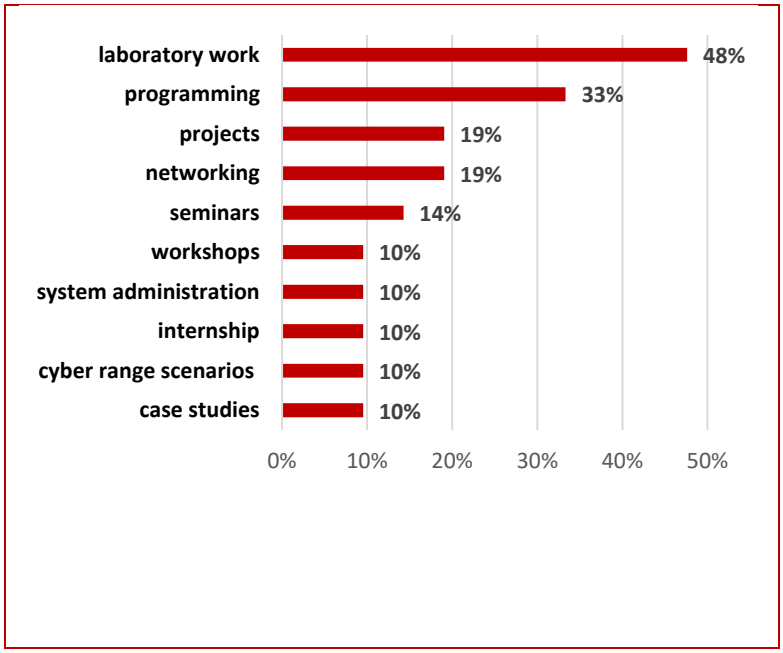


Figure 7: Practical and theory-based learning - student preferences.

To learn more about the students' opinion, we asked for their preferences about the approach to the practical and theory learning. According to a survey conducted for students, most of them expect practical parts of the programs (58% of students, 46 cases) than theory learning, which was indicated just by 5% of all (4 cases). 37% of students (29 cases) thinking that the current approach is well balanced and nothing needs to be changed. Moreover, one additional question was asked related to the preferred ratio mix. The results shows that the average of ratio mix preferences provided by students is very similar, but majority of students which is 53%, prefer practical-based learning and 47% focused on theory. It shows that both the theory and practical parts of the programs should be linked and support each other. The overall information on practical and theory-based learning from students perspective can be found in Figure 7.



In order to deepen the results, we asked the Administrators about the practical techniques they use and the results can be found in Figure 8. 48% of providers (10 respondents) indicated laboratory work as a part of its program. Not much less, 33% of all (7 respondents) uses programming and 19% (4 respondents) pointed out projects and networking. The following techniques were also indicated among the answers: cyberattack modeling, discussions, ethical hacking, forensic, games, practical exercises in virtual environments, presentations, reverse engineering, risk assessment (using special tools), simulation, teamwork, working with hardware.

Figure 8: Practical techniques used by Administrators.

Regarding the students' preferences, we asked about the techniques they would like to use in their program. The most frequently indicated answers were laboratory work (23 cases, 45% of all answers), then programming (12 cases, 24% of answers), so very similar to the answers indicated

by administrators. The students have also provided other techniques that could be used in the program:

- more kind of hacking/vulnerability searching;
- practical trainings/studies at companies, in the field work etc.;
- introduce with more hardware units and software programs in cybersecurity;
- system architecture, database systems, penetration testing;
- ethical hacking;
- something like an Internship (it would be a good way to learn something in practice);
- laboratories based on real topics - combined with external authorities such as ICT company;
- lectures, reverse engineering, software setup & management;
- more short projects, which force students to think about stuff which they are learning;
- more Active Directory / Windows penetration testing lessons;
- data analysis.

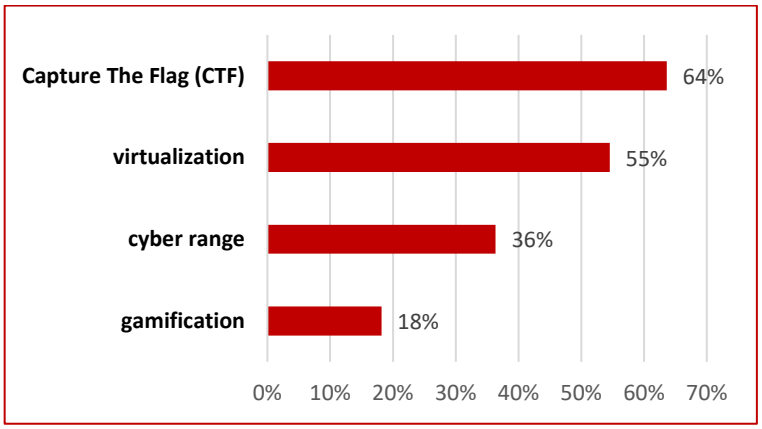
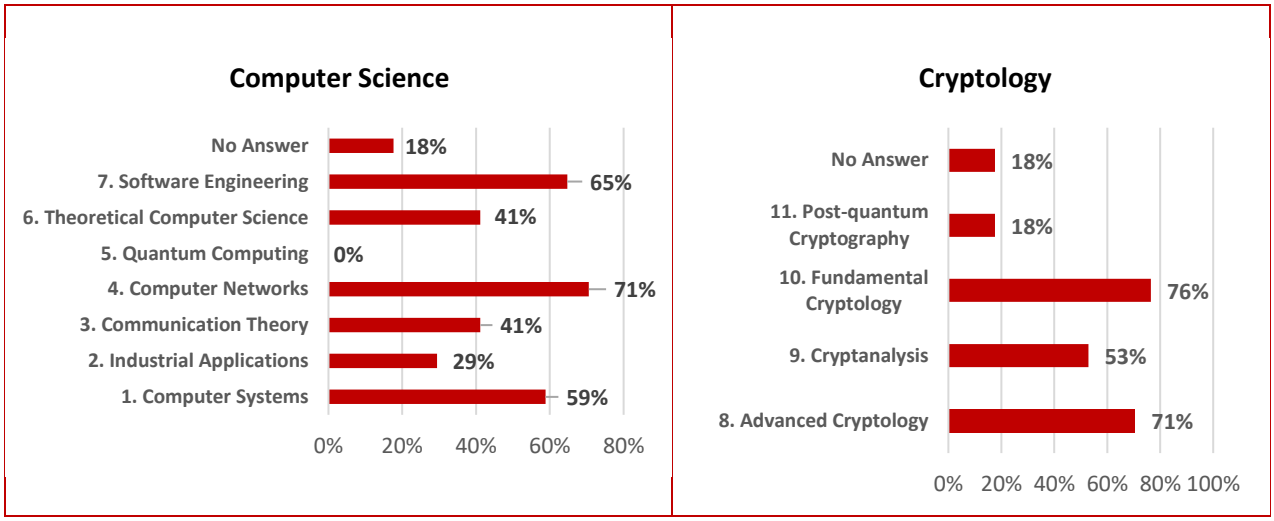


Figure 9: Modern technologies used by Administrators.

Among the modern technologies for training the Administrators use were indicated: ad-hoc samples for training, Cisco, distance learning, ethical hacking, specialized Linux distros, virtual networks, VMware. The answers that have appeared more than once can be found in Figure 9. The most frequency answer, indicated by 64% of the Administrators (7 cases) was Capture The Flag (CTF) event, one way of cybersecurity training. 55% of all so 6 cases use the visualization and 36% of them (4 cases) cyber range technique.

2.2.4 Cybersecurity topic covered at the SPARTA participating universities



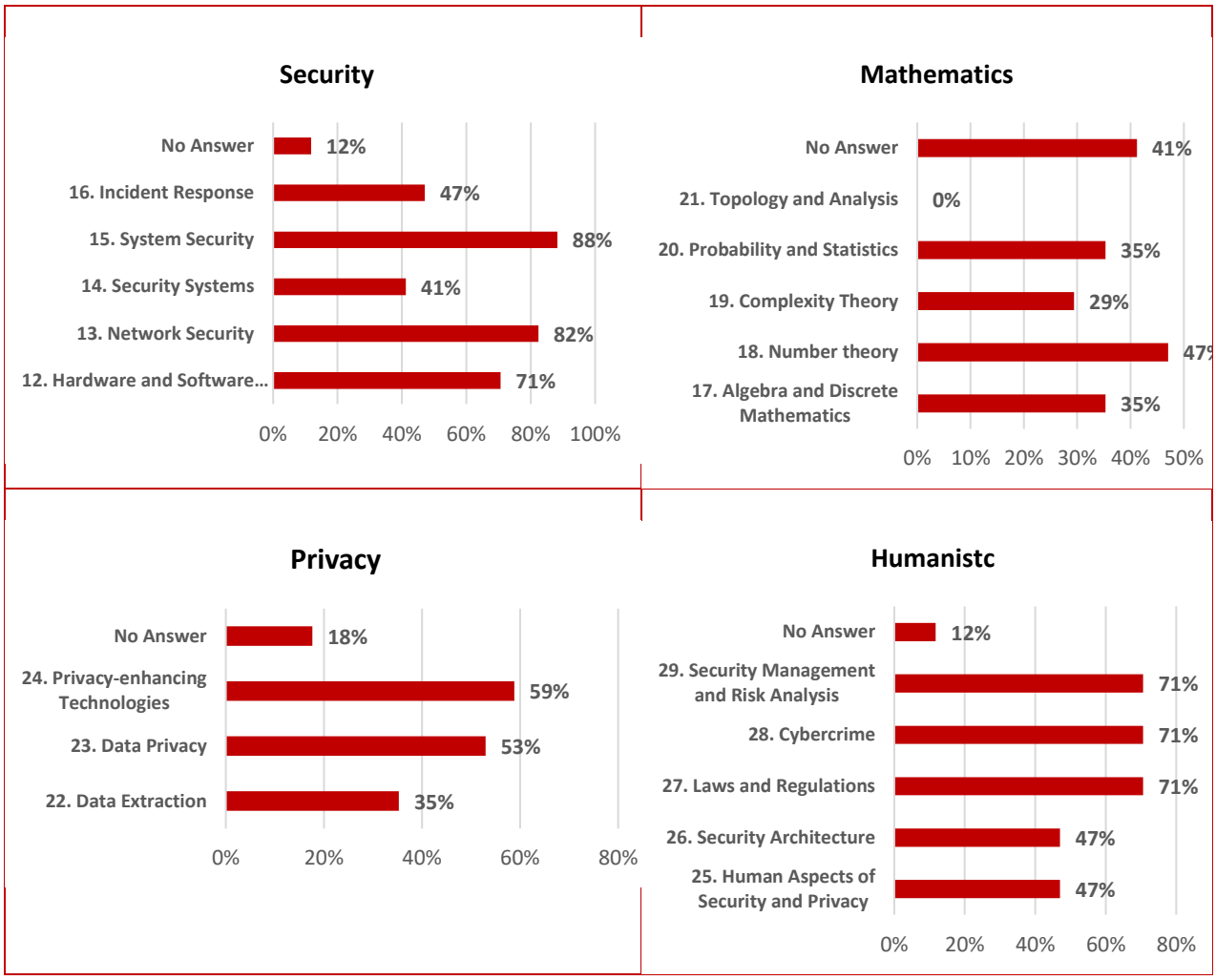


Figure 10: SPARTA topics covered by pilot programs.

The Administrators were asked to indicate the SPARTA topics their program covers. The result of this answers can found in Figure 10. SPARTA topics include all subjects required to get individuals ready to enter the professional workforce. The list of topics shows the most relevant areas and sub-areas of interest in cybersecurity. This list was created taking into account the existing curricula guidelines and, in particular, the deliverable D9.1 where the list of competencies of NICE framework were identified as the most detailed cybersecurity taxonomy. During the creation of this list, 6 areas of main relevance were identified and each topic has been assigned to the belonging area: Computer Science, Cryptology, Humanistic and Social Science, Mathematics, Privacy and Security. The list of topics with a brief description of each of them is shown in Appendix 1.

It is worth noting that any Administrator indicated the Quantum computing as a topic their program covers. It means that the main topics: tensor-product, entanglement, qubits, Grover's search algorithm, Shor's algorithm and quantum secret key distribution are lacking in the curriculum. Also Topology and Analysis topic in the area of Mathematics need to be taken into account as missing.

To synchronize the information from the Administrators with the responses from the students, we asked about the topic would they like to study more of. Among the answers there were only four topics mentioned:

- Interface between Humans and Artificial Intelligence;
- Modern secure networking and in-depth analytics of systems communications;
- Mathematics;
- Theoretical Computer Science (Currently shown as 41% by the administrators).

Table 2: Topics covered by SPARTA programs – students responses.

	I feel I have already covered this topic	We are planning to cover this topic later in the program	My program does not cover this topic
COMPUTER SCIENCE			
1. Computer Systems	**76%**	15%	10%
2. Industrial Applications	20%	15%	**66%**
3. Communication Theory	**72%**	11%	19%
4. Computer Networks	**86%**	9%	5%
5. Quantum Computing	9%	8%	**85%**
6. Theoretical Computer Science	**53%**	24%	25%
7. Software Engineering	**48%**	27%	29%
CRYPTOLOGY			
8. Advanced Cryptology	**44%**	33%	25%
9. Cryptanalysis	**48%**	25%	29%
10. Fundamental Cryptology	**76%**	13%	15%
11. Post-quantum Cryptography	11%	14%	**80%**
SECURITY			
12. Hardware and Software Security	**53%**	27%	24%
13. Network Security	**77%**	18%	5%
14. Security Systems	**58%**	24%	20%
15. System Security	**63%**	27%	13%
16. Incident Response	34%	18%	**51%**
MATHEMATICS			
17. Algebra and Discrete Mathematics	**70%**	3%	28%
18. Number theory	**54%**	10%	38%
19. Complexity Theory	**53%**	9%	39%
20. Probability and Statistics	65%	9%	27%
21. Topology and Analysis	43%	6%	**51%**
PRIVACY			
22. Data Extraction	34%	25%	**46%**
23. Data Privacy	**46%**	18%	38%
24. Privacy-enhancing Technologies	33%	24%	**46%**
HUMANISTIC			
25. Human Aspects of Security and Privacy	**47%**	13%	42%
26. Security Architecture	**46%**	18%	38%
27. Laws and Regulations	**62%**	9%	30%
28. Cybercrime	**49%**	23%	30%
29. Security Management and Risk Analysis	**52%**	16%	34%

Moreover, the students selected the topics their current program covers and the statement that best matches their feeling. The results of this can be found in Table 2. As we can see, there are a few topics which the students feel are not covered by the program. In the area of computer science, 85% of the responses (67 answers) apply the topic Quantum Computing and 66% (52 answers) Industrial Applications. In the Cryptology area 80% (63 answers) of students mentioned Post-quantum Cryptography topic. Almost half of the students (40 answers) think that Incident Response in the area of Security and Topology and Analysis in the area of Mathematics are the biggest gaps. 46% of the responses (36 answers) were obtained for Data Extraction and Privacy-enhancing Technologies in the area of Privacy.

2.2.5 Work roles that most suit program structure and syllabus

The next part of the document was dedicated to the work roles. The structure of work roles of the SPARTA CS Framework in most cases remains unchanged compared to the NICE Framework (NIST Special Publication 800-181). Work roles in the framework are mapped with Knowledge, Skills and Abilities. Appendix 2 provides a description of each of the work roles.

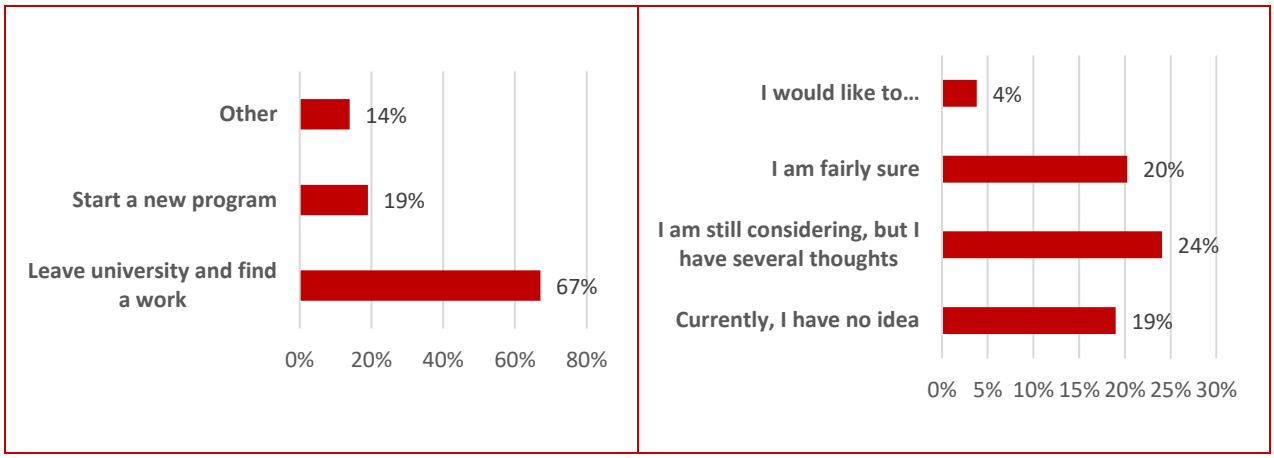


Figure 11: Students future plans (left side) and work roles they want to apply for (right side).

In the survey, we asked students about their future plans after completing their current studies and the next steps that best represents their current feelings. As Figure 11 shows, 67% of them (53 of all students) would like to leave university and find a work and 19% (15 of all students) would like to start a new program. 14% so 10 of them selected the other one option.

Moreover, it turned out that students do not know what work role they will apply for, it is almost 19% of students (15 answers). 24% of them (19 answers) is still considering and 20% of students is (so 16 answers) fairly sure. What is important, 33% students (26 of them) participating in the survey did not respond because they did not chose the answer about leavening the university and finding a work in the previous question.

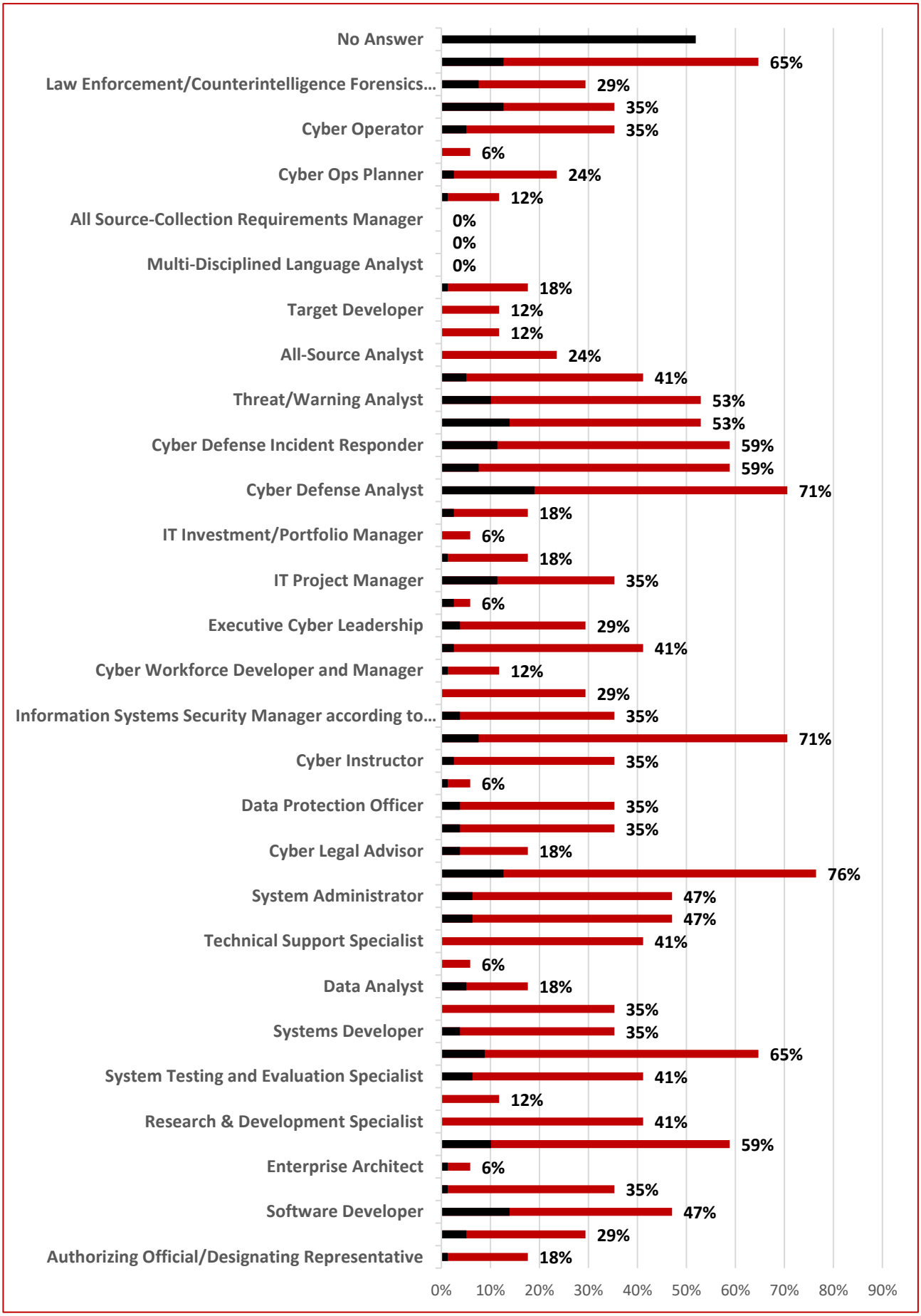
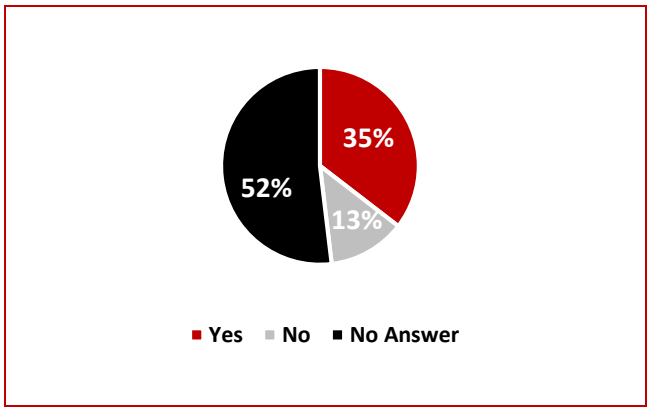


Figure 12: Work roles supported by current SPARTA programs.

Figure 12 presents data analysis about the work roles that most suit the current program structure and syllabus at the universities provided by the Higher Education Program Administrators, compared with the students' answers about the work role they would like to apply the most. 76% of providers (13 answers) pointed out Systems Security Analyst and compared this with to the student answers only 13% of them (10 people) would like to work in this profession. A little less so 71% of all administrators (per 12 answers) indicated a work roles Information Systems Security Manager and Cyber Defense Analyst as the most suit the current program structure at their university. In the students' responses, these work roles were given successively 8% (6answers) and 19% (15 answers). Both the Higher Education Program Administrators and students did not indicate Multi-Disciplined Language Analyst, All Source-Collection Manager and All Source-Collection Requirements Manager work roles.

2.2.6 NICE Competence in the future role



To deepen the previous results with the students feelings, we asked about the competences in their current programs that can be necessary in their possible future role and the results can be found in Figure 13. Just 35% of students (28 answers) think that their current program matches to possible future work. This question was only given to students who are sure of their future role so this 52% of no answer is the result no response to earlier.

Figure 13: SPARTA programs future work adjustment.

In the survey for the Administrators we asked about missing learning paths the NICE competencies that will enable students to fill three key entry-level roles that were highlighted in previous SPARTA deliverables: **Technical Support Specialist, Cyber Defense Incident Responder** and **Cyber Defense Forensics Analyst.**

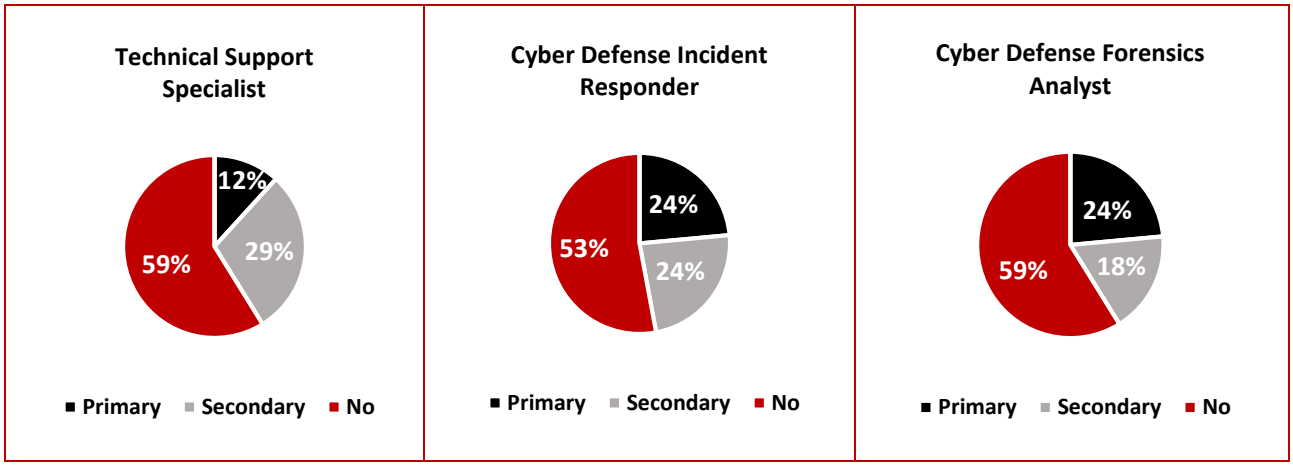


Figure 14: NICE competencies entry level roles coverage.

Figure 14 shows that the most of the Administrators (10 answers, 59% of all respondents) indicated **Technical Support Specialist** as a work role not supported by their program. Technical Support Specialist provides support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable). Regarding **Cyber Defense Incident Responder**, 53% of all respondents (9 answers) indicated that this work role is not supported by their program. Cyber Defense Incident Responder investigates, analyzes, and responds to cyber

incidents within the network environment or enclave. The most of the Administrators (10 answers, 59% of all respondents), indicated that **Cyber Defense Forensics Analyst** work role is not supported by their program. Cyber Defense Forensics Analyst analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

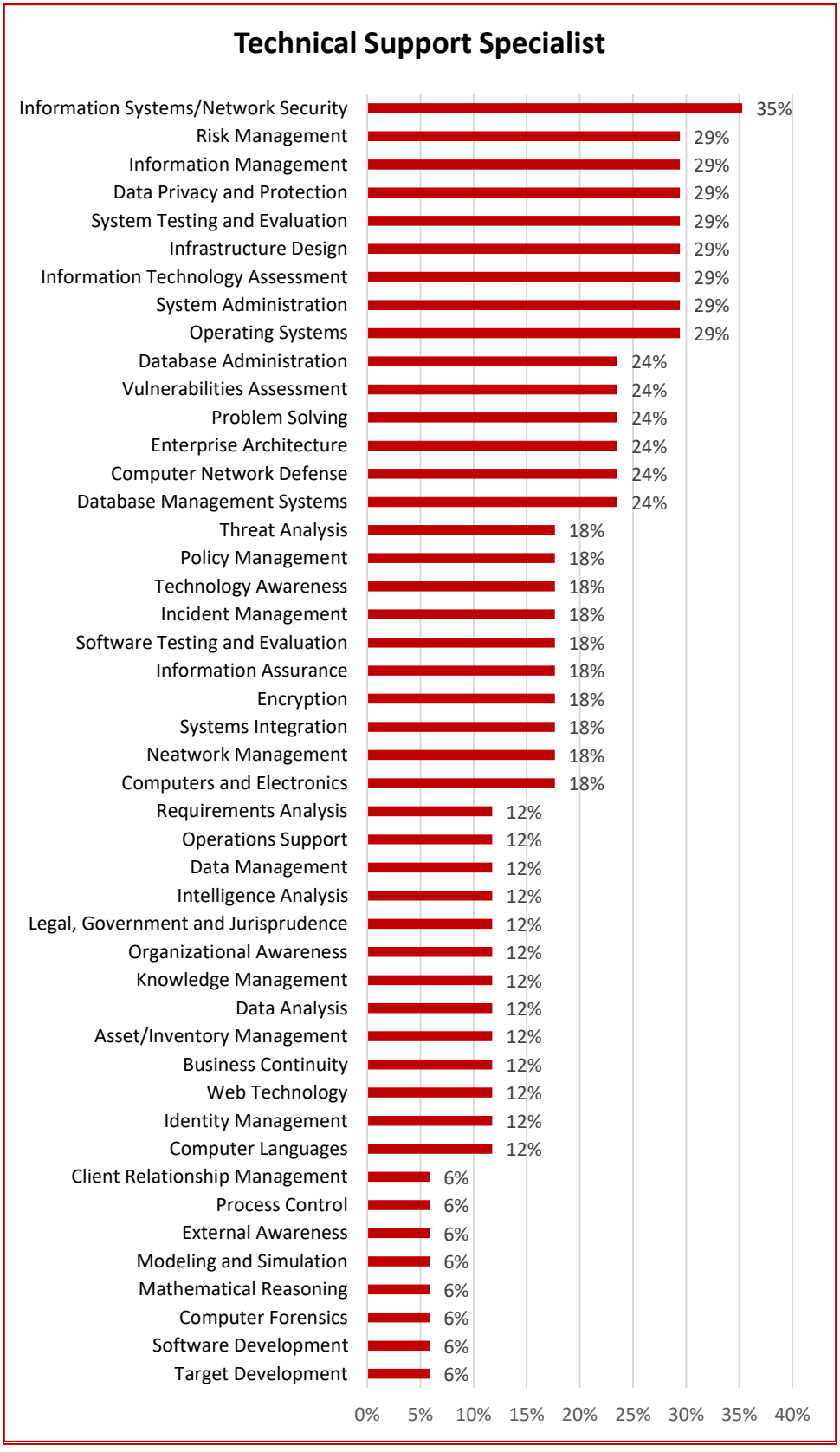


Figure 15: Technical Support Specialist priority competences.

Figure 15 presented NICE competences that need to be covered in order to become a Technical Support Specialist, the most frequently chosen answer was Information System/Network Security (6 answers, 35% of all). This skill enables students to implement, maintain, and improve established network security practices.

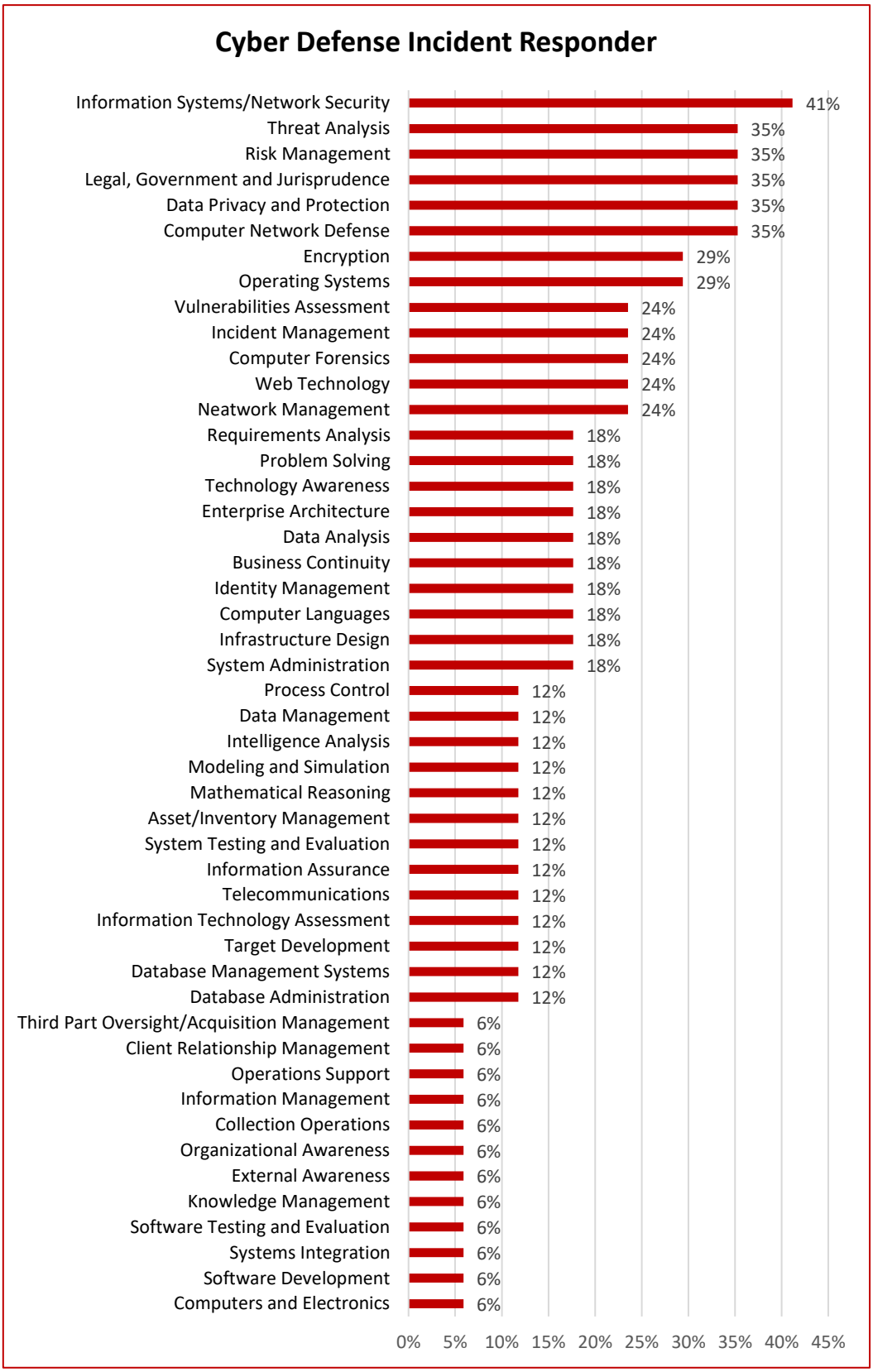


Figure 16: Cyber Defense Incident Responder priority competences.

Figure 16 presented NICE competences that need to be covered in order to become a Cyber Defense Incident Responder, the most frequently chosen answer was Information System/Network Security (7 answers, 41% of all).

Figure 17: Cyber Defense Forensics Analyst priority competences.

Figure 17 presented NICE competences that need to be covered in order to become a Cyber Defense Forensics Analyst, the most frequently chosen answer was Computer Forensics (6 answers, 35% of all). Thanks to this skill the student is capable to collect, process, preserve, analyze,

and present computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

It is worth highlighting that the results from the survey show that that none of these roles are a primary focus for the universities; which strengthens the recommendation that more emphasis and preparation on work roles should be considered. The involvement of industry and perhaps the organization of work placements could also benefit this discussion.

2.2.7 Novel trends in security and changes to the SPARTA university programs.

In the open question about the novel trends in security that university programs covers, the most frequently indicated answers were blockchain, then post quantum cryptography, privacy by design and privacy enhancing technologies. Among the other indicated novel trends in security were:

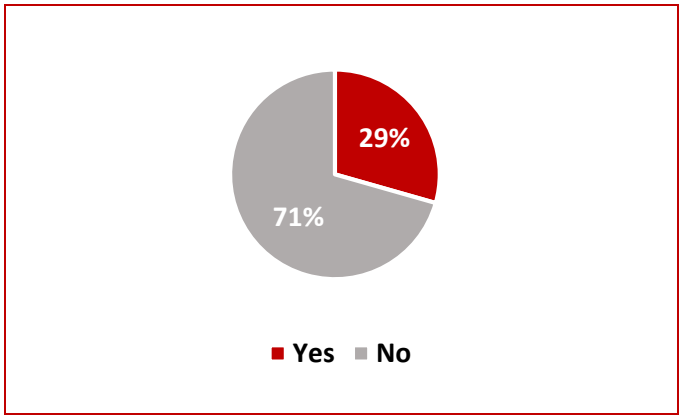
- lightweight cryptography, hardware acceleration;
- advanced obfuscation and evasion techniques'
- encryption with authentication;
- secure computation;
- secure software development programming, tools and techniques;
- secure organizational systems architecture;
- usable security and privacy on the large scale;
- malware analysis;
- artificial intelligence methods;
- privacy by testing and default;
- provable and hardware security;
- electromagnetic side channel analysis;
- localization security;
- micro architectural transient execution attacks;
- wireless sensor networks;
- cybersecurity risk management (ISO 27701);
- software analytics for cybersecurity;
- semantic intelligence for cybersecurity;
- security by design;
- biometric systems and less-constrained biometrics.
- emerging scenarios (cloud/fog/edge computing, data market).

What needs to be emphasized is that only one Higher Education Program Administrator remarked that no changes are expected. Three of the answers are related to legislation, roughly five or six are targeting more practical and advanced training. Among the most important changes on the horizon, the Administrators indicated:

- separate course on legislation and compliance;
- stronger involvement of remotely accessible cyber ranges;
- improvement in the area of security/risk management and governance (space and teachers for this are crucial);
- more Windows hands-on;
- more legal awareness;
- more data analysis applied to cybersecurity operations;
- introduction of more practical subjects (laboratory), more detailed teaching of network architecture;
- additional courses on program analysis and formal methods for cybersecurity;
- shift toward Linux and IoT based malware.

2.2.8 SPARTA Curricula Designer Tool

In the survey for the Administrators we also asked about the SPARTA Curricula Designer Tool software that makes it possible for universities to adapt and build their own customized study programs in cybersecurity and evaluate their validity with respect to the requirements of specific cybersecurity work roles.



Most of the Higher Education Program Administrators (12 of 17 answers, 71% of all respondents) have not used the Curricula Designer as shown in Figure 18. For the 5 providers that are using the SPARTA Curricula Designer Tool, we asked which work roles are supported. The work roles supported from the tool can be found in Table 3.

Figure 18: Curricula Designer Tool usage.

Table 3: Work roles supported from the Curricula Designer.

Work roles	Telecom SudParis		No. of student would like to apply for this work roles	Brno University of Technology	No. of student would like to apply for this work roles
Cyber Defense Forensics Analyst	yes		1	no	3
Law Enforcement/ Counterintelligence Forensics Analyst	no		1	no	3
Cyber Crime Investigator	yes		1	no	1
Cyber Operator	yes		1	no	1
Partner Integration Planner	yes		0	yes	0
Cyber Ops Planner	yes		1	no	0
Cyber Intel Planner	yes		1	no	0
All Source-Collection Requirements Manager	yes		0	yes	0
All Source-Collection Manager	yes		0	no	0
Multi-Disciplined Language Analyst	yes		0	no	0
Target Network Analyst	yes		0	no	0
Target Developer	yes		0	no	0
Mission Assessment Specialist	yes		0	no	0
All-Source Analyst	yes		0	no	0
Exploitation Analyst	yes		2	no	0
Threat/Warning Analyst	yes		1	no	2
Vulnerability Assessment Analyst	yes		4	no	2
Cyber Defense Incident Responder	yes		1	no	1
Cyber Defense Infrastructure Support Specialist	yes		1	no	2
Cyber Defense Analyst	yes		3	no	2
IT Program Auditor	yes		1	yes	1
IT Investment/Portfolio Manager	yes		0	yes	0

Work roles	Telecom SudParis		No. of student would like to apply for this work roles	Brno University of Technology	No. of student would like to apply for this work roles
Product Support Manager	yes		0	no	0
IT Project Manager	yes		1	yes	4
Program Manager	yes		0	yes	
Executive Cyber Leadership	yes		0	yes	1
Cyber Policy and Strategy Planner	yes		0	yes	0
Cyber Workforce Developer and Manager	yes		1	yes	0
Communications Security (COMSEC) Manager	yes		0	no	0
Information Systems Security Manager according to EU Member State legislation	no		0	no	1
Information Systems Security Manager	yes		1	no	0
Cyber Instructor	yes		0	no	0
Cyber Instructional Curriculum Developer	yes		0	yes	0
Privacy Officer/Privacy Compliance Manager	yes		0	no	0
Cyber Legal Advisor	yes		1	no	0
Systems Security Analyst	yes		0	yes	3
System Administrator	yes		2	no	1
Network Operations Specialist	yes		1	yes	1
Technical Support Specialist	yes		0	no	0
Knowledge Manager	yes		0	yes	0
Data Analyst	yes		0	yes	1
Database Administrator	yes		0	yes	0
Systems Developer	yes		0	yes	1
Information Systems Security Developer	yes		1	yes	2
System Testing and Evaluation Specialist	yes		0	yes	4
Systems Requirements Planner	yes		0	yes	0
Research & Development Specialist	yes		0	no	0
Security Architect	yes		3	yes	1
Enterprise Architect	yes		0	yes	0
Secure Software Assessor	yes		0	no	0
Software Developer	yes		1	no	5
Security Control Assessor	yes		1	no	0
Authorizing Official/Designating Representative	yes		0	yes	0

Just two universities indicated work roles from the Curricula Designer. The Table 3 shows the supported work roles; plus the number of students from these universities that would like to apply to the roles. This table also highlights the work roles that the students want to apply for but are not covered by the universities curriculums. For example, Law Enforcement/Counterintelligence Forensics Analyst.

Chapter 3 Recommendations

The analysis of the data, coming from the Administrators and the students, collected through D9.3 Survey, allowed emphasizing a number of recommendations, coming from evaluating the pilot SPARTA programs. They present as follows:

1. A higher focus on practical-based training is expected – the questionnaire responses hinted at the need to shift the focus to cybersecurity practice and to try to make the theory/practice ratio resemble a 50/50 approach. This should be taken into account by the Administrators when designing new SPARTA programs;
2. Additional cybersecurity topics need to be covered by SPARTA programs – the responses collected while evaluating the pilot showed that there is a need to include certain topics in the SPARTA programs, which mostly relates to areas of computer science (quantum computing, industrial applications), cryptology (post-quantum cryptography), security (incident response), mathematics (topology, analysis) and privacy (data extraction and privacy-enhancing technologies).
3. It is advised to include the NICE learning paths allowing the students to fill the key entry-level roles related to Technical Support Specialist, Cyber Defense Incident Responder and Cyber Defense Forensics Analyst. The survey outcomes show that most of the students felt that these paths are not covered by the current programs;
4. Covering topic changes suggested by the Administrators is recommended – the Administrators participating in the evaluation noticed that certain changes need to be made in order to follow the novel trends in cybersecurity (as described in section 2.2.7);
5. The SPARTA Curricula Designer Tool requires awareness actions – more than 70% of Higher Education Program Administrators taking part in the evaluation admitted to not using the Tool for the purposes of designing their courses. A dissemination and promotion actions for the Tool may help in spreading the software among designers.

The recommendations go in line with the students responses collected through the survey and presented in Table 4[1].

Table 4: Students recommendations.

Number	Rough Category	Quantity	Percentage of Total
1	**More Practical Training Exercises**	10	20%
2	**University / Teacher Changes (Identified problems with current procedures, processes, lecturers, courses, etc.)**	10	20%
3	**Less Work / Consolidation of Topics**	2	4%
4	**No Changes Required**	3	6%
5	**Humanistic & Management Topics**	1	2%
6	**More Exams**	1	2%
7	**Topic Changes**	11	22%
8	**Law Related Improvements**	1	2%
9	**Work Placement**	2	4%
10	**More Theoretical Training**	1	2%
11	**Real-life Use Cases**	8	16%
	Total	**50**	**100%**

[1] The individual responses that the students provided were roughly categorized, and each response from the student has been attributed on or more of the categories. The specific responses have been excluded to protect the privacy of the students.

Chapter 4 Summary and Conclusion

The questionnaires provided a plethora of information regarding the programs and the skills and knowledge areas covered. Due to the higher level of participation from students in the Czech Republic and Italy, the results cannot be viewed as representative; however, they do provide some interesting trends. The size of the dataset is limited because this is a tool that is being piloted in this project and not a large study on the topic. The purpose of this deliverable was summarizing the recommendations from trainees. Thus, we recommend that other Universities use the survey, or a similar one, with their own students to gain more accurate results. Moreover, it would be interesting to compare different universities within a country to highlight cultural changes or teaching approaches that may need adjustment. Besides, the qualitative feedback from the students highlighted that certain changes could be considered within specific universities/departments.

One of the most noticeable results was that students would prefer a more practical approach to the programs. Also, the question of practical-based and theory-based ratio showed a marginal difference of opinion between Administrators and Students regarding the actual level of practical training provided. Moreover, the qualitative responses from students also highlighted a need for a higher portion of real-life examples and use cases. Likewise, students commented that some of the individual topics of the programs could be changed to provide greater value and more appropriate and relevant studies. Thus, these three changes could be tackled in unison to make the changes more efficient. Furthermore, using the feedback and opinions of students could help to deliver more effective change. For reference, the topics that were most frequently highlighted for deeper learning were:

- Interface between Humans and Artificial Intelligence;
- Modern secure networking and in-depth analytics of systems communications;
- Mathematics;
- Theoretical Computer Science.

When reviewing the questions related to the topics currently covered. It is also observable that cutting edge topics such as quantum computing and post quantum are not covered by the majority of universities or at the level expected by the students. Other topics distinguished from the rest because of the higher numbers were Incident Response and Industrial Applications. As these topics are pertinent to private industry, they could better prepare students for future work, which is the most recognized step following the end of the current course. Besides, a large number of students were unsure of the role they will apply for following study. Therefore, cooperation between the students and the universities to better prepare for work roles would be recommended. Importantly, the students who do have several ideas, favor certain roles that include: Systems Security Analyst, Cyber Defense Analyst and Cyber Defense Forensic Analyst. It is worth highlighting that the three roles that have been highlighted by SPARTA as entry-level positions that could be followed by students are: **Technical Support Specialist, Cyber Defense Incident Responder** and **Cyber Defense Forensics Analyst**. However, the results from the survey show that none of these roles are a primary focus for the universities; which strengthens the recommendation that more emphasis and preparation on work roles should be considered. The involvement of industry and perhaps the organization of work placements could also benefit this discussion.

Finally, it should also be noted that many of the changes on the horizon for universities match the requirements and requests from students. However, the current dataset – being rather small – could be impacting this result; therefore, our first recommendation of local editions of a survey would be the preferred course of action before the changes are made.

Chapter 5 List of Abbreviations

Abbreviation	Translation
CTF	Capture The Flag
COVID-19	Coronavirus Disease
CSF	Cybersecurity Skills Framework
DG DIGIT	Directorate-General for Informatics of the European Commission
EU	European Commission
EU	European Union
ISA	International Studies Abroad
KSAs	Knowledge, Skills and Abilities
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
SPARTA	Strategic Programs for Advanced Research and Technology in Europe
WP	Work Package

Chapter 6 Bibliography

[1] Questionnaire for Higher Education Program Administrators https://ec.europa.eu/eusurvey/runner/SPARTASurvey2020_HigherEducationProgramAdministrators

[2] Questionnaire for Students https://ec.europa.eu/eusurvey/runner/SPARTASurvey2020_Students

[3] SPARTA. D9.1 - Cybersecurity skills framework https://www.sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf

[4] NIST. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, May 19, 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

[5] SPARTA. D9.2 - Curricula Descriptions https://www.sparta.eu/assets/deliverables/SPARTA-D9.2-Curricula-descriptions-PU-M18.pdf

Appendix 1 List of topics

Computer Science	
Industrial Applications	This topic studies measurement and control technologies, robotics and automation in industrial networks. This topic includes communication protocols and technologies such as ZigBee, Bluetooth, PLC, HAPS, and RFID which are also closely related to SCADA, Smart Factories, Smart Cities, Smart Grid and Smart Industry ecosystems.
Communication Theory	Communication theory studies principles and methods by which the information is transmitted. The topic covers information theory (Shannon theory, entropy), information source and discrete communication systems. In particular, description of data and signal structures, transmission and modulation methods, redundancy reducing and signal processing are provided.
Computer Networks	This topic studies the structure of the computer networks and communication protocols. The main topics are network protocol models (ISO/OSI, TCP/IP), routing, switching, network services (NAT, DHCP, DNS), wireless and mobile networks (Wi-Fi, GSM, LTE, 5G), database and web services.
Quantum computing	Quantum computing studies the main algorithms that can be run in a quantum computer. Main topics: Tensor-product, entanglement, qubits, Grover's search algorithm, Shor's algorithm, and quantum secret key distribution.
Theoretical Computer Science	This topic studies how to develop efficiently an algorithm with the required specifications. Examples of algorithms treated in this topic are: sorting numbers, parallel and sequential algorithms, distributed algorithms, optimization, and genetic algorithms. Data structures such as arrays, records and objects are also introduced.
Software Engineering	This topic covers technical notions related to programming languages, compilation and runtime execution of the software as well as methodological aspects (continuous integration, tools, etc.)
Computer Systems	This topics covers operating systems and their applications. In particular, this topic focuses on upkeep, configuration, and reliability of the set of integrated devices that input, output, process, and store data.
Cryptology	
Advanced Cryptology	This topic focuses on modern cryptographic protocols and technologies, i.e. cryptocurrency (e.g., bitcoins and Etherium), elliptic curve cryptography (e.g., EC Diffie- Hellman protocol, Boneh and Franklin's IBE Scheme and the MOV attack), secure multi- party computation, secret sharing, homomorphic encryption and searchable encryption.
Cryptanalysis	This topic studies the properties of a cryptographic protocol such as indistinguishability or unforgeability, and the possible attacks that a protocol can receive as chosen ciphertext-attack or man in the middle attack.
Fundamental Cryptology	Basic background in cryptology: history of cryptology (e.g., Cesar cipher and Vigenere cipher), symmetric and asymmetric cryptography (stream and block ciphers, certificates, PKI), authentication, authorization, and pseudo-random number generators.
Post-quantum Cryptography	This topic studies that kind of cryptographic protocols which are secure against a quantum computer. Main topics are: lattice-based cryptography (e.g., SVP, CVP, SIVP, LWE and R-LWE problems), multivariate cryptography (i.e., asymmetric cryptography based on non-linear multivariate polynomials over finite fields) and coding theory (e.g., linear codes, parity-check matrices, and syndrome decoding tables).
Humanistic and Social Science	
Cybercrime	Cybercrime revises the literature in computer crime, in particular, it focuses on computer misuse, data protection, criminal damage, software privacy, forgery, and investigative powers which lead to expansion of the internet, pornography, unsuitable material, and social engineering.
Human Aspects of Security and Privacy	This topic studies the cultural, societal, political, psychological, and ethical implications of information security and privacy. For example, how to develop approaches that ensure that individuals make informed decisions about security and privacy.

Security Architecture	Study the design and implementation of security architectures, i.e. analyze governance, risk and compliance issues related to architectures and see how organizations manage their security policies.
Laws and Regulations	This topic covers the laws and regulations both at the national and the international levels.
Security Management and Risk Analysis	This topic focuses on the identification of organization's assets and, therefore, the implementation of policies and procedures for protecting these assets. It also considers law regulations, obligations and liabilities between private parties, and the implications of government regulations for corporate risk management.
Mathematics	
Algebra and Discrete Mathematics	Algebra studies the basic algebraic structures such as groups (and congruence), rings and fields (in particular, finite fields); with a focus on irreducible polynomials over finite fields, extensions and Galois theory. Discrete mathematics studies discrete (non- continuous) structures such as partially ordered sets, graphs and codes; and deals with counting over these finite structures, e.g. methods of counting, principle of inclusion and exclusion and integer partitions.
Complexity Theory	Complexity theory is the study of the complexity of problems and algorithms. In particular, this topic defines algorithms, Turing machines, and the concept of computational hardness. The classification of decision problem (e.g., P, NP, NP-complete) is also presented.
Number Theory	Number theory studies integers, in particular, prime numbers, primality tests and factorization considering the complexity of the studied algorithms. More in specific, Diophantine equations, elliptic curves, binary quadratic forms and quadratic number fields are also considered.
Probability and Statistics	Probability focuses on random variables, distributions and density functions. This topic also deals with stochastic processes, probabilistic methods used to model systems, method of conditioning and Markov chain. Statistics deals with the collection and the analysis of data. Its main methods are parametric estimation, hypothesis testing and regression analysis. It also deals with multivariate analyses such as data exploration, modeling and inference.

Appendix 2 Description of each of the work roles

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
Securely Provision (SP)	Risk Management (RSK)	Authorizing Official/Designating Representative	SP-RSK-001	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009).
		Security Control Assessor	SP-RSK-002	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).
	Software Development (DEV)	Software Developer	SP-DEV-001	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.
		Secure Software Assessor	SP-DEV-002	Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.
	Systems Architecture (ARC)	Enterprise Architect	SP-ARC-001	Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.
		Security Architect	SP-ARC-002	Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.
	Technology R&D (TRD)	Research & Development Specialist	SP-TRD-001	Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.
	Systems Requirements Planning (SRP)	Systems Requirements Planner	SP-SRP-001	Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.
	Test and Evaluation (TST)	System Testing and Evaluation Specialist	SP-TST-001	Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.
	Systems Development (SYS)	Information Systems Security Developer	SP-SYS-001	Designs, develops, tests, and evaluates information system security throughout the systems development life cycle.
		Systems Developer	SP-SYS-002	Designs, develops, tests, and evaluates information systems throughout the systems development life cycle.

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator	OM-DTA-001	Administers databases and/or data management systems that allow for the secure storage, query, protection, and utilization of data.
		Data Analyst	OM-DTA-002	Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modelling, data mining, and research purposes.
	Knowledge Management (KMG)	Knowledge Manager	OM-KMG-001	Responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
	Customer Service and Technical Support (STS)	Technical Support Specialist	OM-STS-001	Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable).
	Network Services (NET)	Network Operations Specialist	OM-NET-001	Plans, implements, and operates network services/systems, to include hardware and virtual environments.
	Systems Administration (ADM)	System Administrator	OM-ADM-001	Responsible for setting up and maintaining a system or specific components of a system (e.g. for example, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures).
	Systems Analysis (ANA)	Systems Security Analyst	OM-ANA-001	Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.
Oversee and Govern (OV)	Legal Advice and Advocacy (LGA)	Cyber Legal Advisor	OV-LGA-001	Provides legal advice and recommendations on relevant topics related to cyber law.
		Privacy Officer/Privacy Compliance Manager	OV-LGA-002	Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams.
		Data Protection Officer	OV-LGA-003-EU	Responsible for overseeing an organization's data protection strategy and implementation as defined in GDPR legislation. Is involved properly and in a timely manner, in all issues, which relate

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
				to the protection of personal data. Role has full autonomy in executing its duties and reports directly to the highest management level of the organization.
	Training, Education, and Awareness (TEA)	Cyber Instructional Curriculum Developer	OV-TEA-001	Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.
		Cyber Instructor	OV-TEA-002	Develops and conducts training or education of personnel within cyber domain.
		Information Systems Security Manager	OV-MGT-001	Responsible for the cybersecurity of a program, organization, system, or enclave.
		Information Systems Security Manager according to EU Member State legislation	OV-MGT-002-EU	In case the Member State has a special legislation, which describes a role of IT/Cybersecurity manager with the special roles / responsibilities, this role is described in the per Member State basis, if applicable
	Cybersecurity Management (MGT)	Communications Security (COMSEC) Manager	OV-MGT-002	Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS).
	Strategic Planning and Policy (SPP)	Cyber Workforce Developer and Manager	OV-SPP-001	Develops cyberspace workforce plans, strategies, and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.
		Cyber Policy and Strategy Planner	OV-SPP-002	Develops and maintains cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.
	Executive Cyber Leadership (EXL)	Executive Cyber Leadership	OV-EXL-001	Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.
	Program/Project Management (PMA) and Acquisition	Program Manager	OV-PMA-001	Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with agency or enterprise priorities.
		IT Project Manager	OV-PMA-002	Directly manages information technology projects.
		Product Support Manager	OV-PMA-003	Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.
		IT Investment/Portfolio Manager	OV-PMA-004	Manages a portfolio of IT investments that align with the overall needs of mission and enterprise priorities.

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
		IT Program Auditor	OV-PMA-005	Conducts evaluations of an IT program or its individual components to determine compliance with published standards.
Protect and Defend (PR)	Cyber Defense Analysis (CDA)	Cyber Defense Analyst	PR-CDA-001	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.
	Cyber Defense Infrastructure Support (INF)	Cyber Defense Infrastructure Support Specialist	PR-INF-001	Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.
	Incident Response (CIR)	Cyber Defense Incident Responder	PR-CIR-001	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
	Vulnerability Assessment and Management (VAM)	Vulnerability Assessment Analyst	PR-VAM-001	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.
Analyze (AN)	Threat Analysis (TWA)	Threat/Warning Analyst	AN-TWA-001	Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/warning assessments.
	Exploitation Analysis (EXP)	Exploitation Analyst	AN-EXP-001	Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.
	All-Source Analysis (ASA)	All-Source Analyst	AN-ASA-001	Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.
		Mission Assessment Specialist	AN-ASA-002	Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness.
	Targets (TGT)	Target Developer	AN-TGT-001	Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
				intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.
		Target Network Analyst	AN-TGT-002	Conducts advanced analysis of collection and open- source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks, and the applications on them.
	Language Analysis (LNG)	Multi-Disciplined Language Analyst	AN-LNG-001	Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates and maintains language-specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects.
Collect and Operate (CO)	Collection Operations (CLO)	All Source-Collection Manager	CO-CLO-001	Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.
		All Source-Collection Requirements Manager	CO-CLO-002	Evaluates collection operations and develops effects- based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.
	Cyber Operational Planning (OPL)	Cyber Intel Planner	CO-OPL-001	Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.