



## D12.1

### Dissemination and communication plan, updates, and evaluation

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

<b>Deliverable type</b>	Report
<b>Deliverable reference number</b>	SU-ICT-03-830892 / D12.1/ V1.0
<b>Work package contributing to the deliverable</b>	WP12
<b>Due date</b>	April 2019 – M03
<b>Actual submission date</b>	30 <sup>th</sup> April, 2019

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

<b>Abstract</b>	The present deliverable contains a detailed dissemination and communication plan based upon a strategic approach with well-established axes and timings. Communication and dissemination objectives have been selected in parallel with SPARTA main objectives in order to leverage efficient actions, promoting audiences' awareness, participation and action in SPARTA and cybersecurity realm.
<b>Keywords</b>	Communication and dissemination strategy, Key audiences, Mixed-channel communication, Monitoring and evaluation



## **Editor**

Catarina Valente (INOV)

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

Vanessa Moreira, Elisabete Carreira (INOV)

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

Diane Bahrami (CEA)

Michael Friedewald (Fraunhofer)

## **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 a detailed communication and dissemination plan based on a strategic approach to the project communication.

The first part of the document identifies basic assumptions in order to guide the overall plan. Here, one can find a brief explanation about the execution of the communication and dissemination plan regarding inputs, deliverables and outcomes, and its main objectives.

Chapter 2 develops the overall strategy for communication and dissemination considering SPARTA's main objectives to define its three axes of action: Awareness, Participation and Action. In order to have a consistent approach, communication and dissemination objectives have also been defined in parallel with SPARTA main objectives. This will help to leverage efficient actions to reach SPARTA main objectives. Key audiences have been identified and described and key messages have been developed to achieve the communication objectives. The contribution of communication and dissemination to the KPIs of the project is also established.

Chapter 3 foresees the communication and dissemination instruments and their management during the project, with focus on information about the website and the social media strategy.

Chapter 4 contains information about the management of Communication and Dissemination actions, such as scientific publications, monthly workshops and other relevant events. Here is also included the presentation of the SPARTA campaigns for diversity in cybersecurity – Gender and the Outermost Regions of Europe. The contribution of partners to the communication activities is presented according to each type of organization.

Chapter 5 describes the methodology for monitoring and evaluation of the implementation of the plan, defining the processes and responsibilities for reporting of activities to WP12.

# Table of Content

<b>Chapter 1</b>	<b>Introduction .....</b>	<b>1</b>
<b>Chapter 2</b>	<b>Communication Strategic Approach .....</b>	<b>2</b>
2.1	Strategic axes .....	2
2.2	Key Audiences .....	3
2.3	Contribution to the KPIs of the project.....	6
2.4	Cybersecurity Pilot projects.....	7
<b>Chapter 3</b>	<b>Communication and Dissemination actions .....</b>	<b>8</b>
3.1	Conferences and events, including trade shows and exhibitions .....	8
3.2	Monthly SPARTA workshops .....	9
3.3	Scientific Publications .....	9
3.4	Campaigns for Diversity in cybersecurity .....	10
3.4.1	The Gender Gap.....	11
3.4.2	Outermost Regions of Europe .....	12
3.5	Contribution of partners to communication and dissemination .....	13
<b>Chapter 4</b>	<b>Communication and Dissemination Instruments .....</b>	<b>15</b>
4.1	Official Website .....	15
4.2	Mailing Lists .....	15
4.3	Intra project communications .....	15
4.4	Identity Brand .....	16
4.5	Official Social Media.....	16
4.5.1	Instagram .....	16
4.5.2	LinkedIn.....	16
4.5.3	Twitter .....	16
4.6	Media relations.....	17
4.7	Other Promotional Tools .....	17
4.7.1	Project leaflet.....	17
4.7.2	Templates for documents .....	17
4.7.3	Factsheets / Infographics.....	17
4.7.4	Brochures / Flyers .....	17
4.7.5	Booklets .....	18
4.7.6	Podcasts.....	18
4.7.7	Videos .....	18
4.7.8	Tutorials and Technical Presentations .....	18
4.7.9	Newsletters.....	18



<b>Chapter 5</b>	<b>Monitoring and Evaluation .....</b>	<b>19</b>
<b>Chapter 6</b>	<b>Summary and Conclusion .....</b>	<b>21</b>
<b>Chapter 7</b>	<b>List of Abbreviations.....</b>	<b>22</b>
<b>Chapter 8</b>	<b>Bibliography .....</b>	<b>23</b>
<b>Chapter 9</b>	<b>Annexes .....</b>	<b>24</b>
9.1	Annex I: Template of attendance list .....	24
9.2	Annex II: Template for monitoring events.....	25

## List of Figures

Figure 1 – Communication Strategic axes.....	2
Figure 2 – Cybersecurity - Horizon 2020 pilot projects .....	7
Figure 3 - Gender Distribution of the Cybersecurity Workforce.....	11
Figure 4 - SPARTA website homepage.....	15
Figure 5 - Communication Outputs, Outtakes, and Outcomes.....	19

## List of Tables

Table 1 - WP12 in SPARTA .....	1
Table 2 – Main objectives, contents and dissemination channel per audience .....	5
Table 3 - Specific Messages per strategic axes .....	5
Table 4 - List of potential events for dissemination.....	9
Table 5 - List of possible journals for SPARTA dissemination .....	10
Table 6 - Dissemination strategy per partner type .....	14
Table 7 - Social media strategy.....	16
Table 8 – Measuring Communication Outputs, Outtakes, and Outcomes .....	20

# Chapter 1 Introduction

SPARTA's Work Package 12 – Dissemination and Communication aims to plan, coordinate and execute all SPARTA activities related to dissemination and communication, including the definition of a detailed dissemination and communication strategy and plan, the organization and participation in activities and events, and the development of materials to support these efforts. Because SPARTA has also identified the importance of reducing diversity gaps in the field of cybersecurity, WP12 also encompasses the development of campaigns to close the gender gap in cybersecurity and to improve the inclusion of the Outermost Regions of Europe. Deliverable 12.1 – Dissemination and Communication Plan provides the initial version of the plan, which will be updated yearly, jointly with an evaluation of the work carried out in each stage.

The following plan focuses on the first year of the project. A successful communication strategy thinks holistically, in a long-term perspective. Therefore, this document defines the overall strategy for the project and a more detailed plan for the first year allowing to monitor, adapt and update the plan in the following deliverables.

## Work package 12 within the project

WP12 is crosscutting to all the project work packages feeding on all the project activity to promote its results and expected impact. Nevertheless, a few key relations are more relevant to the work to be carried out, namely the inputs to receive from WP3 – Roadmap Design and WP8 – Clustering, platforms, and ecosystem activities. In addition to these, WP12 will need inputs from the SPARTA programs, within the scope of WP4 to WP7 (T-SHARK, CAPE, HAIL-T, and SAFAIR), WP1 concerning the governance model for the network, and WP11 regarding certification.

<b>WP1</b> Governance model for the network  <b>WP 3 &amp; WP8</b> Workshops, conferences, trade shows  <b>WP4 – WP7</b> SPARTA programs  <b>WP11</b> Certification  <b>All partners &amp; WPs</b>	<b>D12.1</b> Dissemination and communication plan, updates and evaluation (M03, INOV)	Materials
	<b>D12.2</b> Internal and external IT communication infrastructure and project website (M03, TNK)	
	<b>D12.3</b> Updated dissemination and communication plan and evaluation (M12, INOV)	Events
	<b>D12.4</b> Updated dissemination and communication plan and evaluation (M24, INOV)	Internal and external IT communication infrastructures
	<b>D12.5</b> Final report on dissemination and communication and evaluation (M36, INOV)	
	<b>D12.6</b> Closing the gender and diversity gap (M36, INOV)	
	<b>D12.7</b> Outermost regions engagement (M36, INOV)	

Table 1 - WP12 in SPARTA

## Chapter 2 Communication Strategic Approach

This chapter describes the overall strategy of communication and dissemination for the SPARTA project. This version of the deliverable will be dedicated to communication and dissemination during the first year.

### 2.1 Strategic axes

SPARTA Communication and Dissemination Plan will develop considering three different, interdependent strategic axes:

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

The communication and dissemination axes are aligned with the overall SPARTA objectives. To coordinate and align our action with SPARTA main objectives is crucial to successfully achieve our communication goals and therefore, according to the project objectives and the project audiences, the different strategic axes will have more relevance.

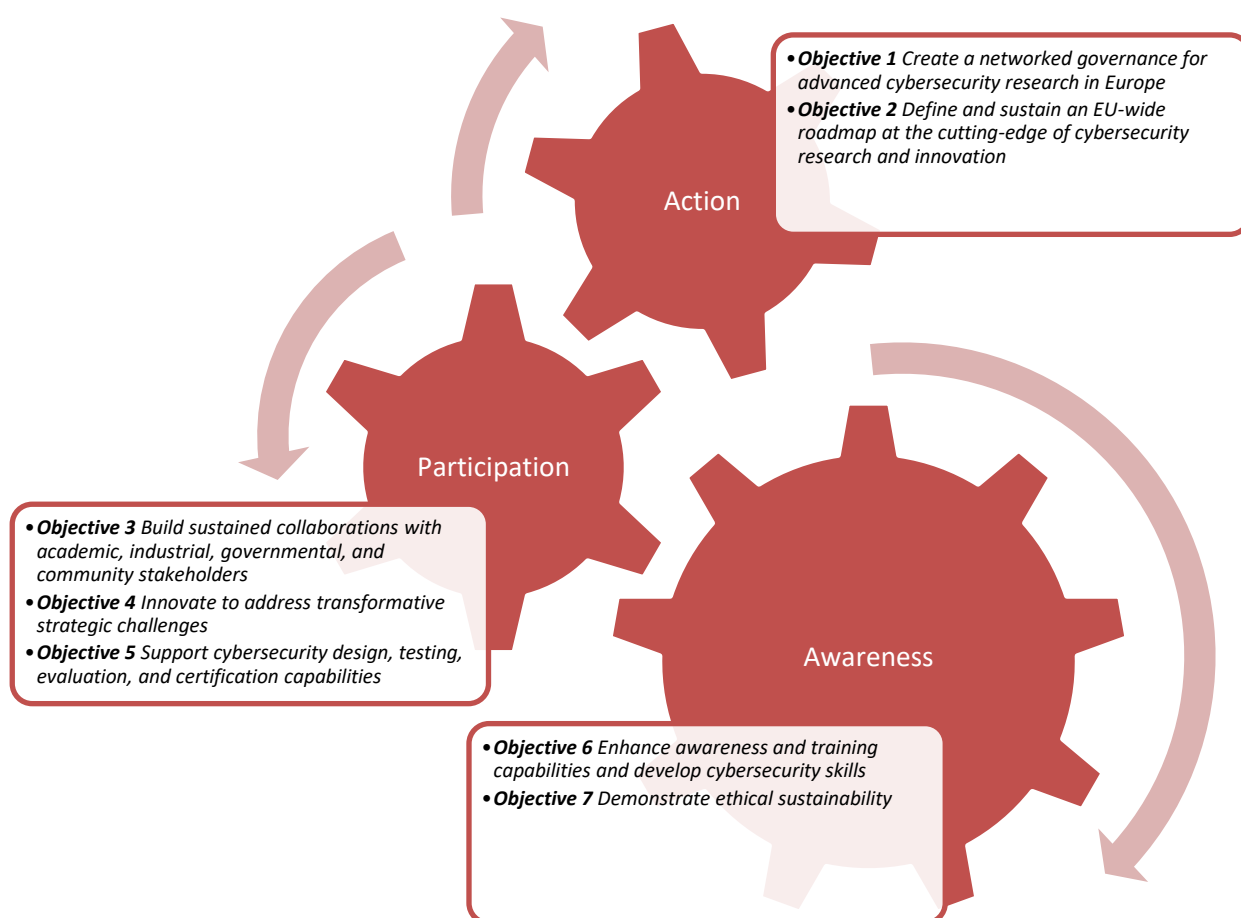


Figure 1 – Communication Strategic axes



The **awareness** axis is designed to be sustained during the entire project. Awareness is the foreground of all our actions, and the following axes are built in order to have project audiences that are informed about the project and aware of the impact it aims to achieve.

The **participation** axis will be deployed among audiences that are aware of SPARTA – have been contacted and received information about the project activities. Here, the communication efforts will aim to reach higher levels of engagement with the project – attendance in SPARTA events, contacts from media, invitation for speaking at external events will be considered demonstrations of interest and engagement with the project.

The **action** axis will take place when our audiences start to engage with SPARTA and change in attitudes and behaviour are perceived. This will encompass our audiences becoming advocates for the project and influencing practices, products and standards in cybersecurity.

The strategic axes identified will contribute to the project objectives by:

- Ensuring outreach to raise knowledge and awareness of cybersecurity issues among a wider circle of professionals, where possible in cooperation with EU and national efforts, and to spread the developed expertise.
- Enhancing awareness, training capabilities and develop cybersecurity skills.
- Engaging with citizens in general, and computer science and cybersecurity scientists and professionals, across geographies, maturity levels, and disciplines.
- Fostering sustained collaborations with academic, industrial, governmental, and community stakeholders.

For the first year of the project, the Awareness axis will aim to:

1. Give visibility to SPARTA in order to:
  - Inform the various key audiences about SPARTA project;
  - Enhance awareness about cybersecurity and the importance of this project;
  - Engage the audiences with SPARTA project.
2. Promote efficient communication between all partners.

## 2.2 Key Audiences

To achieve success in communication careful consideration about the project audiences is needed to understand their status towards the issues presented, i.e. cybersecurity. The SPARTA audiences have been identified and characterized, in order to develop the communication messages that will be used to reach them. The audiences are:



### Academia

SPARTA needs to raise awareness about the project at the academic level – computer scientists and IT security specialists – as they will strongly contribute to feed monthly SPARTA workshops. A second goal is to trigger students' curiosity to pursue their studies on the field of cybersecurity for the creation of a specialized and grand cybersecurity community in Europe.



### Industry

SPARTA aims at building sustained collaborations with the industrial stakeholders, as they will strongly contribute to feed monthly SPARTA workshops. On the one hand, SPARTA will aim to engage with producers of IT security to gather knowledge and expertise for the roadmap design and, on the other hand with potential end-users in order to consider their needs in the development of new solutions.



### Private and Public entities in Europe related to cybersecurity

Private and public entities at regional and national levels and operating in the IT security field will benefit from SPARTA activities and need to be informed about project

achievements and results. An effective partnership between public and private sectors is important as non-government entities manage and operate many critical infrastructures that citizens rely on every day, and both public and private entities need to face cybersecurity challenges of an ever more connected and globalized world.



### End users, end-user networks and associations, EU agencies and bodies

End users, end-user networks and associations, EU agencies and bodies will strongly benefit from SPARTA achievements. An effective communication on the project evolution, progress and importance is important to promote recognition and cooperation with these entities. Within this group, two main objectives will be pursued: SPARTA will engage with end-users for definition of requirements for the solutions to be developed and with the EU agencies and bodies to promote those solutions and give relevant input for the development of frameworks and regulations based on real needs.



### SPARTA partners

Good communication and dissemination inside each organization is crucial for the project success. SPARTA's dissemination and communication activities will leverage a two-way symmetrical model of communication, ensuring mutual understanding and benefits.



### General Public and Media

Because cybersecurity is a matter of public interest, SPARTA aims at ensuring outreach to the community and enhance awareness on the subject. The community needs to know EU is fully committed to setup a European Cybersecurity Competence Network leveraging Europe's strengths and opportunities across multiple disciplines, maturity levels and geographical locations. The media also play a role in communicating SPARTA into academia, industry (business press) and policy making (general media and policy-oriented channels) and therefore, SPARTA will target both general and specialized media according to the audiences and messages to communicate.

It is important to highlight that in order to achieve the different results from different audiences, different messages and channels of communication are necessary. In the following table, some communication supports and channels are identified but other may be considered relevant throughout the project.

	Main Objectives	Contents	Dissemination Channels
<b>Academia</b>	Raise awareness Invite to collaborate Present results	Leaflets, project presentations, scientific papers, posters, newsletters, demos	Journals, workshops, conferences, website
<b>Industry</b>	Present results	Leaflets, project presentations, posters, demos	Trade shows, conferences and exhibitions, public events, website
<b>Private and public entities in Europe related to cybersecurity</b>	Present results	Project presentations, newsletters, demos	Project demonstrations, website
<b>End users, end-user networks and associations, EU agencies and bodies.</b>	Raise awareness Invite to collaborate Present results	Leaflets, project presentations, scientific papers, posters, newsletters, demos	Private and public forums/ events attended by cybersecurity practitioners, project demonstrations, website

	Main Objectives	Contents	Dissemination Channels
<b>SPARTA Partners</b>	Raise awareness Obtain support	Project presentation, Demos	Meetings, newsletters, intranets
<b>Media and General Public</b>	Raise awareness Obtain support	Basic project information.	Website, social media, e-mail.

Table 2 – Main objectives, contents and dissemination channel per audience

As way to support the communication and dissemination efforts, not only by the consortium as a whole but for partners engaging in individual communication activities to promote SPARTA, some messages have been developed to allow for consistency and the transmission of a strong and guided message based on the project objectives and according to its progress.







ACTION	PARTICIPATION	AWARENESS	<p>SPARTA will break new ground on cybersecurity ensuring strategic autonomy of the EU with one of the greatest and most multicultural research ecosystems in the world, connecting excellent talent from diverse backgrounds and cultures, federating efforts to create game changing and technology, becoming a unique innovation force in cybersecurity.</p> <p>SPARTA builds on the local ecosystems and creates synergies to allow scale up at European level, avoiding fragmentation and reducing of existing gaps in research, knowledge, training, and awareness.</p>
			<p>Cybersecurity is a global phenomenon and a complex challenge for governments both at social and technical levels.</p> <p>Because it is an issue with impact in citizens' everyday lives, the involvement of individuals is necessary to raise awareness and promote societies' resilience to cybersecurity risks and threats.</p>
			<p>Understand and work on gender and diversity gap issue is a social responsibility of public interest. In order to reduce the gender gap and lack of cybersecurity human resource in Europe, SPARTA will address this issue by embedding several positive actions, namely the creation of female mentorships programs.</p> <p>Contributing for a more inclusive society, SPARTA addresses diversity in its multiple forms by promoting the engagement of associated partners, stakeholders and end users, taking into account geographical, cultural, societal and sectorial diversity.</p>
			<p>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 EU, to raise awareness and fostering conversations ranging from cutting-edge research advances to concrete problem identification.</p>
			<p>SPARTA's research roadmap starts from horizontal technologies: major technological drivers like digitization, Big Data, artificial intelligence, cognitive Internet, IoT and the Internet of values, based on key 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.</p>

Table 3 - Specific Messages per strategic axes




## 2.3 Contribution to the KPIs of the project

A holistic approach to communication will bring benefits to the project as a whole supporting all the project objectives by, through decision of the best messages and channels, reaching the project target audiences. Therefore, it is expected that the communication efforts will have indirect effects to all project KPIs, but these are the direct contributions anticipated:

**Enhance awareness** and training capabilities and develop cybersecurity skills, which will be measured as follows:

- With WP9: Objective 6.3 - number of directly addressed people (through participation at conferences, workshops, trainings, etc.) by the awareness program by the end of the project.			
	M12	M24	M36
	> 500	> 2 250	> 5 000
- Objective 6.4 - number of indirectly addressed people (through advertisements, social media groups) by the awareness program by the end of the project			
	M12	M24	M36
	> 2 000	> 20 000	> 50 000

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

- With WP8 and WP3 – Objective 3.1 - number of attendees per workshop			
	M12	M24	M36
	> 20	> 30	> 50

## 2.4 Cybersecurity Pilot projects

Within the scope of the EU H2020 Cybersecurity pilot projects, SPARTA is collaborating with ECHO, CONCORDIA and CyberSec4Europe to strengthen Europe's cybersecurity and place Europe in a leading position in cybersecurity.

Besides regular meetings with the Pilots Coordinators, a joint communication working-group of the four pilot projects has also been created to contribute specifically for joint communication and dissemination activities.

This group aims to coordinate efforts and keep track of all the planned communications activities of each project. In addition, it allows having a unique platform to exchange information, share good practices, to joint efforts in mutual events and to create a common visual identity whenever necessary.

Each project will chair the coordination of joint communication efforts on an already defined 6-month schedule.



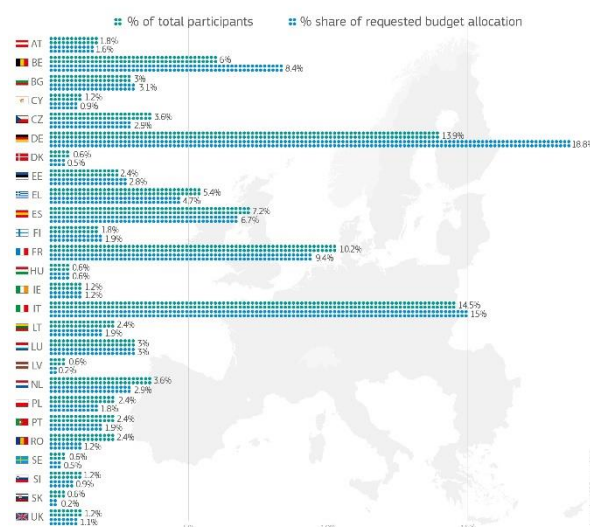
## Cybersecurity Horizon 2020 pilot projects

to prepare a European Cybersecurity Competence Network  
& contribute to the European cybersecurity industrial strategy

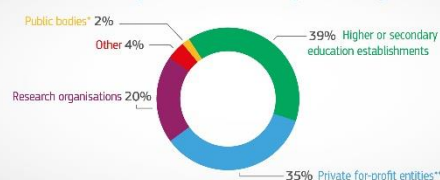
More than **€63.5 million** invested in **4 projects**



More than **160 partners** from **26 EU Member States**



### A diverse cybersecurity ecosystem



European  
Commission

Source: Data European Commission,  
Directorate-General for Research and Innovation (DG RTD) - Unit J5

Figure 2 – Cybersecurity - Horizon 2020 pilot projects



# Chapter 3 Communication and Dissemination actions

All SPARTA partners will disseminate project results by giving talks at conferences, workshops and trade shows, and by writing articles for technical and academic publications.

Because diversity in cybersecurity is an important dimension identified even before the start of the SPARTA project, two campaigns will be deployed throughout the project and parallel to the overall communication activities, one focusing on gender inclusion and the other one on the inclusion of the Outermost Regions of Europe.

## 3.1 Conferences and events, including trade shows and exhibitions

Industry and other non-scientific conferences are efficient platforms to disseminate the project findings and start direct conversations with audiences, particularly regional, national, or international events targeted to cybersecurity practitioners. The consortium aims to get speaking slots and co-host SPARTA workshops at some of the conferences shown in the table below. Moreover, SPARTA aims to promote the project progress at fairs and congresses around Europe to obtain end-users' attention and promote community building.

Conferences and events	Timing
Central European Cybersecurity Conference (CECC)	Annual
Computer Security Applications Conference (ACSAC)	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	Bi-three yearly
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
IEEE International Symposium on Reliable Distributed Systems	Annual
Int. Conference on Cyber Situational Awareness, Data Analytics and Assessment IEEE	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 Computer Recognition Systems (CORES)	Annual
International Conference on Dependable Systems and Networks (DSN)	Annual
International Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMV A)	Annual
International Symposium on Engineering Secure Software and Systems (ESSoS)	Annual
IT-Security conference of the German Informatics Society (GI-Sicherheit)	Biannual

Conferences and events	Timing
CPDP - International Conference on Computers, Privacy and Data Protection	Annual

Table 4 - List of potential events for dissemination

## 3.2 Monthly SPARTA workshops

The consortium will organise monthly SPARTA workshops within the scope of WP3 and WP8 to collect requirements to support mainly the technical work to be developed in the project. The workshops will allow end-users, innovation experts and policy makers to participate in the project and set the ground for the creation of the SPARTA community.

Nonetheless, these events will mobilise key stakeholders and promote exchanges of ideas that will allow promoting the knowledge not only internally among project partners, but also externally, when considered relevant in order to reach audiences with new information about the project. Two templates have been designed in order to collect information about SPARTA events and support the creation of new messages about SPARTA.

## 3.3 Scientific Publications

During the course of the project, SPARTA partners will select the most appropriate journals and conferences in order to disseminate the scientific results. All scientific publications stemming from SPARTA research will be made available through (at least) green open access as mandated for Horizon 2020 actions and the conditions for the SU-ICT-03-2018 call. The Dissemination Committee will define the platform for publication of articles.

There is a defined process to validate/ review the articles described in deliverable 13.1. Some of the targeted titles for scientific publication include:

Name of the scientific Journal	Main Dissemination Aspects
ACM Transactions on Information and System Security (TISSEC)	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. Studies ranging from technologies, systems, applications and policies.
Elsevier Computer Fraud & Security	Every month Computer Fraud & Security enables to see the threats to user's IT systems before they become a problem. It focuses on providing practical, usable information to effectively manage and control computer and information security.
Elsevier Computer Law & Security Review	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.

Name of the scientific Journal	Main Dissemination Aspects
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	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.
IEEE Transactions Dependable and Secure Computing (TDSC )	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.
Springer Ethics and Information Technology	Dedicated to advancing the dialogue between moral philosophy and the field of information and communication technology (ICT).
Springer Journal of Cryptographic Engineering (JCEN)	Offers high-quality scientific articles presenting methods, techniques, tools, implementations, and applications of research in cryptographic engineering, including cryptographic hardware, cryptographic embedded systems and embedded security.
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.

Table 5 - List of possible journals for SPARTA dissemination

### 3.4 Campaigns for Diversity in cybersecurity

“United in diversity” is the motto of the European Union<sup>1</sup>, approved in 2000, and signifies how Europeans have come together, in the form of the EU, to work for peace and prosperity, while at the same time being enriched by the continent's many different cultures, traditions and languages. In a globalized digital world, it also implies that diversity must be leveraged to build knowledge on which to push for a more inclusive, secure and resilient European society.

In order to coordinate the engagement of stakeholders and end users, taking into account geographical, cultural, societal and sectorial diversity at all stages of the SPARTA work process, the consortium has appointed a Gender and Diversity Manager who will work closely with partners addressing community activities throughout the project duration.

<sup>1</sup> [https://europa.eu/european-union/about-eu/symbols/motto\\_en](https://europa.eu/european-union/about-eu/symbols/motto_en)



### 3.4.1 The Gender Gap

Overall and as an initial assumption, SPARTA seems to be gender-neutral since the same requirements for cybersecurity will apply for both genders without any reason to discriminate them. Every single user, beyond gender or sex, shares similar needs when it comes to cybersecurity in our current connected world. Nevertheless, particular attention will be paid in all the phases of the project to gender-related issues that will be considered while investigating case studies and user needs. The design and execution of sessions with stakeholders and end-users are very important in the project and within the project activities special attention will be paid to gender balance. If differences in behaviour between male and female users in dealing with the concepts and technologies will come to light, these will be reflected in the resulting systems (e.g. provision of support, specific strategies, etc.). The project will specifically consider sex and/or gender analysis as regard to adherence and/or persistence and/or resistance in all user interaction activities developed within the SPARTA project.

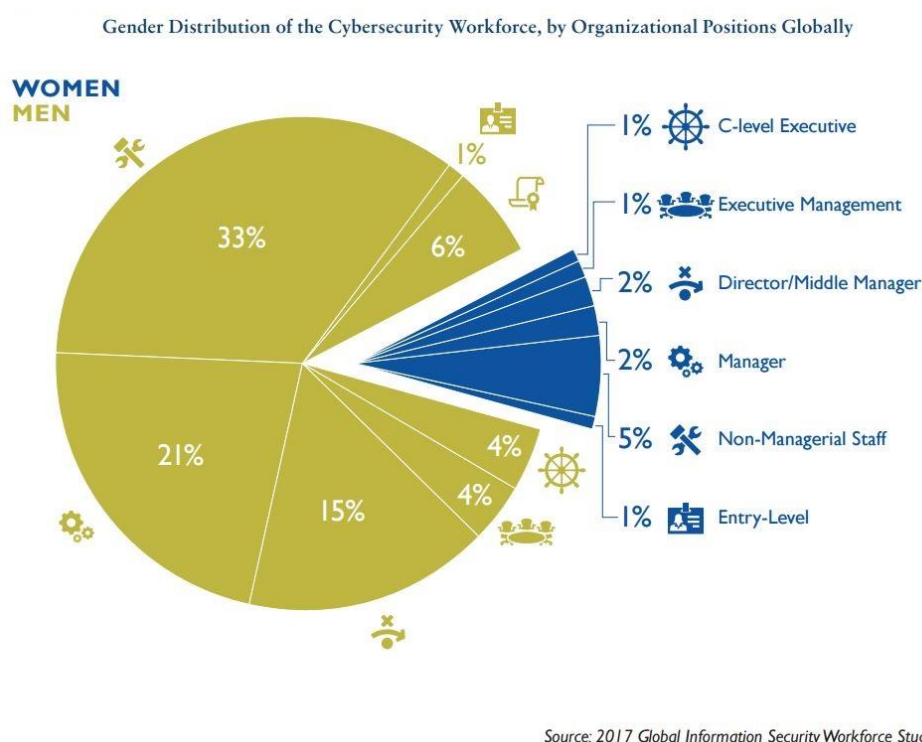


Figure 3 - Gender Distribution of the Cybersecurity Workforce

Various studies have shown that the representation of women worldwide in the field of cybersecurity varies between 8% to 11%<sup>2</sup>, which is a serious limitation taking into account there is a lack of qualified cybersecurity experts in the EU and worldwide. This has encouraged many firms to push for an open-door policy to encourage more women into info-security roles. Given the growing cybersecurity skills gap, it has never been more important for businesses to attract and maintain women into these jobs. It is often highlighted that a low percentage of women go into STEM (Science, Technology, Engineering, Mathematics) fields in comparison to men. This is cited as one of the more obvious reasons fewer women are found in cybersecurity. But recent surveys indicate that lack of specific training, peer incentive and mentorship, as well as discrimination by male colleagues are the strongest barriers to promote gender equality in cybersecurity. In order to maximize the impact

<sup>2</sup> <https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf>

of SPARTA, as well as reduce the gender gap and lack of cybersecurity human resources in Europe, the consortium will proactively address this issue by embedding several positive actions, namely:

- Specifically address a female public, in dissemination and communication activities;
- Prioritize female participation in all training related activities during the project, as to address and incentive female participation, involvement and uptake;
- Create female mentorships programs within SPARTA partner cybersecurity research teams;
- Attempt to understand and correct social barriers related to female participation in all levels of cybersecurity workforce.

The consortium strives to have a strong female representation among the executive members, although the current lack of female cybersecurity researchers will make this objective a challenge that will be proactively addressed. The project is committed to promoting equal employment opportunities and aims to establish a program of action to make the H2020 diversity, gender and equality policies fully effective, by proactively pursuing a set of relevant actions. It will also establish a system for monitoring gender equality in mobility schemes such as equality of access and participation, which causes subsequent impact on professional careers. The project will encourage balanced recruitment of female and male researchers, as well as of family-friendly policies, such as flexible working arrangements. It also relevant to mention that, since 2003, SPARTA's partner Technikon has been hosting the European WiTEC (Women in Science, Engineering and Technology) association which can leverage many of the efforts within the project.

### 3.4.2 Outermost Regions of Europe

The EU currently has nine Outermost Regions (ORs)<sup>3</sup>, which are an integral part of its territory: Guadeloupe, French Guiana, Martinique, Saint Martin, Réunion, Mayotte (France); the Canary Islands (Spain); and the Azores and Madeira (Portugal). The rights and obligations of the European Treaties apply fully to these regions<sup>4</sup>. They are islands and archipelagos located in the Caribbean basin, in the western Atlantic and in the Indian Ocean or landlocked territory in the Amazonian forest. Despite the thousands of kilometres separating them from the European continent, these regions are an integral part of the EU. They welcome 4.8 million citizens, a population equivalent to that of Ireland. Over the last years, the ORs were very active on reducing the gap in digital accessibility and ICT use. Ambitious programmes at the national and regional level have been set up to support infrastructure deployment as well as the development of digital services. In 2017, an expert group on digital accessibility and ICT use contributed to assessing the current situation and the key challenges for the future in the perspective of the renewed EU strategy<sup>5</sup>. Several recommendations were made, with a strong focus on the need to strengthen local infrastructures and promote digital skills and the local ICT sector.

In order to contribute to these objectives and maximize the regional impact of SPARTA, the project includes a specific task that will engage with the ORs to launch a communication campaign **Go Cyber with SPARTA**, which aims to setup 3 actions in 3 ORs geographical regions (Indian Ocean; Atlantic Ocean; Caribbean and South America):

- 1) Encourage small businesses to adopt cybersecurity measures (Caribbean and South America OR)
- 2) Stimulate young people to undertake studies or training at university level within the area of cybersecurity (Atlantic Ocean OR)
- 3) Engage with critical infrastructure operators to stimulate them to adopt state-of-the-art cybersecurity technology (Indian Ocean OR)

---

<sup>3</sup> [http://ec.europa.eu/regional\\_policy/sources/policy/themes/outermost-regions/pdf/rup\\_2017/rup\\_eu\\_lands\\_world\\_en.pdf](http://ec.europa.eu/regional_policy/sources/policy/themes/outermost-regions/pdf/rup_2017/rup_eu_lands_world_en.pdf)

<sup>4</sup> [http://ec.europa.eu/regional\\_policy/index.cfm/en/policy/themes/outermost-regions/](http://ec.europa.eu/regional_policy/index.cfm/en/policy/themes/outermost-regions/)

<sup>5</sup> [http://ec.europa.eu/regional\\_policy/sources/policy/themes/outermost-regions/pdf/ict\\_report\\_en.pdf](http://ec.europa.eu/regional_policy/sources/policy/themes/outermost-regions/pdf/ict_report_en.pdf)

The strategy under the *Go Cyber with SPARTA* campaign will be drawn via three living labs to be created jointly with local stakeholders: a business association (Action 1); a higher educational institution (Action 2); and a critical infrastructure operator (Action 3). The living labs will be chosen for their geographical position, diversity representativeness, and credibility and will constitute a source to strengthen the developments of SPARTA in line with the co-design approach defined for the project. The participants of the living labs will participate in workshops, focus groups and other data gathering exercises. They will also serve as connectors to stakeholders of other ORs in the same region of the world, for dissemination and communication of the SPARTA solutions. These awareness and communications activities will include innovative and appealing ways to communicate SPARTA solutions (hands-on activities and small demonstrators will be prepared) to foster interest of stakeholders for the importance of cybersecurity themes.

The methodology used to develop this approach will rely on Design Science Research. This methodology allows a rigorous process to design artefacts to solve observed problems, to make research contributions, to evaluate the designs, and to communicate the results to appropriate OR audiences. Then, at a second level, techniques such as interviews, focus groups, surveys, game-based sessions, etc., will be selected in order to evaluate the artefacts previously designed and developed. Finally, different methods will be applied to evaluate the results of the different techniques (for quantitative research: statistical analysis, for qualitative analysis: other methods will be analysed and selected).

### 3.5 Contribution of partners to communication and dissemination

INOV leads WP12 as well as lead T12.1, T12.4 and T12.5, while also actively participating in T12.2 and T12.3. TNK leads T12.2 and T12.3 and contribute to T12.1, T12.4 and T12.5. SPARTA WP leaders will contribute to all tasks in WP12. All other partners will participate in communication and dissemination activities as stated in T12.2 and T12.3.

Considering the type of organization, SPARTA will benefit from each partner's strengths and networks of contacts and relations already established to promote the project and build a strong and effective SPARTA community. With this approach, the following map of relations is identified:

RTOs and Universities
<p>The main dissemination activities to be carried out by the RTOs and Universities in the SPARTA Consortium will include authoring or co-authoring of scientific publications for international journals and conferences, press releases in the relevant media, websites, podcasts, newsletters, project dissemination material (e.g. leaflets, brochures, poster), or the attendance at related events, such as technical workshops and fair trades. Moreover, through the monthly SPARTA Workshops the partners will identify potential end-users at local level in order to reach target groups interested in project developments, and to receive relevant feedback. CEA as coordinator, assisted by CNR as Partnership Director will monitor the organization of workshops, inviting external stakeholders, as well as establishing contact and relationship with other related research activities.</p>
Cybersecurity Practitioners
<p>In general, the cybersecurity practitioners involved in SPARTA have the necessary network of contacts with operational and technical practitioners within national, regional and local cybersecurity practitioners to disseminate the results of SPARTA. Practitioners will use all the communication channels with stakeholders, in order to disseminate the results of SPARTA. Dissemination activities will have the purpose of sharing information and knowledge within the cybersecurity practitioner community that will include international partners, mainly at the bilateral co-operation level with counterpart practitioners and services.</p>

**Industry – SMEs**

The main dissemination activities to be carried out by the industrial partners in SPARTA will include participation in scientific publications for international journals and conferences, press releases in the relevant media, websites, newsletters, project dissemination material (e.g. leaflets or brochures). Moreover, SPARTA's industrial partners will exploit their market leadership positions to disseminate the project results in sponsored workshops, to customers and business partners and within national and international security associations.

Industrial partners will use their online and social channels, such as websites and social media, to divulgate relevant information about SPARTA, and will internally disseminate project's results and adopted technologies (e.g. in some cases disseminating project results especially towards their business units, which have currently several customers affected by the results of SPARTA). Communication and collaboration with target groups in order to introduce the SPARTA project and collaborate further in implementation of the project.

Table 6 - Dissemination strategy per partner type

# Chapter 4      Communication      and      Dissemination

## Instruments

### 4.1      Official Website

The website, as well as social media, is the main interface that links the project to its audiences. It is an important tool to engage the community with SPARTA's objectives, principles and purpose in order to raise awareness about cybersecurity and to promote the importance of the project and its impact on European strategy, society and citizen protection. The project website is further explained in the accompanying report of D12.2 – Internal and external IT communication infrastructure and project website.

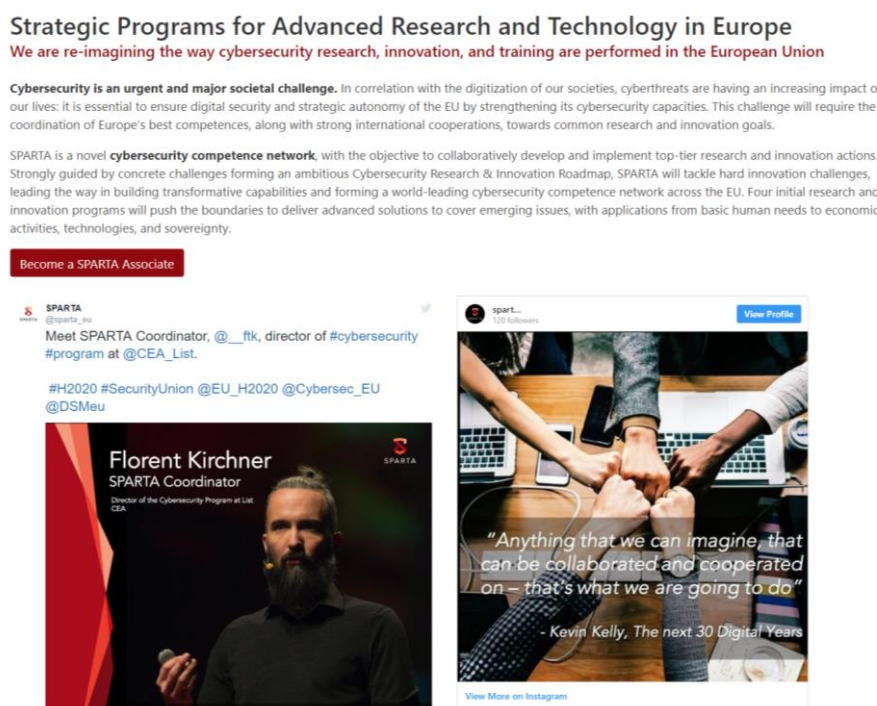


Figure 4 - SPARTA website homepage

### 4.2      Mailing Lists

SPARTA Mailing lists will support direct communication with the audiences engaged with the project. Mailing lists are already active and their management is further developed in D12.2.

### 4.3      Intra project communications

Intra project communications and transfer of knowledge within the consortium will be achieved through the development and maintenance of a project internal infrastructure including collaborative



IT applications further defined in deliverable 12.2. So far, the following set of collaborative tools has been implemented:

- A version control system (SVN) for keeping track of documents;
- Mattermost Chat (for an easy and fast communication within the project consortium);
- GoToMeeting and other systems (for remote telephone conferences);
- A mailing list system for information exchange.

During the first year, meetings will be organised every two months in order to define and then adjust good practices in using SPARTA's communication tools.

## 4.4 Identity Brand

A SPARTA identity brand to provide a strong basis for communication messages has been developed and a project logo and template for presentations were designed to support communication activities. A SPARTA identity brand guide has been created to achieve consistency in communication activities and is included in deliverable 12.2.

## 4.5 Official Social Media

Due to digitalization and globalization, social media is clearly an effective instrument to communicate with our several audiences. Choosing the correct messages and format is important to reach the audiences identified. Since different social networks reach different target groups, it is SPARTA's aim to make use of these differences specifically. The strategy to select the appropriate social media channel is summarized in the following table:

4.5.1 <u>Instagram</u>	4.5.2 <u>LinkedIn</u>	4.5.3 <u>Twitter</u>
<p>✓ <b>For the community</b></p> <ul style="list-style-type: none"> <li>- Informal Approach</li> <li>- Simple Vocabulary</li> <li>- Video, GIPHS and quality images over long text.</li> <li>- SPARTA events</li> <li>- Statistics and News, about cybersecurity</li> </ul>	<p>✓ <b>For partners and end-users</b></p> <ul style="list-style-type: none"> <li>- Formal Approach</li> <li>- Scientific Publications</li> <li>- Project results</li> <li>- Information about the achievements of SPARTA</li> </ul>	<p>✓ <b>For specific communities on Cybersecurity and other H2020 Projects</b></p> <ul style="list-style-type: none"> <li>- Scientific Publications</li> <li>- Project results</li> <li>- Information about the achievements of SPARTA</li> <li>- News about Cybersecurity and other related subjects</li> </ul>

Table 7 - Social media strategy

A social media content management tool will be selected to coordinate and manage all publications efficiently. These tools allow for a streamlined team work to organize, schedule and publish content effortlessly to all SPARTA social media accounts.

Partners will play an important role to give visibility to the project by sharing SPARTA achievements and news through their own social media pages, to which some guidelines are defined in order to maximize reach:

- All partners to follow SPARTA on social media.
- All partners to engage with social media contents (like, share, comment).
- All partners to monitor and report the results from their social media accounts.

- Always identify SPARTA (@sparta\_eu) in publications to maximize impact and attract followers to the SPARTA accounts.

## 4.6 Media relations

SPARTA will engage with the press as a mediator between the project and its audiences. Therefore, both general and specialized media outlets will be targeted according to the specific messages and needs at a given moment of the project. SPARTA will publish projects news and achievements in CORDIS but it will also produce press releases to reach national news outlets.

Press releases will emphasize clear and to-the-point presentation of major achievements, events and initiatives of partners.

Joint press releases by the consortium will be produced to identify the project milestones, which partners can localize (adapt and translate) to national press whenever considered relevant.

Partners can also produce their own press releases to communicate locally. All efforts and results – publications in the press – are to be reported to WP12.

## 4.7 Other Promotional Tools

Selecting a mix of tools to communicate with audiences is important because individuals differ on how they process information. In general, a multi-channel approach is more effective because it gives the opportunity to send the same message through several means making sure it will be fully understood and perceived. Taking this into account, a wider range of materials has been selected to be employed throughout the project according to the needs arising as the project progresses. **Periodic revisions** (quarterly) of the material will be done to refine scientific, promotional and publicity targets.

### 4.7.1 Project leaflet

A general project leaflet has been created to support the initial communication activities and present an overview of the project. Other version of this leaflet will be produced and enhanced according to the progress of the project and its results.

### 4.7.2 Templates for documents

In order to maintain consistency and sustain SPARTA's visual identity, several templates have been developed to be used by partners when communicating the project, including for PowerPoint presentations and deliverables. Whenever necessary, new templates will be created to ensure uniformity of the brand SPARTA.

### 4.7.3 Factsheets / Infographics

Factsheets are an important tool to display information in a way that is simple and easy to understand. Factsheets will be produced whenever there are results and major project achievements relevant to communicate. These instruments will also be considered to share information about cybersecurity in general in order to raise awareness of non-technical audiences for the importance of cyber secure behaviour and the impact of cybersecurity issues in citizens' lives.

### 4.7.4 Brochures / Flyers

Brochures will be developed regarding the achievement of the specific programs of the project to explain the evolution and achievements of each Program (SAFAIR, HAIL-T, CAPE, T-SHARK), SPARTA roadmap and other activities.

#### 4.7.5 Booklets

Booklets are a more extensive communication support, able to gather more information, and will be considered to integrate the overall project achievements, focusing on its progress in the several areas of action.

#### 4.7.6 Podcasts

To communicate a complex set of messages or issues related to SPARTA in a digestible form, podcasts will be produced on a quarterly basis. Podcasts can be published on social media, website and blogs and they will be gathered in a blog/website repository. The first SPARTA Podcast is available [here](#).

#### 4.7.7 Videos

Videos are a tool to communicate in a simple and attractive way about more complex issues. Video material with durations of up to 2 minutes and animated 2D/3D content will introduce audiences to the most recent achievements in the cybersecurity field.

Some videos have already been created within the project launch campaign on social media, including a video for presentation of the project. The video is available [here](#) (SPARTA's Twitter account).

#### 4.7.8 Tutorials and Technical Presentations

Tutorials and technical presentation will be developed to showcase the project results and achievements. These will be available in SPARTA website, social media, other channels to consider.

#### 4.7.9 Newsletters

Newsletters will be used to communicate news about the project progress, to promote discussion on relevant topics and will be targeted to the academy, industry, end-users and EU agencies and bodies. After releasing to the subscribers, newsletters will be made available on the website and shared across social media accounts to raise further public awareness.



## Chapter 5 Monitoring and Evaluation

Efficiently managing and monitoring all the C&D activities in a project as large as SPARTA, is paramount to keep track of all activities and maximize their impact. In order to streamline the flow of C&D information, a digestible support with the main guidelines of C&D activities will be created to guide all partners on how and when to send inputs to WP12. This support will be added to SPARTA activities Handbook developed within T13.1.

Below are some essential guidelines to be implemented in order to coordinate and manage C&D activities:

- WP12 will coordinate with a single contact point per partner responsible for communication and dissemination activities. This contact point is responsible for gathering and reporting all the activities' information. This will be carried out within T12.3.
- Specific information according to the activities is required in order to support the development of communication contents, namely regarding participation at events, scientific publications and social media activities. Templates for this have been developed within T12.1 and are to be reported to the WP12 leader through [spartacomms@inov.pt](mailto:spartacomms@inov.pt)
- Periodic conference calls will occur throughout the project to monitor the status of the WP12 activities.

Monitoring of activities will be closely related to the evaluation of the project's communication efforts allowing for timely adjustments whenever needed. For communication and dissemination evaluation the following model will be followed:



Measuring Metrics That Matter: The 3 O's

Figure 5 - Communication Outputs, Outtakes, and Outcomes

The table below provides examples of how actions will be measured during the project:

Medium	Outputs	Outtakes	Outcomes
<b>Website</b>	Website creation and management. Content creation.	<b>By M12 - 2000 visitors</b> How many visitors per day? What publications have more views?	How many people talk about our website? How many inlinks?
<b>Mailing List</b>	Mailing lists creation and management	How many people subscribe to the mailing list? How many people open/read the emails?	How many people unsubscribe? How many new subscribers?
<b>Social Media</b>	Content creation and content management, planning.	<b>2000 followers by the end of the project.</b> How many publications' likes and shares? What is the reach of publications?	How many comments on publications? Are the comments positive, negative or neutral?
<b>Press Release</b>	Identification of newsworthy achievements, events, and results. Production of press releases.	How many times was our press release mentioned? Which mass media outlets published about SPARTA?	How many follow-up contacts for articles, interviews, extended news pieces?
<b>Events</b>	Event organization.	How many attendees?	How many follow-up contacts for more information? How many requests for engagement with the project? Are people talking about the event on social media?

Table 8 – Measuring Communication Outputs, Outtakes, and Outcomes

## Chapter 6 Summary and Conclusion

The present deliverable provides essential information about SPARTA C&D activities management and strategy.

A strategic approach has been defined, considering three main axes that will guide the whole process: Awareness, Participation and Action. These strategic axes are aligned with SPARTA objectives in order to help their achievement.

Communication and dissemination objectives have been defined for the first year and will serve as main guidance.

Key audiences were selected as well as key messages to disseminate to each audience taking into account their diversity and specificities.

A mixed-channel approach has been selected in order to reach effectively each audience and ensure that every public received and well perceived the messages. From official website and social media accounts to podcasts and leaflets, a set of tools has been deployed and its management have been proposed. Communication and dissemination events have been listed as well as a list of the scientific journals where partners can publish their results and academic research.

Partner's involvement is essential to SPARTA C&D activities and their contribution is established in this deliverable. Tools to monitor and evaluate C&D activities have been selected as well as a comprehensive structure of management that gathers information from all partners.

Gender and Diversity issues have also been addressed in this deliverable, regarding SPARTA coordinated efforts to promote good diversity practices.

SPARTA Communication and Dissemination plan provides a strategic basis for the development of successful C&D activities.

## Chapter 7 List of Abbreviations

Abbreviation	Translation
C&D	Communication and Dissemination
ORs	Outermost Regions
STEM	Science, Technology, Engineering, Mathematics
SVN	Subversion
WiTEC	Women in Science, Engineering and Technology

## Chapter 8 Bibliography

- [1] Ec.europa.eu. (2019). [online] Available at: [http://ec.europa.eu/research/participants/data/ref/h2020/grants\\_manual/amga/h2020-amga\\_en.pdf#page=277](http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/amga/h2020-amga_en.pdf#page=277) [Accessed 7 Apr. 2019].
- [2] Communicating EU research & innovation. (2012). Luxembourg: Publ. Off. of the European Union.
- [3] Armand-Delille, J. (2006). Managing and communicating cultural diversity. *The IABC handbook of organizational communication*, 178.
- [4] Barton, Paul (2016). Choosing the right channels. *Maximizing Internal Communication: Strategies to turn heads, win hearts, engage employees and get results*. Cap. 4
- [5] Okoro, E. A., & Washington, M. C. (2012). Workforce diversity and organizational communication: Analysis of human capital performance and productivity. *Journal of Diversity Management (Online)*, 7(1), 57.
- [6] Ec.europa.eu. (2019). [online] Available at: [https://ec.europa.eu/regional\\_policy/sources/policy/themes/outermost-regions/pdf/rup\\_2017/rup\\_eu\\_lands\\_world\\_en.pdf](https://ec.europa.eu/regional_policy/sources/policy/themes/outermost-regions/pdf/rup_2017/rup_eu_lands_world_en.pdf) [Accessed 9 Apr. 2019].

## Chapter 9 Annexes

### 9.1 Annex I: Template of attendance list

#### Dissemination and Communication Monitoring Events



Attendee	Name	Gender (F/M)	Email *	Filiation
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				

\*(If you would like to be part of our mailing list, please provide your email in the list above)



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

## 9.2 Annex II: Template for monitoring events

### Dissemination and Communication Monitoring Events

Type

- ☐ Conferences
 ☐ Workshops
 ☐ Trade Shows  
☐ Exhibitions
 ☐ Public Event.
 ☐ Public Forums  
☐ Private Forums
 ☐ Meetings
 ☐ Other \_\_\_\_\_

Name of Event: \_\_\_\_\_

Event Abstract (What is it about? Why? Objective)

\_\_\_\_\_

Who are the participants?

\_\_\_\_\_

What were the results?

\_\_\_\_\_

Number of Attendees

\_\_\_\_\_

Female Representation

\_\_\_\_\_

Did you communicate your event on social media? ☐ Yes ☐ No

If "yes", Where?

☐ LinkedIn
 ☐ Twitter
 ☐ Instagram
 ☐ Facebook

Link

\_\_\_\_\_

Text

\_\_\_\_\_

Likes	Shares	Comments	Reach

Did you tell the media? ☐ Yes ☐ No If "yes", who? \_\_\_\_\_

Link to Publication. \_\_\_\_\_

Don't forget to Tag Sparta when you post on social media!