SPARTA

D12.4
Updated dissemination and communication plan and evaluation - v2

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

Deliverable type	Report
Deliverable reference number	SU-ICT-03-830892 / D12.4 / V1.0
Work package contributing to the deliverable	WP12
Due date	January 2020 – M24
Actual submission date	1st February 2021

Responsible organisation	INOV
Editor	Catarina Valente
Dissemination level	PU
Revision	V1.0

Abstract	The present deliverable contains the updates and evaluation of the work carried out in each stage of the dissemination and communication planned actions in the D12.3. Updates have been designed aiming at leverage efficient actions, promoting audiences' awareness, participation and action in SPARTA, and cybersecurity realm.
Keywords	Communication & dissemination strategy, engagement and participation, monitoring and evaluation

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

Editor

Catarina Valente (INOV)

Contributors (ordered according to beneficiary numbers)

Elisabete Carreira (INOV)

Reviewers (ordered according to beneficiary numbers)

Thibaud Antignac (CEA)

Julie Hallinger (SMILE)

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 contains the updates and evaluation of the work carried out in each stage of the communication and dissemination (C&D) plan. Updates have been designed to leverage efficient communication, promoting audiences' awareness, participation, and action in SPARTA and the cybersecurity realm. The communication and dissemination efforts designed for the third year of the project target changing attitudinal behaviour, that is of public interest, towards cybersecurity actions.

Due to the constraints imposed by the pandemic COVID-19 some of the events expected to be organized or attended during the second year of the project were cancelled or re-scheduled. Nonetheless, communication actions were promoted - such as workshops, SPARTA Days, conferences and talks, - and it has been possible to create synergies with relevant stakeholders. During the second year of the project, SPARTA participated in 29 (conferences/workshops/others), organised four conferences, and 13 Monthly Workshops, most of them through virtual platforms. During this period, there were 42 papers accepted, acknowledging SPARTA, and some of them are published in Journals and conferences that are part of the CORE ranking (A, B, and C). These scientific publications are stored and organised on the SPARTA website Results page to facilitate the search and dissemination process.
SPARTA Website is often updated and worked on, in a collaborative work between all WP's, led by INOV and CEA, to ensure SPARTA delivers a dynamic, intuitive, and complete platform to its visitors.

The Communication and Dissemination strategy adopted for the SPARTA social media accounts has contributed to growth in the project's visibility, as it has been able to attract 1105 followers on Twitter, 442 on LinkedIn, and 195 on Instagram, and create a more consistent and engaged audience. These networks have been of utmost importance to ensure SPARTA visibility, fostering conversations, and raising awareness on cybersecurity and its challenges. Advertisements will take place during the third year of the project as they are proven to effectively and efficiently deliver messages to targeted audiences and assure the outreach of publications to many people. Hootsuite, a social media content management tool, was selected to coordinate and manage all publications efficiently.

During the second year of the project, partners conducted several activities to promote awareness of and involvement with the SPARTA project, thus acting accordingly to what was proposed in D.12.1 and D12.3. As for internal communication, NextCloud was chosen to ensure a strong communication flow and to facilitate the exchange of information and ideas. The internal newsletter will be replaced by the timely delivery of the news published on the SPARTA website to the partners through the dedicated e-mail project.consortium@internal.sparta.eu.

The actions designed for the second year of the project related to Task 12.4 – Closing the Gender and Diversity Gap – did not conclude, namely the "SPARTA Goes to School" action, or had to be re-designed, as the "Women In SPARTA" interviews. The activities that were not completed will be considered during the third year of the SPARTA Project along with the creation and implementation of a SPARTA Mentorship Program. The main objectives planned for the second year of the project related to Task 12.5 – Engagement of the Outermost Regions of Europe – were not fully completed due to the imposed travel restrictions and the demand to re-think the usual proceedings of activities. These objectives are updated and will lead to the activities planned for the third year of the project.

Accordingly to the recommendations made to WP12 during the M12 review, the C&D team adopted measures to re-direct efforts from "branding" to "information and engagement" in line with the strategy planned for the Communication & Dissemination activity on deliverable 12.3.

Table of Content

List of Figures

List of Tables

Chapter 1 Introduction

The WP12 – Communication and Dissemination - is conceived to plan, coordinate, and execute all the activities related to dissemination and communication. It foresees the yearly update of the strategic plan designed within the deliverable 12.1 – Dissemination and Communication Plan (hereinafter C&D plan) – jointly with the evaluation of the work carried out during the previous year.

The present deliverable aims to report and evaluate all the communication and dissemination activities carried out during the second year of the project and develop adequate methods to correct possible deviations of the plan, providing suitable updates to deliverable 12.3.

WP12 relies on ongoing interactions with other relevant WP's to receive inputs to implement the C&D plan.

As established in the previous deliverable 12.3 – Dissemination and communication plan, updates and evaluation – interactions with all the partners have been and will continue to be leveraged to ensure strong internal communication and a diverse and complete set of contents to disseminate on SPARTA communication channels, keeping both partners and audiences well informed of SPARTA activities and achievements.

The interaction between WP12 and WP1 – CCN Governance and assessment – has been and will continue to be of utmost importance to align the communication activities with the overall needs of the project.

The relations with WP3 – Roadmap Design and WP8 – Clustering, platforms, and ecosystems have been crucial to the production of communication materials to the events as well as its dissemination on SPARTA social media accounts.

Interactions between SPARTA programs within the scope of WP4 to WP7 (T-SHARK, CAPE, HAII-T, and SAFAIR) and WP12 have started to be implemented during the second year, namely with the dissemination of results.

Chapter 2 Communication Strategic Approach

This chapter reviews the strategic axes established in deliverable 12.1, contains the evaluation of the strategy planned for the second year, and defines the communication and dissemination strategy for the third year.

2.1 Strategic Axes

The three interdependent strategic axes established in deliverable 12.1 serve as the grounding basis to conduct and develop the C&D plan:

- **Awareness**: making the project and its aims acknowledged.
- **Participation**: engaging target groups and enable them to understand SPARTA concepts and results achieved.
- **Action**: promoting action from target groups influencing practices, products and standards.

The first version of the plan defined the Participation axis as the second-year focus, designed to be sustained during the rest of the project. In the Participation axis, the communication efforts aimed to reach higher levels of audience engagement with the project, such as:

1. Attendance in SPARTA events;
2. Contacts from media;
3. Invitation for speaking at external events;
4. Demonstrations of interest.

A second-year general evaluation follows to monitor the achievement of the communication objectives proposed for the **Participation** axis. The Participation axis will have a re-enforcement during the third year of the project as the COVID-19 pandemic negatively impacted some of the activities proposed to reach the goals listed above.
The third year of the project foresees the rising of the **Action** axis among audiences that are aware of and engaged with SPARTA. In the Action axis, the communication and dissemination efforts will target at changing attitudinal behaviour, that is of public interest, towards cybersecurity actions such as:

1. Adoption of cybersecurity habits;
2. Acquisition from the industries of cybersecurity services;
3. Academy starts to direct their interests and activities towards the issue

Besides those, attitudes towards acting alongside SPARTA are essential to the success of the project. These goals are not possible to measure within a short period as they are related to changing attitudinal behaviour. Nevertheless, communication efforts will target these goals with the **Awareness** and **Participation** axes that are to be continuously maintained and nourished and thus constitute the ground to correctly build the path to the Action axis deployment beyond the project end.

2.2 Key Audiences and Messages

SPARTA key audiences were identified and characterized in deliverable 12.1 and are still relevant. Deliverable 12.1 established the key messages to deliver during the placement of each axis, and for the **Action** axis in specific, we establish the following messages:

- Understand and work on the gender and diversity gap issue is a social responsibility of public interest. As to reduce the gender gap and lack of human resources for cybersecurity in Europe, SPARTA will address this issue by embedding several positive actions.

- Contributing to 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 sectoral diversity.
- The project will create value among cybersecurity ecosystems, from end-users to solution providers, from governmental bodies to ethical hacking communities. It will leverage expertise from several audiences in various locations in the European Union to raise awareness and to foster conversations ranging from cutting-edge research advances to accurate problem identification.
- SPARTA's research roadmap starts from horizontal technologies: major technological drivers like digitization, Big Data, artificial intelligence, cognitive Internet, and IoT, based on cybersecurity assets such as blockchain technology, as well as new trends like programmable materials, or quantum computers, will already have significant impacts on all industrial sectors.

Messages related to the SPARTA achievements and results are to deliver during the third year of the project through advertisements on social media. The C&D team will promote straight interactions with the media as they play a role in communicating SPARTA to academia, industry, and policymaking. The C&D team will thus continue to use a mixed channel approach to deliver the SPARTA messages as it has proven to be efficient during the lifetime of the SPARTA project.

2.3 Contribution to the KPIs of the project

The D12.1 anticipated the direct contributions of the communication and dissemination activities to specific project KPIs. The present deliverable provides the achieved results on enhancing awareness and training capabilities and develops cybersecurity skills, which will be measured as follows:

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	
6.4 - number of indirectly addressed people (through advertisements, social media) by the awareness program by the end of the project.	>2000	>10 000	>20000	> 22300	> 50000	

Another key indicator is the extent to which SPARTA **builds sustained collaboration** with academic, industrial, governmental and community stakeholders, which will be measured as:

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 > 30	> 22 >30	> 36 >50	

2.4 Cyber Competence Network

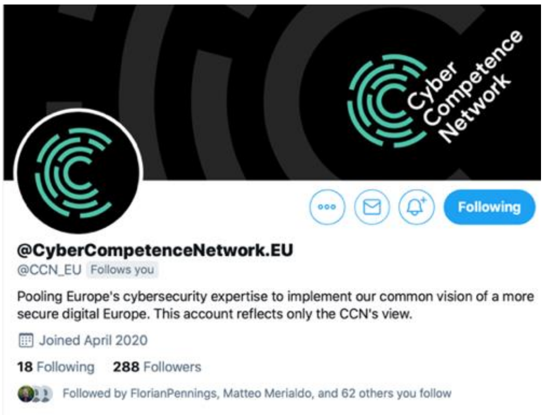
CCN Communication management chair

From January 2020 to July 2020, SPARTA was chair of the CCN's communication management group. Also, from January 2022 to February 2022 (end of project), SPARTA will chair the CCN's communication and dissemination management group.

CCN's Communication Management

During this period, SPARTA established periodic meetings to plan, update, and monitor CCN's coordinated communication activities, with representatives of each pilot. As a result of these meetings, SPARTA:

- Designed and prepared, jointly with the other pilots, the first draft of the CCN Communication and Dissemination strategy, which was then leveraged by the next chair (CyberSec4Europe).
- Created the CCN Twitter account (@CyberCompetenceNetwork.EU /@CCN_EU) aiming to leverage the communication efforts on one social media platform and build an identity and presence of its own. All pilots are responsible for the management and sustainability of the account.



@CyberCompetenceNetwork.EU
@CCN_EU Follows you

Pooling Europe's cybersecurity expertise to implement our common vision of a more secure digital Europe. This account reflects only the CCN's view.

Joined April 2020

18 Following **288** Followers

Followed by FlorianPennings, Matteo Merialdo, and 62 others you follow

Figure 1: CCN Twitter account

9–11 December
Online
CONVERGENCE
Making the European Cybersecurity
Competence Network a Reality

Figure 2: CONVERGENCE event poster

CCN Events

SPARTA, and the other cybersecurity pilots prepared the CONVERGENCE[1] event that aimed at highlighting the European cybersecurity stakeholder community the progress that is being made in harnessing European expertise and resources in the broader context of the proposed legislation relating to a European Cybersecurity Industrial, Technology and Research Competence Centre and a Network of National Coordination Centres.

[1] https://cybercompetencenetwork.eu/events/past-events/convergence/

Chapter 3 Communication and Dissemination actions

Chapter 3 considers the actions developed by the SPARTA partners during the second year of the project to disseminate project results. The list of possible events, conferences, scientific journals, workshops, symposiums for SPARTA dissemination of scientific results and activities are duly updated in this section. The actions designed for the third year of the project related to Tasks 12.4 and 12.5 – *Closing the Gender and Diversity Gap* and *Engagement of the Outermost Regions of Europe* – are also addressed in this chapter.

3.1 Conferences and events

Since March 2020, the COVID-19 pandemic imposed several changes on the strategic actions planned for the second year of the project, namely the presential events. A considerable number of events were cancelled during the first months of the pandemic, re-designed and re-scheduled. Such constraints led to a decrease in participation and preparation of events during the second year of the project. Nonetheless, communication actions were promoted - such as workshops, SPARTA Days, conferences, and talks, - and it has been possible to create synergies with other relevant stakeholders, namely through the Associate and Friends program dedicated events and workshops. The following table is an updated list of potential events for the dissemination activities during 2021:

Name of the event	Frequency
The 36th ACM/SIGAPP Symposium On Applied Computing	Annual
Conference on Computer Privacy and Data Protection (CPDP)	Annual
Conference on Cryptographic Hardware and Embedded Systems	Annual
Conference on Ethics of Computing (ETHICOMP)	Annual
EAFS – European Academy of Forensic Science Conference (2022)	Bi-annual
European Cybersecurity Challenge (ECSC)	Annual
European Symposium on Research in Computer Security (ESORICS)	Annual
IEEE European Symposium on Security and Privacy (Euro S&P)	Annual
Int. Conference on Cyber Situational Awareness, Data Analytics and Assessment IEEE	Annual
IEEE Industrial Electronics Society (IES)	Annual
FMCAD Student Forum 2021	Annual
Int. Conference on the Theory and Applications of Cryptographic Techniques Eurocrypt	Annual
International Conference on Availability, Reliability and Security (ARES)	Annual
International Conference on Dependable Systems and Networks (DSN)	Annual
9th International Conference on Information Technology and Science (ICITS)	Annual

Name of the event	Frequency
23nd International Conference on Enterprise Information Systems (ICEIS 2021)	Annual
18th International Conference on Security and Cryptography (SECRYPT 2021)	Annual
21st Privacy Enhancing Technologies Symposium (PETS 2021)	Annual
36th IFIP TC-11 International Information Security and Privacy Conference (SEC)	Annual
International Conference on Computational Science (ICCS 2021)	Annual
Infosecurity Europe 2021 / 25 year	Annual

Table 1: Updated List of Potential Events for Dissemination

3.2 Scientific Publications

The SPARTA website Results[2] page, where the scientific publications are stored and organised to facilitate the search process, allows for more acute dissemination of these contents. Through this page link, one can share the papers on the SPARTA social media platforms (LinkedIn, and Twitter). In this section is highlighted the list of potential scientific journals to disseminate SPARTA scientific publications, defined in D12.1 and updated in D12.3.

Scientific Journal and main dissemination aspects
ACM Transactions on Information and System Security (TISSEC) is devoted to the study, analysis, and application of information and system security. TISSEC topics include: security technologies; secure systems; secure applications; and security policies.
ACM Transactions on Privacy and security publishes high-quality research results in the fields of information and system security and privacy.
Elsevier Computer Fraud & Security focuses on providing practical, usable information to manage and control computer and information security effectively.
Elsevier Computer Law & Security Review is an international journal of technology law and practice providing a major platform for publication of research, policy and legal analysis within the field of IT law and computer security.
Elsevier Computers & Security provides a unique blend of leading-edge research and sound practical management advice. It is aimed at the professional involved with computer security, audit, control and data integrity in all sectors - industry, commerce and academia.
IEEE security and privacy stimulates and tracks advances in security, privacy, and dependability and presents these advances in a form that can be useful to a broad cross-section of the professional community, ranging from academic researchers to industry practitioners.
IEEE Technology & Society Magazine covers the impact of technology on society, the impact of society on the engineering profession, the history of the societal aspects of electrotechnology, and professional, social, and economic responsibility in the practice of engineering and its related technology.

[2] https://www.sparta.eu/papers/

Scientific Journal and main dissemination aspects
IEEE Transactions Dependable and Secure Computing covers the dependability and security, including the joint consideration of these issues and their interplay with system performance.
IEEE Transactions on forensics and security covers sciences, technologies, and applications relating to information forensics, information security, biometrics, surveillance and systems applications that incorporate these features.
IEEE Access is an award-winning, multidisciplinary, all-electronic archival journal, continuously presenting the results of original research or development across all of IEEE's fields of interest.
Springer Ethics and Information Technology is dedicated to advancing the dialogue between moral philosophy and the field of information and communication technology (ICT).
Springer Journal of Cryptographic Engineering offers high-quality scientific articles presenting methods, techniques, tools, implementations, and applications of research in cryptographic engineering.
Springer Journal of Cryptology is a forum for results in all areas of modern information security. Both cryptography and cryptanalysis are covered, including information-theoretic and complexity-theoretic perspectives as well as implementation, application, and standards issues.
Proceedings on Privacy Enhancing Technologies (PoPETs) is an open access journal for timely research papers on privacy that has been established as a way to improve reviewing and publication quality while retaining the highly successful PETS community event.
SoftwareX aims to acknowledge the impact of software on today's research practice, and on new scientific discoveries in almost all research domains.

Table 2: Updated List of Potential Scientific Journals for Dissemination

3.3 Monthly SPARTA workshops

The SPARTA monthly workshops gather a diverse set of actors to get involved in the project. WP12 helps in the dissemination of these workshops, organized within the scope of WP3 and WP8, through publications on SPARTA's social media accounts and the website.

3.4 Campaigns for Diversity in Cybersecurity

3.4.1 Closing the Gender Gap

Due to the COVID-19 pandemic impacts, some actions planned for the second year of the project did not conclude, namely the “SPARTA Goes to School” action, or had to be re-designed, as the “Women In SPARTA” interviews. The social media campaign designed to raise awareness on the need for a diverse workforce on cybersecurity, from March 2020 to March 2021, is running. The activities not completed will be considered during the third year of the SPARTA Project. The following tables, updated from D12.3, summarize the planned activities for the M24 – M36:

SPARTA Mentorship Programs	
Target	Women in the cybersecurity community and the SPARTA partners
Objective	Provide guidance to SPARTA partners on how to implement a mentorship program
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 a guide 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. This guide will be delivered to SPARTA partners and shared with the cybersecurity community through SPARTA social media accounts and official website.

Table 3: Action 1: SPARTA Mentorship Program Guide

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	10th 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 **exhibition about women in cybersecurity** 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 4: Action 2 - SPARTA Goes to School

3.4.2 Engagement with the Outermost Regions of Europe

The main objectives planned for between M12 and M24 for task 12.5 - Engagement of the Outermost Regions of Europe – were not fully completed due to the COVID-19 impacts, namely because of the imposed travel restrictions and the demand to re-think the usual proceedings of activities. These objectives are updated and will lead to the activities planned for the third year of the project:

- Build sustained collaborations with *Office de L'eau* and *Universidad de las Palmas de Gran Canaria* by ensuring strong communicational bounds.
- Communicate to the SPARTA audience the "Go Cyber with SPARTA" campaign through SPARTA social media accounts and website.

The description and evaluation of the achievements made between M12 and M24 are in the Monitoring and Evaluation chapter.

Action 1 – *Encourage small businesses to adopt cybersecurity measures* (the Caribbean and South America OR) – Interactions with Technopole Martinique led to other contacts, such as the **Direction of Développement Economique et des Entreprises (2D2E),** with whom SPARTA will coordinate efforts to establish a targeted and suitable collaboration with a business association to achieve this action's objectives. A backup plan is being prepared in case no arrangements are possible in Martinique island, with the involvement of a business association from the Azores Island.

Action 2 – *Stimulate young people to undertake studies or training at the university level within the area of cybersecurity* (Atlantic Ocean OR) – collaborations with the Universidad de Las Palmas de Gran Canaria are established, and the two first actions, proceeded in a coordinated action with the SPARTA **Cybersecurity Training and Awareness Program (WP9)**, are now concluded. The third year of the project foresees the following activities:

1. The deployment of the awareness campaign to stimulate students to undertake studies in the cybersecurity field.
2. Provide the Universidad de Las Palmas de Gran Canaria the analysis of the existing "Degree in Computer Engineering" program and its potential for creating a specialized program on cybersecurity, through a workshop.

Action 3 – ***Engage with critical infrastructure operators to stimulate them to adopt state-of-the-art cybersecurity technology* (Indian Ocean OR):** Advances were made during the second year of the project, allowing for a more incisive deployment of the activities established in the D12.3, to develop in a coordinated action with the SPARTA **Cybersecurity Training and Awareness Program (WP9):**

1. Implement an awareness campaign to encourage employees to adopt cybersecurity measures, taking into account their cybersecurity informational needs.
2. A training workshop for non-cybersecurity professionals.
3. Identification of solutions for specific problems using developed knowledge within SPARTA, namely within the JCCI.

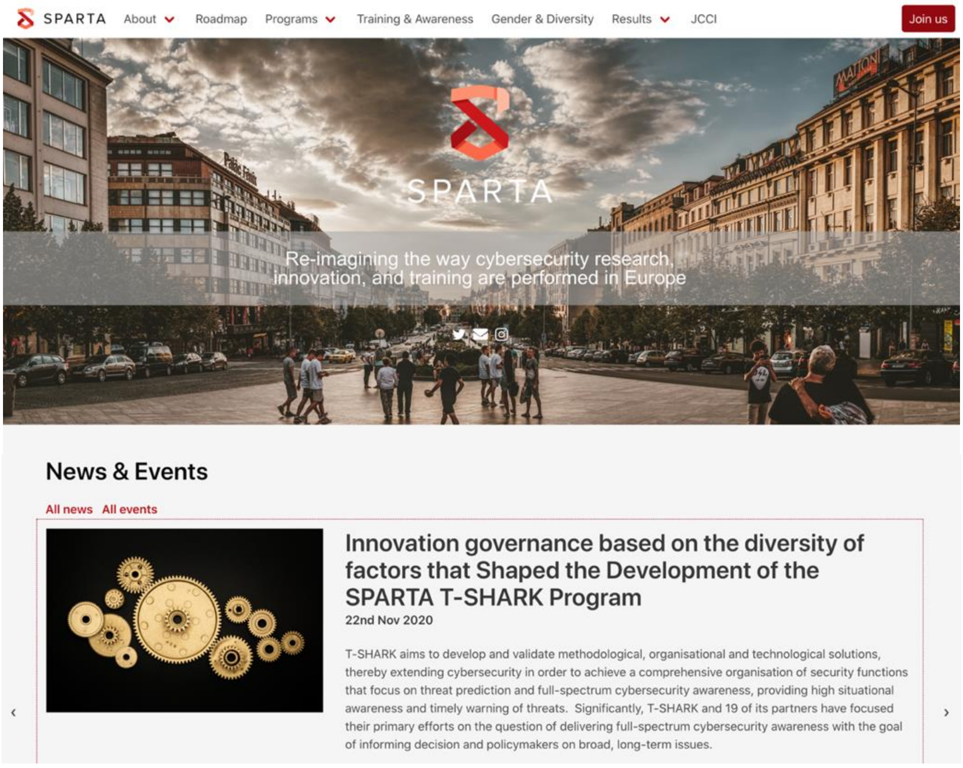
Chapter 4 Communication and Dissemination Instruments

Chapter 4 considers the C&D instruments that have been updated during the second year of the project to improve their efficiency, ensuring that the project's communication objectives have a cohesive instrumental base to be correctly addressed.

4.1 SPARTA Website

The SPARTA website (www.sparta.eu) is often updated and worked on, in a collaborative work between all WP's, led by INOV and CEA, to ensure SPARTA delivers a dynamic, intuitive, and complete platform to its visitors:

- The website provides information about SPARTA, its challenges, structure, and partners on a single page.
- The "Results" page features all the SPARTA publications, deliverables, podcasts, and demonstrators.
- The website has a dedicated section to the training and awareness WP9 and others to the Gender and Diversity dimension of SARTA.
- A "News & Events" section features the frontpage to provide visitors with the latest news, activities, and achievements related to the project.
- The JCCI is part of the SPARTA website and will be leveraged through several publications on social media.



Re-imagining the way cybersecurity research, innovation, and training are performed in Europe

Innovation governance based on the diversity of factors that Shaped the Development of the SPARTA T-SHARK Program

22nd Nov 2020

T-SHARK aims to develop and validate methodological, organisational and technological solutions, thereby extending cybersecurity in order to achieve a comprehensive organisation of security functions that focus on threat prediction and full-spectrum cybersecurity awareness, providing high situational awareness and timely warning of threats. Significantly, T-SHARK and 19 of its partners have focused their primary efforts on the question of delivering full-spectrum cybersecurity awareness with the goal of informing decision and policymakers on broad, long-term issues.

Figure 3: SPARTA Website

4.2 SPARTA project communications

Deliverable 12.3 defined a strategy to be implemented during the second year of the project (M12-M24) that aimed at building a cohesive internal communication flow. As a result, a bi-monthly newsletter was launched to ensure all partners were updated with the latest achievements of the different Activities and Programs. The *Stackfield* tool was deployed to promote easier collaboration among partners.

For the third year of the project, these tools will not continue to be in use as they have not proven to be efficient and popular enough among partners. The evaluation of these tools can be found at the Monitoring and Evaluation chapter.

Instead of the newsletter, the C&D team will deliver the news published on the SPARTA website to the partners through the dedicated e-mail project.consortium@internal.sparta.eu. The adoption of this strategy lies in the simplification of the process and avoids to depend on timely-delivered content. After gathering the partners' inputs on the selection of a new internal tool to ensure a strong communication flow and to facilitate the exchange of information and ideas, *NextCloud* was chosen to accomplish these objectives and is currently under a testing process to replace *Stackfield.*

4.3 SPARTA social media

Advertisements will take place during the third year of the project as they are proven to effectively and efficiently deliver messages to targeted audiences and assure the outreach of publications to many people. The C&D team will select the messages related to the main results of the SPARTA project and SPARTA organized events to advertise on social media accounts.

Hootsuite, a social media content management tool, was selected to coordinate and manage all publications efficiently, allowing for streamlined teamwork to organize, schedule, and publish content effortlessly to all SPARTA social media accounts.

Chapter 5 Monitoring and Evaluation

Chapter 5 reports and evaluates the C&D activities developed during the second year of the SPARTA project, as well as the C&D instruments used. This chapter also monitors the actions Tasks 12.4 and 12.5 – *Closing the Gender and Diversity Gap* and *Engagement of the Outermost Regions of Europe* – and they are reported in this chapter.

5.1 Monitoring Communication and Dissemination actions

5.1.1 Events

Some of the conferences, workshops, and talks expected to be organized or attended during the second year of the project were cancelled or re-scheduled due to the constraints imposed by the COVID-19 pandemic. In this context, between M12 – M24, SPARTA participated in 29 (conferences/workshops/others), organised four conferences and 14 Monthly Workshops most of them through virtual platforms.

At the 100 events attended or organized since the beginning of the project, academia was involved/ represented in 94 of them, and the Industry in 97 making them SPARTA's most preeminent audience at the moment. Most of these events occured at the international level and gather a significant diversity of stakeholders

	Type of activities	Main leader	Title	Place	Description of the event	Level
1	Organisation of a Workshop	BUT	Brno Security Meetings	Brno, Czech Republic	Workshop and awareness event for students, researchers and general public focused on cryptography and implementation aspects on smart cards.	National
2	Participation to other events	CEA	SPARTA booth at Cyber Festival — 10 years of ANSSI	Paris, France	Presentation of SPARTA to the attendees of the CyberFestival organized by ANSSI for its 10 years	National
3	Participation to other events	CEA	SPARTA booth at DigiHall Days	Palaiseau, France	Presentaton of SPARTA to the attendees of DigHall days	National
4	Organisation of a Conference	CEA	SPARTA Day	Palaiseau, France	The SPARTA Day proposes high-level presentation and panels discussing about cybersecurity strategy, collaboration, and stakeholder’s inclusion.	International
5	Participation to other events	CEA	Meeting with Commissioner Mariya Gabriel	Strasbourg, France	Meeting with Commissioner Mariya Gabriel at the European Parliament to present the 4 pilots and discuss cybersecurity challenges Europe faces.	International
6	Participation to other events	CEA	Resilience. Deterrence. Defence – Calls to action for future cybersecurity and privacy policy Concertation meeting of H2020 projects from unit "Cybersecurity & Privacy"	Brussels, Belgium	All four projects now thoroughly active this session will address how each pilot is planning to address the following issues: Cyber-ranges; Threat intelligence; Certification; Cybersecurity skills	International
7	Participation to other events	CEA	Common website for pilots launch	Brussels, Belgium	Welcome from CONCORDIA coordinator and introduction of new project partners, Prof. Dr. Gabi Dreo, Research Institute Cyber Defence (CODE) Panel discussion – True European Cooperation: a Pillar of Digital Sovereignty? Presentation of four pilots -	International

	Type of activities	Main leader	Title	Place	Description of the event	Level
					CONCORDIA, SPARTA, ECHO and CyberSec4Europe Launching of the common web site	
8	Participation to a Workshop	NCSR	H2020 Ghost clustering workshop	Athens, Greece	This workshop is organized by the GHOST project aiming at establishing tight connections with relative H2020 projects in the field of cybersecurity in IoT and relative domains.	International
9	Participation to a Conference	CEA	13th Meeting of the Community of Users on Secure, Safe, Resilient Societies	Brussels, Belgium	Sub-theme 2.2: Building a cybersecurity ecosystem to secure Europe's society	International
10	Participation to other events	CEA	Presentation of the 4 Cybersecurity Centre Networks at ICT Proposer's Day 2018	Vienna, Austria	The focus: support the audience to join, participate and benefit from the 4 Cybersecurity Competence Networks. Targeting mainly the SME and Start-ups to raise awareness on how they can join.	International
11	Participation to a Conference	CEA	This is SPARTA	Erquy, France	Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information	National
12	Participation to a Workshop	CEA	Advances in Usability of Formal Methods for Code Verification	Prague, Czech Republic	InterAVT 2019 Interactive Workshop on the Industrial Application of Verification and Testing	International
13	Participation to other events		SPARTA Project	Palaiseau, France	CEA List General Assembly	National
14	Other	CEA	SPARTA Project	Paris, France	Japanese scientific delegation to France	International
15	Other	CEA	SPARTA Project	Paris, France	Meeting with Ministry of Interior of France	National

	Type of activities	Main leader	Title	Place	Description of the event	Level
16	Participation to other events	CEA	SPARTA booth at CEA List Days	Palaiseau, France	Presentaton of SPARTA to the attendees of CEA List days	National
17	Participation to other events	CEA	SPARTA Project	Saclay, France	"Scientifique, toi aussi !" allows high-school students to meet scientists and understand how research is done.	National
18	Participation to other events	CEA	This is SPARTA	Saclay, France	SPRING Saclay	National
19	Other	CEA	SPARTA Project	Brussels, Belgium	Invitation from the US Embassy in Belgium to present SPARTA	International
20	Other	CEA	SPARTA Project	Palaiseau, France	Presentation to Chief Executive of French Defense Innovation Agency	National
21	Other	CEA	SPARTA Project	Palaiseau, France	Presentation to the Working Group of the Systematic cluster	National
22	Participation to other events	CEA	LeHack2019	Paris, France	Presentation of SPARTA to the attendees of the LeHack 2019 event and engagement with the cybersecurity community.	National
23	Participation to a Conference	JR	Austrian ICT Security Conference	Fürstenfeld, Austria	ICT Security Conference organised by the Austrian Armed Forces, the largest Austrian Cybersecurity conference, that attracted 2.500 interested visitors in two days.	National
24	Participation to a Conference	CETIC	7th europol-interpol cybercrime conference	The Hague, The Netherlands	Attending presentations and discussions on cybersecurity act and cybersecurity ontologies (including UCO and CASE).	International

	Type of activities	Main leader	Title	Place	Description of the event	Level
25	Participation to a Conference	UTARTU	OTM 2019 Conferences, the 27th International Conference on Cooperative Information System	Rhodes, Greece	Attending the presentations, presenting the paper "Security Risk Management in Cooperative Intelligent Transportation Systems: A Systematic Literature Review".	International
26	Participation to a Conference	SAP	Heise devSec	Heidelberg, Germany	Developer conference organized by Heise/dpunkt, during which Eclipse Steady was presented.	International
27	Participation to a Conference	SAP	TechEd	Barcelona, Spain	Industry conference organized by SAP, during which Eclipse Steady was presented.	International
28	Participation to a Conference	SAP	EclipseCon	Ludwigsburg, Germany	Developer conference organized by the Eclipse Foundation, during which Eclipse Steady was presented.	International
29	Participation to a Conference	TEC	XIII Congreso Internacional de Ciberseguridad Industrial en Europa	Madrid, Spain	https://www.cci-es.org/web/cci/detalle-congreso/-/journal_content/56/10694/850611	International
30	Participation to a Conference	TEC	Congreso Protección de Datos Bilbao | Wolters Kluwer	Bilbao, Spain	https://tienda.wolterskluwer.es/p/congreso-privacidad-bilbao	International
31	Participation to a Conference	TEC	IT.SA The IT Security Expo and Congress	Nurember, Germany	https://www.it-sa.de/en	International
32	Participation to a Conference	TEC	Congreso Basque Industry 4.0 and Basque Cybersecurity Day	Bilbao, Spain	https://agenda.spri.eus/meetingpoint/es	International

	Type of activities	Main leader	Title	Place	Description of the event	Level
33	Organisation of a Conference	LEO	SPARTA Event - Cybertech Europe 2019	La Nuvola Convention Center - Rome	https://www.cyberwatching.eu/projects/1136/sparta/news-events/sparta-event-cybertech-europe-2019	International
34	Organisation of a Workshop	CNIT	CY4GAMES	Rome, Italy	https://www.cy4gate.com/cy4games	International
35	Participation to a Conference	CNIT	NETSOFT 2019	Paris, France	https://netsoft2019.ieee-netsoft.org/	International
36	Participation to a Conference	LIST	ICT Spring 2019	Luxembourg	https://www.ictspring.com	International
37	Participation to a Conference	LIST	Information Security Day 2019	Luxembourg	https://securitymadein.lu/events/information-security-day/	International
38	Participation to a Conference	LIST	Luxembourg Internet Days 2019	Luxembourg	https://www.luxembourg-internet-days.com	International
39	Participation to a Conference	BUT	14th International Conference on Availability, Reliability and Security	Canterbury, United Kingdom	https://2019.ares-conference.eu/	International
40	Participation to a Conference	BUT	13th International Conference on Network and System Security	Sapporo, Japan	http://nsclab.org/nss2019/	International

	Type of activities	Main leader	Title	Place	Description of the event	Level
41	Participation to a Conference	BUT	ICT Systems Security and Privacy Protection	Lisbon, Portugal	https://www.ifipsec.org/2019/	International
42	Participation to a Conference	TNK	Österreichischer IT-Sicherheitstag 2019	Klagenfurt, Austria	https://www.syssec.at/de/veranstaltungen/sitag2019	International
43	Participation to other events	CESNET	C2S2 2019	Milovy, Czech Republic		National
44	Participation to a Conference	TECNALIA	SPARTA CAPE	Web	https://www.youtube.com/watch?v=cU1QsdyaNXs&feature=youtu.be	International
45	Participation to a Conference	TECNALIA	SPARTA "Hacía un nuevo escerario de la I+D en Ciberseguridad en Europa"	León, España	https://www.incibe.es/enise	International
46	Participation to a Conference	UTARTU	CAISE 2020	France		International
47	Participation to a Conference	CEA	Information session on Public Private Partnerships in the light of the proposal for a Cybersecurity Competence Center	Brussels, Belgium	Presentation at "Information session on Public Private Partnerships in the light of the proposal for a Cybersecurity Competence Center"	International
48	Participation to a Conference	CEA	OECD's Global Forum on Digital Security for Prosperity	London, UK	Round table at OECD's Global Forum on Digital Security for Prosperity	International

	Type of activities	Main leader	Title	Place	Description of the event	Level
49	Participation to a Workshop	CEA	ECSO WG6 meeting	Brussels, Belgium		International
50	Participation to a Conference	CEA	Data Natives	Berlin, Germany	Presentation of the 4 pilots to the Council of the EU	International
51	Participation to other events	CEA	Presentation to the Director of the French Cybersecurity Grand Challenge	Paris, France		National
52	Participation to a Workshop	CEA	Presentation at "Workshop with Member States about the Network of National Coordination Centres"	Brussels, Belgium		International
53	Participation to a Conference	CEA	Forum International de la Cybersécurité	Lile, France		International
54	Participation to a Conference	JR	SEREN4 Cybersecurity Workshop	Web	WORKSHOP on Cybersecurity, Panel discussion: The perspective of the Cybersecurity Competence Network and future collaboration opportunities	International
55	Participation to a Workshop	BUT	Workshop on Skills Framework	Web	Workshop for other pilots and ENISA on SPARTA Cybersecurity Skills Framework	International

	Type of activities	Main leader	Title	Place	Description of the event	Level
56	Participation to other events	CEA	List General Assembly	Saclay, France		International
57	Communication Campaign	CEA	SPARTA DAY and SPARTA meeting	Brussels, Belgium		International
58	Other	CEA	SPARTA Presentation	Web		International
59	Other	CEA	SPARTA Presentation	Saclay, France		International
60	Participation to other events	CNR	SPARTA Brokerage Event	Web		International
61	Participation to other events	CEA	SPARTA Presentation	Web		International
62	Participation to a Conference	LEO	Cybertech Live	Web		International
63	Participation to other events	CEA	SPARTA Presentation	Web		International
64	Participation to a Conference	CEA	SPARTA Presentation	Web		International
65	Moderation of panel	JR	Cybersecurity in Finance	Web		International

	Type of activities	Main leader	Title	Place	Description of the event	Level
	discussion and participation to a Workshop					
66	Participation to a Workshop	JR	Cyber Security in Österreich 2020: Ein- & Ausblicke für Studierende	Web		International
67	Participation to a Conference	JR	GRAZ SECURITY DAYS FOR INDUSTRY 2019	Graz, Austria		International
68	Participation to a Workshop	JR	Arbeitssitzung der Cyber Security Plattform Austria	Loipersdorf, Austria		International
69	Brokerage event	JR	FORTE und KIRAS Einreichertag (National Security and Defence research programs)	Vienna, Austria		International
70	Participation to a Conference	JR	MILIPOL Paris 2019, Workshop on AI for LEAs	Paris, France		International
71	Brokerage event	JR	SMI2G Meeting 2020	Brussels, Belgium		International
72	Participation to a Conference	JR	KIRAS Fachtagung (National security research program)	Vienna, Austria		International

	Type of activities	Main leader	Title	Place	Description of the event	Level
73	Business meeting	JR	Business meeting with Austrian supplyer of AI plattform, stakeholder from industry (SME) - NDA!	Austria		International
74	Business meeting	JR	Business meeting and lab visit at Austrian university of applied scienece	Austria		International
75	Business meeting	JR	Business meeting with Austrian software project company RISE	Austria		International
76	Participation to a conference	NASK	SECURE 2020 conference	Poland		International
77	Participation to a webinar	INOV, BRN	Gender & Diversity Breakfast Webinars	Web	SPARTA was represented by Sara Ricci, a Post-Doctoral Researcher at the Brno University of Technology, on the INESC HUB *Gender & Diversity Breakfast Webinar* discussions, and addressed the importance of the role-models in gender & diversity in STEM research and technology.	International
78	Participation to a Webinar	CNR	WEBINAR: European Cybersecurity Challenges	Web		
SPARTA Monthly Workshops						
79	Organisation of a Workshop	CEA		France	Held during the SPARTA Kick Off meeting	International

	Type of activities	Main leader	Title	Place	Description of the event	Level
80	Organisation of a Workshop	LEO		Italy	Held during the Cybertech Europe Event	International
81	Organisation of a Workshop	CNR		Italy	Held during Cybersecurity day	International
82	Organisation of a Workshop	UBO		Germany	Held during BDCS	International
83	Organisation of a Workshop	L3C		Lithuania	The objective of the workshop was to disseminate the SPARTA goals and results between national stakeholders and promote international collaboration and networking.	International
84	Organisation of a Workshop	Inria	CominLabs workshop – “Security and Privacy”	Rennes France	The CominLabs is an initiative selected as part of the "Laboratoires d'Excellence" program by the French ministry of research and education. The CominLabs workshop – „Security and Privacy” workshop focused on Cybersecurity including a special track on Sparta.	National
85	Organisation of a Workshop	YWH	-	Madrid, Spain	The workshop was framed in the 6th edition of Mundo Hacker Day.	International
86	Organisation of a Workshop	TEC	Jornada de Trabajo: Pilotos de Ciberseguridad Europeos y el Impacto para España	13ENISE, León, Spain	A SPARTA workshop was organized in Leon (Spain) within the context of the ENISE 2019 conference, and in cooperation with the CONCORDIA and CyberSec4Europe pilots.	National

	Type of activities	Main leader	Title	Place	Description of the event	Level
87	Organisation of a Workshop	CETIC		Brussels, Belgium SPARTA WEEK		International
88	Organisation of a Workshop	LMT, L3CE		Vilnius, Estonia		International
89	Organisation of a Workshop	SPARTA		Brussels, Belgium		International
90	Organisation of a Workshop	CINI		Genova, Italy		International
91	Organisation of a Workshop	CNR		Pisa, Italy		International
92	Organisation of a Workshop	INRIA		Léon, Spain		International
93	Organisation of a Workshop	UTRATU	4th International Baltic Conference on Databases and Information Systems	Tartu, Estonia		International
94	Organisation of a Workshop	L3CE		Virtual		International

	Type of activities	Main leader	Title	Place	Description of the event	Level
95	Organisation of a Workshop	YWH		Virtual		Internacional
96	Organisation of a Workshop	YWH		Virtual		International
97	Organisation of a Workshop	Swiss Core - CNR	European Cybersecurity Challenges	Virtual	https://sparta.eu/events/2020-11-18-webinar-european-cybersecurity-challenges.html	International
98	Organisation of a Workshop	SMILE	How to get privileged access to ground-breaking Cybersecurity innovation and research	Virtual	https://sparta.eu/events/2020-12-09-sparta-workshop-how-to-get-privileged-access-to-groundbreaking-cybersecurity-innovations-and-research.html	International
99	Organisation of a Workshop	INOV	Cybersecurity Challenges for the SMEs - Webinar	Virtual	https://sparta.eu/events/2021-01-18-desafios-de-ciberseguran%C3%A7a-para-pmes-webinar.html	National
100	Organisation of a Workshop	KEMEA	The Greek Cybersecurity Landscape	Virtual	https://sparta.eu/events/2021-01-27-sparta-monthly-workshop-the-greek-cybersecurity-landscape.html	International

Table 3: Update List of Events and Monthly Workshops

*A more detailed report on the SPARTA Monthly Workshops can be found in the deliverable *D8.2 Intermediate results of the Clustering, platforms and ecosystems activities (DEM, PU, M24, VICOM): this deliverable presents the results of all the WP8 monthly workshops until M24.*

5.1.2 Scientific Publications

To date, SPARTA partners have submitted 102 articles that have been accepted for presentation/publication. Accepted papers are listed below:

No.	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
1	Formal Security Verification of Industry 4.0 Applications	Vivek Nigam and Carolyn Talcott	ETFA	http://nigam.info/docs/etfa19.pdf	Cited by 1 (Google Scholar 01, 2021), 77 downloads
2	Fast Keyed-Verification Anonymous Credentials on Standard Smart Cards	Jan Camenisch and Manu Drijvers and Petr Dzurenda and Jan Hajny	ICT Systems Security and Privacy Protection - IFIP SEC 2019	https://eprint.iacr.org/2019/460.pdf	Cited by 3(Google Scholar 01, 2021), 616 downloads
3	A Secure Publish/Subscribe Protocol for Internet of Things	Lukas Malina, Gautam Srivastava, Petr Dzurenda and Jan Hajny	ARES 2019	http://nigam.info/docs/etfa19.pdf	Cited by 27 (Google Scholar 01/2021), ACM: Cited by 16 (ACM 01/2021) 222 Downloads, CORE B
4	Security Risk Management in Cooperative Intelligent Transportation Systems: A Systematic Literature Review	Abasi-amefon O. Affia, Raimundas Matulevičius, Alexander Nolte	27th International Conference on Cooperative Information Systems	https://eprint.iacr.org/2019/460.pdf	Cited by 3 (Springer 01/2021), 942 Downloads CORE A
6	CFI: Control Flow Integrity or Control Flow Interruption?	Paolo Prinetto and Gianluca Roascio	PHISIC 2019 Workshop	10.1109/EWDTS.2019.8884464	Cited by 1 (Google Scholar 01/2021), 202 downloads
7	Experimental analysis of the laser-induced instruction skip fault model	Jean-Max Dutertre, Timothe´ Riom, Olivier Potin, and Jean-Baptiste Rigaud	2019 FDTC workshop	10.1007/978-3-030-35055-0_14	Cited by 1 (Google Scholar 01/2021), 402 downloads
8	Big Data Analytics for Intrusion Detection: An Overview	Luis Dias, Miguel Correia	13th International Conference on Network and System Security	https://www.gsd.inesc-id.pt/~mpc/pubs/Big_Data_Analytics_for_Intrusion_Detection__An_Overview_final.pdf	Cited by 2(Google Scholar 01/2021), NA downloads

No.	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
9	OutGene: Detecting Undefined Network Attacks with Time Stretching and Genetic Zooms	Luís Dias, Hélder Reia, Rui Neves and Miguel Correia	13th International Conference on Network and System Security	https://www.gsd.inesc-id.pt/~mpc/pubs/OutGene___Detecting_Undefined_Attacks_without_Training_Data.pdf	Cited by 1 (Google Scholar 01/2021), 821 downloads CORE B
10	Visual Analytics for Cyber Security Domain: State-of-the-Art and Challenges	R. Damaševičius, J. Toldinas, A. Venčkauskas, S. Grigaliūnas, N. Morkevičius, V. Jukavičius	International Conference on Information and Software Technologies	https://link.springer.com/chapter/10.1007%2F978-3-030-30275-7_20	Cited by 0 (Google Scholar 01/2021), 521 downloads CORE B
11	The feasibility of Deep learning use for adversarial model extraction in the cybersecurity domain	Pawlicki, Choras and Kozik	IDEAL'19	10.1007/978-3-030-33617-2_36	Cited by 0 (Google Scholar 01/2021), 455 downloads CORE C
12	On Computer - Aided Techniques for Supporting Safety and Security Co-Engineering	Vivek Nigam, Antonaneta Kondeva, Carmen Carlan and Harald Ruess	9th IEEE International Workshop on Software Certification (WoSoCer)	http://nigam.info/docs/wosocer02.pdf	Cited by 1 (Google Scholar 01/2021), 46 downloads
13	Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols	Guillaume Celosia, Mathieu Cunche	PoPETs2020 (https://www.petsymposium.org/)	10.2478/popets-2020-0003	Cited by 4 (Google Scholar 01/2021), NA downloads
14	Fingerprinting Bluetooth-Low-Energy Devices Based on the Generic Attribute Profile	Guillaume Celosia, Mathieu Cunche	IoT S&P 2019	https://hal.inria.fr/hal-02359914/document	Cited by 3 (Google Scholar 01/2021), 223 downloads
15	Saving Private Addresses: An Analysis of Privacy Issues in the	Guillaume Celosia, Mathieu Cunche	Mobiquitous 2019	https://hal.inria.fr/hal-02394629/	Cited by 3 (Google Scholar 01/2021), 77 downloads

No.	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
	Bluetooth-Low-Energy Advertising Mechanism				
16	Towards Formal Methods of IoT Application Layer Protocol	Katharina Hofer-Schmitz and Branka Stojanovic	12th CMI Conference 2019: cybersecurity and privacy	https://ieeexplore.ieee.org/abstract/document/8962139/	Cited by 2 (Google Scholar 01/2021), 132 downloads
17	Automated Security Analysis of IoT Software Updates	Nicolas Dejon, Davide Caputo, Luca Verderame, Alessandro Armando and Alessio Merlo	13th WISTP International Conference on Information Security Theory and Practice	https://csec.it/papers/WISTP2019.pdf	Cited by 1 (Google Scholar 01/2021), NA downloads
18	Natural Projection as Partial Model Checking	Costa, G.; Galletta, L.; Degano, P.; Basin, D.; Bodei, C.	Journal of Automated Reasoning	https://arpi.unipi.it/handle/11568/1013170	Cited by 0 (Google Scholar 01/2021), 343 downloads
19	WAF-A-MoLE: An adversarial tool for assessing ML-based WAFs	Luca Demetrio, Gabriele Costa, Andrea Valenza and Giovanni Lagorio	SoftwareX and on ACM Symposium on Applied Computing	https://doi.org/10.1016/j.softx.2019.100367	Cited by 0, (Google Scholar 01/2021), 11 downloads
20	A Survey on Multi-Factor Authentication for Online Banking in the Wild	Federico Sinigaglia, Roberto Carbone, Gabriele Costa, Nicola Zannone	Computers and Security	https://www.researchgate.net/profile/Nicola_Zannone/publication/339076094_A_Survey_on_Multi-Factor_Authentication_for_Online_Banking_in_the_Wild/links/5e5783d1299bf1bdb83e6e6b/A-Survey-on-Multi-Factor-Authentication-for-Online-Banking-in-the-Wild.pdf	Cited by 5, (Google Scholar 01/2021), 29 downloads
21	Building Next Generation Cyber Ranges with CRACK	Enrico Russo, Gabriele Costa, Alessandro Armando	Computers and Security	https://doi.org/10.1016/j.cose.2020.101837	Cited by 2 (Google Scholar 01/2021), 17 downloads
22	Secure Firmware Updates for Constrained IoT	K. Zandberg, K. Schleiser, F. Acosta,	IEEE Access, June 2019	10.1109/ACCESS.2019.2919760	Cited by 6 (Google Scholar 01/2021), 3087 downloads

No.	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
	Devices Using Open Standards: A Reality Check	H. Tschofenig, and E. Baccelli			
23	Cyberphysical Security for the Masses: A Survey of the Internet Protocol Suite for Internet of Things Security	H. Tschofenig, E. Baccelli	IEEE Security & Privacy, October 2019	https://hal.inria.fr/hal-02351892/document	Cited by 2(Google Scholar 01/2021), 786 downloads
24	Requirements for a Lightweight AKE for OSCORE	M. Vucinic, G. Selander, J. Mattsson, D. Garcia	IETF Internet Draft, 2019	https://tools.ietf.org/id/draft-selander-lake-reqs-02.html	No information available yet
25	Advances in Usability of Formal Methods for Code Verification with Frama-C	André Maroneze, Valentin Perrelle, Florent Kirchner	Interactive Workshop on the Industrial Application of Verification and Testing, ETAPS 2019 Workshop (InterAVT 2019)	http://dx.doi.org/10.14279/tuj.eceasst.77.1108	No information available yet
26	Privacy-preserving and yet Robust Collaborative Filtering Recommender as a Service	Qiang Tang	Inscrypt 2019	https://arxiv.org/abs/1910.03846v1	Cited by 11, NA downloads
27	A Privacy-Enhancing Framework for Internet of Things Services	Lukas Malina, Gautam Srivastava, Petr Dzurenda, Jan Hajny and Sara Ricci	13th International Conference on Network and System Security	https://eprint.iacr.org/2019/1471.pdf	Cited by 6 (Google Scholar 01/2021), 940 Downloads, CORE B
28	xMP: Selective Memory Protection for Kernel and User Space	Sergej Proskurin, Marius Momeu, Seyedhamed Ghavamnia, Vasileios P. Kemerlis, and Michalis Polychronakis	IEEE S&P 2020	https://www3.cs.stonybrook.edu /~mikepo/papers/xmp.sp20.pdf	Cited by 6 (Google Scholar 01/2021) 188 downloads

No.	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
29	TSNSCHED: Automated Schedule Generation for Time Sensitive Networking	Aellison Cassimiro T. dos Santos, Ben Schneider and Vivek Nigam	FMCAD	https://www.fortiss.org/fileadmin/user_upload/Veroeffentlichungen/Publikationen/2019_10_FMCAD2019_TSNsched_Santos_Schneider_Nigam.pdf	Cited by 4 (Google Scholar 01/2021), 386 downloads
30	MadDroid: Characterising and Detecting Devious Ad Content for Android Apps	Tianming Liu, Haoyu Wang, Li Li, Xiapu Luo, Feng Dong, Yao Guo, Liu Wang, Tegawendé F. Bissyandé and Jacques Klein	The WebConf 2020	https://arxiv.org/abs/2002.01656	Cited by 6 (Google Scholar 01/2021) 672 downloads
31	Methodology and Feedback about Systematic Cybersecurity Experts Auditing in Belgium	Christophe Ponsard, Jeremy Grandclaudon and Nicolas Point	ICISSP 2020 conference	https://www.cetic.be/Methodology-and-Feedback-about-Systematic-Cybersecurity-Experts-Auditing-in	No information available yet
32	Towards Visual Debugging for Multi-Target Time Series Classification	Udo Schlegel, Eren Cakmak, Hiba Arnout, Mennatallah El-Assady, Daniela Oelke, Daniel A Keim	ACM IUI 2020	https://bib.dbvis.de/publications/view/854	Citated by 0 (Google Scholar 01/2021), 169 downloads
33	Provably Secure Isolation for Interruptible Enclaved Execution on Small Microprocessors	Matteo Busi, Job Noorman, Jo Van Bulck, Letterio Galletta, Pierpaolo Degano, Jan Tobias Mühlberg, Frank Piessens	33rd IEEE Computer Security Foundations Symposium	arXiv:2001.10881v1	Cited by 3 (Research Gate), NA downloads

No.	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
34	Enhancing Security in 6G Visible Light Communications	Simone Soderi	6G Wireless Summit	https://www.researchgate.net/publication/339974971_Enhancing_Security_in_6G_Visible_Light_Communications	Cited by 3 (Research Gate), 353 downloads
35	Achieving Explainability of Intrusion Detection System by Hybrid Oracle-Explainer Approach	Szczepanski, Choras, Pawlicki, Kozik.	IJCNN conference	https://api.semanticscholar.org/CorpusID:221558966	Cited by 2 (Google Scholar 01/2021), NA downloads
36	Machine Learning - the results are not the only thing that matters! What about security, explainability and fairness?	Szczepanski, Choras, Pawlicki, Kozik.	ICCS 2020	https://doi.org/10.1007/978-3-030-50423-6_46	Cited by 4 (Google Scholar 01/2021), 942 downloads
37	On the impact of network data balancing in cybersecurity applications	Pawlicki, Choras, Kozik and Holubowicz	ICCS 2020	https://doi.org/10.1007/978-3-030-50423-6_15	Cited by 0 (Google Scholar 01/2021), 520 downloads
38	Defending Network Intrusion Detection Systems against Adversarial Evasion Attacks	Pawlicki, Choras, Kozik	FGCS (Elsevier)	https://doi.org/10.1016/j.future.2020.04.013	Cited by 4 (Google Scholar 01/2021), 942 downloads
39	Foreshadow-VMM: Feasibility and Network Perspective	Marco Spaziani brunella, Sara Turco, Giuseppe Bianchi, Francesco Quaglia, Nicola Blefari Melazzi		https://www.researchgate.net/publication/334057814_Foreshadow-VMM_Feasibility_and_Network_Perspective	Cited by 0 (Google Scholar 01/2021), 66 downloads
40	Technical Threat Intelligence Analytics:	R. Damasevicus, J. Toldinas, A.	24th International Conference	https://doi.org/10.1109/IEEECONF49502.2020.9141613	Cited by 0 (Google Scholar, 01/2021), 76 downloads

No.	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
	What and How to Visualize for Analytic Process	Venckauskas, S. Grigaliunas, N. Morkevicius	ELECTRONICS 2020 and for publication in the IEEE Conference Proceedings		
41	Towards Formal Methods of IoT Application Layer Protocols	Katharina Hofer-Schmitz, Branka Stojanovi	Proceedings of the 12th CMI conference - Cybersecurity and Privacy (CMI 2019).	DOI: 10.1109/CMI48017.2019.8962139	Cited by 3 (Google Scholar, 01/2021), 132 downloads
42	Disconnection attacks against LoRaWAN 1.0.X ABP devices	Giorgio Bernardinetti, Francesco Mancini, Giuseppe Bianchi	IEEE MetComNet 2020 conference	http://netgroup.uniroma2.it/wp-content/uploads/2021/01/LoRaWAN-ABP-Attacks.pdf	Cited by 0 (Google Scholar, 01/2021), 73 downloads
43	ModelSpeX: Model Specification Using Explainable Artificial Intelligence Methods	Udo Schlegel, Eren Cakmak, and Daniel A. Keim	MLVis 2020 Workshop	https://bib.dbvis.de/uploadedFiles/MLVIS_2020___Model_SpeX__Model_Specification_Using_Explainable_Artificial_Intelligence_Methods.pdf	Cited by 0, Downloaded by NA Impact Score: 2.116 (Eurographics Forum)
44	LITNET-2020: An Annotated Real-World Network Flow Dataset for Network Intrusion	Damasevicius, Robertas; Venckauskas, Algimantas; Grigaliunas, Sarunas; Toldinas, Jevgenijus; Morkevicius, Nerijus; Aleliunas, Tautvydas; Smuikys, Paulius.	Detection Electronics 9, no. 5: 800.	https://www.mdpi.com/2079-9292/9/5/800	No information available yet
45	Borrowing Your Enemy's Arrows: the Case of Code Reuse in Android via Direct Inter-app Code	Jun Gao, Li Li, Pingfan Kong, Tegawendé F. Bissyandé and Jacques Klein	28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the	https://jacquesklein2302.github.io/papers/2020-jun-gao-FSE.pdf	Cited by 1 (Google Scholar, 01/2021), NA downloads

No.	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
	Invocation		Foundations of Software Engineering		
46	Cybersecurity Certification for Agile and Dynamic Software Systems – a Process-Based Approach	Volkmar Lotz	CyberCert 2020	https://conferences.computer.org/eurosp/pdfs/EuroSPW2020-7k9FlVRX4z43j4uE2SeXU0/859700a085/859700a085.pdf	No information available yet
47	Towards Automating Safety and Security Co-Analysis with Patterns	Yuri Dantas, Antoaneta Kondeva, Vivek Nigam	SafeCOMP 2020	https://hal.laas.fr/hal-02931717	No information available yet
48	Less Manual Work for SafetyEngineers: Towards an Automated Safety Reasoning with Safety Patterns	Yuri Dantas, Antoaneta Kondeva, Vivek Nigam	ICLP 2020	https://arxiv.org/abs/2009.10251	Cited by 1 Google Scholar, 01/2021), NA downloads
49	The Results Are Not the only Thing that Matters! What About Security, Explainability and Fairness?	Choras Michal, Pawlicki M., Puchalski D., Kozik R.	Krzhizhanovskaya V.V. et al. (Eds.): Computational Science &#8211; ICCS 2020, LNCS vol. 12140, Springer, Amsterdam, 2020.	https://link.springer.com/chapter/10.1007/978-3-030-50423-6_46	Cited by 4 (Google Scholar, 01/2021), 961 downloads CORE A
50	MobHide: App-level Runtime Data Anonymization on Mobile	Davide Caputo, Luca Verderam, Alessio Merlo	1st International Workshop on Security in Mobile Technologies In Conjunction With ACNS 2020	https://link.springer.com/chapter/10.1007/978-3-030-61638-0_27	Cited by 0 (Google Scholar, 01/2021), 231 downloads CORE B

No.	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
51	Privacy Enhancing Technologies for solving the Privacy-Personalization Paradox	Nesrine Kaaniche, Maryline Laurent and Sana Belguith	Journal of Network and Computer Applications 2020	https://www.sciencedirect.com/science/article/abs/pii/S1084804520302794	Cited by 5 (Google Scholar, 01/2021), NA downloads
52	Backstabber's Knife Collection: A Review of OpenSource Software Supply Chain Attacks	Ohm, M., Plate, H., Sykosch, A., Meier, M. (2020, July)	17th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment	https://arxiv.org/abs/2005.09535	Cited by 5 (Springer 01/2021), NA downloads CORE C
53	Towards Detection of Software Supply Chain Attacks by Forensic Artifacts	Ohm, M., Sykosch, A., Meier, M. (2020, August)	15th International Conference on Availability, Reliability and Security. ACM.	https://www.researchgate.net/publication/342764646_Towards_Detection_of_Software_Supply_Chain_Attacks_by_Forensic_Artifacts	Cited by 3 (Springer 01/2021), NA downloads CORE B
54	*Multiscale Snapshots: Visual Analysis of Temporal Summaries in Dynamic Graphs*	Eren Cakmak, Udo Schlegel, Dominik Jäckle, Daniel Keim, Tobias Schreck	EEE Transactions on Visualization and Computer Graphics (TVCG)	https://arxiv.org/abs/2008.08282	Cited by 0, (Google Scholar, 01/2021), 30 downloadS (early access)
55	*dg2pix: Pixel-Based Visual Analysis of Dynamic Graphs*	Eren Cakmak, Dominik Jäckle, Tobias Schreck, Daniel Keim	VDS at IEEE VIS 2020	https://arxiv.org/abs/2009.07322	No information available yet
56	Towards Incremental Safety and Security8Requirements Co-Certification	Morgagni Andrea, Massonet Philippe, Dupont Sébastien, Grandclaudon Jeremy	CyberCert 2020 workshop	https://conferences.computer.org/eurosp/pdfs/EuroSPW2020-7k9FlVRX4z43j4uE2SeXU0/859700a079/859700a079.pdf	Cited by 0 (Google Scholar, 01, 2021), 33 downloads

No.	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
57	Go With the Flow: Clustering Dynamically-Defined NetFlow Features for Network Intrusion Detection with DYNIDS	Luis Dias, Simão Valente and Miguel Correia	In Proceedings of the 19th IEEE International Symposium on Network Computing and Applications	https://www.gsd.inesc-id.pt/~mpc/pubs/Go_With_the_Flow__Clustering_Dynamically_Defined_NetFlow_Features-final.pdf	Cited by 2 (Google Scholar, 01/2021), NA downloads CORE A
58	Towards Quantum-Enhanced Machine Learning for Network Intrusion Detection	Arnaldo Gouveia and Miguel Correia	In Proceedings of the 19th IEEE International Symposium on Network Computing and Applications	https://www.gsd.inesc-id.pt/~mpc/pubs/Quantum_NIDS_final.pdf	No information available CORE A
59	CryingJackpot: Network Flows and Performance Counters against Cryptojacking.	Gilberto Gomes, Luis Dias and Miguel Correia	In Proceedings of the 19th IEEE International Symposium on Network Computing and Applications (NCA), Nov. 2020.	https://www.gsd.inesc-id.pt/~mpc/pubs/CryingJackpot_final.pdf	No information available CORE A
60	C2BID: Cluster Change-Based Intrusion Detection	Tiago Fernandes, Luis Dias and Miguel Correia	In Proceedings of Trustcom 2020, December 2020.	https://www.gsd.inesc-id.pt/~mpc/pubs/C2BID_final.pdf	No information available CORE A
61	Never Trust Your Victim: Weaponizing Vulnerabilities in Security Scanners	Andrea Valenza, Gabriele Costa, and Alessandro Armando	23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020).	https://www.usenix.org/system/files/raid20-valenza.pdf	No information available yet
62	Challenges in Cyber Security Education	Sara Ricci, Jan Hajny, Edmundas Piesarskas, Simon Parker	CyberEDU Conference	No information available yet	No information available yet
63	Towards Automatic Identification of Typosquatting Attacks in PyPI	Duc Ly Vu, Ivan Pashchenko, Fabio Massacci, Henrik Plate, Antonino Sabetta	WACCO Workshop @ Euro S&P	No information available yet	No information available yet

No.	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
64	Towards Using Source Code Repositories to Identify Software Supply Chain Attacks	Duc Ly Vu, Ivan Pashchenko, Fabio Massacci, Henrik Plate, Antonino Sabetta	CCS 2020	https://www.researchgate.net/publication/345986133_Poster_Towards_Using_Source_Code_Repositories_to_Identify_Software_Supply_Chain_Attacks	Cited by 0 (Google Scholar, 01, 2021), 68 downloads
65	SEkey: A Distributed Hardware-based Key Management System	Matteo Fornero, Nicolò Maunero, Paolo Prinetto, Antonio Varriale	18th IEEE EAST-WEST DESIGN & TEST SYMPOSIUM (EWDTS-2020)	https://ieeexplore.ieee.org/document/9225107	Cited by 0 (Google Scholar, 01, 2021), 32 downloads
66	Hardware-based Capture-the-Flag Challenges	Gianluca Roascio, Paolo Prinetto, Antonio Varriale	18th IEEE EAST-WEST DESIGN & TEST SYMPOSIUM (EWDTS-2020)	https://ieeexplore.ieee.org/abstract/document/9224932	Cited by 0 (Google Scholar, 01, 2021), 35 downloads
67	A FPGA-based Control-Flow Integrity Solution for Securing Bare-Metal Embedded Systems	Nicolò Manueаro (POLITO), Gianluca Roascio (POLITO), Paolo Prinetto (Polito), Antonio Varriale (B5 Labs Ltd.)	IEEE 15th International Conference on Design & Technology of Integrated Systems (DTIS) 2020	https://ieeexplore.ieee.org/document/9081314	Cited by 0 (Google Scholar, 01, 2021), 142 downloads
68	Minimal Virtual Machines on IoT Microcontrollers: The Case of Berkeley Packet Filters with rBPF	K. Zandberg, E. Baccelli	IFIP/IEEE PEMWN 2020	https://arxiv.org/abs/2011.12047	No information available yet
69	Low-Power IoT Communication Security: On the Performance of DTLS and TLS 1.3	G. Restuccia, H.Tschofenig, E. Baccelli,	IFIP/IEEE PEMWN 2020	https://arxiv.org/abs/2011.12035	No information available yet
70	Omega: a Secure Event Ordering Service for the Edge	Cláudio Correia, Luis Rodrigues, Miguel Correia	50th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)	https://www.gsd.inesc-id.pt/~mpc/pubs/Claudio_DSN_camera_ready.pdf	Cited by 1 (Google Scholar, 01, 2021), 72 downloads CORE A

No.	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
71	Deep Learning for Network Intrusion Detection: An Empirical Assessment	Arnaldo Gouveia and Miguel Correia	Advances in Security, Privacy and Trust for Internet-of-Things (IoT) and Cyber-Physical Systems (CPS), 2020	https://www.gsd.inesc-id.pt/~mpc/pubs/DL-book-chapter.pdf	No information available yet
72	Network Intrusion Detection XGBoost(ing)	Arnaldo Gouveia, Miguel Correia	Advances in Security, Privacy and Trust for Internet-of-Things (IoT) and Cyber-Physical Systems (CPS), 2020	https://www.gsd.inesc-id.pt/~mpc/pubs/XGBoost_chapter.pdf	No information available yet
73	A Formal Security Assessment Framework for Cooperative Adaptive Cruise Control	Yuri Gil Dantas (fortiss, Germany), Vivek Nigam (fortiss, Germany), Carolyn Talcott (SRI International, USA)	2020 IEEE Vehicular Networking Conference (VNC)	http://nigam.info/docs/vnc20.pdf	Cited by 0 (Google Scholar), NA downloads
74	An Edge-Fog Secure Self-Authenticable Data Transfer Protocol	Venčkauskas A, Morkevicius N, Jukavičius V, Damaševičius R, Toldinas J, Grigaliūnas Š.	Sensors. 2019; 19(16):3612.	https://www.mdpi.com/1424-8220/19/16/3612#cite https://doi.org/10.3390/s19163612	Cited by 8 (Google Scholar), 1434 downloads
75	Orchestration Security Challenges in the Fog Computing	Šatkauskas N., Venčkauskas A., Morkevičius N., Liutkevičius A.	Information and Software Technologies. ICIST 2020. Communications in Computer and Information Science, vol 1283. Springer, Cham.	https://doi.org/10.1007/978-3-030-59506-7_17	Cited by 0 (Google Scholar), 133 downloads
76	Revisiting the VCCFinder Approach for the Identification of Vulnerability WP5	Timothé Riom, Arthur D. Sawadogo, Kevin Allix, Alexandre Bartel, Tegawendé F. Bissyandé, Naouel	Empirical Software Engineering, journal first, Springer, Accepted for publication on Jan. 22, 2021	No information available yet	CORE A

No.	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
		Moha and Jacques Klein			
77	A First Look at Android Applications in Google Play related to Covid-19 WP5	Jordan Samhi, Kevin Allix, Tegawendé F. Bissyandé, Jacques Klein	Empirical Software Engineering, journal first, Springer, Accepted for publication on Jan. 15, 2021	No information available yet	CORE A
78	On the Impact of Sample Duplication in Machine Learning based Android Malware Detection WP5	Yanjie Zhao, Li Li, Haoyu Wang, Haipeng Cai, Tegawendé F. Bissyandé, Jacques Klein, John Grundy,	ACM Transactions on Software Engineering and Methodology (TOSEM), journal first, ACM, Accepted for publication on Jan. 07, 2021	No information available yet	CORE A
79	Towards an Interpretable Deep Learning Model for Mobile Malware Detection and Family Identification	Giacomo Iadarola, Fabio Martinelli, Francesco, Antonella Santone	Computer & Security, 2021	https://www.sciencedirect.com/science/article/pii/S0167404821000225	No information available yet
80	Detecting Colluding Inter-App Communication in Mobile Environment	Rosangela Casolare, Fabio Martinelli, Francesco Mercaldo, Antonella Santone	International Conference on Information Systems Security and Privacy, *ICISSP 2021*	No information available yet	No information available yet
81	Neural Networks for Driver Behavior Analysis	Fabio Martinelli, Fiammetta Marulli, Francesco Mercaldo, Antonella Santone	Electronics	No information available yet	No information available yet
82	Driver Identification through Formal Methods	Fabio Martinelli, Francesco Mercaldo, Vittoria Nardone, Antonella Santone	IEEE Transactions on Intelligent Transportation Systems	No information available yet	No information available yet

No.	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
83	Call Graph and Model Checking for Fine-Grained Android Malicious Behaviour Detection	Giacomo Iadarola, Fabio Martinelli, Francesco, Antonella Santone	Applied Sciences	https://www.mdpi.com/2076-3417/10/22/7975	Cited by 2 (Google Scholar), NA downloads
84	Detecting Colluding Inter-App Communication in Mobile Environment	Rosangela Casolare, Fabio Martinelli, Francesco Mercaldo, Antonella Santone	Applied Sciences	https://www.mdpi.com/2076-3417/10/23/8351	No information available yet
95	Android Collusion: Detecting Malicious Applications Inter-Communication through SharedPreferences	Rosangela Casolare, Fabio Martinelli, Francesco Mercaldo, Antonella Santone	Information	https://www.mdpi.com/2078-2489/11/6/304	No information available yet
86	Visualizing the outcome of dynamic analysis of Android malware with VizMal	Andrea De Lorenzo, Fabio Martinelli, Eric Medvet, Francesco Mercaldo, Antonella Santone	Journal of Information Security and Applications	https://www.sciencedirect.com/science/article/abs/pii/S2214212619303837	No information available yet
87	Model checking and machine learning techniques for HummingBad mobile malware detection and mitigation	Fabio Martinelli, Francesco Mercaldo, Vittoria Nardone, Antonella Santone, Gigliola Vaglini Model checking and machine learning techniques for	Simulation Modelling Practice and Theory	https://www.semanticscholar.org/paper/Model-checking-and-machine-learning-techniques-for-Martinelli-Mercaldo/df1722134fa85ddf4b124cd034c69a001933dd28	No information available yet
89	VisualDroid: automatic triage and detection of Android repackaged applications	Rosangela Casolare, Carlo De Dominicis, Fabio Martinelli, Francesco Mercaldo, Antonella Santone	15th International Conference on Availability, Reliability and Security (ARES)	https://dl.acm.org/doi/10.1145/3407023.3407074	Cited by 1 (ACM DL, 01/21) 32 downloads CORE B

No.	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
90	Colluding Android Apps Detection via Model Checking	Rosangela Casolare, Fabio Martinelli, Francesco Mercaldo, Vittoria Nardone, Antonella Santone	Web, Artificial Intelligence and Network Applications	https://link.springer.com/chapter/10.1007/978-3-030-44038-1_71	Cited by 1 (Springer, 01/21) 952 downloads CORE B
91	Towards the Use of Generative Adversarial Neural Networks to Attack Online Resources	Lelio Campanile, Mauro Iacono, Fabio Martinelli, Fiammetta Marulli, Michele Mastroianni, Francesco Mercaldo, Antonella Santone	Web, Artificial Intelligence and Network Applications	https://link.springer.com/chapter/10.1007/978-3-030-44038-1_81	Cited by 0 (Google Scholar, 01/21) 930 downloads CORE B
92	Predicting Probability of Default Under IFRS 9 Through Data Mining Techniques	Fabio Martinelli, Francesco Mercaldo, Domenico Raucci, Antonella Santone	Web, Artificial Intelligence and Network Applications	https://link.springer.com/chapter/10.1007/978-3-030-44038-1_87	Cited by 0 (Google Scholar, 01/21) 959 downloads CORE B
93	Code Reordering Obfuscation Technique Detection by Means of Weak Bisimulation	Giuseppe Crincoli, Tiziano Marinaro, Fabio Martinelli, Francesco Mercaldo, Antonella Santone	International Conference on Advanced Information Networking and Applications (AINA-2020)	https://link.springer.com/chapter/10.1007/978-3-030-44041-1_116	Cited by 0 (Google Scholar, 01/21) 936 downloads CORE B
94	Android Run-time Permission Exploitation User Awareness by Means of Formal Methods	Fausto Fasano, Fabio Martinelli, Francesco Mercaldo, Antonella Santone	International Conference on Information Systems Security and Privacy, ICISSP 2020	https://www.scitepress.org/Link.aspx?doi=10.5220/0009372308040814	No information available yet
95	Accidental Sensitive Data Leaks Prevention via Formal Verification	Madalina G. Ciobanu, Fausto Fasano, Fabio Martinelli, Francesco Mercaldo, Antonella Santone	International Conference on Information Systems Security and Privacy, ICISSP 2020	https://www.scitepress.org/Link.aspx?doi=10.5220/0009380608250834	No information available yet
96	Bank Credit Risk Management based on Data Mining Techniques	Fabio Martinelli, Francesco Mercaldo,	International Conference on Information Systems	https://www.scitepress.org/Link.aspx?doi=10.5220/0009371808370843	No information available yet

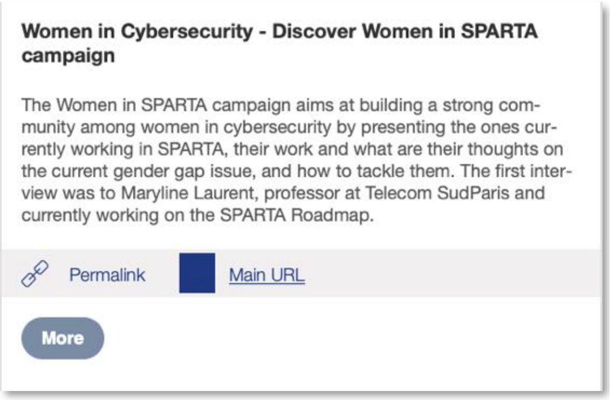
No.	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
		Domenico Raucci, Antonella Santone	Security and Privacy, ICISSP 2020		
97	Malicious Collusion Detection in Mobile Environment by means of Model Checking	Rosangela Casolare, Fabio Martinelli, Francesco Mercaldo, Antonella Santone	International Joint Conference on Neural Networks, IJCNN 2020	https://ieeexplore.ieee.org/abstract/document/9207638	CORE A
98	Enhanced Privacy and Data Protection using Natural Language Processing and Artificial Intelligence	Fabio Martinelli, Fiammetta Marulli, Francesco Mercaldo, Stefano Marrone, Antonella Santone	International Joint Conference on Neural Networks, IJCNN 2020	https://ieeexplore.ieee.org/document/9206801	CORE A
99	Image-based Malware Family Detection: An Assessment between Feature Extraction and Classification Techniques.	Giacomo Iadarola, Fabio Martinelli, Francesco Mercaldo, Antonella Santone	IoTBDS 2020	https://www.scitepress.org/Link.aspx?doi=10.5220/0009817804990506	No information available yet
100	Evaluating Deep Learning Classification Reliability in Android Malware Family Detection.	Giacomo Iadarola, Fabio Martinelli, Francesco Mercaldo, Antonella Santone	2020 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)	https://ieeexplore.ieee.org/document/9307643	No information available yet
101	A Deep-Learning-Based Framework for Supporting Analysis and Detection of Attacks on CAN Buses	Alfredo Cuzzocrea, Francesco Mercaldo, Fabio Martinelli	International *Conference* on Knowledge-Based and Intelligent Information & Engineering Systems KES 2020	https://www.sciencedirect.com/science/article/pii/S1877050920321050	CORE B
102	Machine Learning for Driver Detection through CAN bus	Fabio Martinelli, Francesco Mercaldo, Antonella Santone:	2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)	https://ieeexplore.ieee.org/abstract/document/9129371/	CORE B

Table 4: Updated List of Accepted Papers

5.1.3 Closing the Gender and Diversity Gap Campaigns

5.1.3.1 Women in SPARTA campaign

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. During the second year of the project, the C&D team was able to launch four interviews that can be viewed on the dedicated page of the SPARTA website: "Gender & Diversity"[3]. Besides the website, the interviews were disseminated through SPARTA social media accounts, on the EU's Cybersecurity and Digital Privacy Newsletter (Figure 4), and on the EUvation[4] channels (Figure 5).



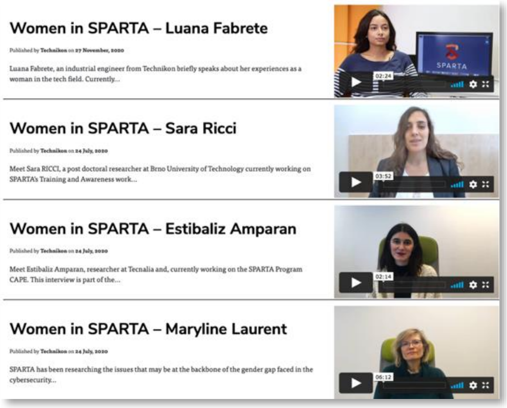
Women in Cybersecurity - Discover Women in SPARTA campaign

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.

Permalink Main URL

More

Figure 4: Women in SPARTA campaign mentioned on the Cybersecurity and Digital Privacy Newsletter



Women in SPARTA – Luana Fabrete

Published by Technikon on 27 November, 2020

Luana Fabrete, an industrial engineer from Technikon briefly speaks about her experiences as a woman in the tech field. Currently...

Women in SPARTA – Sara Ricci

Published by Technikon on 24 July, 2020

Meet Sara RICCI, a post doctoral researcher at Brno University of Technology currently working on SPARTA's Training and Awareness work...

Women in SPARTA – Estibaliz Amparan

Published by Technikon on 24 July, 2020

Meet Estibaliz Amparan, researcher at Tecnalia and, currently working on the SPARTA Program CAPE. This interview is part of the...

Women in SPARTA – Maryline Laurent

Published by Technikon on 24 July, 2020

SPARTA has been researching the issues that may be at the backbone of the gender gap faced in the cybersecurity...

Figure 5: EUvation website page

The second edition of the SPARTA newsletter (Annex 2) was dedicated to the women working in SPARTA, where Tecnalia's cybersecurity team, which is mainly composed by women, was taken as a leading example. Partners helped in the dissemination process through their own channels.

5.1.3.2 "Women4Cyber"

SPARTA is part of the European Cyber Security Organization (ECSO) – Working Group 5: Education, Training, Awareness, Cyber Ranges – and has been actively participating in the Women4Cyber initiative, a non-profit European private foundation to promote, encourage and support the participation of women in the field of cybersecurity. A meeting was held on the 4th of November 2020 to address the next steps and updates on the initiative, such as:

- Women4Cyber Foundation is receiving supporting funding;
- 100 Women in Cybersecurity BOOK;
- Mentorship Program.

SPARTA is committed to support the communication and dissemination activities of Women4Cyber, as well as to work 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.

5.1.3.3 Gender & Diversity Breakfast Webinars

SPARTA was represented by Sara Ricci, a Post-Doctoral Researcher at the Brno University of Technology, on the INESC HUB *Gender & Diversity Breakfast Webinar* discussions, and addressed the importance of the role-models in gender & diversity in STEM research and technology. The

[3] https://www.sparta.eu/diversity/
[4] https://euvation.eu

webinars were held on the 8, 9, and 11th of September and received speakers from several and different areas of knowledge (Annex 3).

5.1.3.4 Engagement with the Media

Rayna Stamboliyska, the Vice President of Governance & Public Affairs at SPARTA partner Yes We Hack, spoke at Jaxenter on the women underrepresentation in the tech sector and mentioned her work in SPARTA. The full interview is available at https://jaxenter.com/women-in-tech-stamboliyska-172586.html

5.1.4 Engagement with the Outermost Regions of Europe

The activities foreseen for the second year of the project in regards with the engagement of Outermost Regions of Europe are partially concluded due to the COVID-19 pandemic restrictions. The table below highlights the achievements made in each action:

Action 1	**Encourage small businesses to adopt cybersecurity measures**
Achievement	Several contacts have been made to different entities in Martinique to foster collaborations, such as the direction of Technopole Martinique, who then forwarded to the Direction du Développement Economique et des Entreprises (2D2E). To date, no collaboration was established, also due to the COVID19 pandemic impact on the natural flow of activities.
Action 2	**Stimulate young people to undertake studies or training at the university level within the area of cybersecurity**
Achievement	The two first actions foreseen for this action proceeded in coordination with the SPARTA **Cybersecurity Training and Awareness Program (WP9)** and were concluded: 1. Define the essentials of computer security that should be present in all computer science curricula. 2. Design new and improve existing curricula for bachelor degrees in computer security based on the Universidad de Las Palmas de Gran Canaria needs. The Universidad de Las Palmas de Gran Canaria courses feature on the SPARTA Cybersecurity Study Programs map: https://www.sparta.eu/study-programs/.
Action 3	**Engage with critical infrastructure operators to stimulate them to adopt state-of-the-art cybersecurity technology**
Achievement	In a collaborative approach, SMILE, a SPARTA partner, proceeded with the cybersecurity risk assessment to Office de L'eau, the water critical infrastructure from La Reúnion, and provided a report that will guide the next steps of this action. One of the considerations made in the report was a cybersecurity training workshop with Office de L'eau employees to raise awareness of cybersecurity and cyber hygiene in the work environment. This will be done during the third year of the project, leveraging on the work that is being developed on WP9 – Cybersecurity Training and Awareness – and bridging with the infrastructure needs highlighted in the report

Table 5: Achievements for the Engagement with the Outermost Regions of Europe

Note: Both the Universidad de Las Palmas de Gran Canaria, and Office de l'eau are now part of the Associates Program.

5.1.5 Contribution of partners to C&D activities

The strategy deployed on the D12.3 to maximize partners' contribution through their direct participation in the production of contents to be shared on SPARTA social media accounts and the website has shown to be efficient, keeping the audiences updated and informed about several aspects related to the SPARTA project and cybersecurity field. This strategy will endure until the end of the project, to guide the contribution of partners to communication and dissemination activities.
During the second year of the project, and although the COVID-19 have had great impact on all the activities planned, partners conducted several activities to promote awareness of and involvement with the SPARTA project, thus acting accordingly to what was proposed in D.12.1.

5.2 Monitoring Communication and Dissemination Instruments

5.2.1 SPARTA website

Partners contribution to ensure diversity, periodicity and relevance of publications on the SPARTA website resulted on a growth of the number of unique visitors per month. Here we present the number of visitors from Jan 2020 (as a reference to the end of the first year) to January 2021:

Jan 2020	Mar 2020	Apr 2020	May 2020	Jun 2020	Jul 2020	Aug 2020	Sep 2020	Oct 2020	Nov 2020	Dec 2020	Jan 2021
1351	2886	2794	3205	3257	3550	3741	3931	4739	4200	1602	1188 (until the 26th Jan)

From 23rd of November, the metrics used to count the numbers are different as the SPARTA webserver. Thus, comparisons are not meaningful and difficult to draw between, before, and after this change.

5.2.2 SPARTA social media

The C&D strategy adopted for the SPARTA social media accounts has contributed to a growth on the project's visibility, as it has been able to attract 1105 followers on Twitter, 442 on LinkedIn, and 195 on Instagram, and create a more consistent and engaged audience. On LinkedIn, the SPARTA Audience is generally interested in STEM areas, being that Research, Information Technology, and Government Administration are the type of industries that the audience mainly comes from – Figure 7.

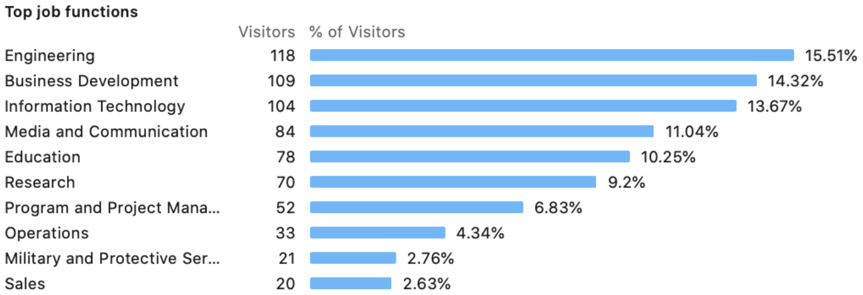


Figure 6: Top Job Functions of SPARTA Audiences on LinkedIn

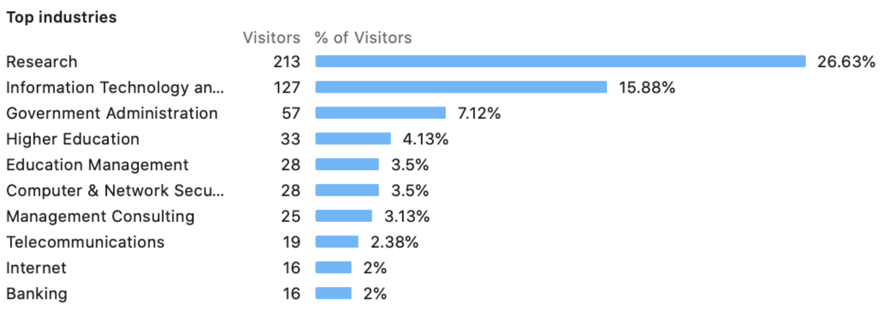


Figure 7: Top Industries of SPARTA Audiences on LinkedIn

On Instagram, the SPARTA Audience is diverse in age, with followers mainly between 18 and 64, and less diverse in gender being that 66% of our audience is male – Figure 8. This gap will be addressed during the third year of the project, aiming to achieve a more diverse audience in terms of gender.

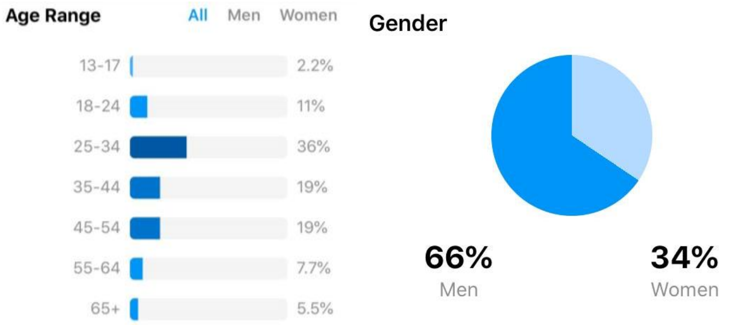


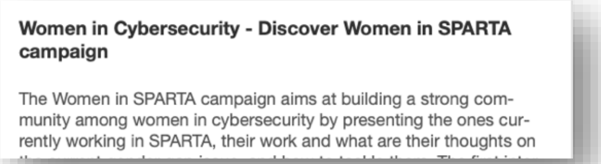
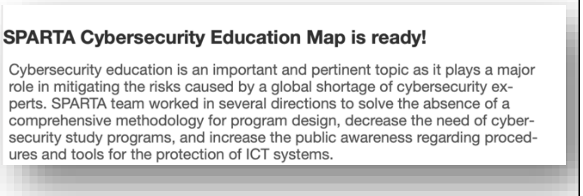
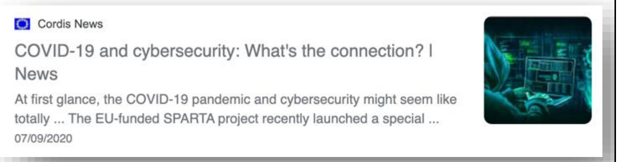
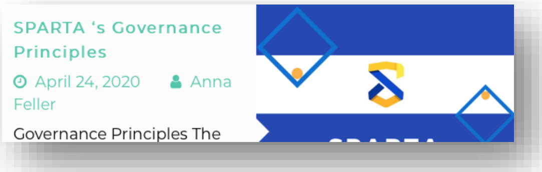
Figure 8: Age and Gender of SPARTA Audience on Instagram

The audience analytics information is not available as Twitter has removed this option since the end of January 2020 - https://www.socialmediatoday.com/news/twitter-is-removing-the-audience-insights-element-from-twitter-analytics/569982/ - making it impossible to evaluate the gender gap among SPARTA audience on Twitter. Nevertheless, the C&D team has been acting towards a more inclusive approach on this platform, as well as actively interacting with posts related to gender issues on cybersecurity and women in cybersecurity. Annex 1 summarizes SPARTA activities on the Twitter social media network.

These networks have been of utmost importance to ensure SPARTA visibility and to communicate projects' main messages, fostering conversations, and raising awareness on cybersecurity and its challenges. Ever since the implementation of restrictions imposed by the COVID19 pandemic, such as to cease all the grand events, the social media networks have served as the primary channel to keep audiences engaged with the project.

5.2.3 Media Relations

During the period M12 – M24, the SPARTA project has gained more visibility and presence on different media platforms. The C&D team has been interacting with the editor of the EU's Cybersecurity & Digital Privacy Newsletter to promote regular publications about the project in this newsletter. Table 5 highlights some of SPARTA presence in the media relative to the second year of the project, with the respective links to publication:

SPARTA on Media Channels	
https://ec.europa.eu/newsroom/index.cfm?service_id=364 Wednesday 18 Nov, 2020 | PROJECTS STORY **T-SHARK: Full-spectrum cybersecurity awareness** SPARTA SPARTA Published by: Digital Single Market Published in: Cybersecurity and digital privacy newsletter	https://ec.europa.eu/information_society/newsroom/cf/dae/newsletter-specific-archive.cfm?get=1&serviceId=364&lang=default&page=2  **Women in Cybersecurity - Discover Women in SPARTA campaign** 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
https://ec.europa.eu/newsroom/index.cfm?service_id=364  **SPARTA Cybersecurity Education Map is ready!** Cybersecurity education is an important and pertinent topic as it plays a major role in mitigating the risks caused by a global shortage of cybersecurity experts. SPARTA team worked in several directions to solve the absence of a comprehensive methodology for program design, decrease the need of cybersecurity study programs, and increase the public awareness regarding procedures and tools for the protection of ICT systems.	https://ec.europa.eu/information_society/newsroom/cf/dae/redirection.cfm?item_id=679353&newsletter=364 **SPARTA H2020 Project podcast: Cyber Security in the EU** In the fifth episode of the SPARTA series, we can hear Ralf Lindner, Head of the Competence Center Policy and Society at Fraunhofer in Germany
https://www.cesnet.cz/projects/special-projects-for-advanced-research-and-technology-in-europe-sparta/?lang=en cesnet About Us Services Research Events Contacts CS > Projects > Special projects for advanced research and technology in Europe (SPARTA) **Special projects for advanced research and technology in Europe (SPARTA)**	https://www.lavanguardia.com/vida/20190708/463351590653/indra-trabaja-en-el-proyecto-europeo-sparta-para-impulsar-soluciones-de-ciberseguridad.html **Indra trabaja en el proyecto europeo Sparta para impulsar soluciones de ciberseguridad** • Indra trabaja dentro del programa de investigación T-Shark, que forma parte del proyecto europeo Sparta, para dotar a la Unión Europea (UE) de capacidades de adquisición de ciberconsciencia situacional con las que "monitorizar, detectar y responder de forma rápida a cualquier amenaza, protegiendo así la economía digital y los derechos de sus ciudadanos en el ciberespacio".
https://cincodias.elpais.com/cincodias/2019/07/05/companias/1562350963_943121.html SEGURIDAD DIGITAL **Indra dotará a la UE de tecnología para responder rápido a ciberataques** MARIMAR JIMÉNEZ • Su solución permitirá monitorizar el ciberespacio para entender qué ocurre en cada momento	https://cordis.europa.eu/article/id/422050-covid-19-and-cybersecurity-what-s-the-connection  Cordis News COVID-19 and cybersecurity: What's the connection? | News At first glance, the COVID-19 pandemic and cybersecurity might seem like totally ... The EU-funded SPARTA project recently launched a special ... 07/09/2020
https://www.ssi.gouv.fr/actualite/sparta-a-cybersecurity-competence-network-to-coordinate-research-innovation-and-training-	https://cybercompetencenetwork.eu/sparta-s-governance-principles/  SPARTA 's Governance Principles April 24, 2020 Anna Feller Governance Principles The

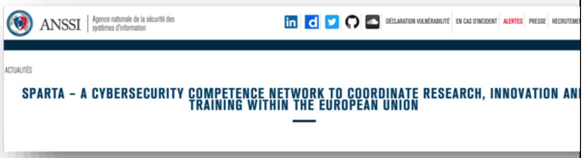
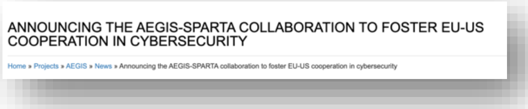
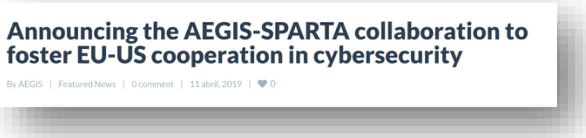
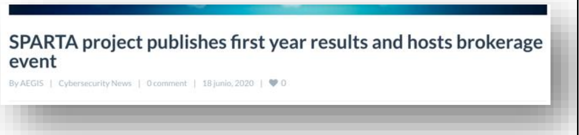
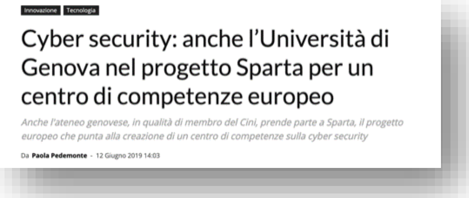
SPARTA on Media Channels	
within-the-european-union/  ANSSI | Agence nationale de la sécurité des systèmes d'information DÉCLARATION VULNÉRABILITÉ EN CAS D'INCIDENT ALERTES PRESSE RECRUTEME ACTUALITÉS SPARTA – A CYBERSECURITY COMPETENCE NETWORK TO COORDINATE RESEARCH, INNOVATION AN TRAINING WITHIN THE EUROPEAN UNION	
https://www.cyberwatching.eu/projects/932/aegis/news-events/announcing-aegis-sparta-collaboration-foster-eu-us-cooperation-cybersecurity  ANNOUNCING THE AEGIS-SPARTA COLLABORATION TO FOSTER EU-US COOPERATION IN CYBERSECURITY Home » Projects » AEGIS » News » Announcing the AEGIS-SPARTA collaboration to foster EU-US cooperation in cybersecurity	https://aegis-project.org/aegis-sparta-h2020-cybersecurity-collaboration/  Announcing the AEGIS-SPARTA collaboration to foster EU-US cooperation in cybersecurity By AEGIS | Featured News | 0 comment | 11 abril, 2019 | ♥ 0
https://aegis-project.org/tag/sparta/  SPARTA project publishes first year results and hosts brokerage event By AEGIS | Cybersecurity News | 0 comment | 18 junio, 2020 | ♥ 0	https://liguria.bizjournal.it/2019/06/cyber-security-anche-luniversita-di-genova-nel-progetto-sparta-per-un-centro-di-competenze-europeo/  Innovazione Tecnologia Cyber security: anche l'Università di Genova nel progetto Sparta per un centro di competenze europeo *Anche l'ateneo genovese, in qualità di membro del Cini, prende parte a Sparta, il progetto europeo che punta alla creazione di un centro di competenze sulla cyber security* Da **Paola Pedemonte** - 12 Giugno 2019 14:03
https://www.senternetwork.eu/everything-is-connected-new-arenas-of-collaboration-sparta-and-eu-hybnet-empowering-a-pan-european-network-to-counter-hybrid-threats/ Everything is connected – New arenas of collaboration SPARTA and EU-HYBNET (Empowering a Pan-European Network to Counter Hybrid Threats)	https://www.senternetwork.eu/cyber-competence-development-ecosystem-started-by-sparta-and-further-explored-by-rewire/ Cyber competence development ecosystem started by SPARTA and further explored by REWIRE

Table 5: SPARTA on Media Channels

5.2.4 Podcasts

The five podcasts launched by Technikon are available on the dedicated SPARTA website page: https://sparta.eu/podcasts/, and are being disseminated on SPARTA social media networks.

- Ep.1: What is SPARTA
- Ep.2: European government and private business preparedness for cyber-attacks
- Ep.3: Responsible Innovation
- Ep.4: Reforming Cybersecurity in the EU through SPARTA project
- Ep.5: Everyone Matters

A three-podcast series entitled "Where Pandemic Meets Cybersecurity" was launched during the outbreak of the COVID-19 pandemic to address how the pandemic impacted partners work and what similarities exist between global pandemic and cyber-attacks. This podcast series was acknowledged[5] at CORDIS and had a good outreach on social media and EUvation. The Greek magazine Koutipandoras has also published[6] a news related to this podcast series.

5.2.5 Videos

During the second year of the project, Technikon produced the video “SPARTA H2020 project: United against cybercrime in Europe”[7], and the C&D team disseminated it on social media.
Other videos are the interviews made within the Women in SPARTA campaign context, published on several platforms as described in section 5.1.2: Closing the Gender Gap.
As acknowledged in deliverable 12.3, videos have shown to be the publications on social media with higher engagement rates.

5.2.6 Internal Communication Instruments

5.2.6.1 Bi-monthly Newsletter

The creation of a bi-monthly newsletter was established in deliverable 12.3 to raise awareness on what is happening within each WP and to enhance the sense of community. The C&D team was able to launch 3 editions of the Newsletter with the inputs provided by each WP leader on their work, achievements, and the latest news. The newsletters were delivered by e-mail to all partners.

SPARTA NEWS
WHERE KNOWLEDGE COMES ACROSS
WELCOME
SPARTA NEWS
WHERE KNOWLEDGE COMES ACROSS
INDEX
SPARTA NEWS
WHERE KNOWLEDGE COMES ACROSS
SPARTA GOVERNANCE PRINCIPLES

Figure 9: Bi-monthly Newsletter

Although partners’ demonstrations of interest in the Newsletter, the editorial workflow proved to require more efforts than expected to fully deliver those communication instruments. It has thus been decided that the internal Newsletter would be replaced by more targeted news sent through the project mailing list, also allowing for more currency.

5.2.6.2 Stackfield

Stackfield was deployed to facilitate internal communication, collaboration among partners, sharing tasks and documents in dedicated rooms to each WP, to simplify the exchange of ideas and practical information. In the timeframe between the deployment of the tool until M24, partners did not use the tool as expected. One of the differentiating features of Stackfield was its client-side encryption feature, preventing the server from seeing the data shared. However, it has not been possible to adapt this tool to the way SPARTA runs in spite of the onboarding actions taken. The process of getting traction has not been deemed satisfactory and it has been decided to move to another

[5] https://cordis.europa.eu/article/id/422050-covid-19-and-cybersecurity-what-s-the-connection
[6] https://www.koutipandoras.gr/article/ti-koino-ehoyn-i-pandimia-tis-covid-19-kai-i-asfaleia-ston-kybernohoro
[7] https://vimeo.com/391466533

platform for the rest of the project. This new platform, NextCloud, will be self-hosted by TNK and will be soon deployed for all the SPARTA partners. It should be more familiar for the users and present more useful functionalities and thus having hopefully a bit more traction. The self-hosting should also provide us a greater room for manoeuvre in its deployment, usage and improvement.

5.2.7 Review Recommendations

Accordingly to the recommendations made to WP12 during the M18 review, the C&D team adopted measures to re-direct efforts from “branding” to “information and engagement” in line with the strategy planned for the Communication & Dissemination activity on deliverable 12.3:

- Mechanisms have been established to collect results and achievements from the programs and activities to disseminate through our several channels (Newsletter, Website, and social media accounts) and other media channels (e.g., Cybersecurity and Digital Privacy Newsletter).
- A calendar was created to collect, each month from a different partner, a set of contents, ensuring diversity and outreach of publications.
- Recommendations made to WP12 during the M21 review are related to the promotion of SPARTA results, claiming for a more incisive approach. The use of advertisements, as planned in this deliverable, was chosen to respond to this recommendation.

5.3 Second-year general evaluation

The novelty of the COVID-19 pandemic caused several impacts on the implementation of the C&D activities planned for the second year of the project, challenging the achievement of the objectives set in deliverable 12.1 and deliverable 12.3.

Nevertheless, activities were re-designed and implemented as we learn how to deal with the pandemic impacts and constraints. It was then possible to achieve communication objectives and not to compromise the SPARTA expected results.

The use of platforms for online meetings and social media networks have shown to be efficient tools to replace face-to-face meetings, events, and communication materials. The participation axis heavily relied on these tools to reach higher levels of audience engagement with the project.

The diversity of actors inherent to the SPARTA pilot has shown, once more, that it enhances the possibility of outreach to a broader set of audiences across geographies, only this time online.

During the second year of the project, SPARTA reached higher levels of (1) attendance on SPARTA (online) events, received (2) contacts from media (e.g., Cybersecurity and Digital Privacy) and several (3) demonstrations of interest through the Friends and Associates programs.

The gender and diversity dimension of the project has been enhanced during this period, allowing for more incisive actions and collaborations. The gender gap of SPARTA social media accounts, namely on Instagram, as well as at the SPARTA events is significant. Similar to the previous year, this is still a factor to be taken into account and to carefully address in the third year of the project.

Chapter 6 Summary and Conclusion

As a result of the evaluation made to the activities developed during the second year of the project, some updates have been made to Deliverable 12.3 as to ensure that the objectives proposed in the initial Communication and Dissemination plan are effectively and efficiently met. Changes were made to leverage the communication among SPARTA partners and to maximize the activities planned within the three axes (Awareness, Participation and Action).
The major changes are summarized as follows:

- **Official SPARTA Website:** The website is continuously under major changes to ensure that visitors always find updated and relevant information on the project, and to facilitate the storage and sharing of public information. SPARTA website is now more complete, organized, and dynamic, as it provides information about SPARTA, its' challenges, structure, and partners on a single page, its results are stored and organized, there is dedicated domains to the Training and Awareness program, and to the Gender and Diversity dimensions of SARTA. A "News & Events" section features the frontpage to provide visitors with the latest news, activities, and achievements related to the project., and the JCCI is now included on the website.

- **Internal Communication:**
  - **Stackfield**, a tool that allows easier collaboration between partners, will not be used during the third year of the project as it has not got the expected traction among SPARTA partners. Instead, ***NextCloud*** was chosen to accomplish these objectives and is currently under a testing process.
  - **The bi-monthly internal Newsletter** will not have more editions during the third year of the project. Instead, the C&D team will deliver the news published on the SPARTA website to the partners through the dedicated e-mail project.consortium@internal.sparta.eu

- **Social Media Management:**
  - **Advertisements** will take place during the third year of the project as they are proven to effectively and efficiently deliver messages to targeted audiences and assure the outreach of publications to many people. The C&D team will select the messages related to the main results of the SPARTA project and SPARTA organized events to advertise on social media accounts.

  - **Social media content management tool: Hootsuite**, a social media content management tool, was selected to coordinate and manage all publications efficiently, allowing for streamlined teamwork to organize, schedule, and publish content effortlessly to all SPARTA social media accounts.

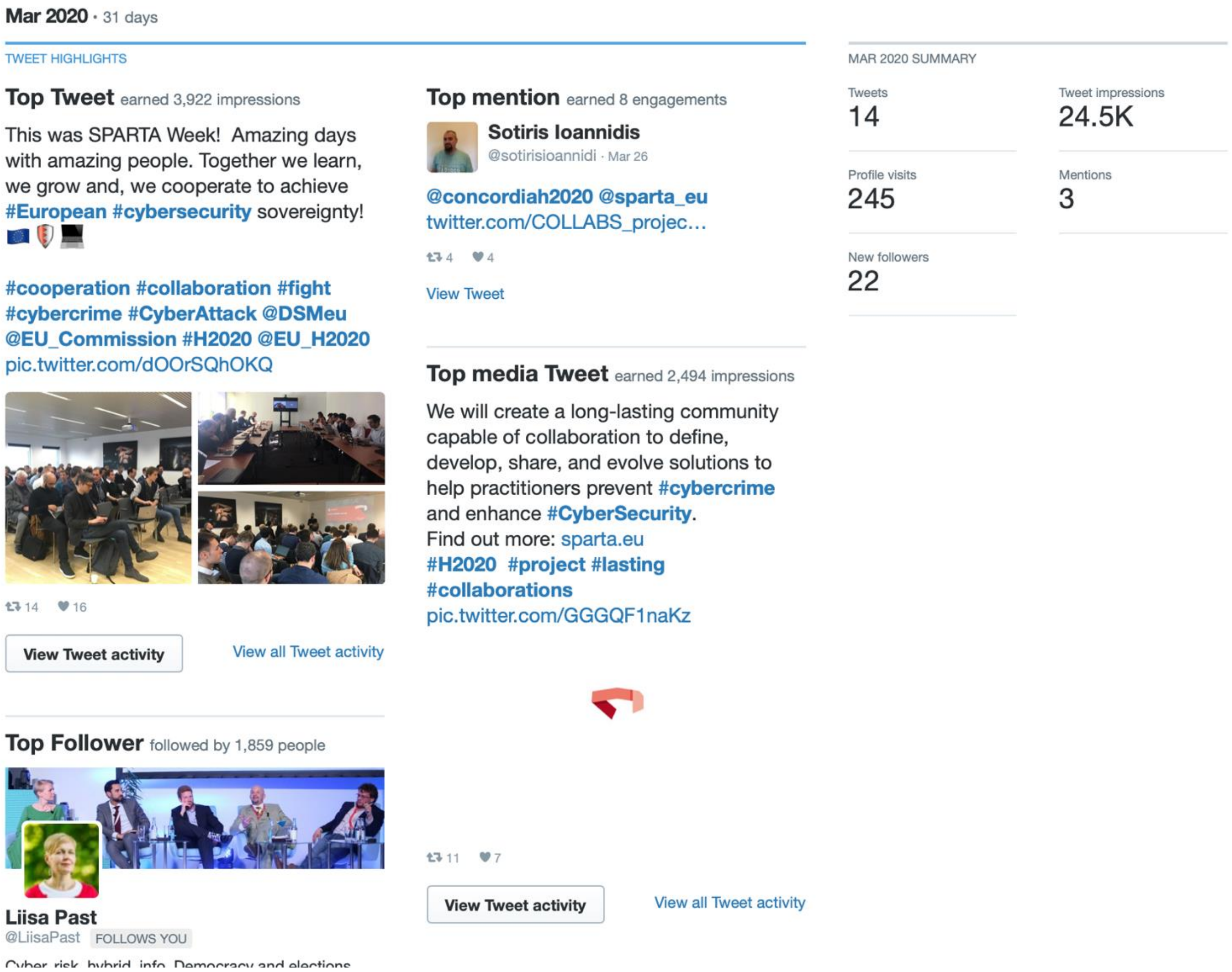
- **Gender and diversity**: Tasks 12.4 and 12.5, related to the promotion of awareness and practices on diversity and inclusion in cybersecurity are also addressed in this deliverable, regarding SPARTA coordinated efforts.

SPARTA Communication and Dissemination plan provides a strategic basis for the development of successful C&D activities. The following year will have stronger attention to the **Action axis** as to promote the engagement of SPARTA stakeholders with the project and with cybersecurity challenges.

Chapter 7 List of Abbreviations

Abbreviation	Translation
C&D	Communication and Dissemination
OR	Outermost Regions of Europe
CCN	Cyber Competence Network

Annex 1 – Twitter Analytics



Mar 2020 · 31 days

TWEET HIGHLIGHTS

Top Tweet earned 3,922 impressions

This was SPARTA Week! Amazing days with amazing people. Together we learn, we grow and, we cooperate to achieve #European #cybersecurity sovereignty! 🇪🇺🛡💻

#cooperation #collaboration #fight #cybercrime #CyberAttack @DSMeu @EU_Commission #H2020 @EU_H2020 pic.twitter.com/dOOrSQhOKQ

14 16

Top Follower followed by 1,859 people

Liisa Past
@LiisaPast FOLLOWS YOU

Cyber, risk, hybrid, info, Democracy and elections

Top mention earned 8 engagements

Sotiris Ioannidis
@sotirisioannidi · Mar 26

@concordiah2020 @sparta_eu twitter.com/COLLABS_projec…

4 4

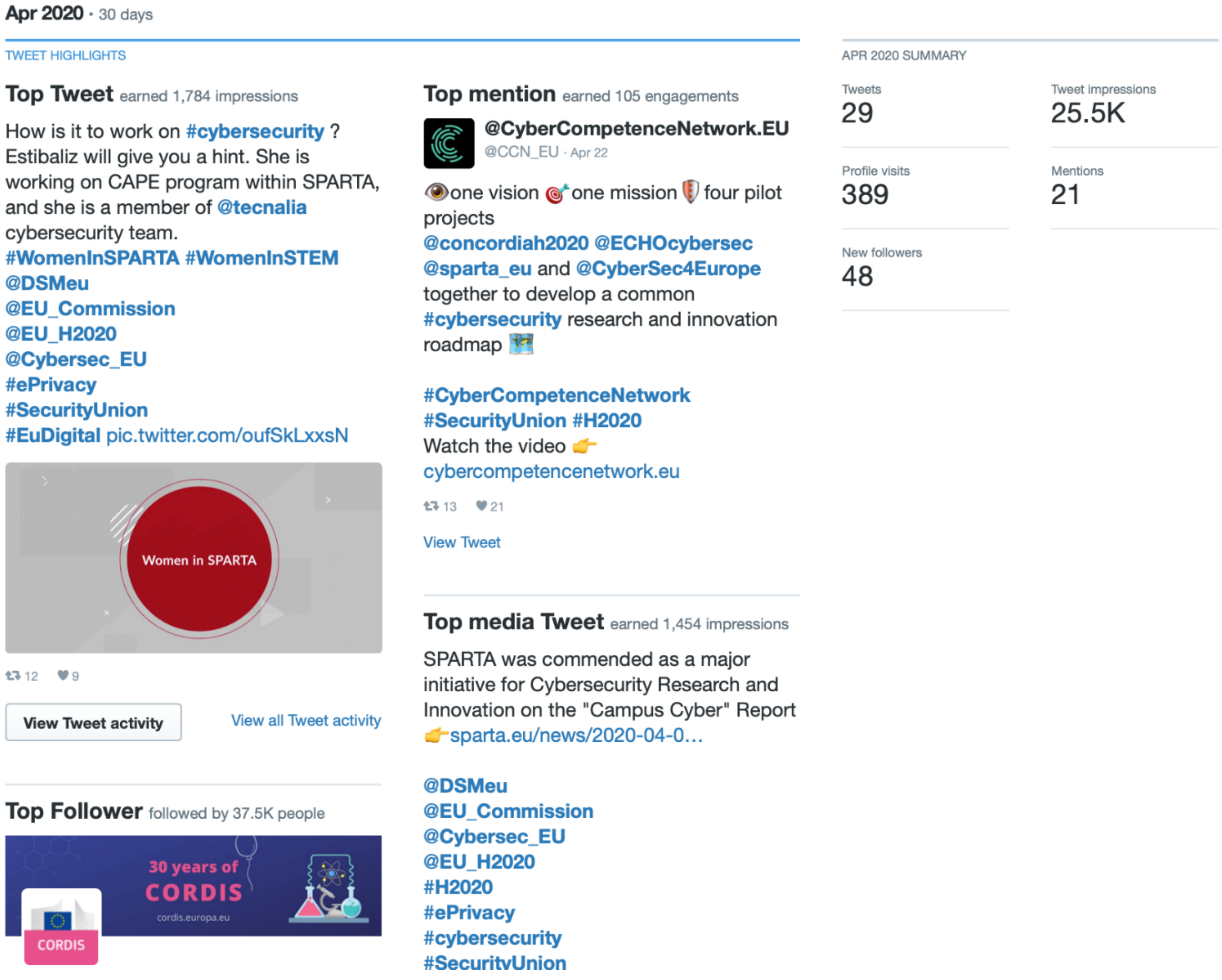
Top media Tweet earned 2,494 impressions

We will create a long-lasting community capable of collaboration to define, develop, share, and evolve solutions to help practitioners prevent #cybercrime and enhance #CyberSecurity.
Find out more: sparta.eu
#H2020 #project #lasting #collaborations
pic.twitter.com/GGGQF1naKz

11 7

MAR 2020 SUMMARY

Tweets 14	Tweet impressions 24.5K
Profile visits 245	Mentions 3
New followers 22	



Apr 2020 · 30 days

TWEET HIGHLIGHTS

Top Tweet earned 1,784 impressions

How is it to work on #cybersecurity ? Estibaliz will give you a hint. She is working on CAPE program within SPARTA, and she is a member of @tecnalia cybersecurity team. #WomenInSPARTA #WomenInSTEM @DSMeu @EU_Commission @EU_H2020 @Cybersec_EU #ePrivacy #SecurityUnion #EuDigital pic.twitter.com/oufSkLxxsN

12 ♥ 9

View Tweet activity

View all Tweet activity

Top Follower followed by 37.5K people

Top mention earned 105 engagements

@CyberCompetenceNetwork.EU
@CCN_EU · Apr 22

👁️one vision 🎯one mission 🛡️four pilot projects @concordiah2020 @ECHOcybersec @sparta_eu and @CyberSec4Europe together to develop a common #cybersecurity research and innovation roadmap 🗺️

#CyberCompetenceNetwork #SecurityUnion #H2020 Watch the video 👉 cybercompetencenetwork.eu

13 ♥ 21

View Tweet

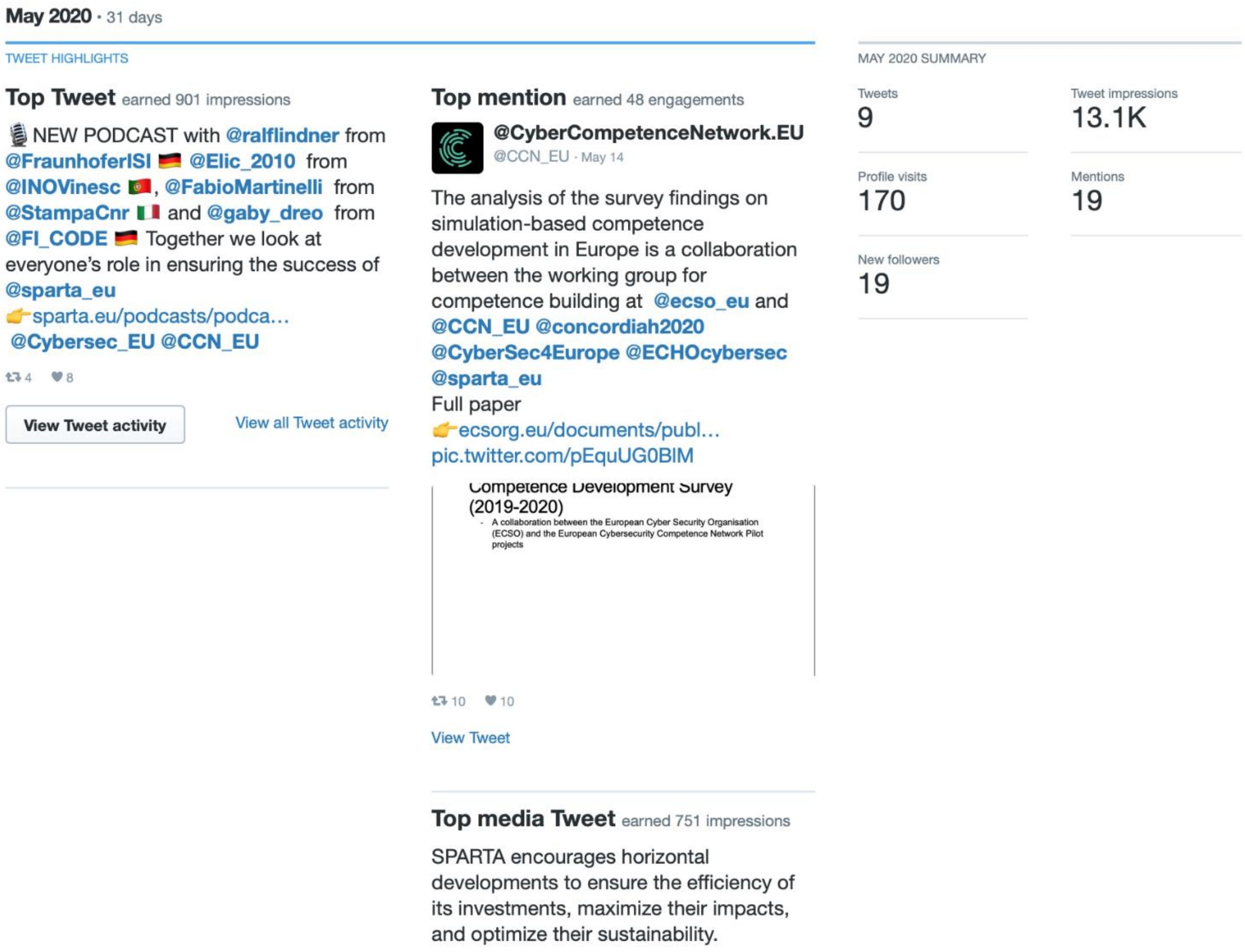
Top media Tweet earned 1,454 impressions

SPARTA was commended as a major initiative for Cybersecurity Research and Innovation on the "Campus Cyber" Report 👉sparta.eu/news/2020-04-0…

@DSMeu @EU_Commission @Cybersec_EU @EU_H2020 #H2020 #ePrivacy #cybersecurity #SecurityUnion

APR 2020 SUMMARY

Tweets	Tweet impressions
29	25.5K
Profile visits	**Mentions**
389	21
New followers	
48	



May 2020 · 31 days

TWEET HIGHLIGHTS

Top Tweet earned 901 impressions

🎙️ NEW PODCAST with **@ralflindner** from **@FraunhoferISI** 🇩🇪 **@Elic_2010** from **@INOVinesc** 🇵🇹, **@FabioMartinelli** from **@StampaCnr** 🇮🇹 and **@gaby_dreo** from **@FI_CODE** 🇩🇪 Together we look at everyone's role in ensuring the success of **@sparta_eu**
👉sparta.eu/podcasts/podca…
@Cybersec_EU @CCN_EU

4 ♥ 8

View Tweet activity

View all Tweet activity

Top mention earned 48 engagements

@CyberCompetenceNetwork.EU
@CCN_EU · May 14

The analysis of the survey findings on simulation-based competence development in Europe is a collaboration between the working group for competence building at **@ecso_eu** and **@CCN_EU @concordiah2020 @CyberSec4Europe @ECHOcybersec @sparta_eu**
Full paper
👉ecsorg.eu/documents/publ…
pic.twitter.com/pEquUG0BIM

Competence Development Survey (2019-2020)
- A collaboration between the European Cyber Security Organisation (ECSO) and the European Cybersecurity Competence Network Pilot projects

10 ♥ 10

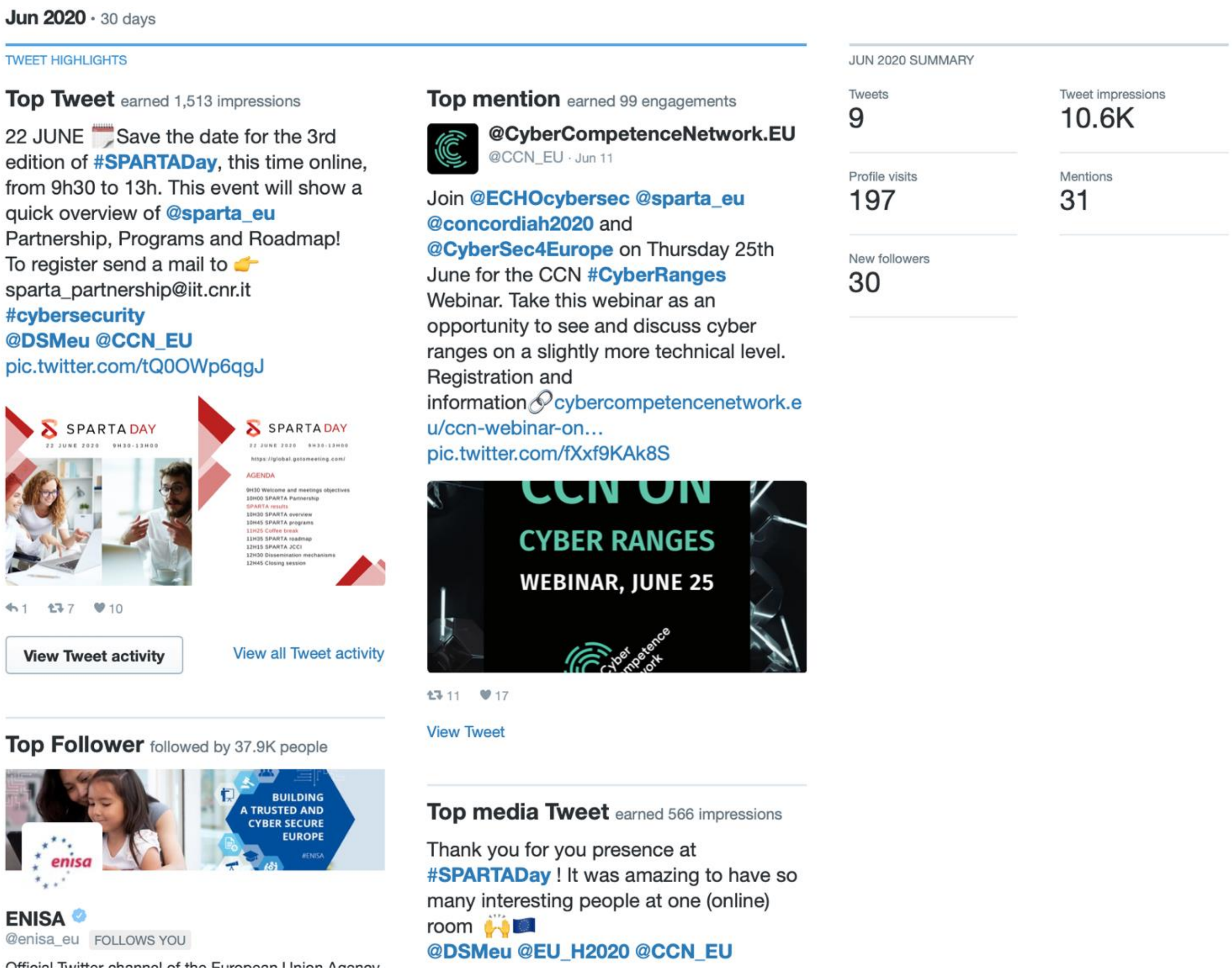
View Tweet

Top media Tweet earned 751 impressions

SPARTA encourages horizontal developments to ensure the efficiency of its investments, maximize their impacts, and optimize their sustainability.

MAY 2020 SUMMARY

Tweets	Tweet impressions
9	13.1K
Profile visits	**Mentions**
170	19
New followers	
19	



Jun 2020 · 30 days

TWEET HIGHLIGHTS

Top Tweet earned 1,513 impressions

22 JUNE 📅Save the date for the 3rd edition of **#SPARTADay**, this time online, from 9h30 to 13h. This event will show a quick overview of **@sparta_eu** Partnership, Programs and Roadmap! To register send a mail to 👉 sparta_partnership@iit.cnr.it **#cybersecurity** **@DSMeu @CCN_EU** pic.twitter.com/tQ0OWp6qgJ

↩ 1 ⟲ 7 ♥ 10

Top Follower followed by 37.9K people

ENISA
@enisa_eu FOLLOWS YOU
Official Twitter channel of the European Union Agency

Top mention earned 99 engagements

@CyberCompetenceNetwork.EU
@CCN_EU · Jun 11

Join **@ECHOcybersec @sparta_eu @concordiah2020** and **@CyberSec4Europe** on Thursday 25th June for the CCN **#CyberRanges** Webinar. Take this webinar as an opportunity to see and discuss cyber ranges on a slightly more technical level. Registration and information🔗cybercompetencenetwork.eu/ccn-webinar-on… pic.twitter.com/fXxf9KAk8S

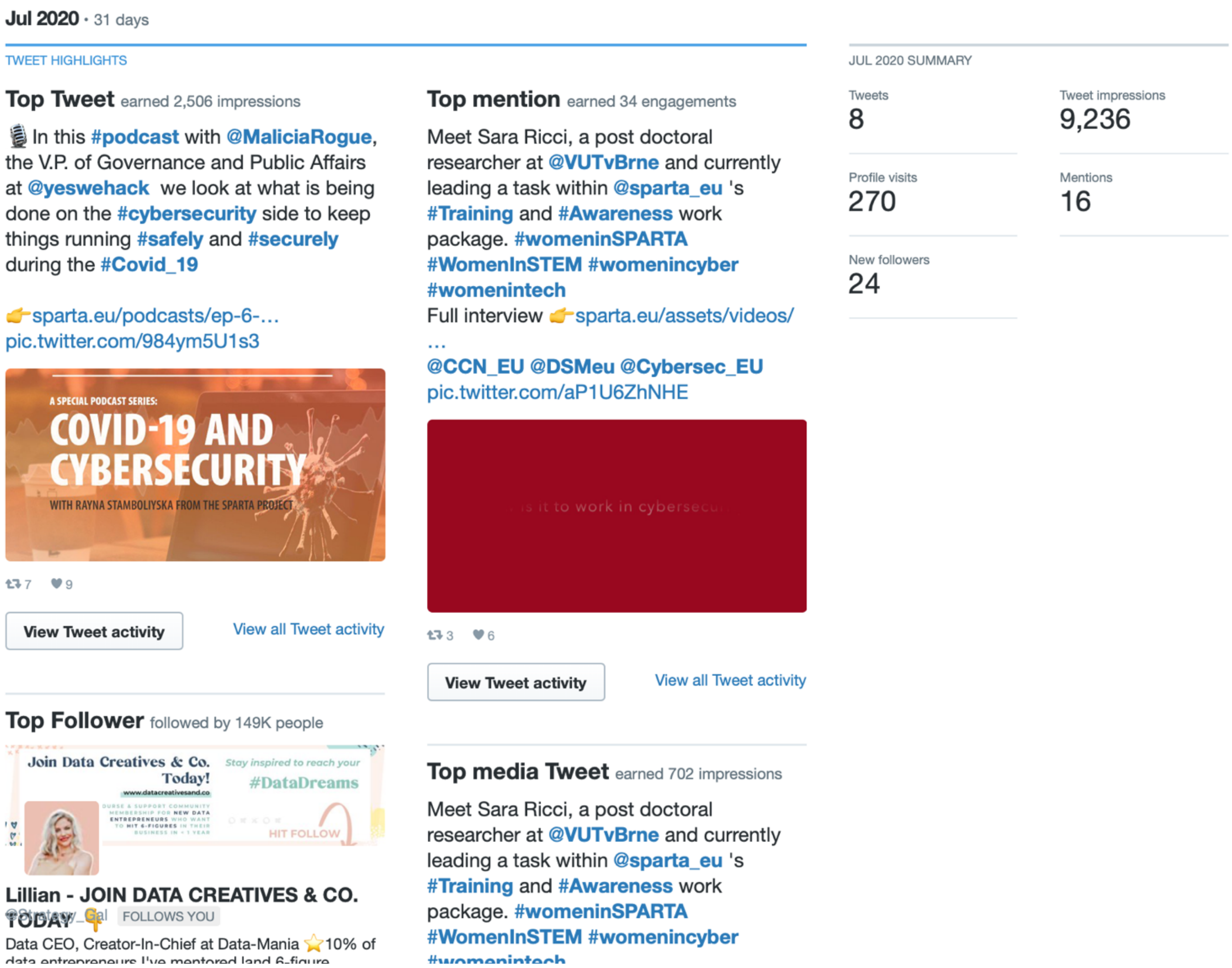
⟲ 11 ♥ 17

Top media Tweet earned 566 impressions

Thank you for you presence at **#SPARTADay** ! It was amazing to have so many interesting people at one (online) room 🙌🇪🇺 **@DSMeu @EU_H2020 @CCN_EU**

JUN 2020 SUMMARY

Tweets 9	Tweet impressions 10.6K
Profile visits 197	Mentions 31
New followers 30	



Jul 2020 · 31 days

TWEET HIGHLIGHTS

Top Tweet earned 2,506 impressions

🎙️ In this #podcast with @MaliciaRogue, the V.P. of Governance and Public Affairs at @yeswehack we look at what is being done on the #cybersecurity side to keep things running #safely and #securely during the #Covid_19

👉sparta.eu/podcasts/ep-6-… pic.twitter.com/984ym5U1s3

A SPECIAL PODCAST SERIES:
COVID-19 AND CYBERSECURITY
WITH RAYNA STAMBOLIYSKA FROM THE SPARTA PROJECT

7 ♥ 9

View Tweet activity | View all Tweet activity

Top Follower followed by 149K people

Join Data Creatives & Co. Today!
Stay inspired to reach your #DataDreams
HIT FOLLOW

Lillian - JOIN DATA CREATIVES & CO. TODAY
@Strategy_Gal FOLLOWS YOU

Data CEO, Creator-In-Chief at Data-Mania ⭐10% of data entrepreneurs I've mentored land 6-figure

Top mention earned 34 engagements

Meet Sara Ricci, a post doctoral researcher at @VUTvBrne and currently leading a task within @sparta_eu 's #Training and #Awareness work package. #womeninSPARTA #WomenInSTEM #womenincyber #womenintech

Full interview 👉sparta.eu/assets/videos/…

@CCN_EU @DSMeu @Cybersec_EU pic.twitter.com/aP1U6ZhNHE

3 ♥ 6

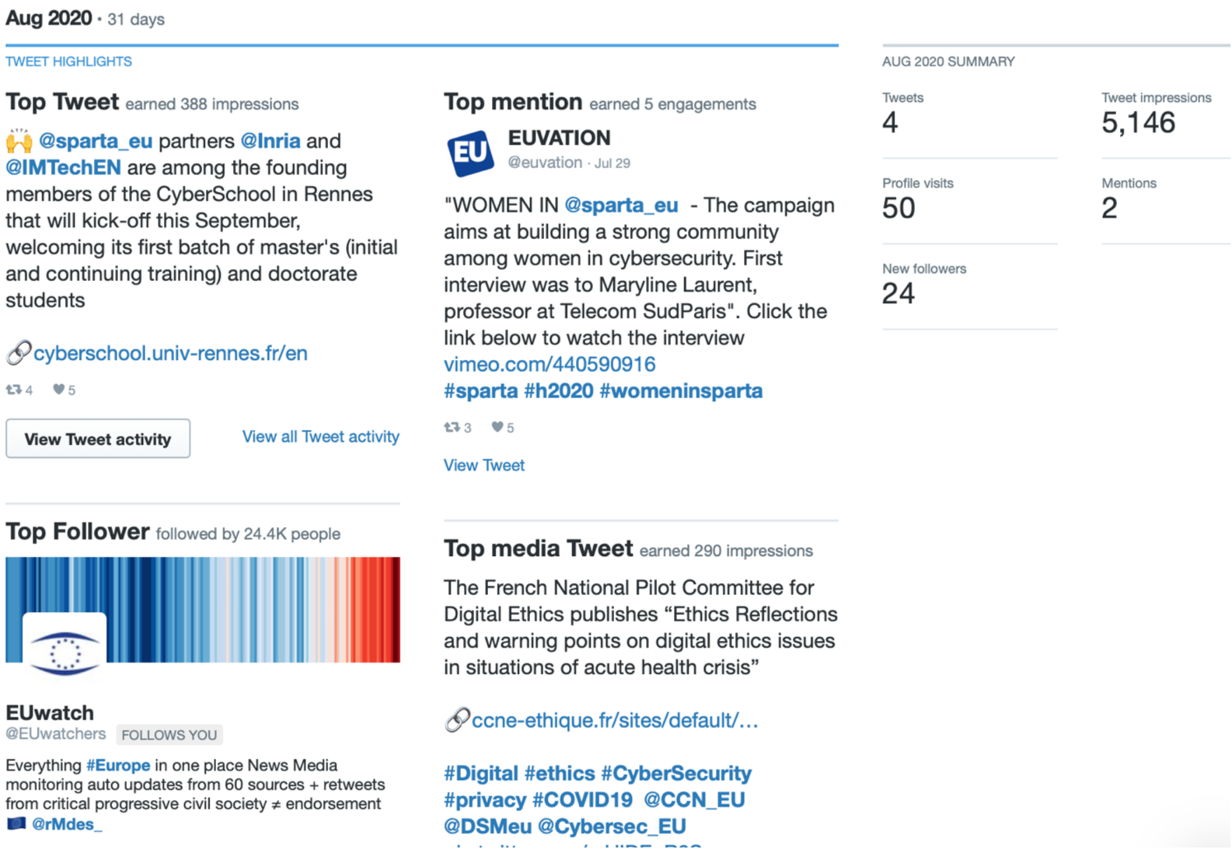
View Tweet activity | View all Tweet activity

Top media Tweet earned 702 impressions

Meet Sara Ricci, a post doctoral researcher at @VUTvBrne and currently leading a task within @sparta_eu 's #Training and #Awareness work package. #womeninSPARTA #WomenInSTEM #womenincyber #womenintech

JUL 2020 SUMMARY

Tweets 8	Tweet impressions 9,236
Profile visits 270	Mentions 16
New followers 24	



Aug 2020 · 31 days

TWEET HIGHLIGHTS

Top Tweet earned 388 impressions

🙌 @sparta_eu partners @Inria and @IMTechEN are among the founding members of the CyberSchool in Rennes that will kick-off this September, welcoming its first batch of master's (initial and continuing training) and doctorate students

🔗cyberschool.univ-rennes.fr/en

4 ♥ 5

View Tweet activity | View all Tweet activity

Top Follower followed by 24.4K people

EUwatch
@EUwatchers FOLLOWS YOU

Everything #Europe in one place News Media monitoring auto updates from 60 sources + retweets from critical progressive civil society ≠ endorsement 🇪🇺 @rMdes_

Top mention earned 5 engagements

EUVATION
@euvation · Jul 29

"WOMEN IN @sparta_eu - The campaign aims at building a strong community among women in cybersecurity. First interview was to Maryline Laurent, professor at Telecom SudParis". Click the link below to watch the interview vimeo.com/440590916 #sparta #h2020 #womeninsparta

3 ♥ 5

View Tweet

Top media Tweet earned 290 impressions

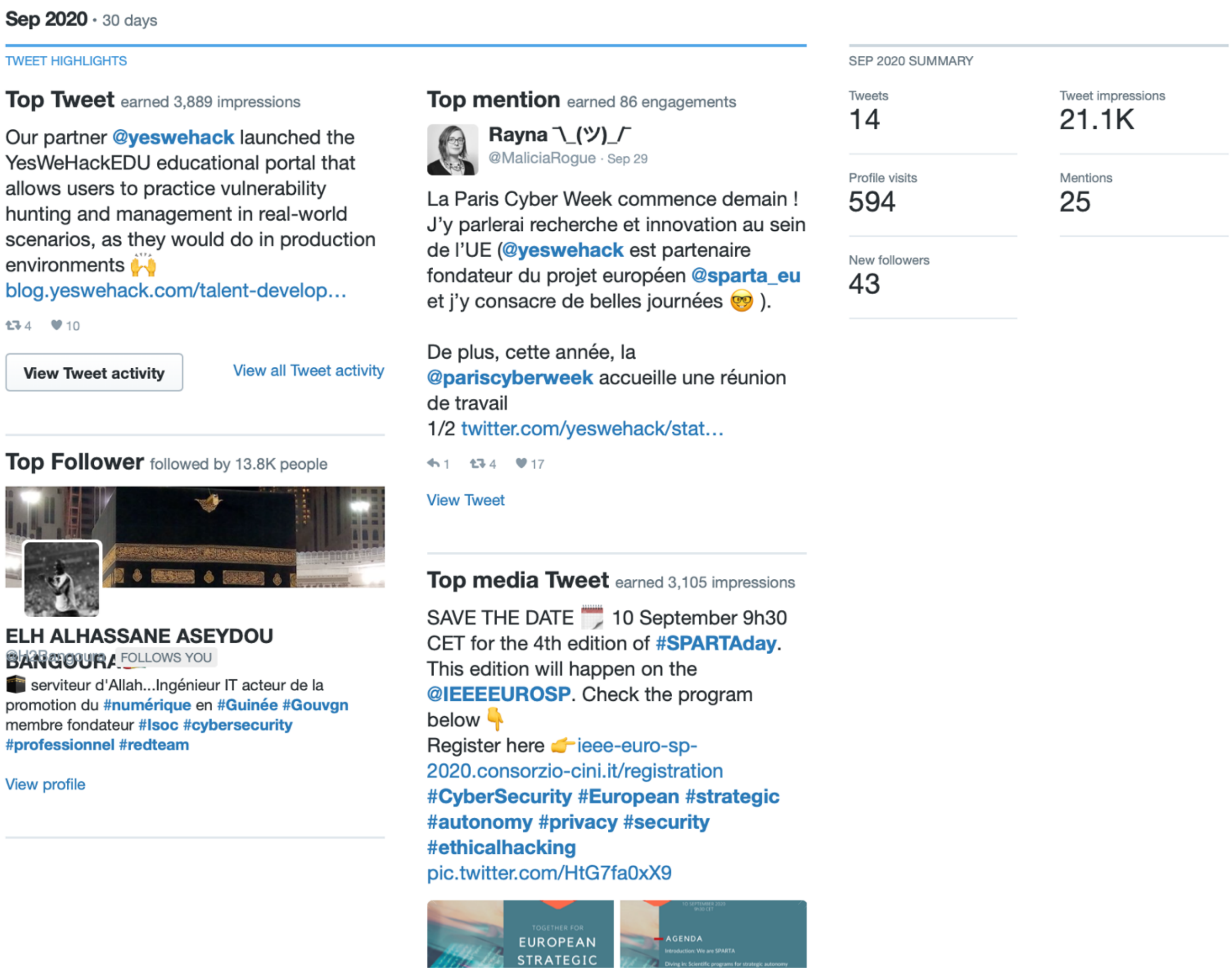
The French National Pilot Committee for Digital Ethics publishes “Ethics Reflections and warning points on digital ethics issues in situations of acute health crisis”

🔗ccne-ethique.fr/sites/default/…

#Digital #ethics #CyberSecurity #privacy #COVID19 @CCN_EU @DSMeu @Cybersec_EU

AUG 2020 SUMMARY

Tweets 4	Tweet impressions 5,146
Profile visits 50	Mentions 2
New followers 24	



Sep 2020 · 30 days

TWEET HIGHLIGHTS

Top Tweet earned 3,889 impressions

Our partner **@yeswehack** launched the YesWeHackEDU educational portal that allows users to practice vulnerability hunting and management in real-world scenarios, as they would do in production environments 🙌
blog.yeswehack.com/talent-develop…

🔁 4 ♥ 10

Top Follower followed by 13.8K people

ELH ALHASSANE ASEYDOU BANGOURA
@H2Bangoura FOLLOWS YOU

🕋 serviteur d'Allah...Ingénieur IT acteur de la promotion du **#numérique** en **#Guinée #Gouvgn** membre fondateur **#Isoc #cybersecurity #professionnel #redteam**

Top mention earned 86 engagements

Rayna ¯_(ツ)_/¯
@MaliciaRogue · Sep 29

La Paris Cyber Week commence demain ! J'y parlerai recherche et innovation au sein de l'UE (**@yeswehack** est partenaire fondateur du projet européen **@sparta_eu** et j'y consacre de belles journées 🤓).

De plus, cette année, la **@pariscyberweek** accueille une réunion de travail
1/2 twitter.com/yeswehack/stat…

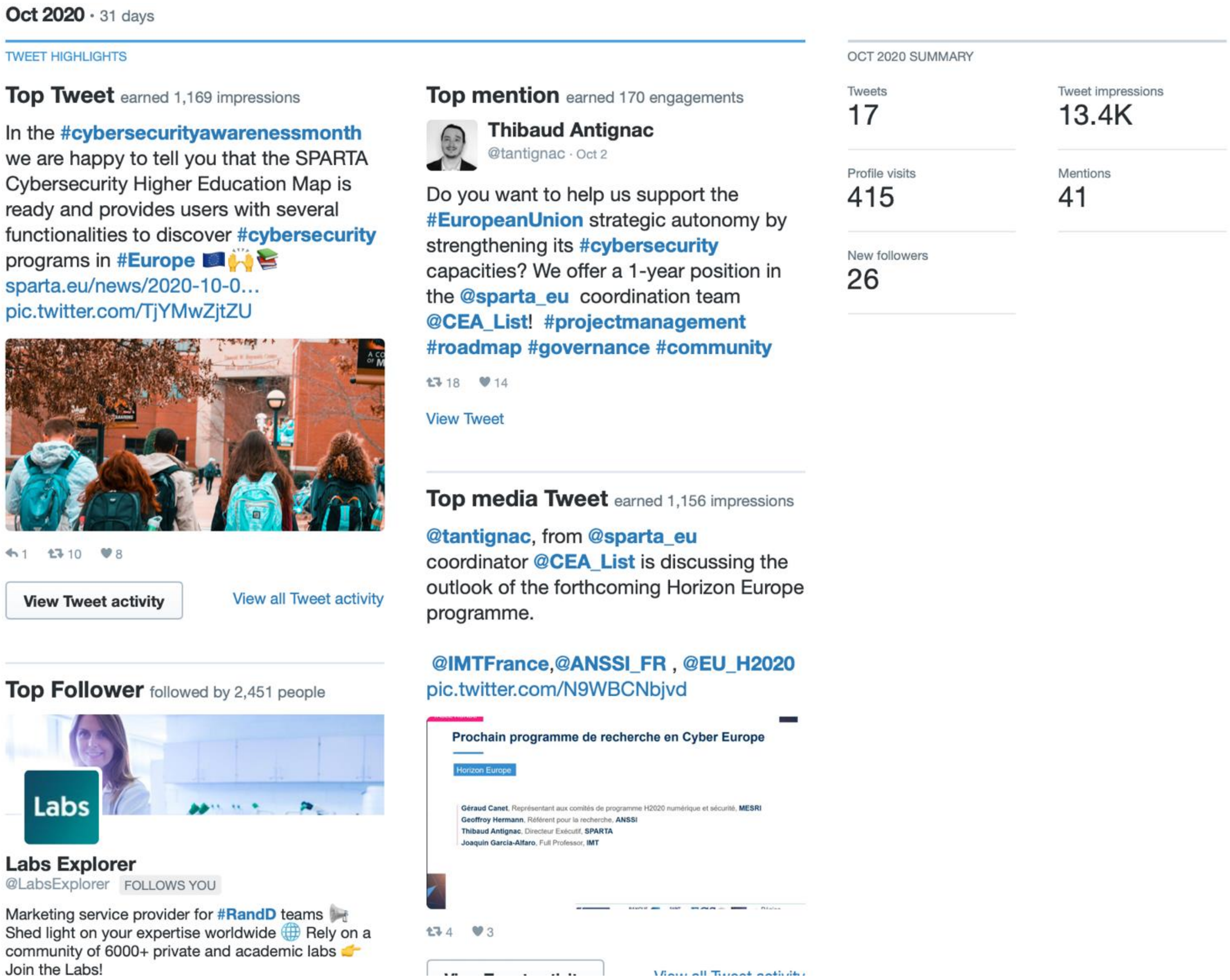
↩ 1 🔁 4 ♥ 17

Top media Tweet earned 3,105 impressions

SAVE THE DATE 🗓️ 10 September 9h30 CET for the 4th edition of **#SPARTAday**. This edition will happen on the **@IEEEEUROSP**. Check the program below 👇
Register here 👉ieee-euro-sp-2020.consorzio-cini.it/registration
#CyberSecurity #European #strategic #autonomy #privacy #security #ethicalhacking
pic.twitter.com/HtG7fa0xX9

SEP 2020 SUMMARY

Tweets 14	Tweet impressions 21.1K
Profile visits 594	Mentions 25
New followers 43	



Oct 2020 · 31 days

TWEET HIGHLIGHTS

Top Tweet earned 1,169 impressions

In the #cybersecurityawarenessmonth we are happy to tell you that the SPARTA Cybersecurity Higher Education Map is ready and provides users with several functionalities to discover #cybersecurity programs in #Europe 🇪🇺🙌📚 sparta.eu/news/2020-10-0… pic.twitter.com/TjYMwZjtZU

↰ 1 ⇄ 10 ♥ 8

View Tweet activity

View all Tweet activity

Top Follower followed by 2,451 people

Labs Explorer
@LabsExplorer FOLLOWS YOU

Marketing service provider for #RandD teams 📢 Shed light on your expertise worldwide 🌐 Rely on a community of 6000+ private and academic labs 👉 Join the Labs!

Top mention earned 170 engagements

Thibaud Antignac
@tantignac · Oct 2

Do you want to help us support the #EuropeanUnion strategic autonomy by strengthening its #cybersecurity capacities? We offer a 1-year position in the @sparta_eu coordination team @CEA_List! #projectmanagement #roadmap #governance #community

⇄ 18 ♥ 14

View Tweet

Top media Tweet earned 1,156 impressions

@tantignac, from @sparta_eu coordinator @CEA_List is discussing the outlook of the forthcoming Horizon Europe programme.

@IMTFrance,@ANSSI_FR , @EU_H2020 pic.twitter.com/N9WBCNbjvd

Prochain programme de recherche en Cyber Europe

Horizon Europe

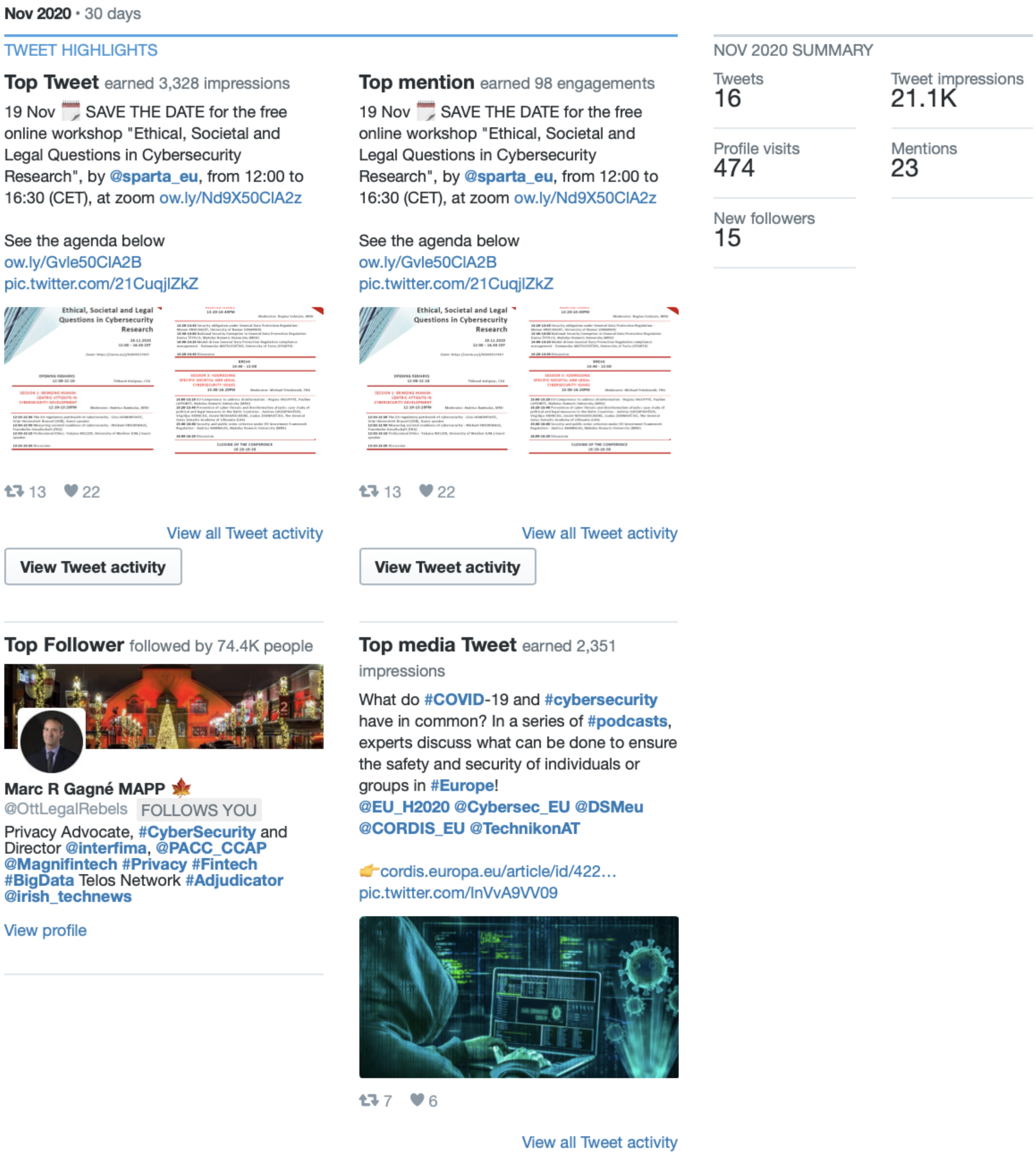
Géraud Canet, Représentant aux comités de programme H2020 numérique et sécurité, **MESRI**
Geoffroy Hermann, Référent pour la recherche, **ANSSI**
Thibaud Antignac, Directeur Exécutif, **SPARTA**
Joaquin Garcia-Alfaro, Full Professor, **IMT**

⇄ 4 ♥ 3

View all Tweet activity

OCT 2020 SUMMARY

Tweets 17	Tweet impressions 13.4K
Profile visits 415	Mentions 41
New followers 26	



Nov 2020 • 30 days

TWEET HIGHLIGHTS

Top Tweet earned 3,328 impressions

19 Nov 📅 SAVE THE DATE for the free online workshop "Ethical, Societal and Legal Questions in Cybersecurity Research", by **@sparta_eu**, from 12:00 to 16:30 (CET), at zoom ow.ly/Nd9X50ClA2z

See the agenda below
ow.ly/Gvle50ClA2B
pic.twitter.com/21CuqjlZkZ

⇄ 13 ♥ 22

View all Tweet activity

View Tweet activity

Top mention earned 98 engagements

19 Nov 📅 SAVE THE DATE for the free online workshop "Ethical, Societal and Legal Questions in Cybersecurity Research", by **@sparta_eu**, from 12:00 to 16:30 (CET), at zoom ow.ly/Nd9X50ClA2z

See the agenda below
ow.ly/Gvle50ClA2B
pic.twitter.com/21CuqjlZkZ

⇄ 13 ♥ 22

View all Tweet activity

View Tweet activity

Top Follower followed by 74.4K people

Marc R Gagné MAPP 🍁
@OttLegalRebels FOLLOWS YOU

Privacy Advocate, **#CyberSecurity** and Director **@interfima**, **@PACC_CCAP** **@Magnifintech** **#Privacy** **#Fintech** **#BigData** Telos Network **#Adjudicator** **@irish_technews**

View profile

Top media Tweet earned 2,351 impressions

What do **#COVID**-19 and **#cybersecurity** have in common? In a series of **#podcasts**, experts discuss what can be done to ensure the safety and security of individuals or groups in **#Europe**!
@EU_H2020 **@Cybersec_EU** **@DSMeu** **@CORDIS_EU** **@TechnikonAT**

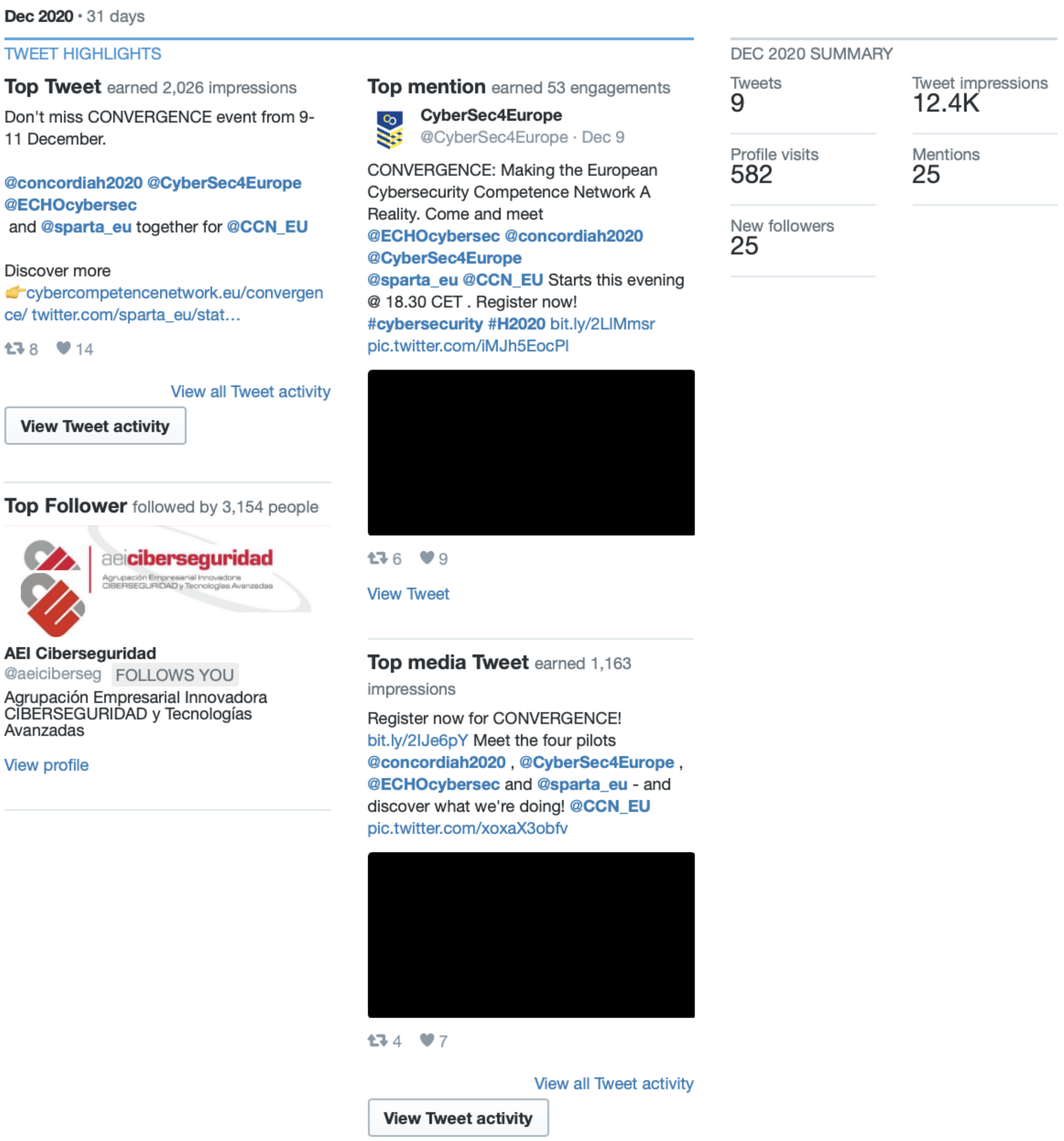
👉cordis.europa.eu/article/id/422…
pic.twitter.com/lnVvA9VV09

⇄ 7 ♥ 6

View all Tweet activity

NOV 2020 SUMMARY

Tweets 16	Tweet impressions 21.1K
Profile visits 474	Mentions 23
New followers 15	



Dec 2020 • 31 days

TWEET HIGHLIGHTS

Top Tweet earned 2,026 impressions

Don't miss CONVERGENCE event from 9-11 December.

@concordiah2020 @CyberSec4Europe @ECHOcybersec and @sparta_eu together for @CCN_EU

Discover more 👉cybercompetencenetwork.eu/convergence/ twitter.com/sparta_eu/stat…

8 retweets, 14 likes

View all Tweet activity

View Tweet activity

Top Follower followed by 3,154 people

AEI Ciberseguridad
@aeiciberseg FOLLOWS YOU
Agrupación Empresarial Innovadora CIBERSEGURIDAD y Tecnologías Avanzadas

View profile

Top mention earned 53 engagements

CyberSec4Europe
@CyberSec4Europe · Dec 9

CONVERGENCE: Making the European Cybersecurity Competence Network A Reality. Come and meet @ECHOcybersec @concordiah2020 @CyberSec4Europe @sparta_eu @CCN_EU Starts this evening @ 18.30 CET . Register now! #cybersecurity #H2020 bit.ly/2LlMmsr pic.twitter.com/iMJh5EocPl

6 retweets, 9 likes

View Tweet

Top media Tweet earned 1,163 impressions

Register now for CONVERGENCE! bit.ly/2lJe6pY Meet the four pilots @concordiah2020 , @CyberSec4Europe , @ECHOcybersec and @sparta_eu - and discover what we're doing! @CCN_EU pic.twitter.com/xoxaX3obfv

4 retweets, 7 likes

View all Tweet activity

View Tweet activity

DEC 2020 SUMMARY

Tweets 9	Tweet impressions 12.4K
Profile visits 582	Mentions 25
New followers 25	

Annex 2 – Dedicated Newsletter to Women in SPARTA

MARCH 2020 | ISSUE NO. 2

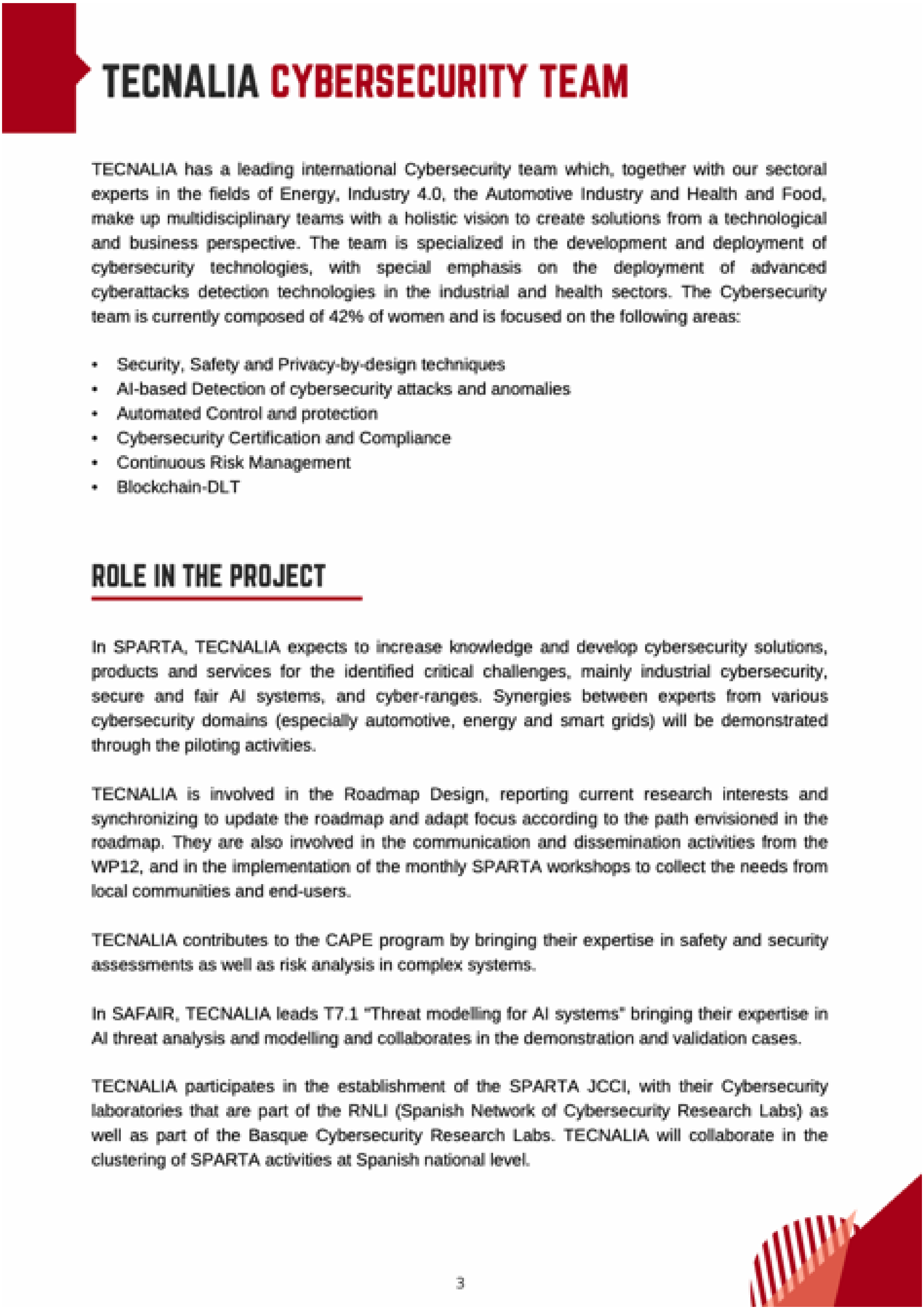
SPARTA NEWS

WHERE KNOWLEDGE COMES ACROSS

INDEX

The second edition of SPARTA NEWS is dedicated to the women working in SPARTA. Tecnalia'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.

1



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.

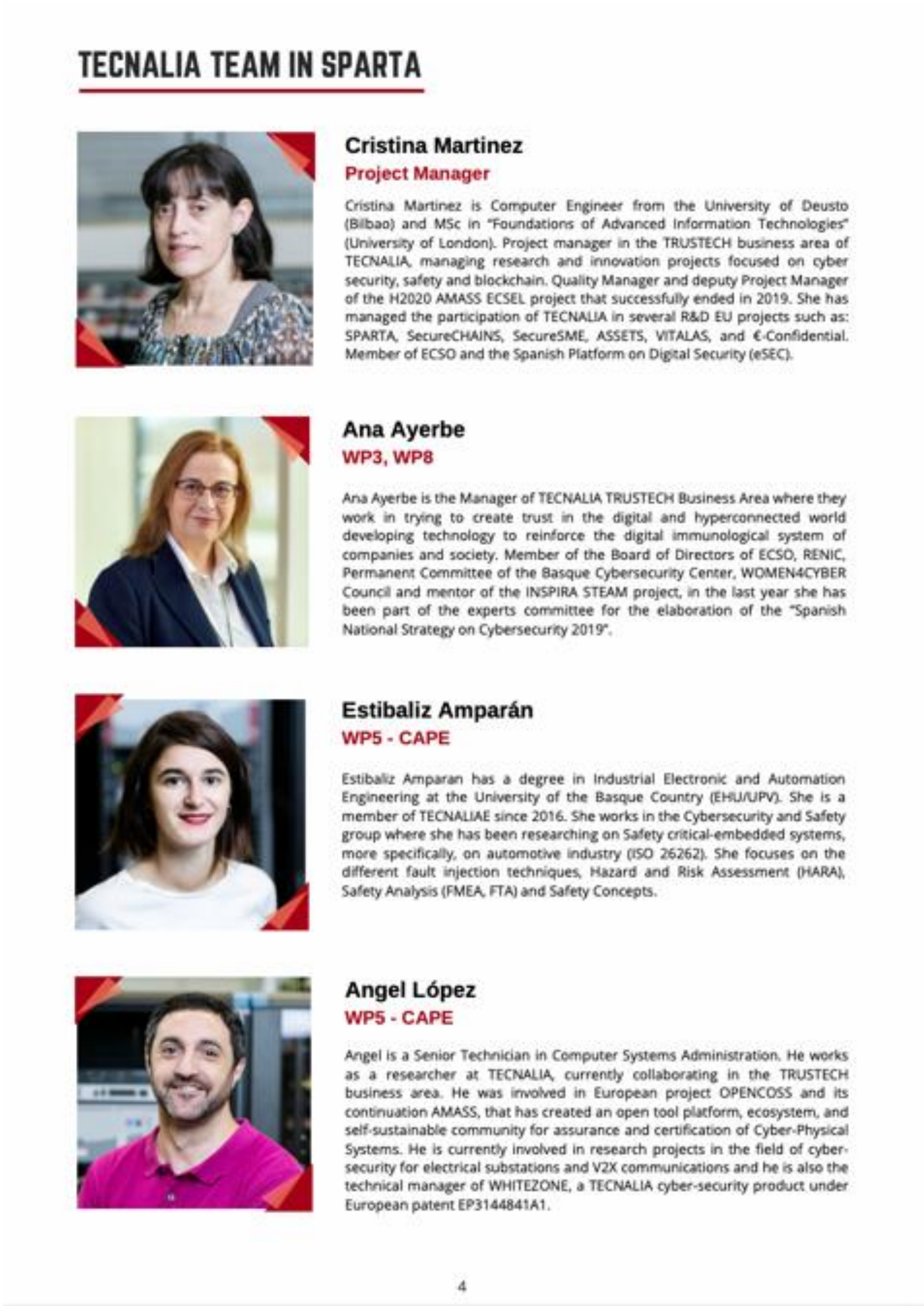
TECNALIA is involved in the Roadmap Design, reporting current research interests and synchronizing to update the roadmap and adapt focus according to the path envisioned in the roadmap. They are also involved in the communication and dissemination activities from the WP12, and in the implementation of 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.

3



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 OPENCOSS 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 cyber-security 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

Mª 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, OPENCOSS, TACIT and FM-BIASED among others.

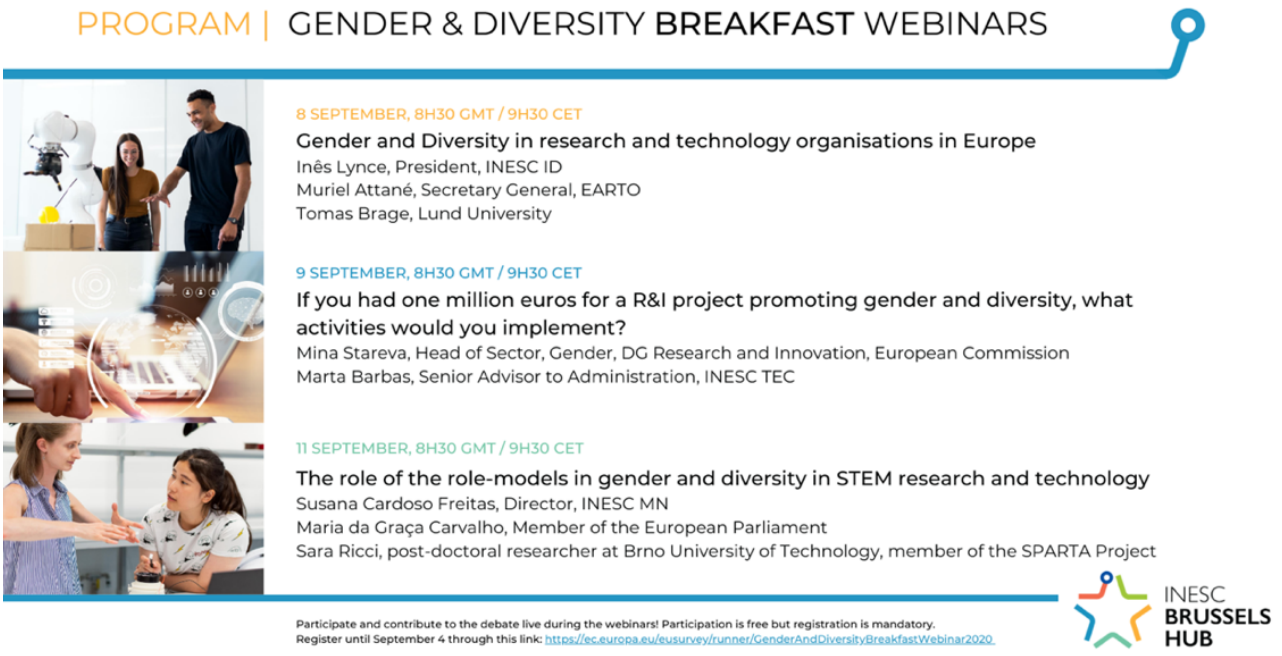
Pilar Ruiz

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.

5

Annex 3 – Gender & Diversity Gender Breakfast Webinars (Program)



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 webinars! Participation is free but registration is mandatory.
Register until September 4 through this link: https://ec.europa.eu/eusurvey/runner/GenderAndDiversityBreakfastWebinar2020