



# SPARTA

## D12.6

### Closing the Gender and Diversity Gap

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

<b>Deliverable type</b>	Report
<b>Deliverable reference number</b>	SU-ICT-03-830892 / D12.6 / V1.0
<b>Work package contributing to the deliverable</b>	WP12
<b>Due date</b>	Jan 2022 – M36
<b>Actual submission date</b>	31 <sup>st</sup> January, 2022

<b>Responsible organisation</b>	INOV
<b>Editor</b>	Catarina Valente
<b>Dissemination level</b>	PU
<b>Revision</b>	V1.0

<b>Abstract</b>	The present deliverable contains the final report on the activities and impact of the actions carried out during the project's lifetime. The activities aimed at reducing the gender gap and lack of human resources in cybersecurity in Europe. Task 12.4. is designed to incentivize female participation, involvement, and uptake; create female mentorships programs; understand and correct social barriers related to women participation in all levels of the cybersecurity workforce.
<b>Keywords</b>	Gender gap, diversity gap, awareness.



## **Editor**

Catarina Valente (INOV)

## **Contributors** (ordered according to beneficiary numbers)

Elisabete Carreira (INOV)

## **Reviewers** (ordered according to beneficiary numbers)

Regina Valutyte (MRU)

Uwe ROTH (LIST)

## **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

The present deliverable provides the report of the activities carried out during the SPARTA project's lifetime, in the scope of task 12.4 *Closing the gender and diversity gap*.

Chapter 1 introduces the scope of this task in relation to the project, its goals and the general lines of action that helped building the activities set in place.

The first section of the Chapter 2 provides the general context of the current gender gap issue in cybersecurity and the main strategic actions to increase women's participation in the digital sector set by the European Commission. The second section presents the SPARTA female participation and the project's commitment to address the gender gap issue in cybersecurity. It follows the third section that presents the strategic plan set to meet the goals of task 12.4, in a straight relation with the project's overall objectives and strategic axes. The fourth section establishes the main messages to be delivered to the project's audiences, regarding the scope of this action. The fifth section summarizes the partners contribution to the success of the activities reported in this deliverable.

Chapter 3 is dedicated to the extensive report on the activities carried out during the project's lifetime, divided in three sections that correspond to the three periods of the project (M01 – M12; M12 – M24; M12 – M36).

Chapter 4 provides a general evaluation of the activities carried out in each stage of the project, along with a summary of the lessons learned and possible improvements in further activities alike.

Chapter 5 is a conclusion of this report and provides a brief summary of all the activities, highlighting the most relevant outcomes.

# Table of Content

<b>Chapter 1</b>	<b>Introduction .....</b>	<b>1</b>
<b>Chapter 2</b>	<b>Closing the Gender Gap Strategic Plan.....</b>	<b>2</b>
2.1	Cybersecurity Gender Gap .....	2
2.2	SPARTA position.....	3
2.3	Action Strategy and goals.....	4
2.4	Main Messages .....	5
2.5	Partners contribution .....	5
2.6	Contribution to the overall project KPIs.....	6
<b>Chapter 3</b>	<b>Activities report.....</b>	<b>8</b>
3.1	M01 – M12 Activities Report.....	8
3.1.1	Women’s Day campaign.....	8
3.1.2	" Women4Cyber " .....	8
3.1.3	ACM Celebration of Women in Computing: womENCourage 2019.....	9
3.1.4	Awareness games at leHack 2019.....	9
3.2	M12 – M24 Activities Report.....	10
3.2.1	SPARTA Partners up with Women4Cyber .....	10
3.2.2	SPARTA Women Campaign on social media .....	11
3.3	M24 – M36 Activities Report.....	13
3.3.1	SPARTA Mentorship Programs .....	13
3.3.2	“SPARTA: The Future Needs You” event .....	14
<b>Chapter 4</b>	<b>Evaluation.....</b>	<b>17</b>
<b>Chapter 5</b>	<b>Summary and Conclusion .....</b>	<b>18</b>
<b>Chapter 6</b>	<b>List of Abbreviations.....</b>	<b>19</b>
<b>Chapter 7</b>	<b>Annexes .....</b>	<b>20</b>
7.1	Annex 1 – Images disseminated for Women's Day Campaign.....	20
7.2	Annex 2 – Activities planned in D12.3 .....	21
7.3	Annex 3 – Activities planned in D12.4 .....	23
7.4	Annex 4 – Dedicated Newsletter .....	24
7.5	Annex 5 – Best-Practices Guide.....	30
7.6	Annex 6 – “Little Stories about Big Women in Cybersecurity” Exhibition.....	36
<b>Chapter 8</b>	<b>Bibliography .....</b>	<b>41</b>

## List of Figures

Figure 1: Workshop "Women in Cyber: A Manifesto for Today" .....	9
Figure 2: ACMWomenEncourage 2019 talks .....	9
Figure 3: Challenge 3 at LeHack 2019 on diversity in cybersecurity .....	10
Figure 4: Rayna at Jaxenter .....	11
Figure 5: EUvation website page .....	12
Figure 6: Women in SPARTA campaign mentioned on the Cybersecurity and Digital Privacy Newsletter .....	12
Figure 7: Gender & Diversity Breakfast Webinars program .....	13
Figure 8: Best-Practice Guide communication on Twitter .....	14
Figure 9: Program of "SPARTA: The Future Needs you" .....	15
Figure 10: "SPARTA: The Future Needs You" event .....	16
Figure 11: "SPARTA: The Future Needs You" event merchandising .....	16

## List of Tables

Table 1: Participation in the SPARTA project by gender .....	3
Table 2: 2020 ELSA audit results on the gender dimension .....	6
Table 3: 2021 ELSA audit results on the gender dimension .....	6
Table 4: Contribution to the KPIs of objective 6 .....	7
Table 5: Contribution to the KPIs of objective 3 .....	7
Table 6: SPARTA Partners up with Women4Cyber, retrieved from D12.3 .....	21
Table 7: SPARTA Women Campaign on social media, retrieved from D12.3 .....	21
Table 8: SPARTA Goes to High School, retrieved from D12.3 .....	21
Table 9: Action 1 - SPARTA Mentorship Program .....	23
Table 10: Action 2 - SPARTA Goes to School .....	23



## Chapter 1 Introduction

The WP12 – Dissemination and communication – aims to plan, coordinate, and execute all SPARTA activities related to dissemination and communication and integrates a specific approach to the gender and diversity dimensions in cybersecurity, concretized in a dedicated task – 12.4 *Closing the gender and diversity gap*.

Task 12.4 aimed at maximizing the impact of the SPARTA project through a collaborative effort to understand the main reasons behind the reduced female participation in the cybersecurity field and work towards the possible ways to tackle this problem.

As such, in a cooperative effort between WP12 and the SPARTA partners, the project embedded a set of actions to incentivize the participation of women in the cybersecurity field, such as 1) specifically addressing the female public in dissemination and communication activities, 2) prioritizing female participation in all training related activities during the project, 3) create the basis for female mentorship programs, and 4) understand (and possibly correct) the social barriers related to female participation in all levels of the cybersecurity workforce.

This deliverable presents the actions set in place to meet such goals and provides a global evolution of the work carried out during the three years of the project, along with a set of recommendations to projects wanting to pursue a similar activity.

## Chapter 2 Closing the Gender Gap Strategic Plan

This chapter reviews the gender gap issue in cybersecurity, analyses the main reasons for the lack of female participation in cybersecurity and reviews the communication objectives.

### 2.1 Cybersecurity Gender Gap

The need for a diverse workforce in the cybersecurity field is already well known among the cybersecurity and tech community. The (ISC)<sup>2</sup> Cybersecurity Workforce Study conducted an online survey in August 2018 that measured various aspects of working in the cybersecurity field, including workforce staffing shortages, education and skills needed and challenges faced among professionals.

This survey led to *The (ISC)<sup>2</sup> Cybersecurity Workforce Report: Women in Cybersecurity: Young, Educated and ready to take charge*. The data collected in this survey shows us that the cybersecurity workforce has been improving in the last few years. The percentage of women currently working in cybersecurity has increased from 11% to 20%. This growth represents an understanding of the need for a gender-balanced representation in the field and of what is needed to attract and retain women in cybersecurity.

Women in the cybersecurity field are generally more educated and younger than men. According to this survey, 44% of men in cybersecurity hold a post-graduate degree, while women in the same conditions make up 52%. Nearly half of women cybersecurity professionals surveyed are millennials – 45% compared to 33% of men. Nevertheless, there is still a long path to establishing a more gender-balanced workforce.

The 2019 report *Exploring the gender gap in cybersecurity* (CSERT, 2020)<sup>1</sup> presents the results of the diversity workshop promoted by [CREST](https://crest-approved.org/)<sup>2</sup> and explores how the cybersecurity industry can properly address the gender gap in the field. This report highlights that 33% of the workshop attendees expressed their love for working in this industry, 59% “classified their experience in the industry as mixed, having received support and enjoyed roles but pointing to obstacles and challenges that had to be overcome as a result of being female”, and the remaining 11% expressed disdain for the industry and their experiences in it”. The workshop participants pointed that they felt that men are ‘heard’ more than women, and some believed that it was because men are “better at putting themselves out there”. Other important take-out from this workshop is that many participants stated that networking events can often be intimidating as they are dominated by their male counterparts, and that the timing of networking events (usually evenings and late afternoons) are problematic for many working mothers.

The 2015 *Closing the Gender Gap in Cybersecurity* (Dallaway, 2015)<sup>3</sup> report written by Eleanor Dallaway concluded that the most important group to prioritise for addressing the gender gap and changing perceptions was secondary school students, followed by university graduates. This was again confirmed in the 2019 report as it showed that the majority of respondents believe that the biggest barriers to increase gender diversity is the gender stereotypes from school age. Others blame it on the marketing of the industry and the perception it creates. Only 4% believes it is because of female lack of interest in cybersecurity.

---

<sup>1</sup> [https://crest-approved.org/wp-content/uploads/CREST-Gender-report\\_202004.pdf](https://crest-approved.org/wp-content/uploads/CREST-Gender-report_202004.pdf)

<sup>2</sup> <https://crest-approved.org/>

<sup>3</sup> <https://www.crest-approved.org/wp-content/uploads/CREST-Closing-the-Gender-Gap-in-Cyber-Security.pdf>

The European Commission has been actively working on this issue and has set three main strategic actions to increase female participation in the digital sector<sup>4</sup>:

1. Challenging digital gender stereotypes;
2. Promoting digital skills and education;
3. Advocating for more women entrepreneurs.

SPARTA, in particular task 12.4, is committed to working towards these three strategic actions and promoting activities that meet such ambitions.

## 2.2 SPARTA position

At an early stage of the project, the SPARTA consortium was committed to address the gender and diversity gap issue in cybersecurity, both in the project and in each organization, by ensuring women's participation and striving to understand the social barriers associated with the problem, unconscious bias, and misperceptions. SPARTA coordinated the engagement of stakeholders and end-users, taking into account geographical, cultural, societal and sectorial diversity at all stages of the SPARTA work process. The consortium has appointed a Gender and Diversity Manager who worked closely with partners addressing community activities during the project's lifetime. Table 1 provides the current state of female participation in the SPARTA project, provided by WP13. At SPARTA only 22,6% of the researchers are female, but for non-researchers there is nearly no difference in the participation of woman and men.

Table 1: Participation in the SPARTA project by gender

No.	Beneficiary Short Name	Number of female researchers	Number of male researchers	Number of female persons	Number of male persons
1	CEA	0	6	1	1
2	JR	2	1	1	1
3	TNK	0	1	5	3
4	CETIC	0	3	0	2
5	Unamur	1	1	1	1
6	CESNET	0	2	0	0
7	BUT	1	6	1	1
8	NIC	0	0	1	2
9	FTS	0	3	1	0
10	Fraunhofer	2	5	0	0
11	SAP	0	2	2	0
12	TUM	1	2	0	2
13	UBO	0	5	0	4
14	UKON	0	4	0	0
15	UTARTU	2	2	0	0
16	KEMEA	2	5	2	0
17	NCSR	0	1	0	0
18	EUT	1	3	0	0
19	IND	4	13	0	0
19.1	IFT	2	5	0	0
20	TEC	8	2	1	0
21	VICOM	3	4	2	2

<sup>4</sup><https://digital-strategy.ec.europa.eu/en/news/more-women-digital-sector-key-europes-successful-digital-future-international-womens-day-2018>



No.	Beneficiary Short Name	Number of female researchers	Number of male researchers	Number of female persons	Number of male persons
22	ANSSI	0	0	0	3
23	IMT	0	0	0	0
24	INRIA	1	10	0	0
25	TCS	3	4	2	2
26	YWH	1	1	2	1
27	CINI	1	10	3	0
28	CNIT	0	8	0	0
29	CNR	1	4	3	0
30	ISCOM	0	0	0	3
31	LEO	0	0	1	4
32	KTU	0	0	0	0
33	L3CE	10	20	5	10
34	LKA	2	4	4	0
35	MRU	1	3	2	0
36	LIST	0	4	0	1
37	SMILE	0	0	6	2
38	UNILU	0	3	0	0
39	LMT	0	0	5	4
40	ITTI	1	8	1	0
41	NASK	0	7	1	0
42	PPBW	0	0	1	3
43	INOV	1	5	6	1
44	IST	0	8	0	8
	<b>total</b>	<b>51</b>	<b>175</b>	<b>60</b>	<b>61</b>

## 2.3 Action Strategy and goals

Deliverable 12.1 – Dissemination and communication plan, updates, and evaluation – set three strategic and interdependent axes, aligned with the overall SPARTA objectives:

**Awareness building:** make the project and its aims acknowledged;

**Participation:** engaging target groups and enabling them to understand SPARTA concepts and results achieved;

**Action:** promoting actions from target groups influencing practices, products and standards.

The activities planned and conducted during the project's lifetime in the scope of task 12.4 are in line with these axes, structural to achieve its goals:

- a) Raise awareness on the need for a diverse workforce on cybersecurity
- b) Raise awareness on the importance of cybersecurity
- c) Engage women within the EU with cybersecurity

To reach such goals, task 12.4 developed a set of actions per year, accordingly to each strategic axis. The first year (M01 – M12) of the project foresaw the establishment of the “awareness building” axis, aimed at informing the audiences about the project and being aware of the impact it seeks to achieve, here in particular regarding the gender dimension. In this period, efforts were mainly for

informing the project audiences about SPARTA position regarding the gender gap issue in cybersecurity and the female participation in the cybersecurity workforce.

The second year of the project (M12 – M24) was dedicated to the “participation” axis, aimed at engaging target groups and enabling them to understand SPARTA concepts and results achieved in the scope of the gender and diversity dimension. To this end, the activities focused mainly on highlighting the women working in cybersecurity (namely, women working in SPARTA), through several publications in the social media channels and understating in-depth the reasons behind the lack of female participation in the field.

The third year of the project (M24 – M36) integrated the uprising of the “action” axis, aimed at influencing practices, and standards, here, once again, in what concerns the gender dimension. WP12 built its activities with the ultimate goal of promoting changes in behaviour and practices, namely by introducing the cybersecurity reality to high-school students, companies and the EU community.

## 2.4 Main Messages

*"The main communication problem is the images that always have been spread of men doing technical jobs and never women. The stereotypes indicate that we have to work deeply and in a multifaced overview of the problem to change the current image." - Pia Ahrenkilde-Hasen, at "Spotlight on Women in Cyber" 2019 event*

The main messages deployed to the target audiences established in the deliverable 12.1 *Dissemination and communication plan, updates and evaluation*, are the following:

1. SPARTA is committed to understanding and working on gender and diversity gap issues as this is a social responsibility of public interest. To reduce the gender gap and lack of cybersecurity human resources in Europe, SPARTA will address this issue by embedding several positive actions;
2. Contributing for a more inclusive society, SPARTA addresses diversity in its multiple forms by promoting the engagement of associated partners, stakeholders and end-users, taking into account geographical, cultural, societal and sectorial diversity;
3. Cybersecurity needs female participation. The gender, as diversity, matters in almost every problem-solving workforce because different people, with different perceptions, experiences and backgrounds will approach problems in distinct yet complementary ways.
4. Areas such as ethics, law, psychology and sociology are also important for cybersecurity issues;
5. It is essential to empower and encourage women to achieve their ambitions and to celebrate their successes when they do, as it helps to change gender stereotypes and unconscious bias;
6. Educate the next generation and correct the misperception that is often unconsciously instilled into girls and boys very early on that tech is not for women is an important step, and SPARTA is committed to doing so.

Along with these main messages, SPARTA ensured that all the activities conducted in the scope of task 12.4 were duly communicated to the target audiences through the social media platforms, the website other media platforms, such as the EU's Cybersecurity and Digital Privacy Newsletter and partners official websites.

## 2.5 Partners contribution

The SPARTA partners were essential in the dissemination and communication process of the activities held during the project's lifetime. Partners also actively collaborated to achieve task 12.4



goals by giving insights on the issue, organizing events in this domain, and, in the foreground, ensuring women’s participation in the project, related events, and beyond.

The internal audits of SPARTA, conducted by WP2: Responsible Innovation: Ethical Legal and Social Aspects (ELSA) introduced the gender and diversity dimensions, along with ethical, legal and social aspects.

Table 2 and

Table 3 provide the audit results of 2020 and 2021, respectively. The control statements were the following:

- A. In the scope of the WP that I lead, I have not encountered significant difficulties and roadblocks related to intercultural communication, understanding, and appreciation.
- B. In the scope of the WP that I lead, I have not encountered significant difficulties and roadblocks related to women's attraction, participation, or retention in the workplace.
- C. In the scope of the WP that I lead, I have not encountered significant gender stereotypes and unconscious bias, that may impact negatively organizational performance.
- D. The SPARTA project provides the necessary and sufficient policies, standards, procedures, and guidelines, related to gender and diversity issues.

Overall, the results are positive and there were improvements made from 2020 to 2021. There are opportunities for improvement, namely on “Policies, Standards, Procedures, and Guidelines” where there are 14% of negative statements.

Table 2: 2020 ELSA audit results on the gender dimension

Per statement							Controls
Fully Agree (FA)	Largely Agree (LA)	Partially Agree (PA)	Not Agree (NA)	Positive (FA+LA)	Negative (PA+NA)		
11	3	0	0	100%	0%	Intercultural enablers	A
9	3	2	0	86%	14%	Negative discrimination	B
11	1	2	0	86%	14%	Negative discrimination	C
3	7	3	1	71%	29%	Policies, Standards, Procedures, and Guidelines	D

Table 3: 2021 ELSA audit results on the gender dimension

Per statement							Controls
Fully Agree (FA)	Largely Agree (LA)	Partially Agree (PA)	Not Agree (NA)	Positive (FA+LA)	Negative (PA+NA)		
12	2	0	0	100%	0%	Intercultural enablers	A
11	3	0	0	100%	0%	Negative discrimination	B
11	3	0	0	100%	0%	Negative discrimination	C
6	6	2	0	86%	14%	Policies, Standards, Procedures, and Guidelines	D

## 2.6 Contribution to the overall project KPIs

Task 12.4 also contributed to the achievement of specific project KPIs, through the awareness building activities. This section provides the achieved results on enhancing cybersecurity awareness measured as follows:

Table 4: Contribution to the KPIs of objective 6

Objectives with WP9:	M12		M24		M36	
	Expected	Achieved	Expected	Achieved	Expected	Achieved
6.3 - number of directly addressed people (through participation at conferences, workshops, trainings, etc.) by the awareness program by the end of the project.	> 500	> 1000	> 2250	> 2452	> 5000	>6574* + 2132** = 8706
6.4 - number of indirectly addressed people (through advertisements, social media) by the awareness program by the end of the project.	> 2000	> 10000	> 20000	> 22300	> 50000	>80 000 (Higher reach of a post)

\* Total of KNOWN numbers of attendees of the several conferences, workshops and trainings promoted by SPARTA. The total number of attendees related to participation at bigger events where SPARTA participated exceeds this number.

\*\* Total of participants at cybersecurity awareness training events, simulation exercises, and specific courses, special SMILE cybersecurity events, Letz Cybersecurity Challenge, and specific missions provided and reported by WP9.

**Build sustained collaboration** with academic, industrial, governmental and community stakeholders, which will be measured as:

Table 5: Contribution to the KPIs of objective 3

Objectives with WP3 and WP8:	M12		M24		M36	
	Expected	Achieved	Expected	Achieved	Expected	Achieved
3.1 - number of workshops organized and number of attendees per workshop	> 12 > 20	> 8 > 30	> 24 > 20	> 17 > 120	> 36 > 50	39 > 120

## Chapter 3 Activities report

SPARTA has been researching the issues that may be at the backbone of the gender gap faced in the cybersecurity field, striving to understand what kind of activities could enhance the inclusion and attraction of women into the cybersecurity workforce. As a result, a set of actions was prepared to promote awareness of the current situation, ultimately aiming to attract women to the field. In this chapter are presented and reported the activities conducted during the project's lifetime, by year.

### 3.1 M01 – M12 Activities Report

In line with the communication strategy established in the D12.1 – Communication and Dissemination Plan – the first period of the activities developed in task 12.4 was sustained by the “awareness building” axis, aimed at informing the audiences about the project and aware of the impact it seeks to achieve, here in particular regarding the gender dimension.

#### 3.1.1 *Women's Day campaign*

The Women's Day campaign was designed to celebrate women in cybersecurity and present Claudia Eckert and Regina Valutyte, members of SPARTA, and leading examples for women choosing to undertake the cybersecurity career path. The campaign aimed at briefly exposing the current cybersecurity gender gap through a short [video](#)<sup>5</sup>. All the contents were published on the SPARTA social media accounts: Twitter, LinkedIn, and Instagram. Annex 1 features the visuals created for the campaign.

Taking into account that, at the time of the publications, the SPARTA project had just started its communication activities on social media, the number of people that were reached by this campaign is significant. On Twitter, SPARTA reached, on average 4000 impressions (number of times people have seen the post) and 57 interactions with the post. On LinkedIn, the publications reached an average of 530 impressions, a total of 28 reactions and 7% of engagement. On Instagram, this campaign was able to reach 138 views, 16 visits to the SPARTA profile and an average of 240 impressions. The main objectives of the campaign were to communicate to our audiences the SPARTA position on gender gap issues and to raise awareness on the need to gather efforts to attract women to the cybersecurity field.

#### 3.1.2 " *Women4Cyber* "

"[Women4Cyber](#)<sup>6</sup>" is an EU-wide initiative, launched by the European Cyber Security Organisation (ECSO) to promote and support cybersecurity female participation. In the early stages of the project, SPARTA got involved in the "Women4Cyber" [LinkedIn Group](#)<sup>7</sup>, where gender balance issues and strategies to solve them are discussed; ideas, experiences, and knowledge are shared. In the first year of the project, SPARTA aimed at engaging with this group to among others understand what kind of activities could enhance the inclusion and attraction of women into the cybersecurity workforce, and position itself as a project committed to addressing such issues.

Through the INOV partner, SPARTA is also part of the Women4Cyber mailing list, aiming at integrating the inside meetings and activities, to better tackle the issues associated with gender balance in cybersecurity.

<sup>5</sup> <https://www.linkedin.com/feed/update/urn:li:activity:6642726395174760448/>

<sup>6</sup> <https://women4cyber.eu/>

<sup>7</sup> <https://www.linkedin.com/groups/12207626/>

### 3.1.3 ACM Celebration of Women in Computing: womENCourage 2019

SPARTA attended the ACM [womENCourage 2019 event](https://womencourage.acm.org/2019/)<sup>8</sup> on the 16<sup>th</sup> of September in Italy, Rome. WomENCourage brings together women in the computing profession and related technical fields to exchange knowledge and experience and provide special support for women who are pursuing their academic degrees and starting their careers in computing. SPARTA engaged with the attendees to understand some of their main concerns and opinions regarding female participation in the cybersecurity field. SPARTA attended some of the workshops, namely one promoted by “Women4Cyber” and Concordia project, technical talks and panel discussions. SPARTA disseminated some of the event activities through Instagram (mainly [stories](https://www.instagram.com/stories/highlights/17844179305514766/)<sup>9</sup> – Figure 1 and Figure 2), Twitter and LinkedIn, promoting awareness on the topic of female participation in cybersecurity.

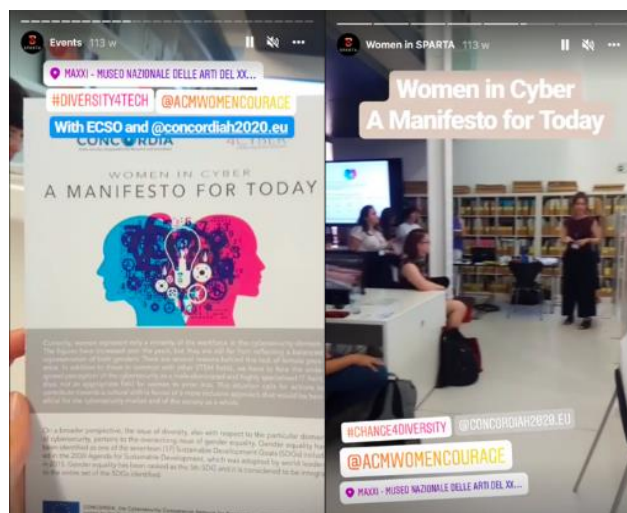


Figure 1: Workshop "Women in Cyber: A Manifesto for Today"

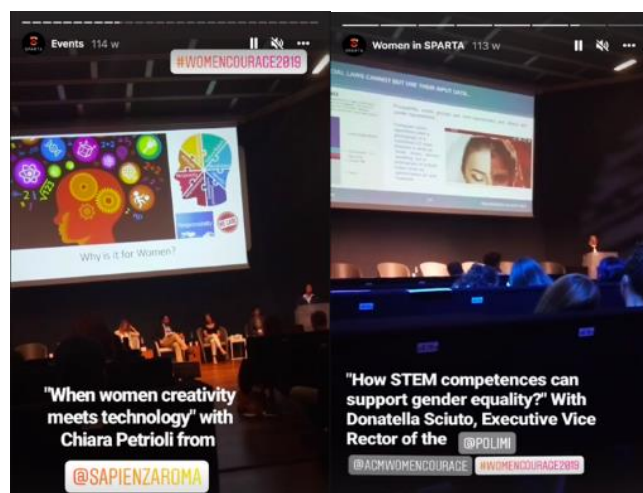


Figure 2: ACMWomenEncourage 2019 talks

### 3.1.4 Awareness games at leHack 2019

SPARTA attended ["leHACK" 2019](https://lehack.org/en)<sup>10</sup>, an underground hackers' event which brings together professionals, and non-professionals around conferences, workshops, lectures, and challenges. More than presenting the SPARTA project at the event, a booth was prepared with a set of five challenges to engage with the attendees. All challenges were disseminated on SPARTA social media accounts, as well as their solutions. One of the challenges was related to the importance of

<sup>8</sup> <https://womencourage.acm.org/2019/>

<sup>9</sup> <https://www.instagram.com/stories/highlights/17844179305514766/>

<sup>10</sup> <https://lehack.org/en>



having diversity within cybersecurity teams, detailed in Figure 3. One lesson to be taken from this challenge organization is that there is a tendency for the hacker community to not use social media accounts, especially when it comes to publishing oneself images. The challenge participants gather some interesting sentences about the importance of diversity in cybersecurity but did not share any images on the social media accounts, as most of them did not have one.



The poster for Challenge 3 is black with white text. At the top, a white box contains the title "Challenge 3". Below this, a numbered list of five steps is provided. At the bottom, there are social media icons for QR code, Twitter, Instagram, and LinkedIn, along with their respective handles. The SPARTA logo is in the bottom right corner, and a small European Union logo with text is in the bottom left corner.

**Challenge 3**

1. Write a sentence about the importance of diversity in cybersecurity.
2. Find a **diverse** group of 4 people who agree with your sentence.
3. Take a photo with them
4. Publish the photo along with the sentence on Instagram using #Challenge3 and tag @sparta\_eu
5. The most-liked publication wins!

The winner will be announced through social media at the end of each challenge!

sparta.eu @sparta\_eu @sparta\_eu SPARTA

SPARTA

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101019163.

Figure 3: Challenge 3 at LeHack 2019 on diversity in cybersecurity

## 3.2 M12 – M24 Activities Report

The second period of the activities developed in task 12.4 was sustained by the “participation” axis, aimed at engaging target groups and enabling them to understand the SPARTA concepts and results achieved, in particular regarding the gender dimension. To note that this was a particularly difficult period as the COVID-19 pandemic – that began in March – had an impact on planned activities. Travelling restrictions, shifts to home-office, social distancing, and other measures difficulties the timely deployment of the planned activities established for the second year in the deliverable D12.3. Such activities are recalled in Table 6, Table 7 and Table 8 in Annex 2 – Activities planned in D12.3 retrieved from D12.3. The activity – SPARTA goes to high school – is described in section 3.3.2 as it had to be re-scheduled to the third year of the project. Activities that were not initially planned but occurred during the second year of the project are also described here.

### 3.2.1 SPARTA Partners up with Women4Cyber

Following on the initial engagements made during the first year of the project through the “Women4Cyber” LinkedIn group and the mailing list, SPARTA become part of the *European Cyber Security Organization (ECSO) – Working Group 5: Education, Training, Awareness, Cyber Ranges* –, and had been actively participating in the Women4Cyber initiative. A meeting was held on the 4th of November 2020 to address the next steps and updates on the initiative, such as the 1) Women4Cyber Foundation started to receive supporting funding; 2) the 100 Women in Cybersecurity Book was being finished and 3) the idea for building a female Mentorship Program. Regarding the

last action, SPARTA proposed collaboration and knowledge exchange as the same action was to be deployed by WP12.

SPARTA is committed to supporting the communication and dissemination activities of Women4Cyber, as well as to working alongside this initiative to promote the participation of women in the field of cybersecurity. As such, SPARTA has been disseminating Women4Cyber initiatives on the project's social media accounts. In turn, "Women4Cyber" has also been actively helping SPARTA in dissemination and communication actions.

### 3.2.2 SPARTA Women Campaign on social media

This campaign involved several actions to be deployed during the second year of the project, with a major incidence on the social media platforms as a channel to properly engage target groups and enable them to understand SPARTA concepts and results in what regards the gender dimension in cybersecurity. To that end, from this main campaign, two actions were set in place: 1) Awareness and Participation on media channels, and 2) "Women in SPARTA" campaign.

Deliverable 12.4 established the need for addressing the gender gap in the audience as at the time we had 66% of male followers on Instagram. Through this campaign, the gender gap shortened where 55% are men and 44,9% are women. Twitter and LinkedIn do not provide gender analytics, but overall, the interactions each post receives are gender balanced.

#### 3.2.2.1 Awareness and Participation on media channels

From March 2020 to March 2021, and beyond, SPARTA social media accounts shared different contents regarding the gender dimension in cybersecurity, and engaged with other publications related to the subject, engaging with the cybersecurity female community.

Besides regular posts on social media, SPARTA was represented in other media platforms such as in [Jaxenter](#)<sup>11</sup>, where Rayna Stamboliyska, the Vice President of Governance & Public Affairs at Yes We Hack (SPARTA partner), gave an interview under the motto *Women in Tech: "Equal pay; less gendering, more mentoring"*, regarding the women underrepresentation in the tech sector. In this interview, Rayna Stamboliyska mentioned her work in SPARTA. The full interview is available [here](#)<sup>12</sup> and constituted a means for promoting SPARTA values in what concerns the gender gap in cybersecurity and for creating awareness on the subject.



Figure 4: Rayna at Jaxenter

#### 3.2.2.2 "Women in SPARTA" campaign

The "Women in SPARTA" campaign derived from the planned activities established in the deliverable D12.3 – SPARTA Women Campaign on social media –, as described in Table 7 and evolved as an independent campaign. The campaign was launched at the beginning of the second year of the project and its mission was to help building a strong community among women in cybersecurity by presenting the ones working in the SPARTA project, their work, thoughts, and ideas on the current gender gap issue on the field, and on how to tackle it. Besides the interviewed initial presentation (name, age, working place and role in SPARTA), the videos contemplate the answers for the following questions:

<sup>11</sup> <https://jaxenter.com/>

<sup>12</sup> <https://jaxenter.com/women-in-tech-stamboliyska-172586.html>



- How is it to work in cybersecurity?
- Have you encountered any form of discrimination/ or constraints in your professional or academic lives?
- From your point of view, what could be changed to increase women's involvement in cybersecurity fields?

Initially, the interviews were to be conducted in person, during the SPARTA internal events, such as the SPARTA Days. That was the case for the first two interviews, with Maryline Laurent and Estibaliz Amparan, at the SPARTA Day held in Brussels. For the others, as the COVID-19 pandemic imposed travelling restrictions and social distancing, such a format was no longer possible. The videos started to be recorded by the interviewed and sent to WP12 for edition and publication.

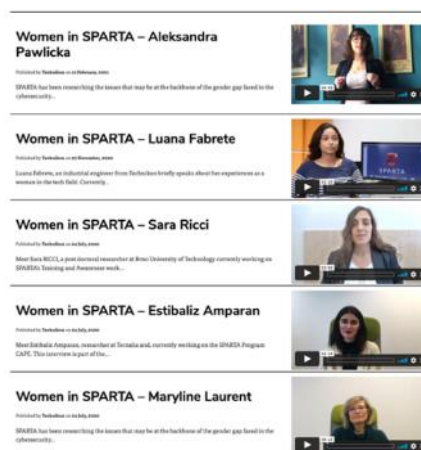


Figure 5: EUvation website page

The Communication and Dissemination team was able to launch five interviews that can be viewed on the dedicated page of the SPARTA website: [“Gender & Diversity”](#)<sup>13</sup>. Besides the website, the interviews were disseminated through SPARTA social media accounts, on the EU’s Cybersecurity and Digital Privacy Newsletter (Figure 5), on the [EUvation](#)<sup>14</sup> channels (Figure 6), and through the SPARTA Newsletter and partners communication channels.

In the scope of this campaign, Anna Felkner wrote an article entitled [“My way in cybersecurity”](#)<sup>15</sup> for SPARTA, also published on the website and social media accounts.

The second edition of the SPARTA newsletter – Annex 4 – was dedicated to the women working in SPARTA, where TecNALIA’s cybersecurity team, mainly composed of women, was taken as a leading example. Partners helped in the dissemination process through their channels. TecNALIA [published](#)<sup>16</sup> the Newsletter on its’ website and social media accounts.



Figure 6: Women in SPARTA campaign mentioned on the Cybersecurity and Digital Privacy Newsletter

<sup>13</sup> <https://www.sparta.eu/diversity/>

<sup>14</sup> <https://euvation.eu/>

<sup>15</sup> <https://sparta.eu/news/2021-11-16-my-way-in-cybersecurity.html>

<sup>16</sup> <https://www.cyberssbytecnalia.com/node/375>

### 3.2.2.3 Gender & Diversity Breakfast Webinars

SPARTA was represented by Sara Ricci, a Post-Doctoral Researcher at the [Brno University of Technology](https://www.vut.cz/en/)<sup>17</sup>, at the INESC HUB *Gender & Diversity Breakfast Webinar* discussions (Figure 7). Sara addressed the importance of the role models in gender & diversity in STEM research and technology. The webinars were held on the 8<sup>th</sup>, 9<sup>th</sup>, and 11<sup>th</sup> of September and received speakers from several and different areas of knowledge. They constituted a means for positioning SPARTA values concerning the gender gap in cybersecurity and creating awareness about the importance of role models in the area. A Member of the European Parliament, Maria da Graça Carvalho, was also a panellist of this event, with Sara Ricci.

**PROGRAM | GENDER & DIVERSITY BREAKFAST WEBINARS**



**8 SEPTEMBER, 8H30 GMT / 9H30 CET**  
 Gender and Diversity in research and technology organisations in Europe  
 Inês Lynce, President, INESC ID  
 Muriel Attané, Secretary General, EARTO  
 Tomas Brage, Lund University

**9 SEPTEMBER, 8H30 GMT / 9H30 CET**  
 If you had one million euros for a R&I project promoting gender and diversity, what activities would you implement?  
 Mina Stareva, Head of Sector, Gender, DG Research and Innovation, European Commission  
 Marta Barbas, Senior Advisor to Administration, INESC TEC

**11 SEPTEMBER, 8H30 GMT / 9H30 CET**  
 The role of the role-models in gender and diversity in STEM research and technology  
 Susana Cardoso Freitas, Director, INESC MN  
 Maria da Graça Carvalho, Member of the European Parliament  
 Sara Ricci, post-doctoral researcher at Brno University of Technology, member of the SPARTA Project

Participate and contribute to the debate live during the webinar! Participation is free but registration is mandatory. Register until September 4 through this link: <https://ec.europa.eu/eusurvey/runner/GenderAndDiversityBreakfastWebinar2020>



Figure 7: Gender & Diversity Breakfast Webinars program

## 3.3 M24 – M36 Activities Report

The third period of the activities developed in task 12.4 was sustained by the “action” axis, aimed at influencing practices, products and standards, here in particular regarding the gender dimension. As mentioned above, due to the pandemic impacts, the “SPARTA Goes to School” action planned for the second year of the project had to be concluded during the third year. The social media campaign designed to raise awareness of the need for a diverse workforce in cybersecurity, from March 2020 to March 2021, continued during the third year. The Table 9 and Table 10 in Annex 3 – Activities planned in D12.4, retrieved from D12.4, summarize the planned activities for the M24 – M36.

### 3.3.1 SPARTA Mentorship Programs

WP12 developed, at the beginning of the third year of the project, a *Best-Practices Guide to attract and retain women in cybersecurity teams* – Annex 5 – Best-Practices Guide. The creation of this guide was sustained by both the insights collected during the “Women in SPARTA” campaign and bibliographic research analysis. This guide is aimed at gathering the essentials to create a female mentorship program that helps build strong relationships of knowledge between students and professionals of cybersecurity. It also aimed at providing the means for mentors and mentees clarify their own objectives, stay engaged and active.

The guide is divided into three parts. The first aims at introducing the problem of the gender gap in cybersecurity, to introduce some of the directions pointed by the European Commission and to introduce the scope of such document. The second presents a set of six best practices for promoting

<sup>17</sup> <https://www.vut.cz/en/>

diverse teams and generating synergies with great multidisciplinary and multicultural value. Links to articles and relevant guides are also provided to complement the given information. For closing this section, a list of initiatives and events around the globe is deployed to inspire readers and promote possible collaborations. The third part of the document provides a practical and simple guide on how to create successful mentorship programs, from the very beginning. It encompasses how to promote self-knowledge, how to create meaningful connections between mentor and mentee, how to explore one's possibilities and capabilities, how to keep a creative process by establishing adequate strategy and goals, and finally how to maintain the program alive, by monitoring and evaluating the progress.

The guide was published on social media and on the website. A highlight goes to the Twitter platform, where the publication reached – with promoted content – 54 239 people and had 8 188 engagements, being that 6 000 was the number of clicks on the link for the Guide, and the rest the interactions with the post (comments, retweets, likes, page views, etc.)

On the 4th of March, the European Commission published the Guide on its official website, available [here](#)<sup>18</sup>.

### 3.3.2 “SPARTA: The Future Needs You” event

Aiming at influencing practices regarding female participation in the cybersecurity field, WP12 organized the event “SPARTA: The Future Needs You”, first thought of “SPARTA Goes to School: Cybersecurity for all” – as planned in the deliverables 12.3 and 12.4. This activity had been planned to be deployed during the second year of the project but due to the COVID-19 pandemic impacts, it was only possible for the third year, when schools started to open and hygiene measures were duly set in place.

Due to the pandemic, the event was rescheduled several times until the date was set for the 14<sup>th</sup> of October.

As October is the cybersecurity awareness month, the event also targeted at celebrating this by giving a talk about cyberspace, entitled: “dangers, threats and safety in the cyberspace”.

The event was targeted at female students who were finishing high school and about to enter university. It was aimed at raising awareness on the importance of cybersecurity and the need for a diverse workforce. As such, the goal behind this action was to raise awareness on the importance of cybersecurity among future university students who may opt for a cybersecurity-related field of study, by providing both theoretical but dynamic talks about cybersecurity and hands-on exercises. The event took place at the secondary school - Escola Secundária Rafael Bordalo Pinheiro - in Portugal. It started at 9h30 with a welcome session by the school's director, followed by the presentation of the SPARTA project. “Dangers, threats and safety in the



Figure 8: Best-Practice Guide communication on Twitter

<sup>18</sup> <https://digital-strategy.ec.europa.eu/en/news/sparta-best-practices-guide-attract-and-retain-women-cybersecurity-teams>

cyberspace” entitled the interactive and dynamic talk given by Sara Ricci. After this talk, there was a coffee break managed by the school’s tourism class.

The second part of this event welcomed three games, divided by different rooms, that happened in parallel, on a rotation scheme. The female students were, therefore, split in three groups and guided to each room. The games were the following:

- Capture the flag game, deployed by the Brno University and coordinated by Sara Ricci. This game is a merge of "capture the flag" and "escape room" games. There are three "cybersecurity rooms" (images) which need to be open by answering a set of questions. Each room has 4 games/questions with hints. If students use hints, they lose points. It allows for assessing the performance of each team.
- LEGO Enigma machine, deployed by the Brno University and coordinated by Petr Cika. The LEGO machine – image y – allows for students to encrypt messages and is complemented with an explanation about its history and how the allies attacked the machine.
- [The Fluge Company<sup>19</sup>](#), developed by Trend Micro and available on the internet, coordinated by Catarina Valente. The game evolves within a targeted attack to the Fugle Company and the player is the CIO who will be in charge of making the decisions that will lead to a safe disclosure of the attack. The player is asked to make the best choices for keeping the company activity steady and manage resources such as time and budget. The game is based on the format of the “Choose Your Own Adventure” books.

After the games, the students went back to the auditorium for the “SPARTA: The Future Needs You” presentation about the need for diverse teams in cybersecurity. The event ended with a Q&A session. A “Little Stories About Big Women in Cybersecurity” exhibition was set near the school auditorium and at the school’s library – Annex 6 – “Little Stories about Big Women in Cybersecurity” Exhibition. This action aimed, ultimately, at being a pilot to be tested in one school and replicated around Europe. The event was disseminated through the social media platforms and the website. Some highlights of the event are gathered on the Instagram’s event [stories folder<sup>20</sup>](#) and [dedicated post<sup>21</sup>](#).



Figure 9: Program of "SPARTA: The Future Needs you"

<sup>19</sup> <http://targetedattacks.trendmicro.com/index.html>

<sup>20</sup> <https://www.instagram.com/stories/highlights/17844179305514766/>

<sup>21</sup> <https://www.instagram.com/p/CVNqnkHMZA2/>





Figure 10: "SPARTA: The Future Needs You" event



Figure 11: "SPARTA: The Future Needs You" event merchandising

## Chapter 4 Evaluation

Overall, the activities designed in the scope of task 12.4 *Closing the Gender and Diversity Gap* were successfully implemented and easily adapted to the new constraints imposed by the pandemic. Flexibility and persistence were of foremost importance to overcome the negative impacts of the pandemic and complete the proposed activities. The general objectives of task 12.4 were achieved through a set of different activities, each targeting a specific objective:

- 1) Specifically addressing the female public in dissemination and communication activities was achieved through the women's day campaign, "Women4Cyber" initiative and the SPARTA Women campaign in social media, which involved posting contents related to female participation in cybersecurity, and engaging with the female cybersecurity community
- 2) Prioritization of female participation in all training related activities during the project was achieved with the commitment of the SPARTA partners to this end and through the "SPARTA: the Future Needs You" event, that specifically addressed the female students and engaged them with the topic of the gender and diversity gap in cybersecurity
- 3) Creation of the basis for female mentorship programs, leveraged was achieved through the collaboration and involvement with the ECSO initiative "Women4Cyber" and the "Women in SPARTA" campaign outcomes, leading to the creation of the Best-Practices Guide to Attract and Retain Women in Cybersecurity Teams.
- 4) Understand and work towards the correction of the social barriers related to female participation in all levels of the cybersecurity workforce, through the deployment of the "SPARTA: the Future Needs You" event and the "Gender and Diversity" breakfast webinar. Also, the Best-Practices Guide to Attract and Retain Women in Cybersecurity Teams was a step to help correct the social barriers related to female participation in all levels of the cybersecurity workforce. The Women in SPARTA interviews helped to understand these social barriers.

The activities designed and implemented contributed to all these objectives through different approaches, complementing each other. Communication activities both on the website and SPARTA social media accounts were maximized through the engagement of the consortium with the publications and helped build a gender-balanced community on social media, aware and informed about the gender and diversity gap issue in cybersecurity, and of the SPARTA position concerning this subject.

Opting for advertisement for relevant posts showed to be an effective way to ensure the messages are correctly delivered and have more reach. The best-practices guide to attract and retain women in cybersecurity teams was communicated to through an advertisement post and reached 54 239 people and had 8 188 engagements, being that 6 000 was the number of clicks on the link for the Guide, and the rest the interactions with the post (comments, retweets, likes, page views, etc.).

The event "SPARTA: The Future Needs You" was an opportunity to engage youth with cybersecurity and call for action towards building gender-balanced and inclusive cybersecurity teams. This event covered the lack of cybersecurity professionals and the gender gap in cybersecurity issues, presenting solutions and inciting the high school students in the area of sciences to undertake cybersecurity studies. The event had positive feedback from the students and professors and can be replicated in other high schools across countries.

The ELSA report helped to assess the consortium position and knowledge regarding the gender dimension of SPARTA and correct deviations, mainly through the deployment of the Best-Practices Guide to Attract and Retain Women in Cybersecurity Team.

## Chapter 5 Summary and Conclusion

The activities designed and implemented in the scope of task 12.4 were in line with the communication and dissemination strategic objectives established in deliverable 12.1.

The efforts made in the first year of the project targeted at promoting awareness on the cybersecurity gender and diversity gap issue and informing SPARTA target groups about the project position regarding it. Activities ranged from the Women's Day campaign, engagement with ECSO's "women4cyber" initiative, SPARTA presence at related events (womENCourage 2019) and SPARTA communication on the subject at cybersecurity events (LeHack 2019).

The second year called for the establishment of the "participation" axis and the activities mainly targeted at involving women in the cybersecurity field with the SPARTA project and collecting their inputs to understand the social barriers and roadblocks encountered when working on cybersecurity. This was achieved through the "Women in Sparta" campaign, which allowed for sharing ideas, experiences, and knowledge on the subject. These inputs were collected and analysed to deliver, during the third year of the project, the Best-practices Guide to Attract and Retain Women in Cybersecurity Teams. Other actions as the "Gender and Diversity Breakfast Webinars" also contributed to the participation axis.

The last year foresaw the deployment of the "action" axis, aimed at influencing practices. As such, WP12 built its activities with the goal of promoting changes in behaviour and practices, namely by introducing the cybersecurity reality to high-school students through the "SPARTA: The Future Needs You!"

Overall, the actions developed in the scope of task 12.4 and the lessons learned during its implementation contributed for a better understanding of the reasons and the context behind the low female participation in cybersecurity. This understanding is the first step for helping to close the gender gap in the field. It allowed for creating meaningful events, campaigns and guides that can be re-used/re-produced in future projects or activities.

## Chapter 6 List of Abbreviations

Abbreviation	Translation
C&D	Communication and Dissemination
ECISO	European Cyber Security Organization
ELSA	Ethical Legal and Social Aspects
INESC	Institute of Systems and Computer Engineering, Technology and Science
WP	Work Package



## Chapter 7 Annexes

### 7.1 Annex 1 – Images disseminated for Women's Day Campaign



SPARTA

**Women's Day**  
8<sup>th</sup> March



**Role in SPARTA**  
As responsible for the implementing the full spectrum cybersecurity awareness demonstration case, Prof. Regina Valutyte will address the relevant legal challenges, in particular privacy and data protection issues.

**Profile**  
Professor at the Institute of International and EU Law at Mykolas Romeris University. Lawyer by profession, she has over 10 years of experience in research around problematic aspects of human rights protection, including data protection. She is also Head of the Security Research Laboratory at MRU and Head of the Lithuanian Center of Excellence for Unmanned Systems.

*"Digitalization nowadays covers almost all spheres of society, affects everyday's life and societal power relations in many ways. Understanding and tackling this challenge demands legal expertise. Protection of human rights is a constant challenge to society and states, therefore, digital rights naturally form a part of my challenges."*



**Regina  
Valutyte**



**Role in SPARTA**  
As SPARTA Scientific Director, Prof. Claudia Eckert will be the chair of the Roadmap Committee and will lead the roadmap design and update.

**Profile**  
Full professor at Technical University of Munich where she holds the Chair for IT Security in the Department of Computer Science. She is founder and director of Fraunhofer AISEC. As a member of various national and international industrial advisory boards and scientific committees, she advises companies, trade associations and the public authorities in all questions related to IT security.

*"My motivation for being a scientist in this field is to make tomorrow's world secure – the digital infrastructure of our economy as well as that of our administration and of our society. This motivation is also nurtured by the firm belief that this is indeed achievable."*



**Claudia  
Eckert**



## 7.2 Annex 2 – Activities planned in D12.3

Table 6: SPARTA Partners up with Women4Cyber, retrieved from D12.3

<b>SPARTA Partners up with Women4Cyber</b>	
Target	Women in cybersecurity Community and SPARTA partners
Objectives	Understand the reasons beyond the gender gap in cybersecurity and cooperate with Women4Cyber to help achieving a more diverse cybersecurity workforce.
Calendar	On going
Description	The framework for our joint cooperation is yet to be established.

Table 7: SPARTA Women Campaign on social media, retrieved from D12.3

<b>SPARTA Women Campaign on social media</b>	
Target	Female audience aged between 16 and 30 Cybersecurity and Tech community
Objectives	Raise awareness on the need for a diverse workforce on cybersecurity Raise awareness on the importance of cybersecurity Engage women of the EU in cybersecurity
Calendar	From March 2020 to March 2021
	From March 2020 to March 2021, SPARTA will have weekly publications about: <ul style="list-style-type: none"> <li>- Achievements of women in cybersecurity</li> <li>- SPARTA commitment to increase the number of women in cybersecurity</li> <li>- SPARTA Women events</li> <li>- SPARTA state of the art regarding female participation in cybersecurity</li> <li>- Set of interviews to highlight the work of women participating in SPARTA</li> <li>- Best practices on how to attract and retain women in the cybersecurity field</li> <li>- Related re-tweets</li> </ul>
Evaluation	By the end of March 2021, SPARTA social media should have decreased its audience gender gap.
Materials	By the end of February 2020, an editorial plan must be deployed as to manage the weekly publications.

Table 8: SPARTA Goes to High School, retrieved from D12.3

<b>SPARTA goes to high school</b>	
Target	Female students who are finishing high school and about to enter university
Objectives	Raise awareness on the importance of cybersecurity and on the need for a diverse workforce.
Calendar	1 day – September 2020
Description	The main idea behind this action is to raise awareness on the importance of cybersecurity, among the future university students, who may opt for a cybersecurity related field of study.  <b>Program</b> 10h00   SPARTA Presentation This presentation should be creative and able to catch the student's attention. It should not be longer than 20 minutes. It should focus on the main, global aspects of the project and its impact for the society.



	<p>10h30   Coffee break  10h45   Cybersecurity Workshop + Challenges  For this workshop, a registration will be needed as to ensure we will have a 60% female presence at the workshop.  10h45   The importance of a diverse workforce in cybersecurity and the current statistics.  11h15   Workshop  13h00   Group photo to spread on social media</p> <p><b>Women in Cybersecurity - Exhibition</b>  As to prolongate the SPARTA impact at school, an exhibition about cybersecurity importance will be set up.  The exhibition should contain:</p> <ol style="list-style-type: none"> <li>1. Story of the first female coders with photos;</li> <li>2. Small sentences about the importance of a diverse workforce in cybersecurity + statistics.</li> <li>3. Our goal, to “reduce the gender gap in cybersecurity”</li> <li>4. The photos of the workshop.</li> </ol>
Evaluation	<p>How many registrations for the workshop / attendees?  How many new followers on social media?  Monitor Kahoot answers to understand the students’ engagement and workshop success.</p>
Materials	<ul style="list-style-type: none"> <li>- SPARTA Roll-up</li> <li>- SPARTA Merchandise (bags and stickers)</li> <li>- Coffee, fruit, and pastéis de nata.</li> </ul> <p>For the exhibition:</p> <ul style="list-style-type: none"> <li>- Photos and text printed.</li> <li>- SPARTA leaflet/ poster.</li> <li>- Infographics about women in cybersecurity.</li> </ul>

### 7.3 Annex 3 – Activities planned in D12.4

SPARTA Mentorship Programs	
Target	Women in the cybersecurity community and the SPARTA partners
Objective	Build synergies between women working and studying on cybersecurity
Calendar	Ongoing
Description	This action aims to create a female mentorship program to build strong relationships of knowledge between students and professionals of cybersecurity. This action will provide the means for training mentors and mentees regarding the program's goals, participant roles, mentoring best practices, and mentoring process. It will help mentors and mentees clarify their own objectives to help participants stay on track and get the most out of the program.

Table 9: Action 1 - SPARTA Mentorship Program

SPARTA Goes to School: Cybersecurity for All	
Target	Female students who are finishing high school and about to enter university, pursuing the Sciences study field.
Objective	Raise awareness on the importance of cybersecurity and the need for a diverse workforce.
Calendar	10 <sup>th</sup> of May 2021
Description	The workshop will open with the presentation of the SPARTA Project, followed by a talk on the "Dangers, threats and security in cyberspace - Always Safe". After the theoretical presentation, there will be cybersecurity hands-on exercises with the students and a discussion on "The importance of diversity in cybersecurity". As to prolongate the SPARTA impact at school, an <b>exhibition about women in cybersecurity</b> will be set up, and should contain the story of the first female coders with photos; small sentences about the importance of a diverse workforce in cybersecurity, and complementary statistics.

Table 10: Action 2 - SPARTA Goes to School

## 7.4 Annex 4 – Dedicated Newsletter



### INDEX

1. Highlights
2. Women In SPARTA
  - a. Women in SPARTA campaign
  - b. Tecnalía Team
3. Abstract for all

The second edition of SPARTA NEWS is dedicated to the women working in SPARTA. Tecnalía's cybersecurity team is a leading example of attracting women to the STEM area. Their team is mainly composed of women, of all ages. Here, TECNALIA presents the work carried in SPARTA as well as their team members.



# H I G H L I G H T S

## SPARTA WEEK

February 2020



The SPARTA Week took place at INESC BRUSSELS HUB, between the 24th and the 27th of February. SPARTA partners met upon a concrete challenge: cooperate to achieve European cybersecurity sovereignty! SPARTA Week welcomed several meetings where ideas were exchanged, knowledge was shared and new strategies and collaborations emerged with the ultimate purpose of leverage the SPARTA mission. Partners were encouraged to push forward on all fronts, and challenged to continue anticipating the state-of-the-art, choosing the best approaches to generate concrete value.

## WOMEN IN SPARTA

### THE CAMPAIGN

The WP12 - Communication and Dissemination - has been researching the issues that may be at the backbone of the gender gap faced in the cybersecurity field, striving to understand what could enhance the inclusion and attraction of women into the cybersecurity workforce. The lack of role models in the industry, related to the lack of visibility of women working in cybersecurity is a real problem. The industry often fails to retain women in cybersecurity workplaces due to its male-dominated environment that it is not inclusive nor attractive for women.

The Women in SPARTA campaign aims at building a strong community among women in cybersecurity by presenting the ones currently working in SPARTA, their work and what are their thoughts on the current gender gap issue, and how to tackle them. The first interview was to Maryline Laurent, professor at Telecom SudParis and currently working on the SPARTA Roadmap.



[Click here to watch the video on our website!](#)



## TECNALIA CYBERSECURITY TEAM

TECNALIA has a leading international Cybersecurity team which, together with our sectoral experts in the fields of Energy, Industry 4.0, the Automotive Industry and Health and Food, make up multidisciplinary teams with a holistic vision to create solutions from a technological and business perspective. The team is specialized in the development and deployment of cybersecurity technologies, with special emphasis on the deployment of advanced cyberattacks detection technologies in the industrial and health sectors. The Cybersecurity team is currently composed of 42% of women and is focused on the following areas:

- Security, Safety and Privacy-by-design techniques
- AI-based Detection of cybersecurity attacks and anomalies
- Automated Control and protection
- Cybersecurity Certification and Compliance
- Continuous Risk Management
- Blockchain-DLT

### ROLE IN THE PROJECT

In SPARTA, TECNALIA expects to increase knowledge and develop cybersecurity solutions, products and services for the identified critical challenges, mainly industrial cybersecurity, secure and fair AI systems, and cyber-ranges. Synergies between experts from various cybersecurity domains (especially automotive, energy and smart grids) will be demonstrated through the piloting activities.

TECNALIA is involved in the Roadmap Design, reporting current research interests and synchronizing to update the roadmap and adapt focus according to the path envisioned in the roadmap. They are also involved in the communication and dissemination activities from the WP12, and in the implementation of the monthly SPARTA workshops to collect the needs from local communities and end-users.

TECNALIA contributes to the CAPE program by bringing their expertise in safety and security assessments as well as risk analysis in complex systems.

In SAFAIR, TECNALIA leads T7.1 “Threat modelling for AI systems” bringing their expertise in AI threat analysis and modelling and collaborates in the demonstration and validation cases.

TECNALIA participates in the establishment of the SPARTA JCCI, with their Cybersecurity laboratories that are part of the RNLI (Spanish Network of Cybersecurity Research Labs) as well as part of the Basque Cybersecurity Research Labs. TECNALIA will collaborate in the clustering of SPARTA activities at Spanish national level.



## TECNALIA TEAM IN SPARTA



### Cristina Martinez

#### Project Manager

Cristina Martinez is Computer Engineer from the University of Deusto (Bilbao) and MSc in "Foundations of Advanced Information Technologies" (University of London). Project manager in the TRUSTECH business area of TECNALIA, managing research and innovation projects focused on cyber security, safety and blockchain. Quality Manager and deputy Project Manager of the H2020 AMASS ECSEL project that successfully ended in 2019. She has managed the participation of TECNALIA in several R&D EU projects such as: SPARTA, SecureCHAINS, SecureSME, ASSETS, VITALAS, and €-Confidential. Member of ECSO and the Spanish Platform on Digital Security (eSEC).



### Ana Ayerbe

#### WP3, WP8

Ana Ayerbe is the Manager of TECNALIA TRUSTECH Business Area where they work in trying to create trust in the digital and hyperconnected world developing technology to reinforce the digital immunological system of companies and society. Member of the Board of Directors of ECSO, RENIC, Permanent Committee of the Basque Cybersecurity Center, WOMEN4CYBER Council and mentor of the INSPIRA STEAM project, in the last year she has been part of the experts committee for the elaboration of the "Spanish National Strategy on Cybersecurity 2019".



### Estibaliz Amparán

#### WP5 - CAPE

Estibaliz Amparan has a degree in Industrial Electronic and Automation Engineering at the University of the Basque Country (EHU/UPV). She is a member of TECNALIAE since 2016. She works in the Cybersecurity and Safety group where she has been researching on Safety critical-embedded systems, more specifically, on automotive industry (ISO 26262). She focuses on the different fault injection techniques, Hazard and Risk Assessment (HARA), Safety Analysis (FMEA, FTA) and Safety Concepts.



### Angel López

#### WP5 - CAPE

Angel is a Senior Technician in Computer Systems Administration. He works as a researcher at TECNALIA, currently collaborating in the TRUSTECH business area. He was involved in European project OPENCROSS and its continuation AMASS, that has created an open tool platform, ecosystem, and self-sustainable community for assurance and certification of Cyber-Physical Systems. He is currently involved in research projects in the field of cybersecurity for electrical substations and V2X communications and he is also the technical manager of WHITEZONE, a TECNALIA cyber-security product under European patent EP3144841A1.





### Erkuden Ríos

#### WP7 - SAFAIR

Erkuden Ríos is expert in cybersecurity and privacy engineering technologies, and lately focused on Cloud Security and Cyber Risk Management. She is currently the coordinator of the Security WP in the H2020 ENACT project on Secure and Privacy-aware Smart IoT Systems as well as in the H2020 SPEAR project on Secure Smart Grids. Previously, she coordinated the H2020 MUSA project on Multi-cloud Security, that successfully ended in 2017. Erkuden is member of ECSO, ETSI Secure Artificial Intelligence Working Group, AIOTI WG4 Policy and Privacy and the Spanish National Network on Cybersecurity.



### Eider Iturbe

#### WP7 - SAFAIR

Senior researcher of Cybersecurity team of TRUSTECH unit in TECNALIA. Eider graduated in Telecommunication Engineering from the University of the Basque Country (Spain) and in the European Master of Project Management at the same university. She has worked in multiple large European and Spanish projects on cybersecurity, privacy and trust such as SPEAR, ENACT, SPARTA, POSEIDON, PDP4E, TACIT, and MUSA. Her main research interests include Cyber Security, Privacy, Risk Management, and AI for Cybersecurity.



### Maria Carmen Palacios

#### WP7 - SAFAIR

M<sup>o</sup> Carmen Palacios, bachelor in Physics at the Basque Country University (1989) with more than twenty years working experience in TECNALIA. Within R&D Programmes, she has been involved in many projects both at national and European level in the field of assurance for critical systems (both safety and security properties). For example, she has been heavy involved in SafeAdapt, OPENCROSS, TACIT and FM-BIASED among others.



### Pilar Ruiz

#### WP12 - C&D

Pilar Ruiz holds a Master Degree in Education from University of Granada and Master in Digital Marketing and Business Communication on the Internet (Web 2.0) from ESDEN Business School. She is certified in Community Program Manager and as an expert in Ecommerce from ESDEN Business School. Hands-on experienced international web strategist, with over 15 years' experience in managing and working on on-line marketing and IT projects. She is responsible for defining the digital marketing strategy, promo plan and content timeline on TRUSTECH Area. Her current research areas are digital marketing with a special focus on web trends.



# SPARTA

"Anything that we can imagine, that can be collaborated and cooperated on, that's what we are going to do"

Kevin Kelly, The next 30 digital years

**CONTACT**

[contact@sparta.eu](mailto:contact@sparta.eu)

[www.sparta.eu](http://www.sparta.eu)

[@sparta\\_eu](https://twitter.com/sparta_eu)



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



## 7.5 Annex 5 – Best-Practices Guide

# A BEST-PRACTICES GUIDE

*to attract and retain women in cybersecurity teams*



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



# A BEST-PRACTICES GUIDE

## *to attract and retain women in cybersecurity teams*

### WHY?

Cybersecurity needs to build a diverse workforce, able to respond to the challenges of a globalised and ever-changing world. Different ways of approaching problems, when coordinated, bring a competitive advantage to cybersecurity teams as they can strategically and satisfactorily meet such challenges. Today, women only account for 20% of the poorly diverse cybersecurity workforce worldwide. On top of that, Cybersecurity Ventures predicts that there will be 3.5 million unfilled jobs globally by 2021, leading to a huge increase in cybercrime, which is predicted to cost the world \$6 trillion annually by the same year. The female underrepresentation in cybersecurity is accounting for this reality.

The European Commission has been actively working on this issue and has set three main strategic actions to increase women's participation in the digital sector:

1. Challenging digital gender stereotypes;
2. Promoting digital skills and education;
3. Advocating for more women entrepreneurs.

But why does the industry fail to attract and retain women in cybersecurity workplaces? Women point to the competitive, gamified, and male-dominated cybersecurity environment as one of the main reasons for not taking nor following the path of cybersecurity. We need to start breaking down these stereotypes and make your cybersecurity environment more welcoming and attractive to women. SPARTA gathered some of the best-practices you can adopt!



# BEST-PRACTICES

Targeting on integration strategies and equity at work will promote diversity, and generate synergies with great multidisciplinary and multicultural value.

*“It doesn’t have to be expensive: companies can make the simple change of diversifying their security team. If implemented optimally as part of a firm’s recruitment strategy, this brings more views to the table and increases the range of skills available.” (O’Flaherty, 2019)*

## 1. UNDERSTAND THE PROBLEM

You can only successfully help to close the cybersecurity gender-gap if you are aware of the bigger picture. You should know and understand the numbers, the challenges we face, and the current policy initiatives. Here are some links for enlightening readings, and interesting interviews with women working in Cybersecurity:

<https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx>  
<https://www.crest-approved.org/wp-content/uploads/CREST-Closing-the-Gender-Gap-in-Cyber-Security.pdf>  
<https://eige.europa.eu/publications/gender-equality-and-digitalisation-european-union>  
<https://sparta.eu/diversity/>

## 2. LEARN TO COMMUNICATE CYBERSECURITY

Cybersecurity is viewed as being incredibly technical, gamified, and competitive, leading to a lack of interest. Yet it’s very interdisciplinary and diverse and it needs to be communicated as such. Cybersecurity goes further beyond tech as it needs a holistic team, from different areas and backgrounds, like psychology, law, communication, education, and business. Re-think the messages that are being sent and don’t forget to train your Human Resources to be aware of what kind of cybersecurity profiles should be understood. To start, the images used should be more inclusive and not perpetuating stereotypes of a faceless man with black hoodies invading a computer, nor introducing only male figures performing tech activities.

## 3. USE GENDER-SENSITIVE LANGUAGE

This toolkit on how to use more gender-sensitive language, by EIGE, helps you! Also, try not to use tech jargon while speaking.

[https://eige.europa.eu/sites/default/files/20193925\\_mh0119609enn\\_pdf.pdf](https://eige.europa.eu/sites/default/files/20193925_mh0119609enn_pdf.pdf)

## 4. ENSURE WOMEN VISIBILITY

The lack of role models in the industry, related to the lack of visibility of women working in cybersecurity leads to less involvement of pupils in the field. We urgently need to put female cybersecurity professionals in the spotlight through news, podcasts, interviews, meetings, speaking at conferences and so breakdown the stereotype that cybersecurity is a man’s job.



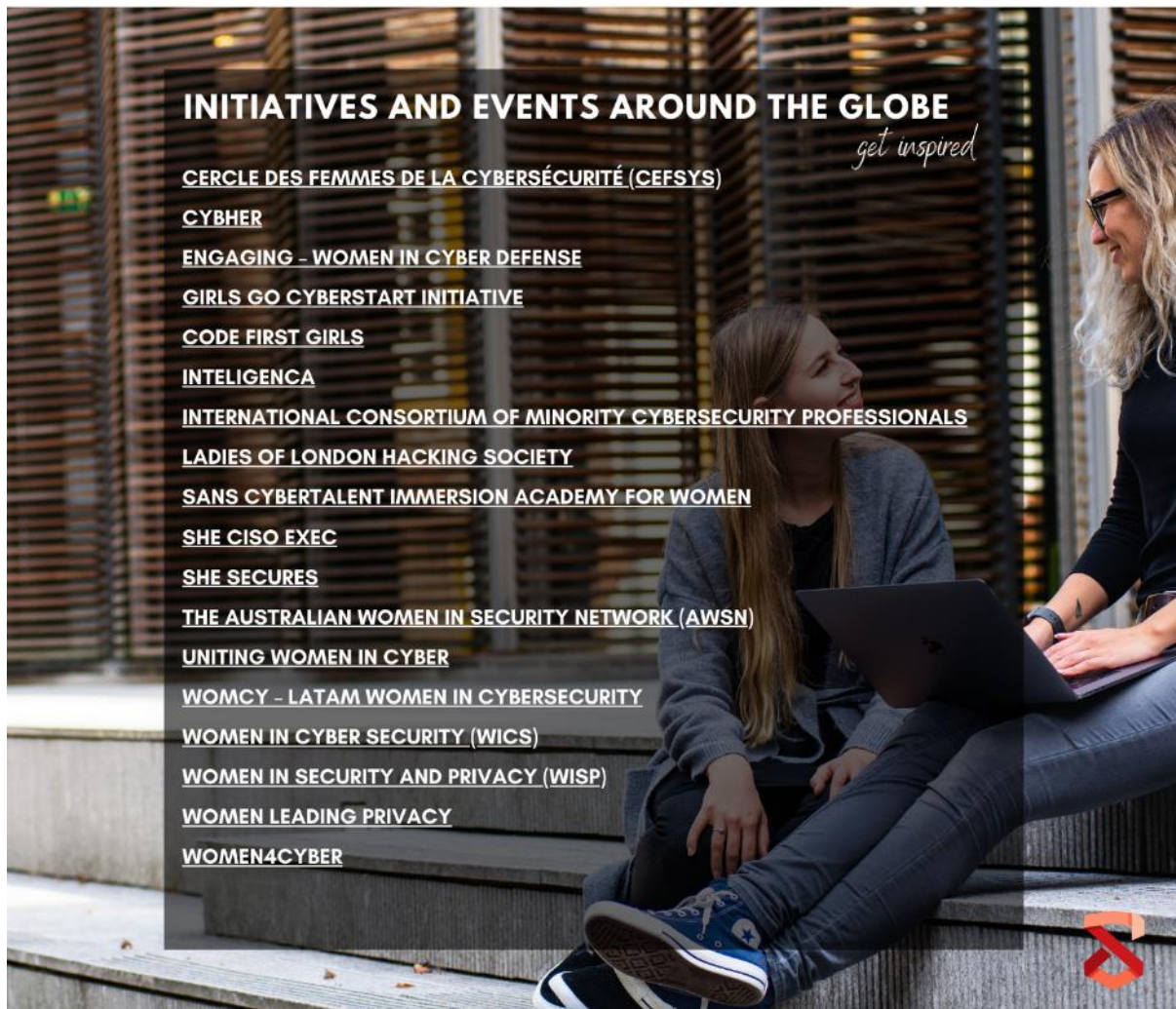


## 5. ENSURE EQUAL PAY FOR EQUAL WORK

Accordingly to an [ISC2 study](#), women working in cybersecurity earn 12% less than men. "Some of this inequity may be explained by age and tenure," they write "But this doesn't erase the reality revealed in previous research that women in cybersecurity managerial positions earn about \$5,000 less than men". We must reach equity in salaries.

## 6. EMPOWER WOMEN AND PROMOTE NETWORK

The European Institution for Gender Equality (EIGE) [reported](#) that more than nine out of ten boys and girls aged between 16-24 have sufficient competences to use digital technologies in their daily life, but boys (73%) are more confident of their abilities than girls (63%). This reflects the need to empower women, through strategies to build self-awareness and self-confidence, especially of their capabilities. To empower also means to invest time networking and developing leadership skills, which is as important as developing technical skills. A mentorship program is an excellent way to start going down this road of women empowerment! SPARTA has gathered a few steps to guide your company through a successful mentorship program.



# A MENTORSHIP GUIDE

## STEP 1: SELF-KNOWLEDGE

Start with sessions designed to help mentees getting to know themselves better – their story, values, and strengths. Mentors should be able to help to build mentees' self-confidence and help them understand how their story and character connects to the path they want to take, the choices they want to make, the changes they want to create.

## STEP 2: CONNECT

Buy a ticket for two! For a fruitful mentorship program, it is important for mentees and mentors to connect. Establish periodic meetings and change environments! Always protect mentoring time. Bridge interests besides cybersecurity and get to know each other.

## STEP 3: EXPLORE

Create spaces – physical and temporal – for mentees to explore their development possibilities, take risks, learn, and lead the way to start creating meaningful outcomes! Mentors should try to explore and present new possibilities for mentees, opening doors, and introducing them to people in the area to help them build a network. Mentees should also get to know the diversity of people working in the organisation, interact with them, and discover possible means for collaboration.

## STEP 4: CREATE

Don't let ideas die on paper. After exploring – which should be daily task – you are prepared to start bringing to life the ideas and projects mentees and mentors reached together. Mentors should, when they feel appropriate, incite mentees to establish SMART goals for their career and draw a coherent strategy. Remember to create a safe space to provide constant feedback and evolve together.

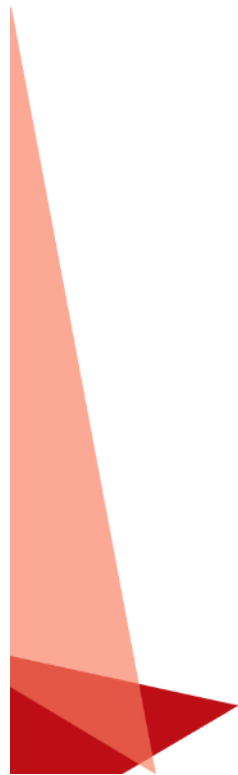
## STEP 5: PERSIST

Monitoring and evaluating your actions help you to stay on the right track. Mentors and mentees should always try to assess if changes are needed, be aware of the world that surrounds you and the challenges it imposes. Persist in your journey! It will lead you to amazing places.





**This content is licensed under a Creative Commons Attribution 4.0 International license**



Published on 2021



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



## 7.6 Annex 6 – “Little Stories about Big Women in Cybersecurity” Exhibition

# Little stories about big women in Cybersecurity



Ada Lovelace (1815-1852)

Augusta Ada Lovelace is known as the first computer programmer

“Mathematical science shows what is. It is the language of unseen relations between things. But to use and apply that language, we must be able to fully appreciate, to feel, to seize the unseen, the unconscious.”



Powered by:



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

LEARN  
MORE





Elizebeth Smith Friedman (1892 - 1980)

She taught herself how to solve secret messages without knowing the key. That's codebreaking. And she started from absolutely nothing.

She wasn't a mathematician. She was a poet. But she turned out to be a genius at solving these very difficult puzzles, and her solutions changed the 20th century. She caught gangsters and organized-crime kingpins during Prohibition. She hunted Nazi spies during World War II.

She also helped to invent the modern science of secret writing—cryptology—that lies at the base of everything from government institutions like the NSA to the fluctuations of our daily online lives. Not bad for a Quaker girl from a small Indiana town! - National Geographic



Powered by:



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

LEARN  
MORE  






Grace Hopper (1906 - 1992)

Grace Brewster Murray Hopper was a computer pioneer and naval officer. She received a master's degree (1930) and a Ph.D. (1934) in mathematics from Yale. One of the first three modern "programmers," Hopper is best known for her trailblazing contributions to the development of computer languages. Known as irreverent, sharp-tongued, and brilliant, she enjoyed long and influential careers in both the U.S. Navy and the private sector.



Powered by:



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

LEARN  
MORE  









Hedy Lamarr (1914 - 2000)

What do the most ravishingly beautiful actress of the 1930s and the inventor whose concepts were the basis of the cell phone and Bluetooth technology have in common? They are both Hedy Lamarr, the glamour icon of inspiration for Snow White and Cat Woman, and a technological trailblazer who perfected a secure radio guidance system for Allied torpedoes during WWII. She patented the frequency-hopping spread spectrum for signaling torpedoes. This became the basis for the secure Wi-Fi, GPS, and Bluetooth technologies used today!



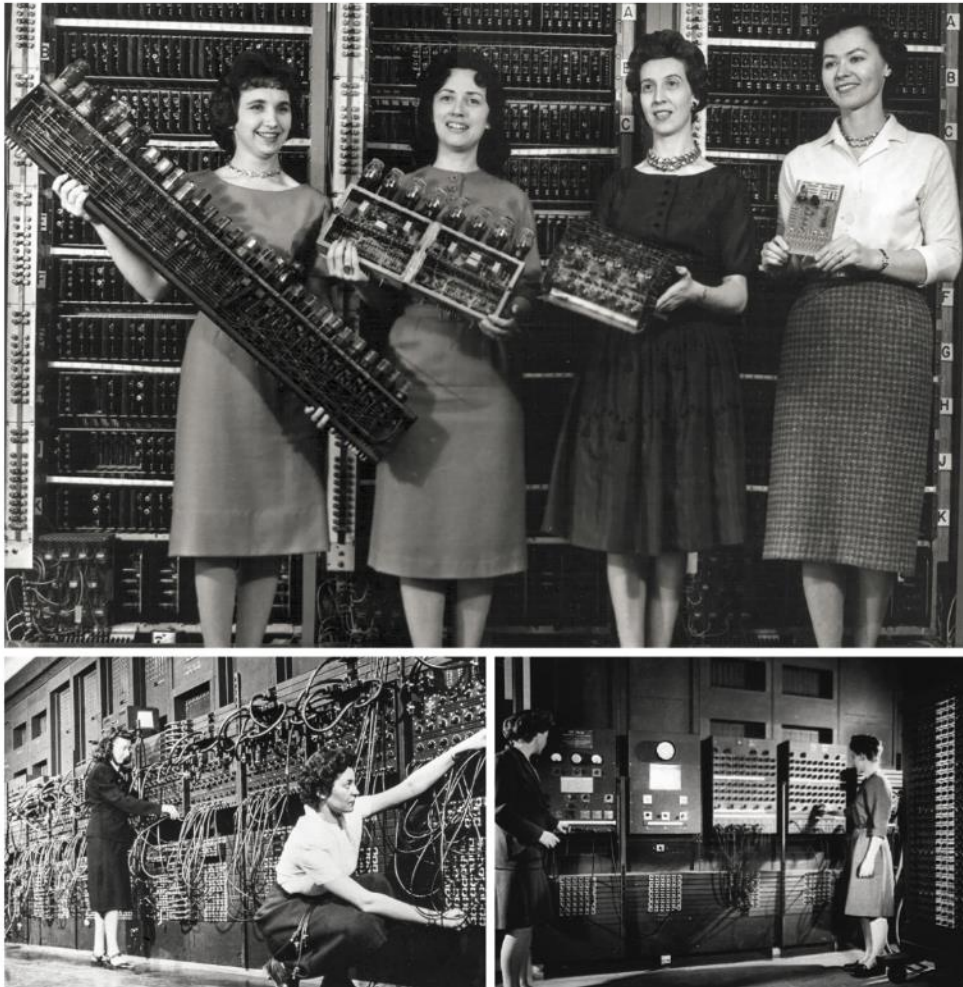
Powered by:



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

LEARN  
MORE





### The ENIAC Programmers

Jean Jennings, Marlyn Wescoff, Ruth Lichterman, Betty Snyder, Frances Bilas, and Kay McNulty were the first programmers, calculating weapons trajectories by hand and entering them into the Electronic Numerical Integrator and Computer (ENIAC) at the University of Pennsylvania, in the 1940s. In fact, the term “computer” originally referred not to the machine but to the women who programmed it.



Powered by:



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

LEARN  
MORE





## Chapter 8 Bibliography

- (ISC)<sup>2</sup>. (2019). *Women in Cybersecurity: YOUNG, EDUCATED AND READY TO TAKE CHARGE*. . online: (ISC)<sup>2</sup> Cybersecurity Workforce Report.
- CSERT. (2020). *Exploring the gender gap in cybersecurity - Have we made a difference yet?* UK: CSERT. Retrieved from [https://crest-approved.org/wp-content/uploads/CREST-Gender-report\\_202004.pdf](https://crest-approved.org/wp-content/uploads/CREST-Gender-report_202004.pdf)
- Dallaway, E. (2015). *Closing the Gender Gap in Cybersecurity*. UK: CSERT.
- SPARTA on LinkedIn: *Women in STEM 2022*. (n.d.). Retrieved from LinkedIn: <https://www.linkedin.com/feed/update/urn:li:activity:6642726395174760448/>
- SPARTA on LinkedIn: *Women in STEM, 2022*. . (n.d.). Retrieved from LinkedIn.com.