



SPARTA

D9.5

Workplace Integration Evaluation Report

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

Deliverable type	Report
Deliverable reference number	SU-ICT-03-830892 / D9.5 / V1.0
Work package contributing to the deliverable	WP9
Due date	Jan 2022 - M36
Actual submission date	31st January 2022

Responsible organisation	IMT
Editor	Olivier Levillain
Dissemination level	PU
Revision	V1.0

Abstract	The present deliverable is the final one for WP9. It summarizes the results obtained during the SPARTA project regarding education, training and awareness.
Keywords	Curricula, education, training, courses, study programs, awareness, pilots.



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

Editor

Olivier Levillain (IMT)

Contributors (ordered according to beneficiary numbers)

Jan Hajny, Sara Ricci, Tomas Lieskovan, Vladimir Janout (BUT)
Olivier Levillain (IMT)
Šarūnas Grigaliūnas, Stasys Maciulevičius, Nerijus Morkevičius (KTU)
Edmundas Piesarskas, Evaldas Bruze (L3CE)
Jérôme Jacob (SMILE)

Reviewers (ordered according to beneficiary numbers)

Claudio Porretti (LEO)
Olga Navickiene (LKA)

Disclaimer

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author's view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

Executive Summary

To address the skills gap in cybersecurity we are witnessing in the EU (and more generally in the world), education and professional training are the tools we need to develop and improve to improve the situations. Since information technology has become pervasive, we also need the whole population using IT systems to have fundamental knowledge about cybersecurity, which is the goal of awareness campaigns.

SPARTA WP9 aims to develop these topics (education, professional training, and awareness) within the consortium. The present report provides a summary of WP9 activities and results.

During the project, the following results have been achieved:

- the development of a Cybersecurity Skills Framework, based on the NICE Framework proposed by the NIST,
- the development of best practices for university programs and professional training,
- the publication of a tool to identify existing actors and university programs worldwide, the Education Map,
- the publication of another tool helping program and course administrators design their content with cybersecurity skills and topics in mind, the Curricula Designer,
- the development of federated infrastructure of Cyber training & exercise Framework,
- the delivery of many awareness campaigns, and of cybersecurity workshops.

Moreover, during the last year of the project, we identified 50 piloting courses that were part of university programs and professional training run by SPARTA partners, to assess our impact on workplace integration. These courses, which follow the guidelines described during the project, reached more than 2,000 students in 2021, with very positive feedback.

Beyond these achievements, we plan to continue our efforts to propose and update courses that follow the new trends and emerging, as well as to adopt modern practical learning techniques. Indeed, cybersecurity education, training, and awareness is a fast-evolving domain, which will need many trained professionals in the foreseeable future.

Table of Content

Chapter 1 Introduction	1
1.1 Purpose of the Document	1
1.2 Implications for the SPARTA Project	1
1.3 Applicability beyond the SPARTA Project	1
Chapter 2 Cybersecurity Skills Framework Model Development	2
2.1 Overview of Past Activities and Achieved Results	2
2.1.1 Motivations Leading to a Framework Proposal	2
2.1.2 Analysis of the Existing Material	2
2.1.3 Main Outcomes	3
2.1.4 Activities Following Framework Development	3
2.2 Current Status and Next Development	4
Chapter 3 Academic Programs in Cybersecurity	5
3.1 Overview of Past Activities and Achieved Results	5
3.1.1 Study Program Survey	5
3.1.2 Education Map	7
3.1.3 Curricula Designer	8
3.2 Current Status and Next Development	11
3.2.1 Curricula Designer	11
Chapter 4 Professional Training in Cybersecurity	12
4.1 Overview of Past Activities and Achieved Results	12
4.1.1 Best Practice to Design Professional Training	12
4.1.2 Cyber Ranges	13
4.2 Current Status and Next Development	14
4.2.1 New Trends in Training Modalities	14
4.2.2 Inclusion of New Topics with a Critical Eye	15
4.2.3 Build on Existing Cursus	15
Chapter 5 Raising Awareness in Cybersecurity	16
5.1 Overview of Past Activities and Achieved Results	16
5.1.1 Introduction about human and cybersecurity	16
5.1.2 Figures and information about human and cyber incident	17
5.1.3 The approach OTT : Observe-Train-Test	18
5.1.4 The best way to raise awareness in cybersecurity	20
5.2 Current Status and Next Development	22
Chapter 6 Piloting Activities	23
6.1 Education and Training Pilots	23
6.1.1 Pilot Overview	23
6.1.2 Sample Pilots	25
6.1.3 Questionnaire for the Students	27
6.2 Go Cyber with SPARTA	33
6.2.1 Workshop Description	34
6.2.2 Feedback Analysis	35
Chapter 7 Summary and Conclusion	36



Chapter 8 Bibliography	37
Chapter 9 List of Abbreviations	38

List of Figures

Figure 3.1	SPARTA Topics to NICE Competencies mapping.	5
Figure 3.2	On the left chart, ULPGC bachelor curriculum analysis. On the right chart, good-practice curriculum analysis.	7
Figure 3.3	Analyses and comparison of ULPGC bachelor study program and good-practice curriculum.	7
Figure 3.4	Education Map	9
Figure 3.5	graphical user interface (GUI) of the application	9
Figure 3.6	Adding courses.	10
Figure 3.7	Statistical data about the curricula.	10
Figure 3.8	Analysis of "Information Security" bachelor study program.	11
Figure 4.1	This federated infrastructure of Cyber training & exercise Framework presents wide range of exercises for solving cybersecurity challenges and using different cybersecurity tools.	14
Figure 6.1	Repartition of SPARTA WP9 Pilots per Country.	24
Figure 6.2	Repartition of SPARTA WP9 Pilots per Type. The blue portions represent courses from University Programs (for different levels) and the orange portion is for courses from Professional Training.	24
Figure 6.3	Repartition of SPARTA WP9 Pilots per Age. The dates correspond to the creation or the last major revision of the course.	25
Figure 6.4	Proportion of SPARTA WP9 Pilots covering each Skill Category.	26
Figure 6.5	Proportion of SPARTA WP9 Pilots covering each Topic.	26
Figure 6.6	Repartition of the answers to the questionnaire per country.	28
Figure 6.7	Practical- and theory-based training ratio of the pilot courses, as perceived by students, with a focus respectively on University Programs and Professional Training.	29
Figure 6.8	Student Preferences regarding the ratio between practical- and theory-based learning, with a focus respectively on University Programs and Professional Training.	30
Figure 6.9	Proportion of SPARTA WP9 Pilots covering each Skill Category (restricted to the 20 pilots with answers), compared to the student perception.	30
Figure 6.10	Proportion of SPARTA WP9 Pilots covering each Skill Category (restricted to the 20 pilots with answers, left column), compared to the student perception (right column).	31
Figure 6.11	Student Satisfaction for SPARTA WP9 Pilots.	32
Figure 6.12	Evaluation by students of the amount learned during SPARTA WP9 Pilots.	32
Figure 6.13	Evaluation by students of the usefulness of the material learned during SPARTA WP9 Pilots for their professional life.	32

List of Tables

Table 3.1	Topics analysis on all the collected curricula. "B." stands for bachelor and "M." for master.	6
Table 6.1	Repartition of the answers to the questionnaire sent to the students of the pilots. The U/P column describes the typo program the course is part of (University or Professional training).	28

Chapter 1 Introduction

1.1 Purpose of the Document

The purpose of this deliverable is to evaluate the outcome of the cybersecurity skills framework and the training evaluation pilot. It provides feedback on the appropriateness of the developed framework and the courses executed by WP9 partners in academic programs and training programs.

This document first provides a summary of the project activities in the domains covered by SPARTA WP9:

- the Cybersecurity Skills Framework (Chapter 2) from design to application;
- the Academic Programs in Cybersecurity (Chapter 3), including the developed tools (the Education Map and the Curricula Designer);
- the Professional Training in Cybersecurity (Chapter 4), including best practice and the development of cyber ranges;
- campaigns to raise Awareness in Cybersecurity (Chapter 5).

This first part allowed us to define criteria and select piloting activities that were run in 2021. Chapter 6 describes these activities: courses that were influenced by SPARTA and workshops from the Go Cyber With SPARTA initiative. We collect feedback from these different pilots to assess their quality and relevance.

One of the difficulties for a project like SPARTA, which spans on a 3-year period, is that it is hard to follow a complete cycle for an Academic Program. Indeed, designing, approving, running and evaluating a new Bachelor or Master Program requires a longer time. This is why our piloting activities focus on courses, both in academic programs and professional training, which have a somewhat shorter life cycle.

1.2 Implications for the SPARTA Project

This document allows us to present in a concise way the overall results for SPARTA WP9 on Education, Training, and Awareness. It is also a means to evaluate the impact of our various activities during the project.

Since this document is the final one for WP9, the results will help feed the reflection of SPARTA partners for future activities and projects.

1.3 Applicability beyond the SPARTA Project

Several initiatives at the European level have already built on some of the WP9 results, in particular for the Cybersecurity Skills Framework and the Education Map. This document will help publicize the results of WP9 beyond the SPARTA project.

Chapter 2 Cybersecurity Skills Framework Model Development

2.1 Overview of Past Activities and Achieved Results

2.1.1 Motivations Leading to a Framework Proposal

In the proposal Strategic Programs for Advanced Research and Technology in Europe (SPARTA) one of Objectives (Objective 6 Enhance awareness and training capabilities and develop cybersecurity skills) was to:

- point out the differences,
- survey the current status of knowledge,
- characterise the role of cybersecurity professionals as well as other related roles regarding cybersecurity assurance and,
- based on these results, provide a consolidated cybersecurity skill framework throughout the EU.

The framework was intended to be complemented by unified curricula, supported by a collection of collaborative tools and processes.

It was understood that efforts to fill the skills gap and strengthen EU cybersecurity capabilities require different stakeholders to take an active role at EU level, cascading this to the national environment. To undertake such efforts skills framework was considered as one of the instruments. Well-structured tasks, performed by practitioners on the daily bases, can lead to the understanding what skills, abilities, knowledge or competencies are needed to fulfil those tasks.

Initial task (Task 9.1) of SPARTA WP9, was to propose the framework, that can be used within the project scope and extended beyond it. From the proposal development stage, the aim of this task was formulated as defining roles of cybersecurity practitioners by creating a skills matrix for each role.

Expected impact of the above mentioned activities was that a developed cybersecurity skills framework model, would be used as a reference by education providers to develop appropriate curricula; by employers, to help assess their cybersecurity workforce, and improve job descriptions; by citizens to reskill themselves.

The concept of skills framework was taken from previous experience and industrial practice. Modern human resource management is based on similar methodology. Understanding different task, performed by different positions in the organization is a key for employment, career management and selection of relevant trainings.

2.1.2 Analysis of the Existing Material

As the project started, SPARTA Work Package 9, Task 9.1. designated its efforts to analyse the state of knowledge on skills management, reviewing best practices and proposing the way forward with the development of an EU based cybersecurity skills framework.

It was assumed that a construct that aspires to be used as a comprehensive “Skills framework” must include at least the principal components such as roles and skills/knowledge, which should be defined and mapped accordingly, providing the full picture of the skills framework.

D9.1 “Cybersecurity skills framework” chapter dedicated to methodology describes how the Framework was constructed and what major methodological changes were made compared to the original intention.

Several different relevant materials were reviewed in-depth, including EU and outside EU initiatives. Some to be mentioned where: CEN European e-Competence Framework 3.0, UK developed the Cyber Security Body of Knowledge (CyBOK), Study “The changing faces of cybersecurity Closing the cyber risk gap” developed by Deloitte Canada Consulting Group & Toronto Financial Services Alliance, etc.

Review of available materials focused on the search for answers to two main questions:

- Which cybersecurity roles should be defined in the framework?
- How relevant skills / knowledge should be structured and mapped to roles?

The purpose of this review was not to criticise or challenge the works presented, but to focus on the evaluation of how the proposed taxonomies can be adapted to the SPARTA approach, how they address cybersecurity workforce management needs and how they can contribute to the development of the skills framework.¹

Search for best practice, that can serve as foundation for further development of the Framework, was based on the assumption that a construct must include at least the principal components such as roles and skills/knowledge, which should be defined and mapped accordingly. Proper definition of roles and proper definition of skills were the main criteria to make the choice. Definition of roles usually is a starting point. Only by understanding activities, described by tasks, can one acquire a full understanding of the skills needed to perform those tasks.

For the definition of best practices in the present context four criteria were applied. Those were relevance of structure, applicability, granularity, and sustainability. Detailed

2.1.3 Main Outcomes

Review of available materials led to conclusion that the JRC Cybersecurity domains taxonomy and the US-based National Initiative for Cybersecurity Education (NICE) are the most reasonable starting points for such an effort, providing a comprehensive and accommodative structure to incorporate the EU specific realities and emerging skills landscape.

Deliverable D9.1 describes guiding main principles for EU skills framework development. One of them is worth mentioning:

“Though cybersecurity is an international and deeply technical phenomenon, and is not bound to national states, nevertheless, some specifics do exist. These mainly arise from legislative differences. In developing the SPARTA CS Framework, we will aim to respect EU specificities enabling frictionless use of the framework in the EU environment.”²

As a main outcome SPARTA Cybersecurity Skills Framework (SPARTA CSF) was proposed. It was based on the structure of the NICE Framework, amended with EU specifics. During the project execution the Framework was tested and validated for applicability, adaptability by industry and academia. It is important to note, that efforts made developing SPARTA CSF should be considered as aiming to set in motion a process of development of a comprehensive European cybersecurity skills framework, as there were no such instrument available at this time. There was no intent to produce a point-in-time snapshot of a skills framework.

Another important conclusion, provided in D9.1, was stressing the importance of governance of such frameworks. Rapidly changing environment constantly provides new challenges and requirements for cybersecurity practitioners. Those are to be reflected in the framework, providing smooth way to communicate those changes to different stakeholders involved in the area of cybersecurity.

2.1.4 Activities Following Framework Development

After SPARTA CSF was developed, validated by project internal partners and EC reviewers, and well accepted, activities were directed in two directions:

1. Application of the Framework in further developments in the project.
2. Dissemination and promotion of the outcomes in different formats outside the project.

¹D9.1 Cybersecurity Skills Framework [1], page 12.

²D9.1 Cybersecurity Skills Framework [1], page 26.

Within SPARTA the Framework was applied in a few deliverables providing structured approach to cybersecurity skills. One of the most successful applications was made in developing Curriculum designer - easy tool for education institutions, allowing to evaluate study programs in different light.

Three main successes factors for further implementation of EU wide CSF were identified and communicated for different groups within and outside SPARTA project. To make any framework, including SPARTA SCF, vibrant special attention should be given for:

- Governance – to properly maintain the framework, update it by including emerging task, followed by required skills.
- Recognition – acceptance and application of the framework among main stakeholders makes it a strong tool.
- Involvement – wide application of the framework by leading academia & professional training providers from all MS, industry and policy makers; making it the core of benchmarking, roadmapping, research and other relevant activities.

Activities outside SPARTA were mainly focused on Cyber Competence Network (CCN) group, uniting all four pilot projects. Discussions on different approaches to cybersecurity skills framework development and applicability were held. Maximum target was to make SPARTA CSF recognized by all pilot projects, so they can apply it in their developments. Activities in CCN Education group led to the conclusion, that EU wide unifying skills framework can be very relevant and add value to improved development of the sector. Significant attention was also given for cooperation with ENISA on the subject. As cross-pilot dialog developed, major initiative occurred, changing the landscape of the subject.

2.2 Current Status and Next Development

As SPARTA project WP9 team initiated and facilitated discussions on the importance of the skills framework, this got some echo in different environments. European Union Agency for Cybersecurity (ENISA) took the initiative on this subject. In 2020, an Ad Hoc Expert Group on Cybersecurity Skills Framework (AHEG) [6], dedicated to the development of European cybersecurity skills framework, was formed. The scope of this ad hoc working group is to advise ENISA in developing a cybersecurity skills framework, which permits a common understanding of the roles, competencies, skills and knowledge used by individuals, employers and training providers across the European Member States.

The task of the Group is to develop a European Cybersecurity Skills Framework [5]. It is expected to be of recommendation nature.

Currently, the Framework is under developments. It is expected to make the Framework available in late 2022.

It is to be mentioned that SPARTA WP9 team members (two representatives from BUT and L3CE) were and still are actively involved in the above-mentioned ad hoc group, representing SPARTA approach, and sharing knowledge and experience acquired during the project.

REWIRE project³ is another initiative, that resulted from SPARTA WP9 activities. The aim of the project is to provide concrete recommendations and solutions that could lead to reduction of skills gaps between industry requirements and sectoral training provision, and contribute to support growth, innovation and competitiveness in the field of cybersecurity. The Skills framework and its application are one of the core components within this project, providing a new environment to continue the work done in SPARTA.

³Cybersecurity Skills Alliance — A New Vision for Europe (REWIRE) project has received funding from the European Union's Erasmus+ programme Cooperation for innovation and the exchange of good practices action under grant agreement No 621701-EPP-1-2020-1-LT-EPPKA2-SSA-B.

Chapter 3 Academic Programs in Cybersecurity

3.1 Overview of Past Activities and Achieved Results

3.1.1 Study Program Survey

In order to propose novel good-practice curricula in cybersecurity, SPARTA ran an analysis of world-wide cybersecurity-related study programs. The collected data considered 89 higher-education cybersecurity curricula (19 bachelors and 70 masters) spread over 19 countries of which 5 are non-European ones. A strategy to compare the curricula needed to be developed. Accordingly, 6 main cybersecurity-related areas (i.e., Computer Science, Cryptology, Humanistic and Social Science, Mathematics, Privacy, Security.) were identified as fundamental knowledge that needs to be taught. Moreover, a higher granularity was enforced by splitting the main areas into topics. Figure 3.1 depicts the SPARTA topics and their relationship with NIST NICE competencies. We refer to SPARTA D9.2 [2] for more details.

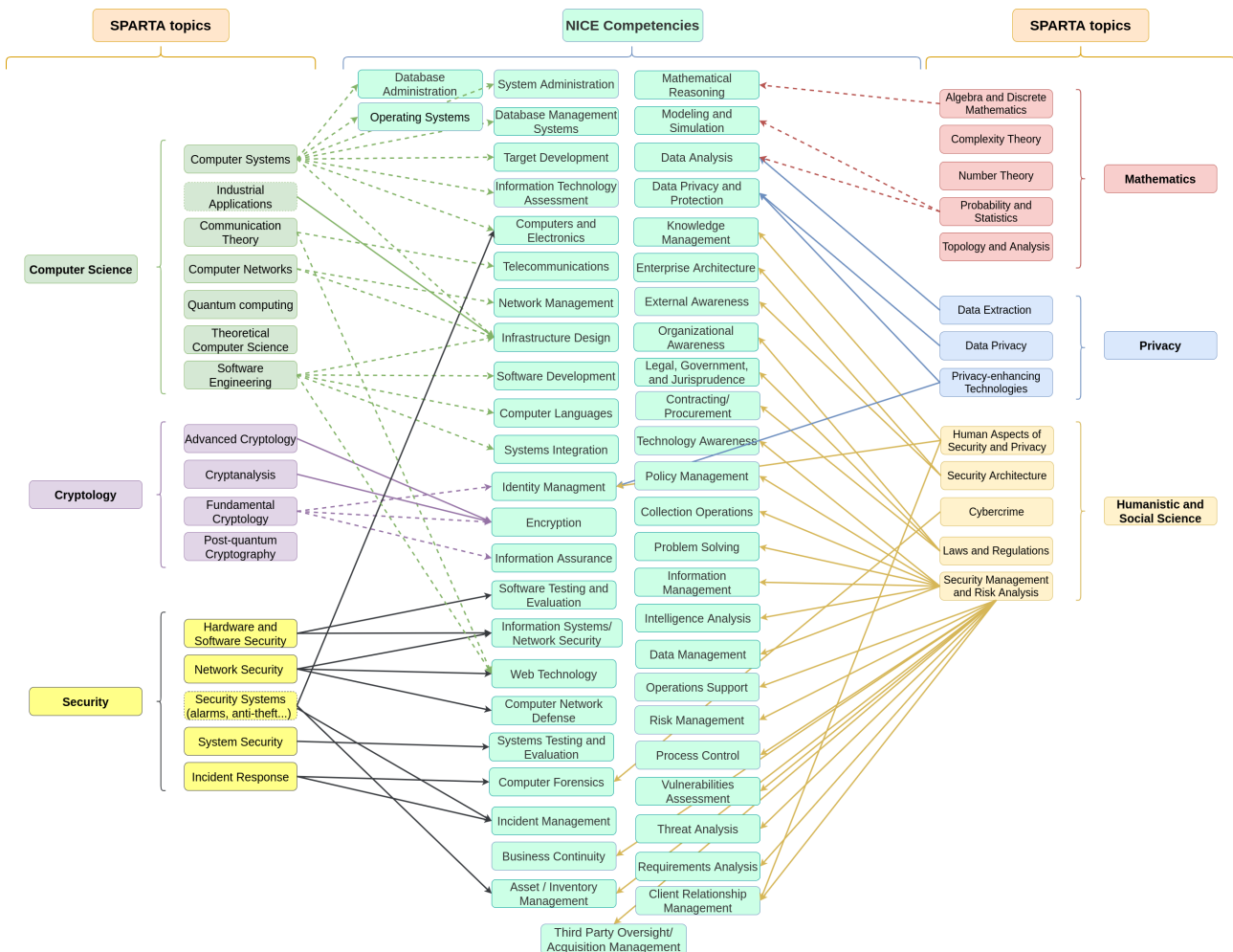


Figure 3.1: SPARTA Topics to NIST NICE Competencies mapping.

The analyses of bachelor lectures highlight computer science topics as the main fundamental background, followed by humanistic and social science, and mathematics. Moreover, security has also a big component of the training, which in non-European curricula is presented as a priority. In the case of masters curricula, humanistic and social science, security and cryptology are strong components, whereas privacy remains an area only partially covered in most of the programs. Table 3.1 shows in percentage the number of study programs where that topic can be found. For example, "Computer

Network” is taught practically in all the bachelor study programs focusing on cybersecurity. Moreover, a solid cybersecurity study program should give big space for practical lectures. In the analyzed European curricula, study programs have on average 30% practical lectures for bachelors and 40% for masters.

Table 3.1: Topics analysis on all the collected curricula. "B." stands for bachelor and "M." for master.

Computer Science			Cryptology		
Topic	B.	M.	Topic	B.	M.
Industrial Applications	50%	31%	Advanced Cryptology	33%	46%
Communic. Theory	61%	34%	Cryptanalysis	22%	38%
Computer Networks	94%	71%	Fundamental of Cryptology	83%	81%
Computer Systems	83%	52%	Post-quantum Cryptography	11%	18%
Quantum computing	11%	12%			
Theoretical Computer Science	67%	32%			
Humanistic			Mathematics		
Topic	B.	M.	Topic	B.	M.
Cybercrime	56%	43%	Algebra and Discr. Math.	72%	31%
Human Aspects of Sec. and Priv.	56%	53%	Complexity Theory	28%	22%
Security Architecture	56%	49%	Number Theory	22%	26%
Security Manag. & Risk Analysis	56%	68%	Probability and Statistics	72%	22%
Laws and Regulations	50%	54%	Topology and Analysis	28%	10%
Privacy			Security		
Topic	B.	M.	Topic	B.	M.
Data Extraction	28%	37%	Hardware and Software Sec.	89%	81%
Data Privacy	44%	52%	Network Security	94%	85%
Privacy-enhancing Technologies	44%	28%	Security Systems	56%	53%
			System Security	89%	88%

This analysis as well as recommendations by key EU institutions, such as ENISA, European Cyber Security Organization (ECSO), and inputs from other Cyber Competence Network (CCN) pilots, were considered for the development of a bachelor and a master good-practice curricula. The process of designing the curricula turned out more significant than the good-practice curricula themselves. Therefore, the idea to develop a web application "Curricula Designer" came up as described in Section 3.1.3. We refer to SPARTA D9.2 for more details.

It is worth noting that this preliminary analysis not only helps to develop novel good-practice curricula but also permits to turn an existing study program into a cybersecurity one. During the Go Cyber with SPARTA campaign, the bachelor in Computer Engineering of the Universidad de Las Palmas de Gran Canaria (ULPGC) was analyzed and several recommendations were proposed based on the analyses and the comparison with the good-practice curriculum.

Figure 3.2 shows the statistical analysis of both ULPGC and good-practice bachelor curriculum. In particular, the percentages represent the amount of ECTS credits taught in the related SPARTA topic and area by ULPGC and good-practice curricula, respectively. In comparison, the ULPGC study program mainly focuses on Computer Science Topics as it is expected to do. Cybersecurity is a multidisciplinary discipline. Therefore, Cryptography and Security areas should be more covered to make the curriculum more cybersecurity-oriented. Then a deeper analysis was ran to specifically identify which cybersecurity topics might have been undertaken. Figure 3.3 shows the comparison in details with the percentages assigned to each topic in both curricula. The reddish percentages are the one that may be considered to change. Accordingly, the analysis and the comparison give an idea of how the existing curriculum can be modified, which subjects either might need to be added or might be merged.

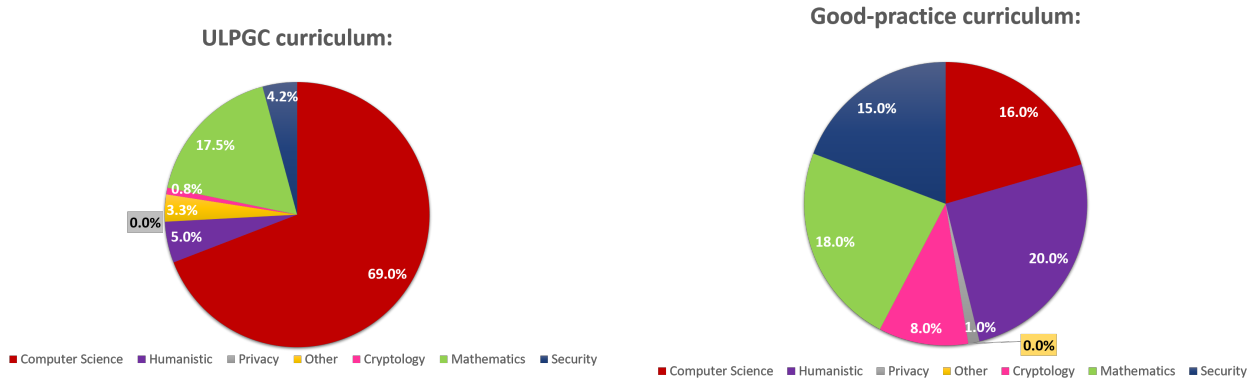


Figure 3.2: On the left chart, ULPGC bachelor curriculum analysis. On the right chart, good-practice curriculum analysis.

	ULPGC %	Good-practice %		ULPGC %	Good-practice %
Computer Science	69	16	Cryptology	0.8	8
Industrial Applications	0.0	0	Advanced Cryptology	0.0	3
Communication Theory	16.7	3	Cryptanalysis	0.0	0
Computer Networks	5.8	2	Fundamental Cryptology	0.8	5
Quantum computing	0.0	0	Post-quantum Cryptography	0.0	0
Theoretical Computer Science	17.5	4			
Software Engineering	20.0	4			
Computer Systems	9.2	3			
Humanistic	5.0	20	Mathematics	17.5	18
Cybercrime	0.0	4	Algebra and Discrete Mathematics	3.3	4
Human Aspects of Security and Privacy	1.7	0	Complexity Theory	1.7	0
Security Architecture	0.0	0	Number Theory	1.7	2
Laws and Regulations	1.7	8	Probability and Statistics	4.2	3
Security Management and Risk Analysis	1.7	8	Topology and Analysis	6.7	9
Privacy	0.0	1	Security	4.2	15
Data Extraction	0.0	0	Hardware and Software Security	0.8	2
Data Privacy	0.0	0	Network Security	0.8	11
Privacy-enhancing Technologies	0.0	1	Security systems	0.0	0
			System Security	2.5	2
Other	3.3	0	Incident Response	0.0	0

Figure 3.3: Analyses and comparison of ULPGC bachelor study program and good-practice curriculum.

3.1.2 Education Map

The Education Map is a dynamic web application that serves for visualizing the collected existing study programs in cybersecurity. This application was developed as a part of the existing study programs mapping activity. Compared to only PDF reports, this map allows a more interactive and comprehensive way of results presentation. The web application lists universities and their study programs in cybersecurity. Users have the possibility of filtering using specific criteria. More than 120 cybersecurity study programs (i.e., 102 masters and 27 bachelors) are uploaded in the map. These data were collected from 91 worldwide universities. Basic information with the links to the university’s web page can be found for each curriculum as shown in Figure 3.4. Moreover, a simple pie chart sketching the statistical analysis is also shown. The web application also contains an administration part, which can be used to add and modify the records about the study programs and universities. The app is publicly available at <https://www.sparta.eu/study-programs/>.

3.1.3 Curricula Designer

The SPARTA Curricula Designer¹ is an online tool for building cybersecurity study programs that makes use of the previously developed SPARTA Cybersecurity Skills Framework (CSF). While the CSF is an abstract construction described in the respective documentation [1], the aim of the Curricula Designer is to be a concrete and practical tool that increases the impact of the CSF. By using the SPARTA Curricula Designer, the study program administrators will be able to easily design novel cybersecurity programs and assess their compliance with needs of the job market.

Curricula Designer helps to identify what content needs to be taught for particular work roles. Therefore, it relies on the links between SPARTA Topics (which characterize the content of courses) and NICE Competencies (which are defined for cybersecurity Work Roles by the NIST NICE Framework [7]). The mapping between Topics and Competencies is depicted in Fig. 3.1.

SPARTA Topics were defined mainly to allow applications of CSF in higher-education, as NICE Competencies cannot be applied directly there due to their focus on cybersecurity only. The definition of SPARTA Topics allowed us to reflect the need of fundamental subjects (such as mathematics, physics, etc.) in cybersecurity study programs, which would not be possible with using the Competencies directly. On the other hand, SPARTA Topics may be omitted when applying the SPARTA CSF in professional education. NICE Competencies may be used directly there.

After the fundamental "engine" of Curricula Designer was specified in the form of the enhanced SPARTA CSF, we had to focus on the usability of the tool. Here, the main objective was simplicity and user friendliness that makes the tool useful even without any explanation or training. The user interface is based on the well-known approach used in similar applications, such as accommodation search tools, where the screen is split into 3 parts which are depending on each other. The Curricula Designer interface is shown in Fig. 3.5 and consists of the Course Definition section (1) on the left side, the Composition section (2) in the middle and the Analytic section (3) on the right side.

Adding Courses

The left section 1 allows users either to load sample courses from a good-practice curriculum (button "Load sample courses") or define own courses using the button "Add course". When adding courses (see Fig. 3.6), users must fill in data about the course, i.e. the name, type, semester, whether it includes a practical training, number of European Credit Transfer System (ECTS) credits and Topics, that the course covers. For a detailed description of SPARTA Topics, see D9.2 (<https://www.sparta.eu/assets/deliverables/SPARTA-D9.2-Curricula-descriptions-PU-M18.pdf>).

Composing Programs

When courses are added, the study program may be composed by simply dragging the course box into the middle section, to the area representing a particular semester (summer/winter, year 1, 2, 3). The app automatically checks the semester and does not allow insertion into a wrong semester. The final program can be exported to a json format for a future work.

Reading Analytical Data

In the right section 3 (see Fig. 3.7), statistical information about the study program is displayed. This information includes distribution of credits in semesters, distribution of ECTS credits to SPARTA Areas and SPARTA Topics, supported NIST NICE Competencies, and, most importantly, NIST NICE Work Roles supported by the study program. The Work Role is considered supported if required competence is covered in at least one subject. The user can display the necessary Competencies of a particular Work Role by hovering with a mouse over the Work Role. The information is dynamically updated as the study program is being created.

The Curricula Designer was published on the SPARTA website <https://www.sparta.eu/curricula-designer/> including the documentation <https://www.sparta.eu/curricula->

¹<https://www.sparta.eu/curricula-designer/>

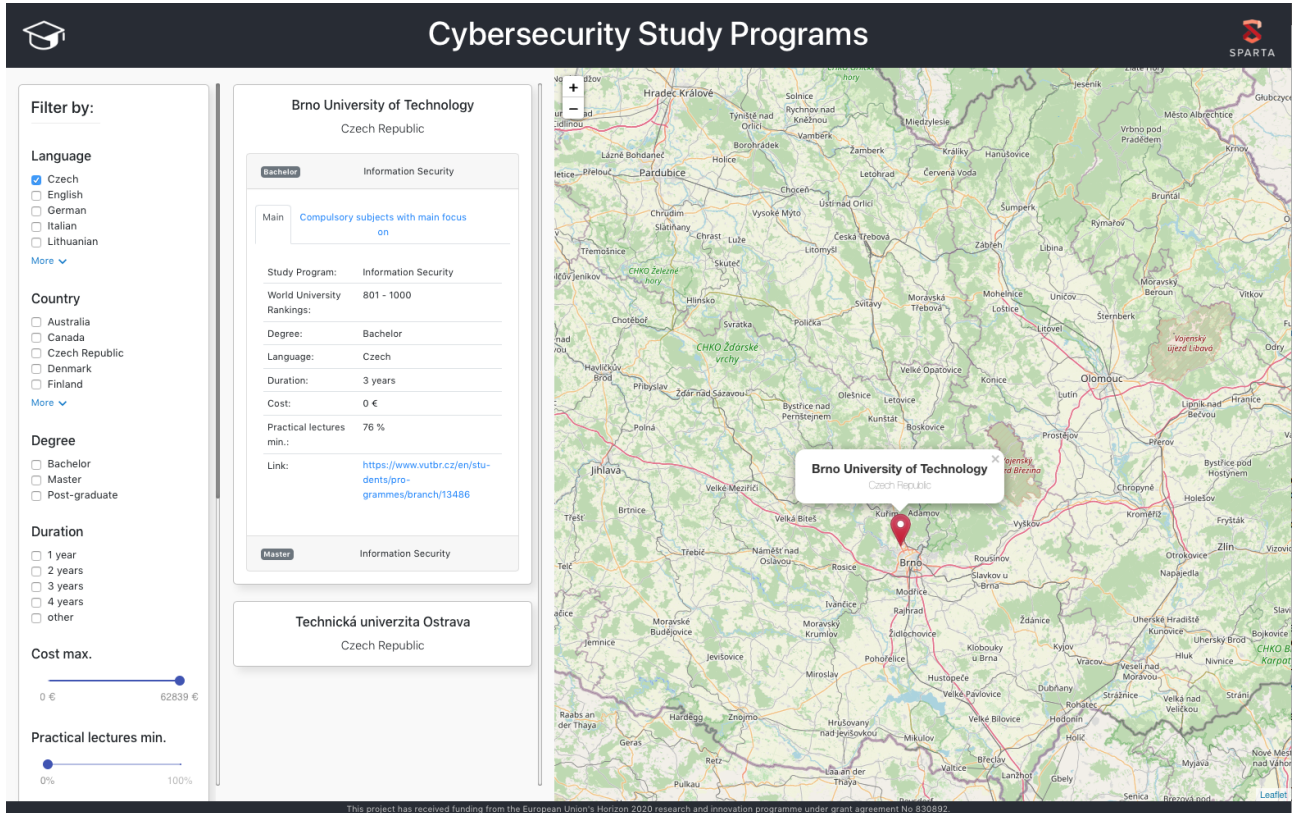


Figure 3.4: Education Map

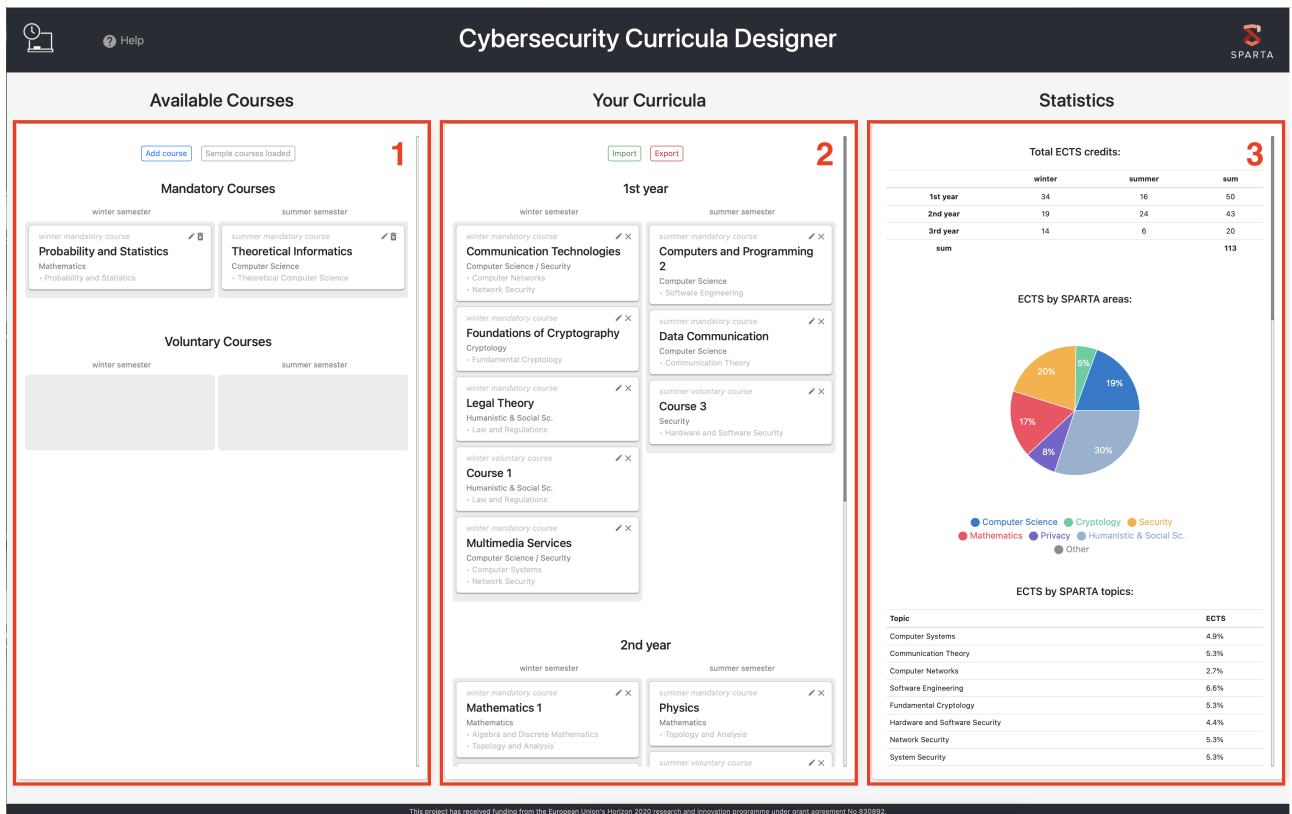


Figure 3.5: GUI of the application

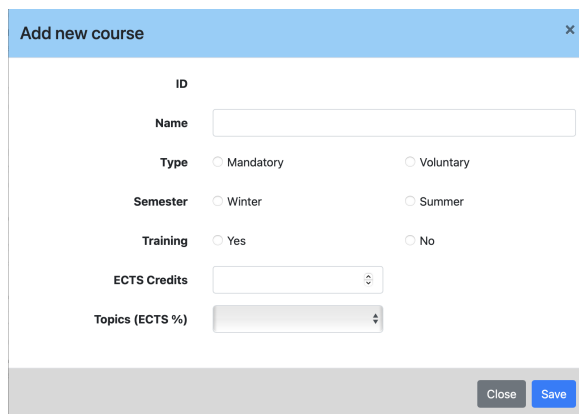


Figure 3.6: Adding courses.

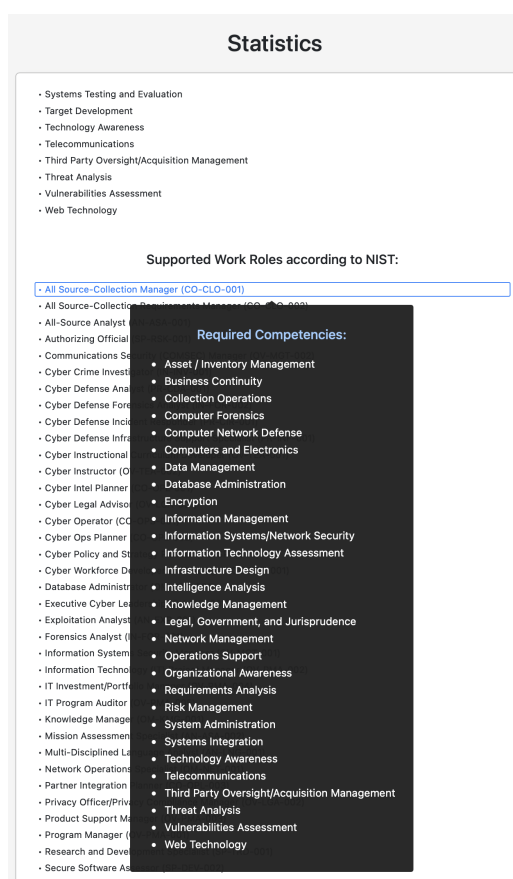


Figure 3.7: Statistical data about the curricula.

designer/files/DesignerHowTo.pdf and is available for general public for free under the MIT license, including the source code <https://bitbucket.org/MarekSikora/curricula-designer/src/master/>. The tool has been used to evaluate both internal SPARTA curricula (such as the good-practice curriculum specified in D9.2, see Fig. 3.8) and external study programs, such as the Universidad de Las Palmas de Gran Canaria (ULPGC) study program during the Go Cyber with SPARTA campaign. According to the internal statistics, the tool has been used by more than 400 unique users by 10/2021. The design, implementation and evaluation of the tool is also described in a peer-reviewed paper [8].

Total ECTS credits:

	winter	summer	sum
1st year	31	27	58
2nd year	29	30	59
3rd year	16	8	24
sum			141

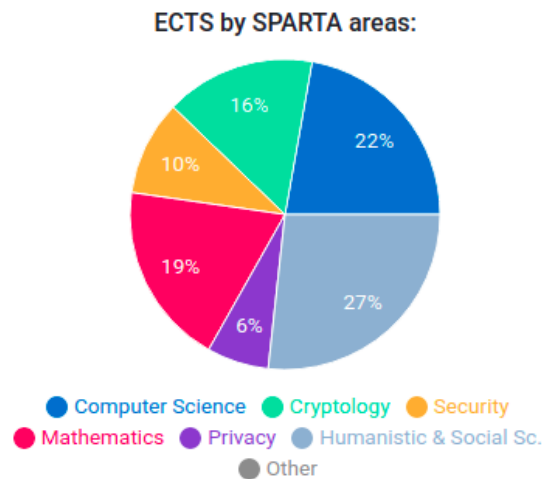


Figure 3.8: Analysis of "Information Security" bachelor study program.

3.2 Current Status and Next Development

3.2.1 Curricula Designer

Currently, the Curricula Designer application allows only the design and analysis of Bachelor's study programs with duration of 3 years. Master's programs can be analyzed, but only indirectly, by using the Bachelor's template. Furthermore, the application has no support for professional training programs that would require different course classification and flexibility in duration specification. Finally, the application works with the updated NIST NICE framework only and has no support of emerging frameworks, such as the EU Cybersecurity Skills Framework (EUCSF)² that may be released soon in the future. Therefore, our next activities are aimed at fixing these shortcomings, namely (sorted according to priority):

- Include the option to choose the underlying framework, which is used for curricula analysis, between SPARTA/NIST NICE and EU CSF.
- Include the option to choose between Bachelor's and Master's program template.
- Enhance the tool to support also professional training programs.
- Implement the features suggested by users.

²<https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework>

Chapter 4 Professional Training in Cybersecurity

Professional training represents another way to respond to the current cybersecurity skills shortage. Since university and higher education programs have a time constant of 4 to 5 years, we need to rely on professional training to help fill in the immediate gap.

Actually, cybersecurity has become a pervasive topic that is progressively becoming part of a lot of jobs, in the technical departments of course, but also at the management and top decision levels. This perspective advocates the need of training for many professionals to acquire at least basic knowledge and skills in cybersecurity.

Moreover, even when the gap is filled, it will still be interesting to rely on professional training to offer complementary and recent skills, since professional training is more dynamic by nature, and can adapt its contents more quickly.

4.1 Overview of Past Activities and Achieved Results

First, this section describes general guidelines proposed during the project for Professional Training. Then, we describe in more details the achievements in the domain of cyber ranges.

4.1.1 Best Practice to Design Professional Training

The Need for Immediate Applicability

One of the main difference between University Programs and Professional Training is that in the latter, we need to teach immediately applicable material to people who are currently in the work force, because it is generally hard to find the time required to train employees, especially in IT departments where skills shortage are common.

Moreover, it is important to adapt course material to the public, since students can have different backgrounds, which is very different from University Programs where students generally represent a more homogeneous cohort.

For these reasons, we believe it is very important to find the right balance between reusable fundamental knowledge and concrete applicable hands-on exercises in Professional Training. The balance should be different from the one proposed in University Programs: when possible, theoretical parts should be refreshers more than formal presentations describing concepts from scratch. For the practical sessions, professional training should focus on real-world applications using state-of-the-art tools used by the industry.

It is thus of the utmost importance that these cursus include relevant practical sessions (case studies for organisational topics and human sciences, hands-on courses such as programming for technical topics) for a significant proportion of the course.

The Need for Soft Skills

In addition to technical capabilities, cybersecurity roles need also have require behavioral and business-oriented skills, defining both recruitment and career development success.

These so-called “soft skills” are essential for career evolution occurring in organisations today. Indeed, they will allow a person to move forward in the structure towards leadership and executive positions.

Indeed, one of the current challenges of Human Resources regarding cybersecurity roles, beyond recruiting them, is to manage to keep the people within the structure by offering them career evolution opportunities. Professional training should thus help develop soft skills such as the ability to supervise or mentor more junior colleague, handle knowledge transfer or develop business-oriented skills.

Toward More Future-Proof Courses

One way to make the courses useful in the long term is to make sure professional training include

modern technologies for training (e.g. cyber ranges, virtualization), and tackle novel trends in cybersecurity (e.g. blockchain, (post)quantum, privacy by design), as much as possible.

One way to achieve this is to include cybersecurity experts from the field in the teaching staff, who can both bring real-world use cases and discuss current and emerging topics as they envision them. This is in particular the case for CZ.NIC training sessions, where courses are proposed by internal experts on various topics they face as a national CERT/CSIRT team. They also offer courses taught by associated experts (cybersecurity community professionals) or external experts in general. This helps them cover and further develop current topics and ideally emerging ones.

IMT developed the same idea with new courses for a professional cursus. First, they created a course about the legal and regulation aspects of cybersecurity, which are currently a hot topic, especially for the European Union. They also added a course on the cybersecurity of industrial systems, which are becoming a very important trend. In both cases, most of the courses are given by external experts from both public and private sectors.

4.1.2 Cyber Ranges

Facing risk of being attacked by various threat actors, even by state-sponsored attackers from some countries, calls for measures to be taken to raise the level of cyber security, both at national and organizational level. One effective solution to achieve this is to use cyber ranges. Many sources emphasize the lack of well-trained cyber security professionals. According to the World Economic Forum Report 2021 [9], there is a global gap of over 3.12 million cyber security workforce.

A **cyber range** is a platform that provides a secure, legal environment for cybersecurity education, practice, and cyber warfare training. Cyber ranges are virtual Internet-level representations of an organization's local network, system, tools, and applications. Providing cybersecurity training in such case guarantees that client infrastructure and data is never at risk as a result of possible errors of trainees.

Today, cyber ranges are used in the cybersecurity sector to effectively train IT professionals in all industries and help improve defense against cyber attacks. As technology advanced, cyber range training advanced as well, both in scope and potential.

IT security professionals are educated at universities and colleges. In most cases university or college diploma is not sufficient for successful work in cyber security, and the missing knowledge and skills they acquire at various specialized professional certifications, where employees with other IT specialties also can acquire the necessary qualifications in IT security.

Here cyber ranges play important role while:

- they perfectly complement the knowledge and skills acquired through formal learning, using a safe environment;
- they can help learn specialized skills — such as digital forensics or cloud security;
- they present a training space that simulates a wide range of security incidents, enabling cybersecurity professionals to practice and learn how to respond to cyber threats effectively;
- they are a great tool for introducing in practice the new emerging cyber threats and ways to deal with them;
- they deliver continuous development of security competencies at a reasonable cost;
- they play an important role in cyber security research and the development of new security products.

During SPARTA project, KTU and partners developed federated infrastructure of Cyber training & exercise Framework (see Fig. 4.1).

- KTU presented its own training platform and Red Team / Blue Team training scenario ("story-line") as a pilot of using this framework in training. The implemented framework allows participants to choose the history of attacks, their descriptions and the collected evidence. The

experience of using this framework show that the Cyber training & exercise Framework is well-suited for actual training activities in terms of features, usability and execution performance.

- CNIT delivers a cyber range platform with a strong orientation towards a knowledge-sharing platform. The platform represents a reliable training tool to advance cybersecurity skills at all levels, enables quick deployments and configurations as well as effective sharing of the gathered information on cyber security threats and corresponding defense strategies.
- KYPO Cyber Range Platform is an open-source platform for cyber exercises, which is built on the OpenStack cloud platform. It allows the simulation of devices, networks, and computers with any operating system. It provides a graphical user interface through which the entire training is available. These pieces of training can be available both locally and remotely.
- The University of Bonn developed a framework to measure IT security awareness within working staff. This framework facilitates the comparison of different exercises based on effectiveness, the capture and analysis of the behavior of employees as an expression of their IT security awareness.
- All presented tools are federated by the SPARTA JCCI integrator.

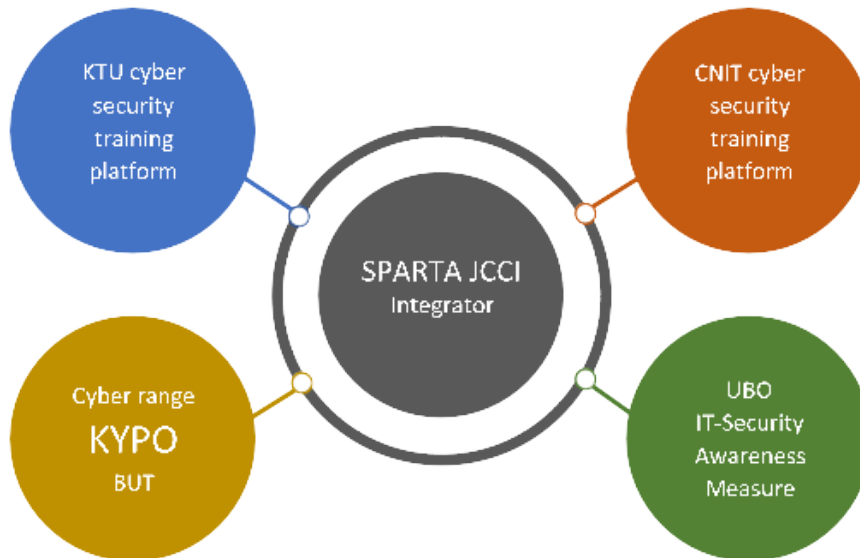


Figure 4.1: This federated infrastructure of Cyber training & exercise Framework presents wide range of exercises for solving cybersecurity challenges and using different cybersecurity tools.

4.2 Current Status and Next Development

As discussed in this chapter, the need for more professional training is still very pressing, and might still be for a long time, especially since professional training allows to quickly adapt to new technologies and paradigms.

We believe our approach is relevant, and we encourage professional training administrators to pursue and follow the best practices.

In this section, we propose several development axes for the future.

4.2.1 New Trends in Training Modalities

During the pandemic, professional training faced a difficult time, and had to adapt to provide courses remotely, whereas they are usually taught in person.

For many reasons (e.g. pandemic-related constraints, travel restrictions due to ecological considerations), remote training will probably become more prevalent in the years to come. This will require

a lot of work from the professional training administrators to explore remote learning technologies, while at the same time ensuring the course is delivered in a customized way to the students, who all have different experiences and backgrounds.

To help solve this difficulty, it might be useful to develop so-called blended courses, where in-person and remote classes are both used. If the learning material is accordingly prepared, this allows to get the best of both world: limiting the need for travel and in-person meeting, while still developing the rapport between teachers and students.

4.2.2 Inclusion of New Topics with a Critical Eye

Even if it is important to include trending topics in Professional Training to help employees keep up with new technologies, course administrators should always aim at teaching their students to know how to take a step back on these technologies, and to be critical from time to time with regards to them.

In cybersecurity, we know that there is indeed no silver bullet, and it is often important to put new tools into perspective. This makes it especially difficult to propose courses on emerging subjects such as blockchains, artificial intelligence or quantum computing in Professional Training.

Indeed, a good teacher has to explain how these technologies work, what they can bring in realistic use cases, while at the same time describing the hypotheses they rely on, the threat models within which they are relevant, and their limitations. All of this in relatively short sessions.

This is why professional training is so challenging, and requires a constant evolution and regular content revisions if we want it to be relevant in the long run.

4.2.3 Build on Existing Cursus

Today, some professional certifications exist, but they are usually rather generic or they describe a very broad spectrum of working roles. There is thus still room for more focused and dynamic references to help us train the professional.

This idea has been developed by ANSSI (the French cybersecurity agency), with *SecNumedu - Formation Continue*, an initiative around several training specifications for professional training. Currently, three references have been published:

- an initiation to ICS cybersecurity;
- a syllabus to train SME professionals to cybersecurity;
- guidelines for a risk analysis course using Ebios Risk Manager.

There is need for such problem solving-oriented references, and it would be interesting to develop and promote such specifications at the European level.

For example, it might be relevant to push for such references in topics such as Health System Cybersecurity or Incident Response.

Chapter 5 Raising Awareness in Cybersecurity

5.1 Overview of Past Activities and Achieved Results

5.1.1 Introduction about human and cybersecurity

Twenty years ago, people have not always been at the heart of cybersecurity processes and efforts focused essentially on technology. Indeed, if we analyze investments in the field of cybersecurity, the priority was always to technically secure data and services through investments such as firewalls, anti-viruses, network security, backups, etc.

It is only later that humans found a more significant place with the emergence of security procedures and policies dedicated to them:

- Creation of secure passwords,
- Secure Internet browsing,
- Systems updates,
- ...

However, the human factor has actually been reconsidered in cybersecurity strategy because of the evolution of the threat. In recent years we witnessed human targeting in cyberattacks, in particular through phishing and social engineering. The impacts of these two types of attacks were so important that it was necessary to rethink the cybersecurity model by giving a greater part to the human factor, by integrating it at the base of all the security processes. Awareness has therefore become one of the essential and complementary tools to the technical and technological arsenal dedicated to securing data and systems.

All of this leads us to one observation: people are at the heart of the cyber world and must be considered as one of the most sensitive links of the chain. In a way, cybersecurity should be everyone's business and not only the job of specialists. It is on this principle that cybersecurity awareness has taken an increasingly important part in the processes.

The main objective of Cybersecurity Awareness is to explain what a cybersecurity risk is:

$$\text{Risk} = \text{vulnerability} \times \text{threat} \times \text{impact}$$

The goal for each awareness campaign is to present the risks for each participant by making them think intrinsically about the following three variables:

Vulnerability: How am I vulnerable? How can I reduce my exposure?

The objective is to help participants think about these questions and make their own vulnerability diagnosis.

- Are my passwords strong enough?
- Is my use of social networks appropriate?
- ...

Threat: Who wants to destroy me? What type of threat am I facing?

The objective is to discover the multitude of threats that users could be confronted with:

- Economic intelligence from a competitor or a State seeking to collect sensitive information,
- A hacker seeking to destabilize an organization or an individual,
- A colleague seeking revenge,
- A group of cybercriminals trying to extort money,
- ...

Impact: What happens if I am affected by a cyberattack?

The objective is to demonstrate the multitude of impacts that would be the consequence of a cyber-attack:

- Loss of reputation,
- Loss of money,
- Loss of confidentiality,
- Service unavailability,
- ...

Only by understanding this matrix will the participant be able to integrate good cyber reflexes into their daily lives.

For example, we can apply this approach to the risk of a cyberattack using a ransomware:

$$\text{Risk (ransomware)} = \text{Vulnerability (employees clicking by curiosity on a link)} \times \text{Threat (hacker with skills)} \times \text{Impact (unavailability of service and / or financial loss)}$$

The goal is to explain what the consequences of this type of attack are by insisting on the fact that if the employee is aware of the threat and the impact, he will be less vulnerable and therefore will have the reflex to think before clicking on a potentially dangerous link.

5.1.2 Figures and information about human and cyber incident

During each cybersecurity awareness campaign, an informal survey of participants' practices is carried out. Each time, the results are explicit and almost similar in terms of cybersecurity maturity. Here are some recurring examples.

Passwords

- Complexity: 75% of people use the same password for many applications and never change it.
- Password manager: 95% of people do not use a password manager.

Updates

- Frequencies and control: 80% of people don't care about updates and never check which versions are used.

Social networks

- Configuration: 65% of people do not know how to secure their applications (Facebook, Instagram, etc.).

Geolocation

- Configuration: 90% of people do not know that their trips are recorded on their smartphone or via their GMail account.

USB Keys

- Recklessness: 80% of people agree to connect a USB key found or offered to their computer.

IOT

- Configuration: 85% of people have no questions about security configurations.

Wireless

- Connection: 90% of people connect to available WiFi networks by trusting them.

Bluetooth

- Activation: 95% of participants' smartphones have Bluetooth permanently activated.

Phishing

- Routine: 65% of participants do not see that the presented URLs contain an error.

These results show that the human factor can easily become the weakest link in an organization if cybersecurity awareness is neglected.

5.1.3 The approach OTT : Observe-Train-Test

Considering the information presented above, it is undeniable to consider awareness as the cornerstone of any cybersecurity strategy. Therefore, it is important to recognize that most incidents can be anticipated by a preparatory phase including the following:

- An observation phase dedicated to emerging threats in order to be able to understand and anticipate them,
- A training / awareness phase to give the knowledge related to the observation phase,
- A test phase to control the acquisition of knowledge or know-how.

In this sense, an initiative has been undertaken since 2018 in the Grand Duchy of Luxembourg in terms of in-depth awareness and testing of know-how. It is within the Cybersecurity Competence Center (C3) of this country that research has been carried out through an approach reconciling scientific, technical and human observations. This experiment was carried out with the aim of creating a cyberattack simulator with humans as its central point.

The findings that led to the launch of this concept was based on a key element: *Reconsidering the human factor and reinserting it at the center of the incident*. The idea was simple. It was about putting people back at the heart of cyber by giving them back their legitimacy rather than following a trend involving the establishment of additional layers of technology to manage an incident.

Based on the analysis of cyber incidents, the initial and preliminary conclusions to the launch of this new concept always led to the same observation:

- The *Time* factor, which is always an aggravating variable in an incident.
- The *Human* factor, which is often neglected because management relying too much on technology. This factor is based on the following aspects:
 - the ability to detect an incident,
 - the ability to decide on immediate contingency measures,
 - the fear of “psychological notions” as to one’s ability to face an unfamiliar situation and to have to decide (whether or not to make the right choice depending on the lack of information or the need for availability of service, for example),
 - the ability to absorb stress,
- The *Awareness* factor, which is the answer to a simple question: “If I face a threat or vulnerability tomorrow, do I have the knowledge to deal with it?”

This observation shows that crisis management is based on the following equation:

$$\text{TIME factor} \times (\text{HUMAN factor} \times \text{AWARENESS factor})$$

TIME = Deadlines for detection, understanding, decision

HUMAN = Stress, fear, emotion, external influence

AWARENESS = Practical and theoretical skills and knowledge

In this equation, a simple relationship has been highlighted: the undeniable link between humans and awareness. In a structured and organized system in which a service must be delivered, it is imperative that people are “aware” of the cyber risks associated with their activity. As a result, it follows that in a critical situation, humans must not only be aware but they must also be able to

understand the situation, to decide according to the psychological pressure in a short time and to analyze the effects of the decision-making process. No system is able to respond to this type of issue and therefore replace humans.

In this sense, the Cybersecurity Competence Center in Luxembourg has therefore undertaken the development of the ROOM # 42, a cyberattack simulator aiming at testing the above-mentioned equation.

The concept is simple and consists in projecting 5 to 8 people representative of a working environment (director, marketing department, IT, HR, customer service, lawyer, etc.) in the simulator in order to expose them to cyberattacks and to observe their behavior.

In order to meet the requirements of such a means dedicated to testing and developing cyber skills, the C3 has given priority to orienting its overall reflection on the association of the following three pillars:

Observe — Test — Train

As part of the development of ROOM # 42, this concept was not only applied but reinforced at the level of the first pillar “observe”.

Observe — Test — Observe — Train

Phase 1 - Observe

In order to be able to achieve the objectives of the *Test* and *train* pillars, it is essential to have a permanent observation capacity of the global cyber context in order to know and fully understand:

- *The threat.* What type of threat are we exposed to (cybercriminals, terrorism, Insider, script kiddies. . .)? What are their methods? When is it most active? ...
- *The impacts.* Depending on the known exploits, what were the financial, reputational, legal consequences, etc.
- *The types, occurrences and frequencies of attacks.*
- *The countermeasures.* Are there reliable means to fight or respond to an incident?
- ...

Phase 2 - Test

Based on the observations made in Phase 1, this step consists of creating attack scenarios and simulating them in ROOM # 42 in order to expose a team to near-reality attacks.

Phase 3 - Observe

This step consists in the most pragmatic way possible of observing the participants during the “simulation” test phase. The key points observed are the following:

- Ability to detect an incident,
- Delay before detection,
- Understanding of the incident
- Communication of the incident,
- Immediacy of the decision-making,
- ...

Phase 4 - Train

The purpose of a simulation within the ROOM # 42 is to evaluate maturity level of an entity to face a succession of incidents and to present a diagnostic of points to be improved by awareness. As a result, many key points, such as those mentioned above, are analyzed; in the event of a failure, typical

training is offered. However, ROOM # 42, beyond the "test" aspect, is itself a particularly effective means of training because it allows to apply cybersecurity skills in a simulated context. It is always very instructive to move from the theory to the benefit of the practice.

After 3 years of operation, the observations made during the simulations in ROOM # 42 proved that human processes in terms of cybersecurity require greater attention from managers. For example, here is a sample of observations made over the 2018/2021 period:

Cryptoransomware

- 85% took more than 15 minutes to detect and react.
- 60% of countermeasures were not sufficient.

Fake news

- 65% of the participants were not able to handle this type of incident.

Defacing

- 35% of the participants were unaware of this type of attack.

Social Engineering

- 10% of the participants gave a password over the phone to a stranger.

Cybercriminals

- 40% of the participants paid a ransom.

Crisis

- 45% have difficulties or do not know how to manage a crisis.

CERT

- 70% of the participants do not think about asking a CERT for help.

Communication

- 80% of the participants neglect internal communication in times of crisis.

Evidence

- 95% of the participants do not think about preserving evidence of a cyberattack.

These data, derived from observations of simulations, prove the deficit in terms of skills and investment in people and should question the priority rules for cybersecurity training.

5.1.4 The best way to raise awareness in cybersecurity

The best way to educate the public about cybersecurity is to take a comprehensive approach including the following steps:

1. Define the need,
2. Hold the legitimacy of management and make it known,
3. Define a budget,
4. Design an awareness strategy based on the expressed need,
5. Monitor and analyze the effects of the awareness-raising strategy.

Define the need

An awareness strategy must meet a need. This one can be totally different depending on the business requirements and the objectives sought by management. Here are some examples:

- A company wants to educate its employees against phishing because it has already understood the impacts of cryptoransomware,
- A political group wants to protect itself against any kind of influence,
- Teachers want to improve their knowledge of cyber threats that can target them and learn how to protect themselves against them.

Hold the legitimacy of management and make it known

When the need is expressed by the management, it is important that the entire target audience understands the importance of awareness. This is why management must communicate its decision and the reasons for it.

Define a budget

Before starting to design the strategy, it is essential to obtain a budget that will allow the means of the project to be defined.

Design an awareness strategy based on the expressed need

To succeed in an awareness-raising strategy, efforts must take into account a mix of formal and informal actions:

Formal

- Organize an annual awareness session with a trainer,
- Use of educational tools on the Internet (online training),
- Organize thematic awareness raising (phishing, social engineering, social media...),
- Regularly test awareness levels through exercises,
- Phishing test campaign.

Informal

- Regularly inform employees or the public through:
 - Internet publications
 - Press articles
 - Newsletters and internal communications
- Organize / Participate to cyber conferences or conferences on the topic of cybersecurity

In this sense, the organization of cybersecurity awareness raising should be considered as the management of media planning by a communication service. It should be understood that the whole must be balanced and organized according to:

- Targeted objectives,
- Time and deadlines,
- Approach models (formal and informal).

As indicated previously, the purpose depends on the need for awareness. For example:

- Maintain a permanent level of alertness to be able to quickly detect a threat,
- Simply fight against phishing,
- ...

Monitor and analyze the effects of the awareness-raising strategy

Any awareness campaign must be able to be analyzed from a quantitative and qualitative point of view:

- Number of people sensitized,
- Quality of awareness,
- In the case of tests or exercises, the results thereof,
- ...

The aim is to be able to present a report to management showing the level of awareness reached and the negative points that still need to be addressed.

5.2 Current Status and Next Development

It is important to consider that awareness in terms of cybersecurity is not an end result but must be maintained over time. This is why, within the SPARTA project and beyond, efforts will have to be continuously exerted in this direction.

The key points to develop is to teach participants to create an awareness campaign mixing:

- Awareness,
- Exercises,
- Various and targeted communications,
- Tests,
- Conferences.

Participants will need to be able to balance an awareness program annually.

In addition, it is important to teach participants to be autonomous in creating awareness content so that they can properly adjust their messages to the needs of their businesses or according to the vulnerabilities of their ecosystems.

Finally, a last point, which is very important, consists in teaching participants to measure the effect of their awareness in order to be able to demonstrate to their management the importance of this activity and to prove that it is essential to maintain it in the time.

Chapter 6 Piloting Activities

6.1 Education and Training Pilots

6.1.1 Pilot Overview

To build our list of pilots, we asked WP9 partners to describe some of their courses that were influenced by SPARTA during the project.

To this aim, we gathered the following information on the different courses:

- the name of the course,
- the type (University Program or Professional Training) and level (Bachelor, Master or PhD) of the course,
- the number of executions of the course,
- the date of creation (or last major update) for this course,
- the number of hours for this course,
- the covered topics (among the SPARTA skills described in D9.2 [2]),
- whether this course follows the D9.2 guidelines.

Among SPARTA Partners involved in education and professional training, we selected 50 pilot courses that ran during the year 2021 and were conformant to the SPARTA guidelines described in D9.2 [2]. For pilot courses, the guidelines can be summarized as follows:

- the course is dedicated to Cyber Security (Cryptography, Security, Privacy, etc.) instead of being a general course on Computer Science,
- the course contains practical hands-on education in labs, programming, etc.
- when relevant to the topic, the course involves modern technologies for training, such as cyber ranges, virtualization, etc.
- when relevant to the topic, the course covers novel trends in security (blockchain, (post)quantum, privacy by design, etc.)

Fig. 6.1 and 6.2 present the repartition of these pilot courses relative to their country and to the type of program they are part of. The 50 pilots initially selected thus represent a good variety for both criteria.

Since cybersecurity is a fast-evolving domain, it is also interesting to look at the data from an age perspective. Fig. 6.3 shows the repartition of the pilots with regards to their date of creation of last major revision. Thus, we can see that the material used in these classes is usually fresh, which is consistent to our guidelines. It is also interesting that 36 out of the 50 pilots were only run once or twice in total, showing there again a dynamic trend in course design.

In Fig. 6.4, we represent, for each category of SPARTA skills, the proportion of pilots covering at least one topic in the corresponding category. As expected, most categories are well represented, with a notable exception in Mathematics. This is explainable since Mathematics mostly are a building block for cybersecurity-related topics, and may be part of a program as a standalone course. Apart from this category, we can thus conclude our pilot corpus covers rather well all the relevant domains.

The tables in Fig. 6.5 gives a more detailed view of this coverage, with the proportion of pilots covering each specific skill for each category.

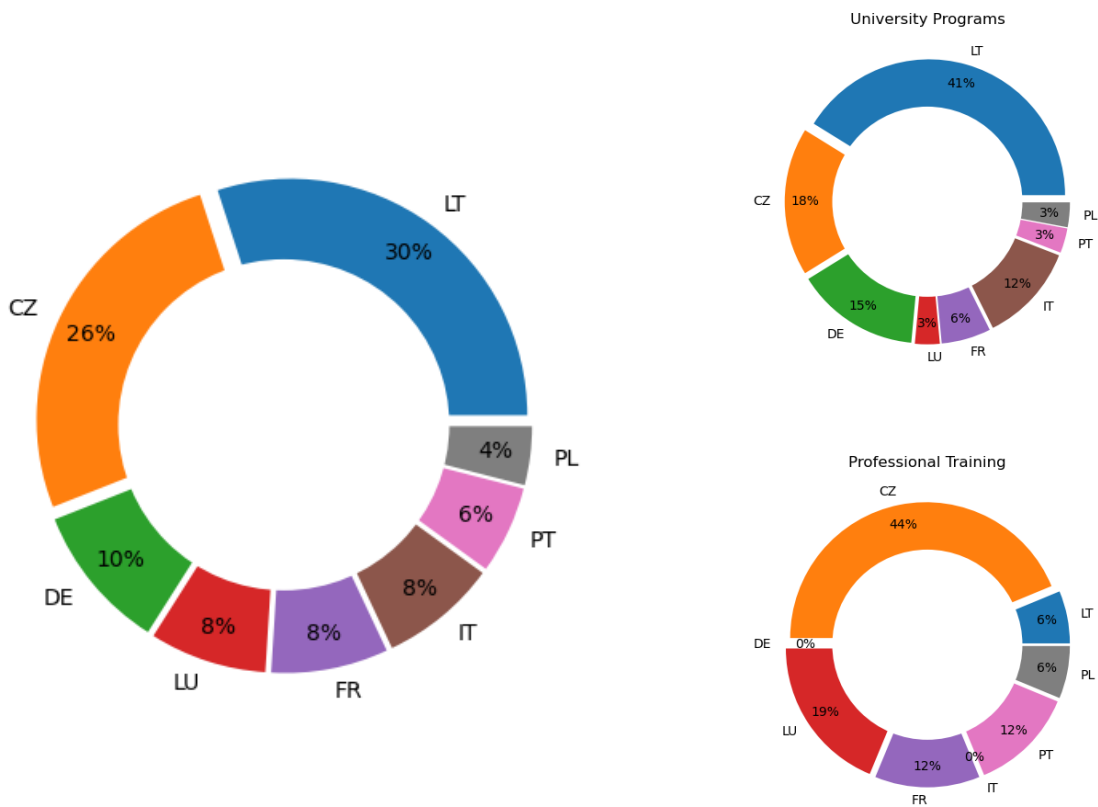


Figure 6.1: Repartition of SPARTA WP9 Pilots per Country.

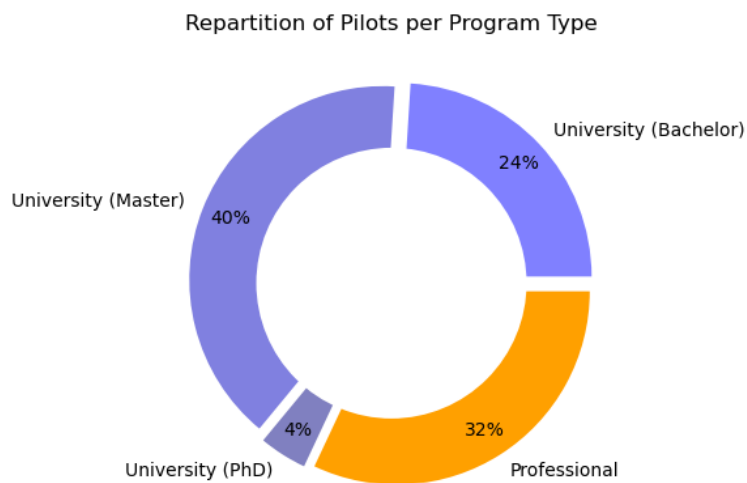


Figure 6.2: Repartition of SPARTA WP9 Pilots per Type. The blue portions represent courses from University Programs (for different levels) and the orange portion is for courses from Professional Training.

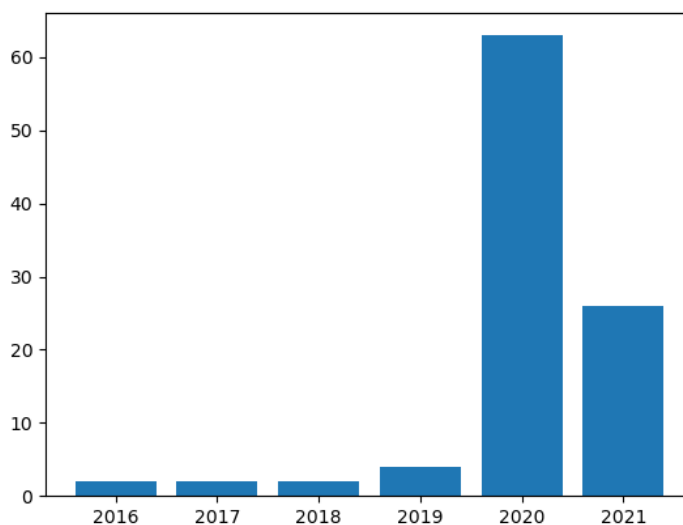


Figure 6.3: Repartition of SPARTA WP9 Pilots per Age. The dates correspond to the creation or the last major revision of the course.

6.1.2 Sample Pilots

This section describes some of the pilot courses retained. For each partner contributing at least one pilot that ran in 2021 and for which we had a significant number of answers to our questionnaire from the students, we give a short presentation of the most represented course in the poll.

BUT — Foundations of Cryptography

- Course from a University Program at the Bachelor level
- Creation / Major Revision in 2020
- Covered Topics in Mathematics and Cryptology
- This is a 26-hour course about theoretical foundations of cryptography and computer security. Based on these foundations, students will be able to analyze and design security solutions for information and communication technologies.

IMT — Security-Oriented Programming

- Course from a University Program at the Master level
- Creation / Major Revision in 2020
- 45-hour course (50 % lectures, 50 % practical exercises)
- Covered Topics in Computer Science and Security
- The course is a 45-hour initiation to software vulnerabilities and to standard tools and methodologies in software engineering, such as git, Continuous Integration and Test-Driven Development. It is composed of 50 % lectures and 50 % practical exercises. It includes in particular two graded labs on parser development and bug finding in a Python application.

KTU — Security of Information Technology

- Course from a University Program at the Bachelor level
- Creation / Major Revision in 2020
- Covered Topics in Security, Privacy and Humanistics
- This course is a 64-hour course

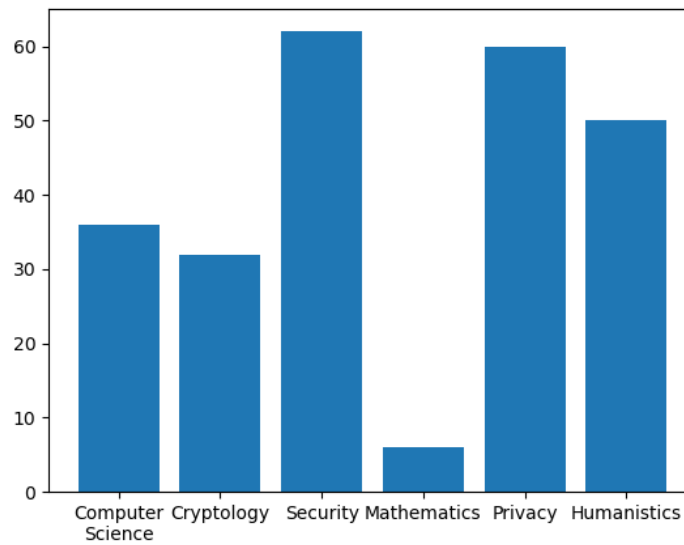


Figure 6.4: Proportion of SPARTA WP9 Pilots covering each Skill Category.

Computer Science	
Computer Systems	10 %
Industrial Applications	12 %
Communication Theory	6 %
Computer Networks	28 %
Quantum Computing	2 %
Theoretical Computer Science	4 %
Software Engineering	2 %

Cryptology	
Advanced Cryptology	8 %
Cryptanalysis	8 %
Fundamental Cryptology	24 %
Post-quantum Cryptography	4 %

Security	
Hardware and Software Security	46 %
Network Security	44 %
Security Systems	16 %
System Security	34 %
Incident Response	24 %

Mathematics	
Algebra and Discrete Mathematics	4 %
Number Theory	4 %
Complexity Theory	4 %
Probabilistly and Statistics	2 %
Topology and Analysis	0 %

Privacy	
Data Extraction	18 %
Data Privacy	40 %
Privacy-enhancing Technologies	26 %

Humanistics	
Human Aspects of Security and Privacy	32 %
Security Architecture	6 %
Laws and Regulations	30 %
Cybercrime	32 %
Security Management and Risk Analysis	22 %

Figure 6.5: Proportion of SPARTA WP9 Pilots covering each Topic.

CZ.NIC — Introduction to Forensic Analysis of Memory

- Course from Professional Training
- Creation / Major Revision in 2019
- 6-day Practical Exercises
- Covered Topics in Security and Privacy
- The course introduces participants to the issue of forensic memory analysis and introduces them to the open source tool Volatility, the use of which they will try in practical exercises on pre-prepared samples. The content will focus on the memory of the Windows operating system.

UBO — IT Security

- Course from a University Program at the Bachelor level
- Creation / Major Revision in 2020
- Covered Topics in Computer Science, Cryptology, Security, Privacy and Humanistics
- This course is a 270-hour course (60 % lectures, 40 % practical exercises)

Overall, the 50 pilots represent 2,100 students in 2021 (1150 for university programs and 950 for professional training).

6.1.3 Questionnaire for the Students

The purpose of this questionnaire was to capture the opinions of students participating in the selected pilot courses. 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 proportion of practical exercises in the course,
- the skills they believe the course covers,
- the roles that they believe the course provides skills for,
- the roles that they would like to work in after passing this course,
- the improvements that can be gained through changes to the program structure.

Respondents Structure and Quantity

The questionnaire was conducted in the period from July 1st till July 15th, 2021 for the Spring courses, and in the period from October 20th till December 1st, 2021 for the Fall courses. The very late (and consequently short) period for the Spring session can explain why many courses were not very well represented by the questionnaire.

Among the 50 pilots identified for this study, we obtained 89 answers from students who attended 20 different courses. Overall, this represents around 10 % of the enrolled students for the period for these courses. The detailed information on survey respondents can be found in Table 6.1.

Most of the students participating in the survey were from the Czech Republic (38 people, 41 % of all), with a high representation of students from Germany (23 people, 25 %) and France (17 people, 18 %). The overall information on participants locations can be found in Figure 6.6.

Practical-based learning ratio

An indicator we identified to evaluate the content of the course was the perceived proportion of the course that was dedicated to practical-based learning. In Deliverable 9.3 [3], which proposed a similar study at the program level, the result was that program administrators set this ratio at 61 % of practical-based training (for 39 % of theory-based training); students, on the other hand, perceived that 65 % of the programs were practical-based learning, which seems to show that the different points of view were aligned.

For the selected courses, the percentage of practical-based training, as seen per the course administrators, was between 40 to 60 %, with an average around 50 %. The perception of the proportion

Name of the Partner	Course	U/P	Answers
Brno University of Technology (BUT, Czech Republic)	Liability in ICT Law	U	4
	Foundations of Cryptography	U	15
	ICT Security 3	U	1
	Information Security Seminar	U	8
	MPA-MOK Modern Cryptography	U	5
Télécom SudParis (IMT, France)	Security-oriented Development	U	10
	Systems Security	U	5
	Cybersecurity for industrial systems	P	1
	Legal aspects of cybersecurity	P	1
Kaunas University of Technology (KTU, Lithuania)	Security of Information Technology	U	4
	Cyber Security	U	1
Sapienza University of Rome (CINI, Italy)	Cybersecurity	U	1
University of Roma Tor Vergata (the CNIT Unit, Italy)	Vulnerability and Defense of Internet Systems	U	7
Mykolas Romeris University (MRU, Lithuania)	Personal Data Protection in Technology Business	U	1
CZ.NIC (Czech Republic)	Cyberbullying and other risk phenomena on the Internet	P	2
	Introduction to forensic analysis of memory	P	3
University of Bonn (UBO, Germany)	Moderne Kryptographie und ihre Anwendung	U	2
	Netzwerksicherheit	U	1
	Reaktive Sicherheit	U	2
	IT-Sicherheit	U	15
		Total	89

Table 6.1: Repartition of the answers to the questionnaire sent to the students of the pilots. The U/P column describes the typo program the course is part of (University or Professional training).

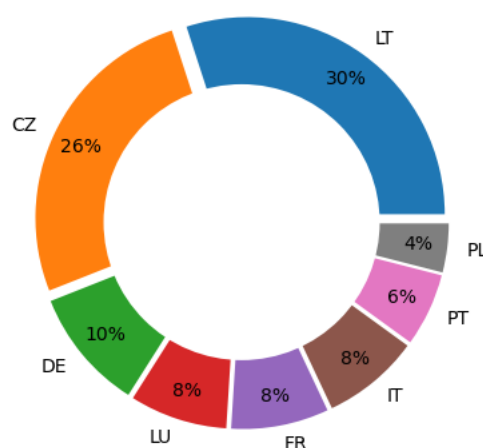


Figure 6.6: Repartition of the answers to the questionnaire per country.

of practical-based learning for these courses, as seen by the students here again align with the administrators' point of view, with a 55 % ratio for practical-based learning.

It is however interesting to say that the standard deviation for this indicator is rather high, with a value of 22. For example, for a given course with 15 answers, the students average ratio was 56 %, for values ranging from 25 % to 100 %.

The consolidated results for the practical-based learning ratio are given in Fig. 6.7

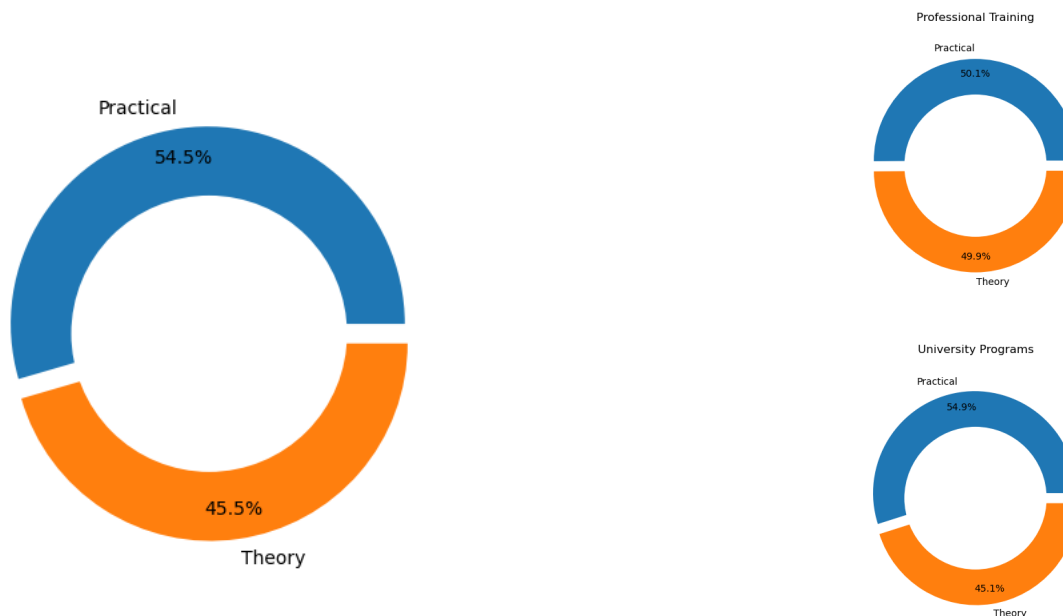


Figure 6.7: Practical- and theory-based training ratio of the pilot courses, as perceived by students, with a focus respectively on University Programs and Professional Training.

Building on this ratio, we asked the students tell us what the evolution of the ratio should be. Overall, two thirds of them believe the approach is well balanced, whereas 30 % would like to have more practical-based learning and 4 % would prefer to have more theory. If we look at professional training, the expectations are more significant toward more practical-based material, as shown in Fig. 6.8.

Category and Topic Coverage

We tried to study the category and topics covered by the different pilots, comparing the points of view of course administrators and students. First, we restricted the data from Fig. 6.4 to the 20 pilots for which we had received answers. Then we compared the results to the perception from the students. We did the same for the detailed view per SPARTA topics.

The result, present in Fig. 6.9 for the broad categories and in Fig. 6.10 for detailed topics. However, it seems the students selected an important number of topics (and consequently a big number of categories) for each course, which mostly seems to demonstrate that the topic distribution was not adapted to the students' perception.

In particular, for the "Security-oriented Programming" course, it was quite surprising to have the students select the following topics as covered by the course: Fundamental Cryptology, Number Theory, Data Extraction, Data Privacy and Cybercrime. Indeed, the course administrator definitely does not feel this topics are covered in the course.

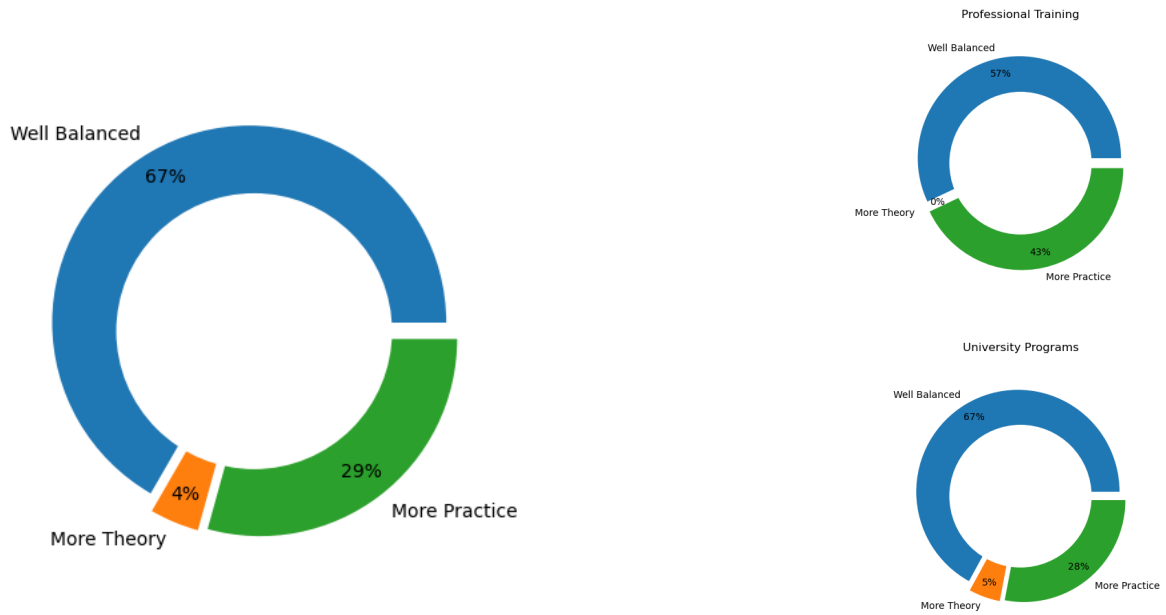


Figure 6.8: Student Preferences regarding the ratio between practical- and theory-based learning, with a focus respectively on University Programs and Professional Training.

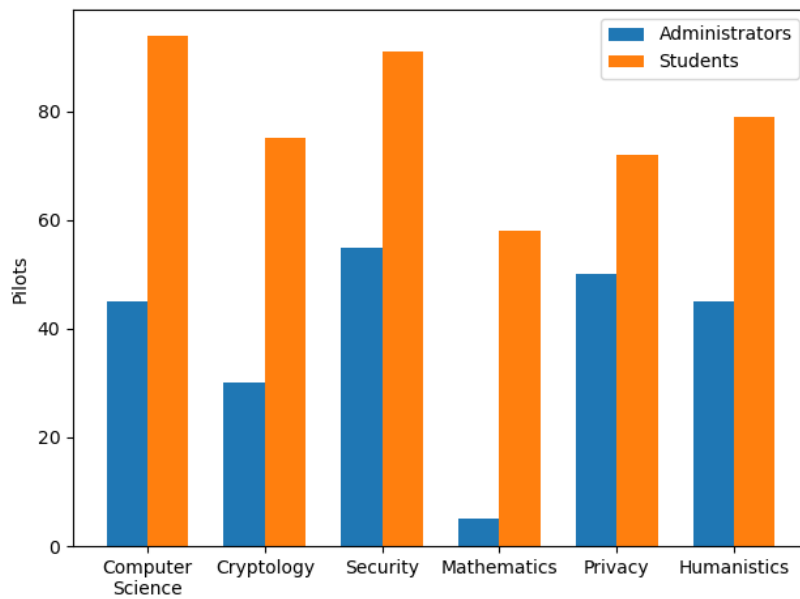


Figure 6.9: Proportion of SPARTA WP9 Pilots covering each Skill Category (restricted to the 20 pilots with answers), compared to the student perception.

Computer Science			Mathematics		
Computer Systems	15%	57%	Algebra and Discrete Mathematics	5%	38%
Industrial Applications	15%	18%	Number Theory	5%	30%
Communication Theory	15%	44%	Complexity Theory	5%	28%
Computer Networks	25%	52%	Probabilistly and Statistics	0%	24%
Quantum Computing	5%	15%	Topology and Analysis	0%	16%
Theoretical Comp. Sci.	0%	47%			
Software Engineering	5%	37%			

Cryptology			Privacy		
Advanced Cryptology	10%	66%	Data Extraction	20%	27%
Cryptanalysis	0%	33%	Data Privacy	40%	63%
Fundamental Cryptology	25%	25%	Privacy-enhancing Technologies	20%	30%
Post-quantum Cryptography	10%	15%			

Security			Humanistics		
Hardware & Software Security	35%	43%	Human Aspects of Security & Privacy	25%	37%
Network Security	35%	52%	Security Architecture	10%	34%
Security Systems	20%	38%	Laws and Regulations	30%	34%
System Security	25%	67%	Cybercrime	25%	47%
Incident Response	25%	15%	Security Management & Risk Analysis	10%	20%

Figure 6.10: Proportion of SPARTA WP9 Pilots covering each Skill Category (restricted to the 20 pilots with answers, left column), compared to the student perception (right column).

Link between courses and roles

For similar reason, the data collected about work roles were not really exploitable. Moreover, the three following questions were marked as optional:

- For which Work Roles does the course provide skills/knowledge?
- What is your expected Work Role you want to work in after passing the courses?
- Was the training relevant to your expected Work Role?

The questions about Work Roles, which can already be perceived as very abstract for the students, are even harder to grasp at the course level than at the program level.

Overall satisfaction

In the questionnaire, we also asked three questions about the overall satisfaction. The first one was an overall appreciation, on a scale of -3 (the course was awful) to 3 (the course was absolutely fabulous), the pilots obtained an average grade of 1.83. For courses included in professional training only, the grade was 2.00, whereas it was 1.82 for university programs. The exact repartition of the students' answers is given in Fig. 6.11.

In the next question, students were asked to grade how much they believe they had learned from the given course, on a scale from 0 (I learned nothing) to 3 (I learned a lot). The overall grade for the pilots was 2.37, as well as for the university programs; professional training got a better feedback, with a grade of 2.47.

Finally, we asked the students whether they thought that what they learnt would be useful in their professional life, again on a scale from 0 (not at all) to 3 (a lot). Overall, the pilots obtained 2.10, with 2,57 for professional training courses and 2.06 for courses included in university programs.

The details of these two questions are givent in Fig. 6.12 and 6.13.

It thus seems the pilots were overall appreciated by students, who think they have learned from these courses, including material that they think will be useful for their professional life. It is worth noting

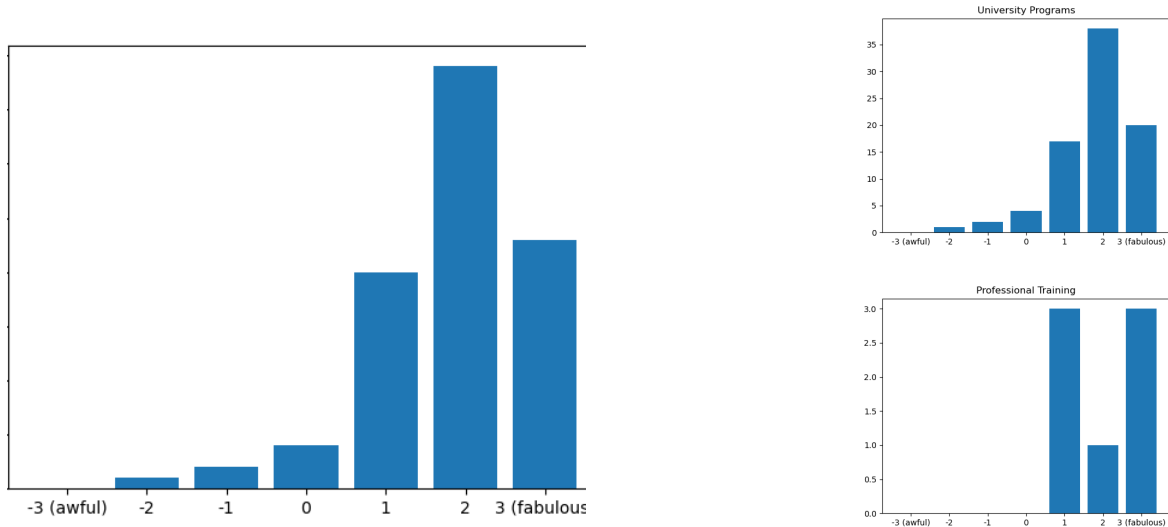


Figure 6.11: Student Satisfaction for SPARTA WP9 Pilots.

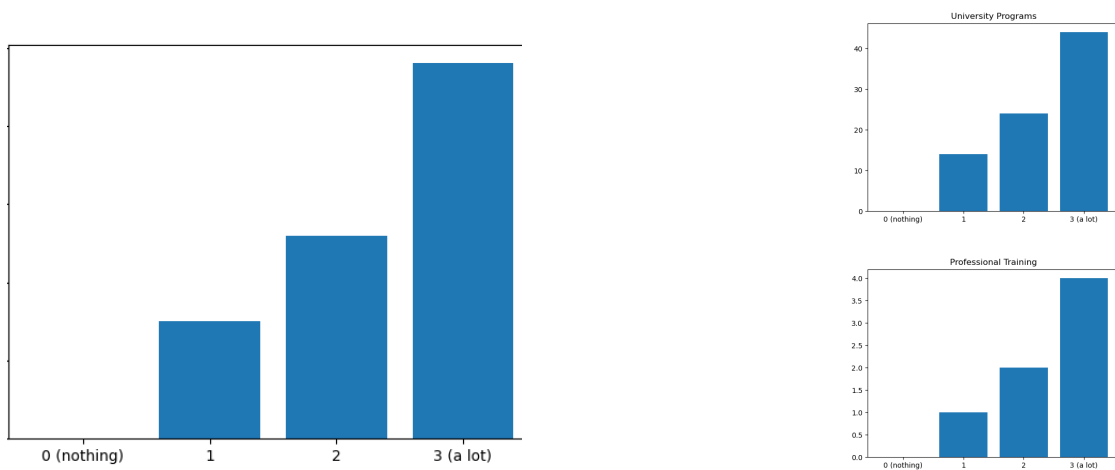


Figure 6.12: Evaluation by students of the amount learned during SPARTA WP9 Pilots.

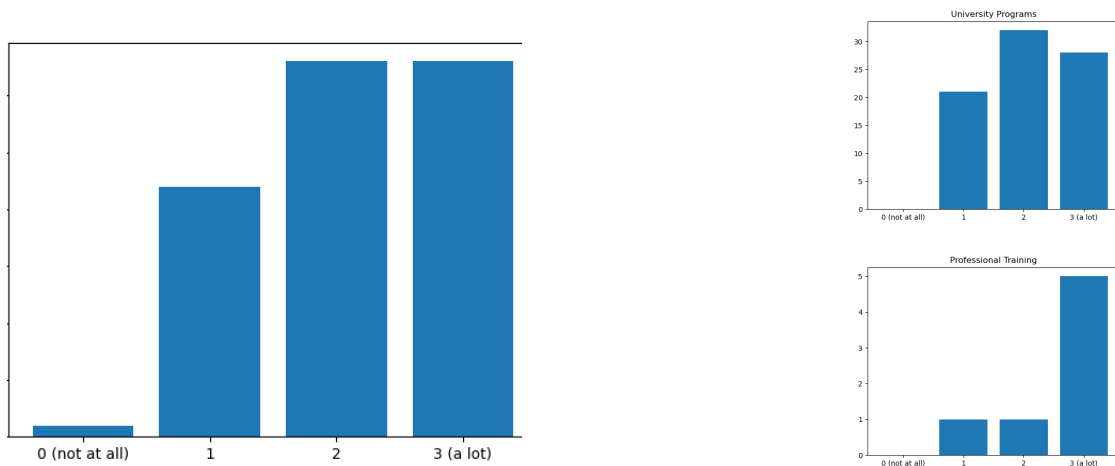


Figure 6.13: Evaluation by students of the usefulness of the material learned during SPARTA WP9 Pilots for their professional life.

that professional training benefit from slightly better grades, in particular for the applicability of the acquired skills.

These figures are rather good and encouraging, but there is still some room for improvement. In the final paragraph of this section, we will analyse the proposals from the students to make our courses better.

Improvement perspectives

Overall, we received only 26 comments from the students.

Among these comments, several of them (8) were just positive feedback about the balance of the course or praising the great skills of the teachers.

Excellent topics and interesting professors!

Two comments indicated that courses should be longer, either because the student wished to cover more aspect, or because they wanted more theory to better understand the hands-on exercises.

More theory so that the practical part is more doable.

The next concern that was shared by five students is the need for more practice in several courses. Several comments were about programming exercises, and the others were about the addition of real-world use case studies. In the same vein, two comments were about the need for more real-life applications, to better prepare students for their future.

I'd love to hear about more actual references to real-life applications.

Besides these easy-to-analyse remarks, there were several comments (7) criticizing pilot courses, either due to their perceived lack of overall structure, or because they were not cybersecurity-oriented enough. However, the comments did not propose much constructive thoughts. It is worth noting that all of these comments were about courses included in university programs, and it would probably require to analyse the whole program to understand the underlying problems.

More cryptography and pentesting, less telecommunication.

In the same spirit, two students seemed to have trouble with programming exercise, leading in particular to the following cry for help, that is hard to understand out of context:

Less hexadecimal in code.

Finally, among the miscellaneous remaining comments, one was about the difficulty for students to stay involved when having to attend classes remotely due to the COVID pandemic.

Overall, the take-away messages seem to be consistent with previous results, and we should pursue our efforts of proposing more practical exercises and real-world applications to the students.

6.2 Go Cyber with SPARTA

During SPARTA, WP9 partners organized 4 workshops for the Go Cyber With SPARTA initiative:

- Universidad de Las Palmas de Gran Canaria in the Canary Islands, in June 2021,
- SMEs in Madeira, in October 2021,
- Digital Reunion¹ in La Réunion, in Novembre 2021,
- Office de l'Eau² in La Réunion, in November 2021.

Each of these workshops spanned over 1 to 5 days. Due to COVID-related restrictions, some of the classes have been taught remotely.

¹<https://digitalreunion.com>

²<https://www.eaureunion.fr>

6.2.1 Workshop Description

Workshop in La Réunion

The most comprehensive workshop is the one that was given in La Réunion for the Office de l'Eau in November 2021.

Cybersecurity Awareness	
Lecturer	Jérôme Jacob (SMILE)
Content	Introduction Adopting initial reflexes Protecting yourself Managing your security
Duration	2 hours

Cryptography and Data Privacy	
Lecturer	Sara Ricci (BUT)
Content	Terminology Basic Mathematical Foundations Symmetric Cryptography Asymmetric Cryptography Protocols Data privacy Anonymization
Duration	4 hours

Legal Aspects of Privacy and Personal Data Protection	
Lecturer	František Kasl and Pavel Loutocký (BUT)
Content	Personal data - principles, EU framework - GDPR, other frameworks worldwide (US, UK, China, Africa, Australia) Privacy - principles and concept of privacy, privacy in workplace (case-law of European court of human rights regarding permissible monitoring of employees), practice worldwide (US, UK, China, Africa, Australia) Cybersecurity requirements - EU law and NIS directive, recommended measures and procedures / other legal regulation (US, China) Authentication and access control, identity management Cross-border aspects and contract law with practical implications Examples and practical cases
Duration	5 hours

System Security	
Lecturer	Petr Dzurenda (BUT)
Content	OS security (MS Windows, Linux, macOS): focus on MS Windows security User Authentication Data Security (File and Folder Permissions, Encryption) Windows Firewall
Duration	4 hours

System and Network Security	
Lecturer	Petr Dzurenda and Lukas Malina (BUT)
Content	Ethical hacking, penetration testing, vulnerabilities L2-L7 security protocols (MACSec, IPsec, TLS) VPN Firewall and IDS/IPS Logging and Monitoring
Duration	5 hours

Network Security in Practice	
Lecturer	Lukas Malina (BUT)
Content	Secure configuration (hardening) of network devices (switches, AAA, routers, firewalls, IPS) in practice, focused on CISCO (packet tracer)
Duration	4 hours

ICS Security	
Lecturer	Alexandre Delaby (ANSSI)
Content	Main Concepts about ICS Analysis of ICS Cybersecurity
Duration	6 hours

Workshop in the Canary Islands

On June 7th, 2021, WP9 and WP12 proposed a workshop on how to successfully design and implement a bachelor study program on cybersecurity to the University of Las Palmas de Gran Canaria (ULPGC).

The different sessions of this day were about the following topics:

- The SPARTA project and the Go Cyber with SPARTA campaign,
- The Cybersecurity Skills Framework as a part of the response to the skills gap challenge in the EU,
- The Education Map Application, or how to get information about cybersecurity education providers worldwide,
- The Curricula Designer: theory and practice.

The workshop ended with the common will to establish a Cybersecurity bachelor degree on ULPGC, in a collaborative effort with SPARTA.

6.2.2 Feedback Analysis

Overall, around 25 trainees were taught during the 4 workshops. The informal feedback we collected in the moment were very positive. However, we only received 2 answers to the formal satisfaction questionnaire we sent to the participants afterwards, which is very low.

These answers came from people new to the cybersecurity who were attending their first cybersecurity workshop. Overall, the feedback was rather positive on the content (2.5 on the scale from 0 to 3), which was believed to be useful for their professional life (2 on the same scale). Finally, they would recommend participating similar cybersecurity workshops.

If the travel conditions had been simpler, WP9 partners could have proposed more workshops during the SPARTA project. We actually plan to reuse the material to propose similar workshops in 2022.

Chapter 7 Summary and Conclusion

There is a recurring need for cybersecurity professionals in the EU, and the situation will persist for the foreseeable future. It is thus important to develop awareness, education and training capabilities in the EU to fill in the gap.

To this end, WP9 was proposed within the SPARTA project to analyse, develop and accompany university programs, professional training and awareness campaigns. Beside delivering courses, awareness campaigns and workshops, WP9 partners developed best practices and associated tools to help design new courses or update existing ones. These tools are important achievements which will probably have an impact on education, training and awareness activities, beyond the scope of the SPARTA project.

First, a Cybersecurity Skills Framework was developed. Based on the NICE framework proposed by NIST, it was a valuable input in the discussions at the European level to develop a common framework. We also used the developed framework within WP9 to establish links between the skills developed in a course or a program on the one hand, and the targeted work roles on the other hand. Within WP9, two tools were developed to help identify and design university curricula. The first one, the Education Map, is an online application allowing to search for existing programs worldwide, with different search criteria; as for the Skills Framework, the Education Map has been used in various exchanges with the other pilots and the ENISA, to help provide a unified and collective map. The second tool is the Curricula Designer, which allows program administrators to describe their courses and assess their relevance to train students towards given work roles; it was successfully used to evaluate existing programs or to help design new ones.

Regarding professional training, several WP9 partners developed a federated infrastructure of Cyber training & exercise Framework, to help build cyber ranges from reusable components. The resources developed cover both the infrastructure (including an open-source platform) and the training material (scenario, exercises).

In 2021, WP9 partners selected courses among their education and training programs, that followed the best practices described during the project. The result was a corpus of 50 courses, that were described and analysed. These so-called pilots represented more than 2,000 students in 2021.

Using student feedback for these pilots, we confirmed the relevance of our best practices, and the general satisfaction of the students. In particular, the skills acquired from these courses were generally perceived as useful for the professional life.

However, it is important to understand that there is always room for improvement, and that cybersecurity education, training and awareness is a fast-evolving domain, which will require following new trends and emerging topics, as well as adopting modern practical learning techniques (e.g. CTF and cyber ranges).

Chapter 8 Bibliography

- [1] SPARTA. *D9.1: Cybersecurity skills framework*. <https://www.sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf>
- [2] SPARTA. *D9.2: Curricula descriptions*. <https://www.sparta.eu/assets/deliverables/SPARTA-D9.2-Curricula-descriptions-PU-M18.pdf>
- [3] SPARTA. *D9.3: Training Evaluation Pilot*.
- [4] *European e-Competence Framework*. <https://www.ecompetences.eu/>
- [5] ENISA. *European Cybersecurity Skills Framework*. <https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework>
- [6] ENISA. *Ad-Hoc Working Group on the European Cybersecurity Skills Framework*. https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/adhoc_wg_calls
- [7] NIST. *NICE Framework Supplemental Material*, July 2020. <https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-supplemental-material>
- [8] Jan Hajný, Sara Ricci, Edmundas Piesarskas, Marek Sikora. *Cybersecurity Curricula Designer*. In Proceedings of ARES 2021: The 16th International Conference on Availability, Reliability and Security. ACM, 2021. p. 1-7. ISBN: 978-1-4503-9051-4.
- [9] Sandra Wheatley Smerdon. *Cybersecurity training can close skills gap for a safer digital world*. <https://www.weforum.org/agenda/2021/05/cybersecurity-training-skills-gap-digital/>

Chapter 9 List of Abbreviations

Abbreviation	Translation
5G	Fifth Generation of Mobile Networks
ACCSE	Academic Centres of Cyber Security Excellence
ACM	Association for Computing Machinery
ACM CSEC	Association for Computing Machinery Cybersecurity Education
ACS	Australian Computer Society
AGH	Akademia Gorniczko-Hutnicza
AI	Artificial Intelligence
AIS SIGSEC	Association for Information Systems Special Interest Group on Information Security and Privacy
APAC	Asia Pacific
API	Application Programming Interface
ARP	Address Resolution Protocol
APSACS	Advanced Professional Specialist Accreditation in Cyber Security
BIBIFI	Build-it Break-it Fix-it contest
BYOD	Bring Your Own Device
CAE	National Centers of Academic Excellence
CAE-CD	National Centers of Academic Excellence - Cyber Defense
CAE-CDE	National Centers of Academic Excellence - Cyber Defense Education
CAE-CO	National Centers of Academic Excellence - Cyber Operations
CAE-R	National Centers of Academic Excellence - Cyber Defense Research
CAPEC	Common Attack Pattern Enumeration and Classification
CBoK	Core Body Of Knowledge
CBK	Cybersecurity Common Body of Knowledge
CCTV	Closed-Circuit Televisions
CEP	Cyber Education Project
CISM	Certified Information Security Manager
CISA	Certified Information Systems Auditor
CNN	Cyber Competence Network
COMSEC	Communications Security
CPS	Cyber-Physical System
CPU	Central Processing Unit
CSEC2017 JTF	Joint Task Force on Cybersecurity Education
CSF	Cybersecurity Skills Framework
CSSS	CyberSecurity Skills Shortage
CTF	Capture the Flag
CVE	Common Vulnerabilities and Exposures
CVP	Closest Vector Problem
CWE	Common Weakness Enumeration
CYBERSEC	Cybersecurity
CyberSec4Europe	Cybersecurity for Europe
CyBOK	Cyber Security Body of Knowledge
DAC	Discretionary Access Control
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DES	Data Encryption Standard
DevOps	Software Development in Information Technology Operations
DHS	Department of Homeland Security
DMZ	Demilitarized Zone

Abbreviation	Translation
DNS	Domain Name System
DOE	Department of Energy
DPA	Data Protection Act
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSA	Digital Signature Standard
EC	European Commission
ECC	Elliptic Curve Cryptography
ECSC	European Cyber Security Challenge
ECISO	European Cyber Security Organization
ECTS	European Credit Transfer and Accumulation System
EEA	European Economic Area
EFTA	European Free Trade Association
EIT	European Institute of Innovation & Technology
EITC	European Information Technology Certification
EITCA	European Information Technology Certification Academy
EITCI	European Information Technology Certification Institute
EITCI	European Information Technology Certification Institute
ENISA	European Union Agency for Cybersecurity
EPF	Ecole Polytechnique Federale
ETH	Swiss Federal Institute of Technology
EU	European Union
FAS	Fire Alarm Systems
GDPR	General Data Protection Regulation
GSM	Global System for Mobile Communications
GSOC	Global Security Operations Center
HAPS	Health Assessment Program for Seniors
HCI	Human Computer Interface
HEI	Higher Education Credit Framework for England
HTML DOM	Hypertext Markup Language Document Object Model
HTTP	Hypertext Transfer Protocol
HW	Hardware
IaaS	Identity as a Service
IAS	Intruder Alarm Systems
IADF	Instructional and Assessment Design Framework
IAPP	International Association of Privacy Professional
IBE	Identity-Based Encryption
ICMP	Internet Control Message Protocol
ICPC	International Collegiate Programming Contest
ICS	Industrial Control Systems
ICT	Information and Communication Technology
IDL	Interactive Data Language
IDS	Intrusion Detection System
IEEE-CS	Institute of Electrical and Electronics Engineers - Computer Society
IETF	Internet Engineering Task Force
IFIP WG 11.8	International Federation for Information Processing Technical Committee on Information Security Education
I/O	Input/Output
IoT	Internet of Things
IP	Internet Protocol
IPC	Inter-Process Communication

Abbreviation	Translation
IPS	Intrusion Prevention Systems
IS	Information Security
ISA	Instruction Set Architecture
ISACA	Information Systems Audit and Control Association
ISO/OSI	International Standards Organization Open Systems Interconnection
ISSM	Information Systems Security Manager
IT	Information Technology
JCCI	Joint Competence Centre Infrastructure
JRC	Joint Research Centre
JS	JavaScript
JSON	JavaScript Object Notation
JTAG	Joint Test Action Group
KA	Knowledge Area
KAIST	Korea Advanced Institute of Science & Technology
KSA	Knowledge, Skills and Abilities
KTH	Royal Institute of Technology in Stockholm
KU	Knowledge Unit
LAN	Local Area Network
LTE	Long-Term Evolution
LWE	Learning With Error
MAC	Mandatory Access Control
MAC OSX	Macintosh Operating System X
MD4	Message-Digest 4
MD5	Message-Digest 5
MOOC	Massive Open Online Course
MOV	Menezes–Okamoto–Vanstone
MTRJ	Mechanical Transfer Registered Jack
NA	Not Available
NAT	Network Address Translation
NATO CCDCOE	North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence
NCSC	National Cybersecurity Centre
NICE	National Initiative for Cybersecurity Education
NIS	Directive 2016/1148 on security of network and information systems
NIST	National Institute of Standards and Technology
NP	Nondeterministic Polynomial Time
NPM	Node Package Manager
NSA	National Security Agency
NTNU	Norwegian University of Science and Technology
NTP	Network Time Protocol
OS	Operating System
OSI	Open Systems Interconnection Reference
OSVDB	Open Sourced Vulnerability Database
OWASP	Open Web Application Security Project
P	Polynomial Time
PC	Personal Computer
PCI	Peripheral Component Interconnect
PCI DSS	Payment Card Industry Data Security Standard
PET	Privacy-enhancing Technology
PHP	Hypertext Preprocessor
PIA	Privacy Impact Assessment

Abbreviation	Translation
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PSACS	Professional Specialist Accreditation in Cyber Security
RBAC	Role-Based Access Control
RFID	Radio-Frequency Identification
RJ	Registered Jack
RMIP	Risk Management Implementation Plan
R-LWE	Ring - Learning With Error
RSA	Rivest-Shamir-Adleman
SASS CSS	Syntactically Awesome Style Sheets Cascading Style Sheets
SC	Standard Connector
SCADA	Supervisory Control and Data Acquisition
SDC	Statistical Disclosure Control
SDN	Software-Defined Networking
SDLC	Systems Development Life Cycle
SETA	Security Education, Training, and Awareness
SFIA	Skills Framework for the Information Age
SHA-	Secure Hash Algorithm-
SIVP	Shortest Independent Vectors Problem
SMTP	Simple Mail Transfer Protocol
SPARTA	Strategic Programs for Advanced Research and Technology in Europe
SPD	Sensitive Personal Data
SSH	Secure Shell
ST	Straight Tip
STEM	Science, Technology, Engineering, Mathematics
SVP	Shortest Vector Problem
SW	Software
TCP	Transmission Control Protocol
TLS	Transport Layer Security
ToR	The Onion Router
UART	Universal Asynchronous Receiver-Transmitter
UCL	University College London
UDP	User Datagram Protocol
UK	United Kingdom
URL	Uniform Resource Locator
USA	United States of America
UX	User Experience
VLAN	Virtual Line Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
WP	Work Package