**D8.1**

**Initial results of the clustering, platforms, and ecosystems activities**

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

|  |  |
| --- | --- |
| ****Deliverable type**** | **Demonstrator** |
| ****Deliverable reference number**** | **SU-ICT-03-830892 / D8.1/ DRAFT** |
| ****Work package contributing to the deliverable**** | **WP8** |
| ****Due date**** | **DEC 2019 – MNN** |
| ****Actual submission date**** | **<Filled in by the Coordinator>** |

|  |  |
| --- | --- |
| ****Responsible organisation**** | **CNR** |
| ****Editor**** | **Fabio Martinelli** |
| ****Dissemination level**** | **PU** |
| ****Revision**** | **DRAFT** |

|  |  |
| --- | --- |
| ****Abstract**** | **< Add your abstract / short summary (mandatory!). Proposed length: 2-4 sentences. >** |
| ****Keywords**** | **Clustering, community building, Joint Competence Centre Infrastructure, national hubs** |

**Editor**

Fabio Martinelli (CNR)

**Contributors**

<name>, <name> (CEA)

<name>, <name> (CESNET)

<name>, <name> (TUM)

<name>, <name> (UBO)

<name>, <name> (UKON)

<name>, <name> (TEC)

<name>, <name> (VICOM)

<name>, <name> (INRIA)

<name>, <name> (YWH)

Fabio Martinelli, Artsiom Yautsiukhin (CNR)

<name>, <name> (L3CE)

<name>, <name> (SMILE)

<name>, <name> (NASK)

<name>, <name> (INOV)

**Reviewers**

Florent Kirchner (CEA)

Ana Ayerbe Fernandez-Custa (TEC)

**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

< Shall include a summary of the content of the deliverable and main conclusions. The aim of the executive summary is simply to entice the reader to read the complete document. Recommended length of ½ to 1 page! >

<fill in>

Table of Content

[2.1 Purpose 9](#_Toc28433081)

[2.2 JCCI components 9](#_Toc28433082)

[2.2.1 WorkBench 9](#_Toc28433083)

[2.2.2 Virtual Learning Centre 10](#_Toc28433084)

[2.2.3 Cyber Range 10](#_Toc28433085)

[2.3 Tentative usage workflow 12](#_Toc28433086)

[2.4 Next steps 13](#_Toc28433087)

[2.4.1 State of the Art 13](#_Toc28433088)

[2.4.2 Hands-on tasks 13](#_Toc28433089)

[2.5 Cyber Range 13](#_Toc28433090)

[3.1 National level 14](#_Toc28433091)

[3.1.1 France (CEA) 14](#_Toc28433092)

[3.1.1.1 Current status 14](#_Toc28433093)

[3.1.1.2 SPARTA’s actions 15](#_Toc28433094)

[3.1.1.3 Future activities 15](#_Toc28433095)

[3.1.2 Belgium (CETIC) 15](#_Toc28433096)

[3.1.2.1 Current status 15](#_Toc28433097)

[3.1.2.2 SPARTA’s actions 16](#_Toc28433098)

[3.1.2.3 Future activities 16](#_Toc28433099)

[3.1.3 Greece (KEMEA) 16](#_Toc28433100)

[3.1.3.1 Current status 16](#_Toc28433101)

[3.1.3.2 SPARTA’s actions 16](#_Toc28433102)

[3.1.3.3 Future activities 16](#_Toc28433103)

[3.1.4 Austria (Joanneum) 16](#_Toc28433104)

[3.1.4.1 Current status 16](#_Toc28433105)

[3.1.4.2 SPARTA’s actions 16](#_Toc28433106)

[3.1.4.3 Future activities 17](#_Toc28433107)

[3.1.5 Poland (NASK) 17](#_Toc28433108)

[3.1.5.1 Current status 17](#_Toc28433109)

[3.1.5.2 SPARTA’s actions 17](#_Toc28433110)

[3.1.5.3 Future activities 18](#_Toc28433111)

[3.1.6 Germany (TUM) 18](#_Toc28433112)

[3.1.6.1 Current status 18](#_Toc28433113)

[3.1.6.2 SPARTA’s actions 18](#_Toc28433114)

[3.1.6.3 Future activities 19](#_Toc28433115)

[3.1.7 Czech Republic (CSNET) 19](#_Toc28433116)

[3.1.7.1 Current status 19](#_Toc28433117)

[3.1.7.2 SPARTA’s actions 19](#_Toc28433118)

[3.1.7.3 Future activities 19](#_Toc28433119)

[3.1.8 Lithuania (L3C) 19](#_Toc28433120)

[3.1.8.1 Current status 20](#_Toc28433121)

[3.1.8.2 SPARTA’s actions 20](#_Toc28433122)

[3.1.8.3 Future activities 20](#_Toc28433123)

[3.1.9 Spain (TECNALIA) 20](#_Toc28433124)

[3.1.9.1 Current status 20](#_Toc28433125)

[3.1.9.2 SPARTA’s actions 22](#_Toc28433126)

[3.1.9.3 Future activities 23](#_Toc28433127)

[3.1.10 Luxemburg (CIRC) 24](#_Toc28433128)

[3.1.10.1 Current status 24](#_Toc28433129)

[3.1.10.2 SPARTA’s actions 25](#_Toc28433130)

[3.1.10.3 Future activities 25](#_Toc28433131)

[3.1.11 Portugal (INOV) 25](#_Toc28433132)

[3.1.11.1 Current status 25](#_Toc28433133)

[3.1.11.2 SPARTA’s actions 26](#_Toc28433134)

[3.1.11.3 Future activities 26](#_Toc28433135)

[3.1.12 Latvia 26](#_Toc28433136)

[3.1.12.1 Current status 26](#_Toc28433137)

[3.1.12.2 SPARTA’s actions 26](#_Toc28433138)

[3.1.12.3 Future activities 26](#_Toc28433139)

[3.1.13 Italy (CNR,CINI) 26](#_Toc28433140)

[3.1.13.1 Current status 26](#_Toc28433141)

[3.1.13.2 SPARTA’s actions 27](#_Toc28433142)

[3.1.13.3 Future activities 27](#_Toc28433143)

[3.1.14 Estonia (UTARTU) 27](#_Toc28433144)

[3.1.14.1 Current status 27](#_Toc28433145)

[3.1.14.2 SPARTA’s actions 27](#_Toc28433146)

[3.1.14.3 Future activities 27](#_Toc28433147)

[3.1.15 Summary Table [ALL] 27](#_Toc28433148)

[3.2 European level 28](#_Toc28433149)

[3.3 Specific cooperation with EU projects [ALL partners] 29](#_Toc28433150)

[3.3.1 NECS 29](#_Toc28433151)

[3.3.2 StandICT 30](#_Toc28433152)

[3.3.3 SAPPAN 31](#_Toc28433153)

[3.4 Monthly workshops 31](#_Toc28433154)

[3.4.1 SPARTA Workshop in Madrid, Mundo Hacker 31](#_Toc28433155)

[3.4.2 SPARTA Workshop in León, Mundo Hacker 33](#_Toc28433156)

[5.1 Organisations 39](#_Toc28433157)

[5.1.1 ECSO 39](#_Toc28433158)

[5.1.2 ENISA 39](#_Toc28433159)

[5.2 EU Projects 39](#_Toc28433160)

[5.2.1 Cyberwatching 39](#_Toc28433161)

[5.2.2 Aegis 40](#_Toc28433162)

[5.2.3 EUnity 40](#_Toc28433163)

List of Figures

[Figure 1. Components of the Joint Cybersecurity Center Infrastructure. 7](#_Toc27998923)

[Figure 2. Conceptual draft of usage workflow. IdP = identity provider, SDL = service description language. 10](#_Toc27998924)

[Figure 3. Example draft of a list of available resources on the web app. 10](#_Toc27998925)

[Figure 4. Expanded details of an available resource. 11](#_Toc27998926)

[Figure 1: Agenda of the SPARTA workshop in León (Spain) 28](#_Toc27998927)

List of Tables

[Table 1: Example table 3](#_Toc467844844)

< the document editor can decide whether to keep the “List of Figures” and “List of Tables” or not; generally we would recommend to *keep it* since it helps the reader to grab figures and tables fast and easily on the one hand and it helps us to maintain a “common look” within all deliverables on the other hand >

# Introduction

<text>

# Joint Competence Centre Infrastructure [VICOM]

## Purpose

One of the objectives for SPARTA is to strengthen cybersecurity capabilities across the EU and closing the cyber-skills gap. In order to boost fundamental capacities and to lower the said skill gap, the Joint Competence Center Infrastructure (onwards, JCCI) will offer leverage and horizontal domain synergies among organizations. The idea for JCCI is to become a reference location for companies and also a research experimentation platform. Start-ups and SMEs will have infrastructure and technologies available through a catalogue, managed by local clusters and authorities.

## JCCI components

The JCCI will be formed by 3 main components: a workbench for a shared and distributed testbed where computation and communication resources can be shared, a virtual learning center to share and spread knowledge for learning purposes, and a federated cyber range with different scenarios to gain skills in cyber-attacks and defenses (Figure 1). The different components will consist of integrations of existing means of SPARTA partners, but clustered and available through a web application that will either give direct access or will redirect to the corresponding access site. The aim of the JCCI would be to ease collaboration among them and to allow external organizations to access these shared facilities.

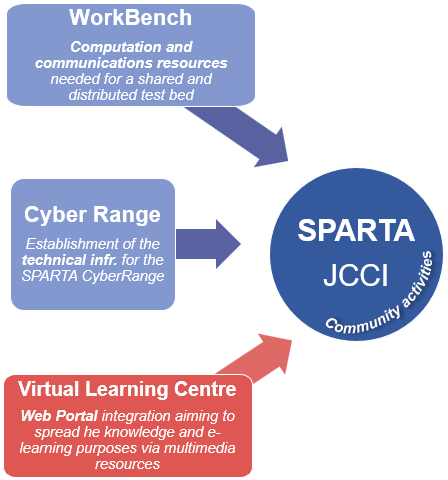


Figure 1. Components of the Joint Cybersecurity Center Infrastructure.

### WorkBench

The WorkBench will gather computation and communication resources needed for a shared and distributed test bed. As mentioned before, the WorkBench will be a compound of already existing assets from the partners, and they will be offered through a common platform. So far, **13 partners have contributed 25 assets’ information** to the common asset inventory. For that, a document template was prepared with specific parameters that each partner had to fill in about the resources they owned, and how they could be shared and utilized by others. Among these assets, there are solutions for co-creation processes, secure hosting/storage, collaborative platforms, large scale experimentation equipment, intrusion detection systems, cyber-incident detection, monitoring systems, standards compliance, benchmarking, evaluation/certification, etc. Moreover, partners have contributed extensive information about their computing equipment. The integrated document can be found in Annex.

### Virtual Learning Centre

The Virtual Learning Centre will be a web portal integration aiming to spread the knowledge and e-learning purposes via multimedia resources. This will be available through a web portal, either openly or with specific requirements for access. These requirements will be detailed in the web application on the details area.

So far, **6 partners** have contributed their learning contents to the common learning catalogue. For that, a document template was prepared with specific parameters that each partner had to fill in about the learning resources they owned, and how they could be shared and utilized by others. Among the learning contents, there are online courses, in-person courses, hackathons, competitions and practical courses, which will offer a variety of resources available to share or access under certain conditions.

This integrated document can be found in Annex. The catalogue will be expanded as more contributions are gathered in the following action steps.

### Cyber Range

Based on the asset inventories from Section 2.1, and once the WorkBench is outlined, it will be possible to select a subset of the testbed to be included in the cyber-range of SPARTA. These already existing cyber-range facilities will be united in a federated and distributed way. Moreover, based on the hands-on section of the Virtual Learning Center, different scenarios will be built for cyber-range training. So far, these testbeds have been pre-selected for the CyberRange: VICOM’s Secure Industry 4.0 and **TECNALIA´s Smart Grid Facilities, Industrial Blockchain Facilities, Automotive Cybersecurity Facilities and Cyber Range Facilities, and the KYPO cyber-range.**

**A quick summarized overview of all contributed assets and learning contents can be seen on** Table 1**.**

Table 1. Contributed assets and learning contents from partners.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Partner** | **Assets for workbench** | **Keywords** | **Learning contents** | **Cyber-range?** |
| L3CE | SENTER | Center of excellence | - |  |
| INRIA | LHS NGE | Data collection, secure hosting/storage, large-scale experimentation | 4 online courses |  |
| LHS RBA | HW security evaluation, ransomware IDS |
| TEC | IDSOTER | IDPS, electrical network and equipment | 5 in-person courses | ✓ |
| OPENCERT | Assurance cases, Standards Compliance, Assurance Accountability, GSN |
| SABOTAGE | Fault Injection, Simulation, Safety |
| Smart Grid Facilities | Machine Learning, Honeypots |
| Industrial Blockchain Facilities | DLT, blockchain |
| Automotive Cybersecurity Facilities | ECUs, V2V, V2I |
| INOV | BP-IDS | **Intrusion detection, Incident detection, business processes** | - |  |
| CESNET | Nemea | **Flow traffic analysis, network monitoring** | 1 CTF competition |  |
| IPFIXcol | **Flow record collector** |
| Warden | **Network security, event sharing, platform** |
| NERD | **Network entity reputation DB** |
| LIST | Node in Infrachain Blockchain | **Blockchain, smart contracts** | - |  |
| UKON | Visual Computing Center for Cibersecurity | Powerwall, Control Room, Machine Learning Infrastructure | 1 visual analytics competition |  |
| UBO | IT-Security Awareness Pentesting Framework | **Employee awareness assessment, Intrusion Detection, Phishing** | - |  |
| TUM | Malware Zoo | **Large-Scale Malware Analysis** | 4 in-person courses |  |
| LEO | Cyberthreat Intelligence Services | **Vulnerability detection, attack detection, monitoring, Darknet, real-time analysis, Fraud detection** | - |  |
| Intelligence enabled Next Gen SOC | **Security operation center, dynamic risk assessment** |
| Security Evaluation Facility | Security evaluation |
| CNR | Cybersecurity Osservatorio | **Cyber threats, risk assessment, malware detection, CVE, CWE, spam analysis, security reports** | - |  |
| JR | CTTC | **Data collection, data analysis, IoT security, intrusion detection, APT** | - |  |
| CEA | - | - | 3 in-person courses, 1 hackathon |  |
| VICOM | Secure Industry 4.0 | Equipment and process monitoring, flexible robotics, big data analytics | - | ✓ |
| KYPO | - | - | - | ✓ |

## Tentative usage workflow

As mentioned, the three components of the JCCI will be available through a web application that can be accessed by any organization. A first conceptual draft of how the usage workflow will be can be found on Figure 2. Different customers (either partners or external organizations) could access a list of all available resources. This index would be available through SDLs that would return the existing labs and learning equipment, contents and datasets, as well as workbench resources and how to access them. These could either be directly accessed or the site would redirect the organization to the corresponding place.

When requested, the list of available resources could appear with just a few hints of what is available. These could be filtered by different parameters or tags, and a button for either directly downloading or requesting access to the resource (Figure 3). Then, a particular entity from the list could be expanded when clicking on it (Figure 4).

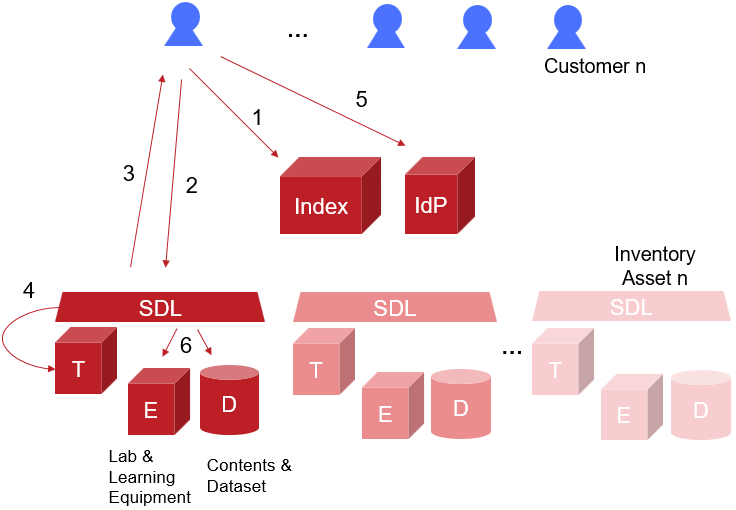


Figure 2. Conceptual draft of usage workflow. IdP = identity provider, SDL = service description language.

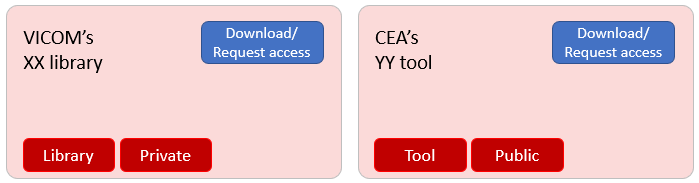


Figure 3. Example draft of a list of available resources on the web app.

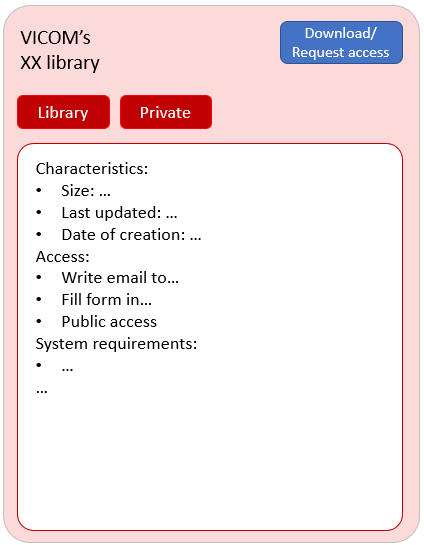


Figure 4. Expanded details of an available resource.

## Next steps

For steering the creation of the SPARTA JCCI, our tentative next steps are:

### State of the Art

In order to consider some possible solutions or approaches for our final goal, firstly an overview will be obtained on a few matters:

1. Cybersecurity information sharing protocols (considering CSIRT standards, as information should also be available to them).
2. Best practices for federation mechanisms and their different scopes.
3. Analysis of business models (including ticketing and renting schemes).
4. Analysis of Service Description Languages, considering also the interactivity issue of SDLs.

### Hands-on tasks

Once the state of the art has been reviewed, partners will start building the JCCI by:

1. Analyzing the features of the Asset Inventory:
   1. Characterization of possible common services
   2. Common language for assets definition
   3. Suggested integration levels
2. Selecting and uploading the assets catalogue in a web application as main index.

## Cyber Range

<Report activities related to SPARTA Cyber Range>

# National and European Level Clustering [CNR,ALL]

<The description of the work done on clustering at National and European level during the first 12 months>

## National level

<All partners describe the clustering situation, explaining how they (plan to) use SPARTA for clustering. Describe: current situation, activities done, and desired situation>

### France (CEA)

#### Current status

* **System@tic cluster:** strategic roadmap development and validation, presentation of roadmap to local actors (industry, focus on SME), support to development of SMEs, communication, labelling of project proposals for French national funding schemes to provide additional funding for dedicated specific projects. Link with FUI, FSN and PIA French funding schemes.
* **Image et Réseaux cluster:** strategic roadmap development and validation, presentation of roadmap to local actors (industry, focus on SME), support to development of SMEs, communication, labelling of project proposals for French national funding schemes to provide additional funding for dedicated specific projects.
* **SAFE cluster:** strategic roadmap development and validation, presentation of roadmap to local actors (industry, focus on SME), support to development of SMEs, communication, labelling of project proposals for French national funding schemes to provide additional funding for dedicated specific projects.
* **CNRS**: major host for academic research in joint units with universities or own units (e.g. LAAS), contribution to programmes and research output. The Pré-GDR Security created by « l'Institut des sciences de l’information et de leurs interactions » has launched several working groups to address security-related scientific challenges (secure coding, cryptography, formal methods for security, privacy, multimedia security, network & infrastructures & Software & Systems security)
* **IRT SystemX:** research and demonstration/communication platform, additional funding and hosting for dedicated specific projects and/or teams for collaborative work. Link with ANR funding schemes.
* **Ile de France region:** for additional funding of specific programmes, with a focus on PhDs. Dissemination and communication, and economic development at the regional level.
* **Brittany region:** for additional funding of specific programmes, with a focus on PhDs. Dissemination and communication, and economic development at the regional level
* **Pole d’Excellence Cyber:** for additional funding of specific programmes, with a focus on PhDs. Dissemination and communication, and economic development at the regional level. Link with the military ecosystems and the French military procurement agency.
* **Direction Générale de l’Armement (DGA) :** for additional funding of specific programmes, with a focus on PhDs. Link with the military ecosystem, both for research and use, and large development programmes. Link with RAPID and ASTRID French funding schemes.
* **COFIS**:
* **ACN**:
* **Hexatrust**:
* **ARCSI**:

#### SPARTA’s actions

SPARTA project has established contact with the following organisations to establish the national cluster for France:

|  |
| --- |
| * Paris Region |
| * AdaCore |
| * PEC |
| * Brittany Region |
| * CAN |
| * Systematic |
| * Irisa |
| * Loria |
| * Cybersecurity Institute, univ Grenoble Alpes |
| * LAAS |
| * Quarkslab |
| * AMOSSYS |
| * Region Bretagne |
| We have already received a sign of interest in joining SPARTA from:   * Montimage |

#### Future activities

### Belgium (CETIC)

#### Current status

In Belgium network cybersecurity is overseen by the Centre for Cybersecurity Belgium (CCB). CCB is the central authority for cybersecurity in Belgium and manages the Computer Emergency Response Team (CERT) for the purpose of carrying out activities relating to the detection, observation and analysis of online security problems. CCB has the following network related responsibilities:

* Monitoring, coordinating and supervising the implementation of Belgian cyber security;
* Managing the various projects on the topic of cybersecurity using an integrated and centralized approach;
* Ensuring coordination between the relevant government departments and governments, as well as the public authorities and the private or scientific sectors;
* Formulating proposals aimed at adapting the regulatory framework in the field of cybersecurity;
* Ensuring crisis management in case of cyber incidents in cooperation with the government's Coordination and Crisis Centre;
* Preparing, disseminating and supervising the implementation of standards, guidelines and security standards for the various information systems of the governments and public institutions;
* Coordinating the Belgian representation in international cybersecurity forums, coordinating the monitoring of international commitments and national proposals on this subject;
* Coordinating the security evaluation and certification information and communication systems;
* Informing and raising awareness among users on information and communication systems.

CERT.be is as a neutral specialist in Internet and network security that is responsible for:

* coordination in the event of cyber incidents;
* advice about finding a solution when cyber incidents arise;
* support to prevent these security incidents occurring

In the Walloon Region of Belgium the "Agence du Numérique", responsible for digital public policy, is preparing a cybersecurity label for SME based on CIS 20 controls and the NIST cybersecurity framework version 1.1. Although the cybersecurity label is very general, some of the CIS 20 controls are network related such as "limitation and control of network ports, protocols ans services", "secure configuration for network devices such as firewalls, routers and switches", or "wireless access control".

#### SPARTA’s actions

SPARTA project has established contact with the following organisations to establish the national cluster for Belgium:

|  |  |  |  |
| --- | --- | --- | --- |
| |  | | --- | | * CCB | | * INFOPOLE Cluster TIC | | We have already received a sign of interest in joining SPARTA from:   * Dynsecu | |

#### Future activities

### Greece (KEMEA)

#### Current status

In Greece thus far, there isn’t a well-established cyber security network with long standing tradition on the topic. The main effort is the Greek Cybercrime Centre, (www.cybercc.gr/en/), is a DG-HOME funded project aimed primarily at improving research and education, which is maintained by Center for Security Studies and Hellenic Police. The objectives of GCC are to i) advance cyber security training and University education in Greece, ii) improve research in focused areas of cyber security and crime, iii) mobilize the Greek constituency in the area of cyber security and crime and iv) collaborate with similar centres so as to maximize the uptake of the results. Also OWASP Chapter of Greece provides a network on software security. Furthermore, there are several ad-hoc networking activities in the form of Annual Cyber deference national exercise “PANOPTIS”, the KEMEA annual conference on CI protection, and the Hellenic Team of European Cyber Security Challenge. Furthermore, there are several ICT oriented Clusters and Associations that include cyber security but not as a core business. One could quote the Maritime Center of Excellence – Strategis, the Hellenic Semiconductor Industry Association, Hellenic Association of Space Industry, Hellenic Emerging Technologies Industry Association (HETIA) and Hellenic Association of Mobile Applications Companies (HAMAC) that have members in the cyber-security domain, as the ICT clusters Technopolis of Thessaloniki Business Park and si-Cluster gi-Cluster in Athens.

#### SPARTA’s actions

SPARTA project has established contact with the following organisations to establish the national cluster for Greece:

|  |  |
| --- | --- |
| |  | | --- | | * N/A | |

#### Future activities

### Austria (Joanneum)

#### Current status

#### SPARTA’s actions

SPARTA project has established contact with the following organisations to establish the national cluster for Austria:

|  |  |
| --- | --- |
| |  | | --- | | * Bundeskanzleramt * MoD Austria   We have already received a sign of interest in joining SPARTA from:   * BMI | |

#### Future activities

### Poland (NASK)

#### Current status

The key objective of National Framework of Cybersecurity Policy of the Republic of Poland

is to expand the national cybersecurity system and ensure a consistent approach taken across the Republic of Poland. National Framework of Cybersecurity Policy requires involvement of

different actors who are either public sector, telecommunications sector as well as Trust Service Providers, Competent ministers responsible for preparing proposals of legal changes in the field of cybersecurity.

Development of the cybersecurity system at the national level also entails the further

development of structures dealing with cybersecurity at the operational level, including the

National Cybersecurity Centre (NC Cyber), the CSIRT at national level, sectoral incident response teams (sectoral CSIRT), information exchange and analysis centres (ISAC). To make these developments possible the Government introduced new legislation setting out the revised competencies of the relevant institutions. In particular they will be amending the role of NC Cyber and the CSIRT capabilities at the national level.

In the framework of cooperation between the national government administration and the local government administration, the national government strongly supports development of security clusters:

**CERT Polska (**<https://www.cert.pl/en/>) The team operates within the structures of NASK (Research and Academic Computer Network) — a research institute which conducts scientific studies, operates the national .pl domain registry and provides advanced IT services. Since its launch, the core of the team’s activity has been handling security incidents and cooperation with similar units worldwide. CERT Polska also conducts extensive security-related R&D.

**Poznan Supercomputing and Networking Center (PSNC)** <http://www.man.poznan.pl/online/en/>. Since 1993 integrating and developing the information infrastructure for science has been the mission of Poznan Supercomputing and Networking Center (PSNC) affiliated with the Institute of Bioorganic Chemistry at the Polish Academy of Sciences.

**CYBERSEC HUB** (<http://cybersechub.eu/>) is network of integrated activities supporting and promoting companies in Malopolska Region from cybersecurity sector

#### SPARTA’s actions

SPARTA project has established contact with the following organisations to establish the national cluster for Poland:

|  |  |
| --- | --- |
| |  | | --- | | * AGH * ENERGA Group * The John Paul II Hospital in Krakow * PKP Informatyka   We have already received a sign of interest in joining SPARTA from: | |

#### Future activities

### Germany (TUM)

#### Current status

In Germany there are multiple competence centers for cybersecurity, with activities in a wide range of research topics. For instance, Center for  Research in Security and Privacy (CRISP) has a core topic "Security  at Large", focusing on security of large  systems consisting of multiple interacting components. They bring  together experts from multiple areas: engineering, philosophy, physics,  psychology, law and economics through interdisciplinary projects. CISPA Helmholtz Center in Saarbruecken combines theoretical topics with innovative application-oriented research  projects in cybersecurity and privacy.  Some of their core research  topics are: Secure and Privacy-Friendly Information Processing, Threat  Detection and Defenses, Secure Mobile and Autonomous  Systems and Empirical and Behavioral Security. Furthermore, this Center  has an additional focus on technology transfer and societal outreach.  In addition, Competence Center for Applied Security Technology (KASTEL) addresses security problems of the interconnected systems under a motto "Comprehensible security in the networked world".  Their goal is to "develop a widespread approach instead of isolated  partial solutions". This network pays special attention to critical infrastructures, such as industrial production, energy and networked mobility.

Still there are already a lot of cybersecurity efforts located in the Munich area that aim to connect academic research (institutions) with industrial partners or provide consulting services in case of cybersecurity related incidences (incident response):

* The Munich Competence Center for IT-Security (Münchner Sicherheitsnetzwerk) coordinates a lot of (around 100) global and local partner companies and research institutions located in the metropolitan area around Munich.
* Platform for Cybersecuriy of the Zentrum Digitalisierung Bayern (ZD.B), a Bavarian cooperation- and research network, funded by the Bavarian government. The goal is to support different projects between industry, research and governmental partners. An additional goal of ZD.B is to fund and support young scientists.
* WG Security of the "Münchner Kreis" connects even more organizations and enterprises spread around Germany.
* The Bavarian Landesamt für Sicherheit in der Informationstechnik (LSI) aims to protect and defend governmental IT infrastructures and acts as a council in case of security breaches of local authorities.
* ZITIS (Zentrale Stelle für Informationstechnik im Sicherheitsbereich) aims to enable law enforcement to use and enhance their technical capabilities to defend against cybercrime and cyberespionage. ZITIS is a branch of the German Federal Ministry of the Interior.
* CODE, a research institution for cyber defense located at the university of armed forces in Munich that aims to fund 12 new professorships.

In summary, Munich already is a strong security hub within Germany providing a strong network for not only academia and industry, but also for public authorities (with ZITIS and the LSI).

#### SPARTA’s actions

SPARTA project has established contact with the following organisations to establish the national cluster for Germany:

|  |  |
| --- | --- |
| |  | | --- | | * Bitkom * ASW Bundesverband * KASTEL * IHK Bonn/Rhein-Sieg * ZD.B * T-Systems * City of Bonn * BSI * Cyber Security Cluster Bonn e.V.   We have already received a sign of interest in joining SPARTA from:   * UNIVERSUM Business GmbH | |

#### Future activities

### Czech Republic (CSNET)

#### Current status

Cybersecurity networking in Czech Republic appears and is being developed at several levels. At the national and governmental level, the Czech Republic’s National Cyber Security Strategy and the associated Action Plan were drafted by the Czech National Security Authority (NSA) and adopted by the Government in 2015. Both cover the years 2015 to 2020. CERT & CSIRT Capacity Building Strategy defined in the Action Plan 2015-2020 propose enhancement of all relevant structures, processes, and of cooperation in ensuring cyber security and in developing an effective cooperation model at the national level among the cyber security actors – CERT and CSIRT teams. Namely, the most relevant teams, the CSIRT.CZ (operated by CZ.NIC) and govCERT.CZ (operated by NCISA) establish various partnerships with academic as well as industrial partners (e.g. Microsoft, Cisco) via Memoranda of understanding or via joint projects. Building of national competence centres is also supported by the Czech governement through Technology Agency of the Czech Republic and the Security Research Program of the Ministry of the Interior. At the industrial level, there exist Czech ICT alliance and ICT union, however these consortia cover whole ICT and do not specifically focus on cybersecurity.

The only private cyber security cluster operates through the Network Security Monitoring Cluster (NSM Cluster; <http://www.nsmcluster.com/en/>) covering the region of South Moravia.

At the academic level, CESNET acts as a common platform were various research centres and universities meet and cooperate on joint cybersecurity projects utilizing their specific competences. In parallel to the above levels, various cybersecurity players meet at the local cybersecurity conferences such as C2S2, QuBit, ISS world.

#### SPARTA’s actions

SPARTA project has established contact with the following organisations to establish the national cluster for Czech Republic:

|  |  |
| --- | --- |
| |  | | --- | | * AT&T   We have already received a sign of interest in joining SPARTA from:   * NÚKIB * Státní pokladna Centrum sdílených služeb, s. p. | |

#### Future activities

### Lithuania (L3C)

#### Current status

Lithuania is currently in the process of developing a national cybersecurity strategy under the lead of the Prime Minister’s Office and the Ministry of National Defence (MoND). Until now, Lithuania has undertaken several steps to enhance national strategic capacity to manage cybersecurity, such as the Programme for the Development of Electronic Information Security (Cyber-Security) for 2011–2019. Lithuania’s incident response capacity is at an establishedstage of maturity and is on the verge of reaching the strategicstage. The government developed the National Lithuanian Computer Emergency Response Team (CERT-LT) in 2008. **CERT-LT (**<https://www.nksc.lt>) coordinates and collaborates with sub national/sectorial/international incident-response organizations and reports to the relevant responsible authorities. The National Cybersecurity Centre (NCSC), developed recently under the auspices of the MoND, undertakes cyber incident management, acts as an information sharing platform and publishes vulnerabilities and related legal measures.

**Lithuanian Research and Education Network (LITNET)** (<https://www.litnet.lt/lt/>)

connects computer networks of all research, study and education institutions of Lithuania. LITNET CERT is the Computer Emergency Response Team of LITNET, targeting the fields of computer security incident response, forensics, detection and prevention and is devoted to attracting and retaining successful and responsible development to provide novel technology solutions to target groups.

INFOBALT association is a locally and internationally recognized representative of Lithuanian ICT industry. INFOBALT Cyber Security Committee organizes and coordinates the activities of the Lithuanian ICT companies in the field of cyber security.

#### SPARTA’s actions

SPARTA project has established contact with the following organisations to establish the national cluster for Lithuania:

|  |  |
| --- | --- |
| |  | | --- | | * INFOBALT * NCSC (under Ministry of National Defence Republic of Lithuania) * Strategic Communications Department (Lithuanian Armed Forces) * JSC "Lithuanian Railways" * LITNET CERT   We have already received a sign of interest in joining SPARTA from: | |

#### Future activities

### Spain (TECNALIA)

#### Current status

Spain counts since 2013 with the National Cybersecurity Strategy that provides a basis for developing the provisions of the National Security Strategy (reviewed in 2017) on the protection of cyberspace in order to implement cyber threat prevention defence, detection, response and recovery actions against cyber threats.

The [National Security Strategy 2017](https://www.dsn.gob.es/sites/dsn/files/2017_Spanish_National_Security_Strategy_0.pdf) has consolidated the fact that cyber security must have a differential and own space, taking into account both the impact of the digitalization as an engine of change with implications for cybersecurity beyond the field only the technological Heritage into the political, economic and social, such as the nature of cyberspace as a vector of strategic communication, that can be used to influence public opinion and in the thinking of people through the manipulation of information, misinformation campaigns or actions of hybrid nature. The Strategy sets a new framework, with five general goals running across all fields. Crisis management, National Security Culture, global common spaces, technological development and international projection for Spain shape a strategic grid where cybersecurity is used to open up new paths leading to Spain’s present and future security model.

The [National Cybersecurity strategy 2019](https://www.dsn.gob.es/es/file/2989/download?token=EuVy2lNr) published in the BOE 30 April 2019 develops forecasts of the National Security Strategy 2017 in the field of cyber security, according to the general objectives, the target of area of cybersecurity and lines of action set to achieve this. Responds well to the mandate of the National security council of 16 July 2018 published in the BOE 10 August.

The overall objective is to ensure the safe use and reliable of cyberspace in Spain, protecting the rights and freedoms of citizens and promoting economic partner progress. Further objectives are:

* security and resilience of networks and information and communications systems of the public sector and essential services
* safe and reliable use of cyberspace against illicit or malicious use
* protection of business and social ecosystem and citizens
* culture and commitment to cyber security and empowerment of the human and technological capacities
* security of cyberspace in the international arena.

The document is structured in five chapters:

* **Cyberspace**, beyond a common global space, which provides an overview of the scope of cybersecurity, the progress made in this area since the adoption of the 2013 Strategy, the reasons which support the development of the 2019 National Cybersecurity Strategy, as well as the main features which drive its development.
* The **threats and challenges in cyberspace**, it determines the main threats to cyberspace which derive from its status as a common global space, the high level of technology and the great connectivity that makes it possible to amplify the impact of any attack.
* **Purpose, principles and objectives for cybersecurity**, it applies the guiding principles of National Security Strategy 2017 (Unity of Action, Anticipation, Efficiency and Resilience) to five specific objectives.
* **Lines of action and measures**, where seven lines of action are established and the measures for the development of each of them identified: (1) strengthen capabilities to deal with threats from cyberspace; (2) guarantee security and resilience for Spain’s strategic assets; (3) reinforce capabilities for investigation and prosecution of cybercrime, to guarantee citizen security and protect rights and freedoms in cyberspace; (4) boost cybersecurity for citizens and companies; (5) Strengthen the Spanish cybersecurity industry and its capacity to nurture and retain talent, to bolster digital autonomy; (6) contribute to cyberspace security internationally, promoting open, plural, secure and trustworthy cyberspace, supporting national interests; and (7) Develop a cybersecurity culture.
* **Cybersecurity in the National Security System**, it defines the organic architecture of cybersecurity. Under the direction of the President of the Government, the structure is composed of three organs: the *National Security Council*, as the Government's Delegate Commission for National Security; the *National Cybersecurity Council*, which supports the National Security Council and assists the President of the Government in the direction and coordination of national security policy in the area of cybersecurity, and fosters relations of coordination, collaboration and cooperation between public administrations and between these and the private sector, and the *Situation Committee* which, with the support of the National Security Department, will support the management of crisis situations in any area which, due to their transversality or dimension, exceed the response capacities of the usual mechanisms.

Concerning the **Spanish Cyber Security Ecosystem,** it´s mainly formed by:

* [**INCIBE**](https://www.incibe.es/en)as the **Cyber Security National Institute** works in public-private policy initiatives to raise cybersecurity levels in Spain, the follow-up and review of emergent risks in order to be able to anticipate needs, adopt pre-emptive measures and have recourse to early warning mechanisms.
* The [**National Center for the Protection of Infrastructures and Cybersecurity**](http://www.cnpic.es/en/index.html) **(CNPIC)** is the organism in charge of promoting, coordinating and supervising all critical infrastructure protection-related activities for which the Secretariat of State for Security is competent at national level.
* The [**INCIBE-CERT**](https://www.incibe-cert.es/en) is the National CERT responsible for the prevention and mitigation of, and the response to, cyber-incidents in the corporate, citizen and critical infrastructure operator spheres. In the case of incident management affecting critical private sector operators, INCIBE-CERT is jointly operated by INCIBE and CNPIC, the National Center for Infrastructure Protection and Cybersecurity of the Ministry of the Interior. INCIBE-CERT is one of the reference incident response teams that coordinates with the rest of the national and international teams to improve the efficiency in the fight against crimes involving networks and information systems, reducing their effects on public security
* The **CCN-CERT** is the **Information Security Incident Response Team** of the [**National Cryptologic Centre, CCN**](https://www.ccn.cni.es/), accountable to the [**Spanish National Intelligence Centre (CNI**](https://www.cni.es/)**)**, to ensure protection from cyber-attacks on classified systems and systems belonging to Public Administrations, and to companies and organizations of strategic interest (those essential for Spanish security and economy).
* TheSpanish [Network of Excellence on Cybersecurity Research](https://www.renic.es/es) **(RENIC)** is a membership based sectoral association that includes research centres and other agents of the research cybersecurity ecosystem in Spain. RENIC mainly aims to promote scientific research, technological development, innovation, knowledge and technology transference to industry and the development of R&D in the field of cybersecurity in Spain.
* The Spanish[Cybersecurity Innovation Cluster](https://www.clustercollaboration.eu/cluster-organisations/aei-ciberseguridad-y-tecnologias-avanzadas) **(AEI Ciberseguridad y Tecnologías Avanzadas)** brings together companies, research centres, universities, public and other private organizations interested in promoting new technologies in the industrial sector and other related stakeholders, wishing to contribute to the objectives of the Association regarding Security Technologies, at national and international level.
* The ecosystem is completed with regional agencies like the [Basque Cybersecurity Center](https://www.basquecybersecurity.eus/en/)in the Basque Country whose objective is to generate a culture of cybersecurity in the Basque Country.

#### SPARTA’s actions

SPARTA project has established contact with the following organisations to establish the national cluster for Spain:

|  |  |
| --- | --- |
| |  | | --- | | * AEI Ciberseguridad * SPRI * INCIBE * Ingeteam * Schneider Electric * CCI * Arteche * PESI * Ertzaintza * Cluster Energia * Mondragon * Atos * BCSC * IKERLAN   We have already received a sign of interest in joining SPARTA from:   * GRADIANT | |

#### Future activities

The following companies have been identified as potential members of the SPARTA Partnership program:

* S21SEC
* ACCENTURE
* CSIC
* Universidad de Granada
* Universidad Politécnica de Madrid
* Universidad de la Laguna
* ITS
* EUROCYBCAR
* IDIADA
* NATURGY
* Panda Security
* Universidad de León
* Innotec - Entelgy
* CounterCraft
* Enigmedia
* CITIC
* IMDEA Software
* Universidad Carlos III de Madrid
* Universidad de Castilla La Mancha
* Universidad de Vigo
* Universidad Rey Juan Carlos
* S2 Grupo
* SGSS
* APPLUS-LGAI o IDIADA
* GMV
* Bit4id
* ClilckAlba
* Integrasys
* Leet Security
* BBVA
* i2CAT
* Ziur

During the 2020 period, we are planning to implement some collaboration actions at national level. Some workshops will be organized, supported by INCIBE and BCSC, in collaboration with the other CCN pilots (CONCORDIA, CyberSec4Europe and ECHO). Concretely, we are planning to organize 4 wokshops in the Basque Country, León, Catalonia and Galicia.

We will also analyze, together with INCIBE, the possibility to organize a new SPARTA workshop in Spanish Cybersecurity Research Conference (JNIC), Ciudad real, June 2020 (http://2020.jnic.eu) or in any thematic workshops related to Cyber Ranges.

### Luxemburg (CIRC)

#### Current status

In Luxembourg, the cybersecurity ecosystem has radically evolved within the last 20 years, a shift accompanied by the Ministry of the Economy, with a vision of inclusion and access to security services and products for all parties of society. The OECD papers from 2002 [1] as well as the more recent one from 2015 [2] strongly inspired this development.

Today, the Luxembourg cybersecurity ecosystem is dynamic, vibrant and represents a strong diversity of innovative products and services, involving players like public entities, administrations, companies, associations, independents as well as start-ups.

The “Cybersecurity Board (CSB)”, chaired by the Prime Minister and involving all relevant ministries and state bodies, represents the highest level of the Luxembourg cybersecurity public governance. On a strategic level, the “Interministerial Coordination Committee for Cyberprevention and Cybersecurity (CIC-CPCS)” strengthens, sustains and facilitates the implementation of the National Cybersecurity Strategy (the third revision was published in May 2018 [3]).

The responsible for security of government, public entities and operators of critical value for the nation is the “High Commissioner for National Protection (HCPN)”. The ANSSI Luxembourg (the national agency, a department of the HCPN) establishes security policies and recommendations. Finally, the GOVCERT Luxembourg (a department of the HCPN) gives a response and support in case of a cyber incident.

Complementarily, Security made in Lëtzebuerg (SMILE) is turned towards the private sector, communes and stakeholders from the economy addressing all questions related to cybersecurity via its three departments: CASES (organisational, governance risk and compliance) ; CIRCL (the CSIRT for the private sector) and C3 (help develop competences at all levels).

Besides HCPN and SMILE, is the CIC-CPCS composed of the “Luxembourg defence department”, the Media and Communication Unit, the state IT centre, the State Intelligence Service as well as the Foreign Affairs Department.

On the regulatory side, Luxembourg has 5 regulators strongly involved in cybersecurity: CSSF (banking sector), ILR (telecom and NIS), CNPD (GDPR), ILNAS (specific e-archiving law), while the HCPN (critical infrastructure protection) striving in a continuous effort to harmonise cybersecurity requirements and as such the compliance burden for private and public entities.

To combat cybercrime, the national prosecutor’s office as well as the police forces have dedicated units to deal with « cyber » cases. They collaborate and are supported on an operational level by the CERT.LU [4] community, composed of the 5 public and 5 private CSIRTs from Luxembourg.

Finally, the national safer internet awareness centre is called BEE SECURE [5] and is dedicated to inform citizens and especially youngsters about the dangers and opportunities of the Internet.

In addition to all this, there are several associations and clusters like CLUSIL [6], ISACA [7], CPSI [8], APDL [9], OWASP [10]… as well as the interdisciplinary institute for security, reliability and trust (SnT) of the University of Luxembourg [11] and other research centres, dedicated to topics around cybersecurity.

[1] Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security (OECD 2002 ; <https://www.oecd.org/sti/ieconomy/15582260.pdf>)

[2] Digital Security Risk Management for Economic and Social Prosperity (OECD 2015 ; <http://www.oecd.org/sti/ieconomy/Digital-Security-Risk-Management.htm>)

[3] National Cybersecurity Strategy III / Stratégie nationale en matière de cybersécurité III (<https://gouvernement.lu/fr/publications.gouv_hcpn%2Bfr%2Bpublications%2Bstrategie-nationale-cybersecurite-3%2Bstrategie-nationale-cybersecurite-3.html>)

[4] Luxembourg Cyber Emergency Response Community (<https://cert.lu/>)

[5] <https://bee-secure.lu/>

[6] Information Security Association Luxembourg (<https://clusil.lu/>)

[7] ISACA Chapter Luxembourg (<https://www.isaca.org/chapters2/Luxembourg/>)

[8] College of Information Security Professionals (<https://cpsi.lu/>)

[9] Data Protection Association Luxembourg (<http://apdl.lu/>)

[10] OWASP Chapter Luxembourg (<https://www.owasp.org/index.php/Luxembourg>)

[11] <https://snt.uni.lu/>

#### SPARTA’s actions

SPARTA project has established contact with the following organisations to establish the national cluster for Luxemburg:

|  |  |
| --- | --- |
| |  | | --- | | * Luxinnovaton * HCPN   We have already received a sign of interest in joining SPARTA from:   * Silent breach | |

#### Future activities

### Portugal (INOV)

#### Current status

With currently 35 members, including representatives from the CNCS, military, finance, telecom, government, academia, cybersecurity national industry and cloud providers, the Portuguese National CSIRT Network (RNCSIRT) is the main operational forum for CSIRT's in Portugal, as well as the "key" cybersecurity forum in the country. The RNCSIRT aims to build trusted, direct communication channels among its members, facilitate incident response and disseminate best practices on computer security incident handling. INOV is an active member of RNCSIRT.

#### SPARTA’s actions

SPARTA project has established contact with the following organisations to establish the national cluster for Portugal:

|  |  |
| --- | --- |
| |  | | --- | | * CNCS   We have already received a sign of interest in joining SPARTA from:   * Município do Barreiro | |

#### Future activities

### Latvia

#### Current status

#### SPARTA’s actions

SPARTA project has established contact with the following organisations to establish the national cluster for Latvia:

|  |  |
| --- | --- |
| |  | | --- | | * CERT.LV (the Information Technology Security Incident Response Institution of the Republic of Latvia) * Vidzeme University of Applied Sciences * PIKC SALDUS TEHNIKUMS   We have already received a sign of interest in joining SPARTA from: | |

#### Future activities

### Italy (CNR,CINI)

#### Current status

The Italian community started already time ago a process of cooperation and clustering of the rich competences in cyber security present in the research and academia landscape.

* CINI has set up the largest laboratory in Italy on cybersecurity (CINI Cybersecurity National Laboratory) that puts together 44 universities and collect expertise from more than 300 researchers actively working in Cybersecurity. It contributed to create the Italian cyber security framework and several successful initiatives as the Italian cybersecurity challenge.
* CNR had a interdepartmental security project and later a cyber security one putting together the expertize and resources of more than 100 researchers in the field and contributed with Leonardo to set up the Italian Technological Platform in Security Research (SERIT).
* CNIT has a rich competence in networking and cyber security aspects.

All together these created on Feb 2017 the National Committee for Research in Cyber Security under the auspices of Italian Department of the Information for Security (DIS). This is a successful example of national cooperation.

All these actors are part of the SPARTA Consortium, that is also complemented by the main Italian industry in the defence sector, i.e. Leonardo and the Italian CERT run by MISE-ISCOM also in SPARTA.

#### SPARTA’s actions

SPARTA clustering is thus really representative of the Italian one and the clustering activities of SPARTA in the sector useful. Nevertheless, the plan is to enlarge also to other partners especially in the field of vertical sectors.

SPARTA project has established contact with the following organisations to establish the national cluster for Italy:

* Sogei
* ENEL

We have already received a sign of interest in joining SPARTA from:

* IDS
* Torino wireless foundation

#### Future activities

The plan is to continue to work at SPARTA project level as well as at national one. CNR and CINI have a major role in the Tuscan Cyber security centre and we would be pleased to embody also this in the SPARTA activities.

### Estonia (UTARTU)

#### Current status

In 2010, by a decision of the Government of the Republic, the Estonian Informatics Centre was given government agency status. The Estonian Information System Authority (RIA) (<https://www.ria.ee/en/>) received additional powers and resources for organizing protection of the state’s ICT infrastructure, and exercising supervision over the security of information systems. For the purposes of organizing the protection of infrastructure, the Department of Critical Information Infrastructure Protection (CIIP)( <https://www.ria.ee/en/ciip.html>) was formed within the RIA. The creation of the Estonian Defense League’s Cyber Unit (EDL CU) (<http://www.kaitseliit.ee/en/cyber-unit>), which took place as a result of collaboration between the public, private and third-sector, has been instrumental in ensuring national defense. The EDL CU is also engaged to support civilian institutions and protect critical infrastructure in a crisis situation. The main provider of training and awareness-raising in the field of cybersecurity is Information Technology Foundation for Education (HITSA) (<https://www.hitsa.ee>) formerly known as the Tiger Leap Foundation. HITSA training is offered to pre-schoolers well as older children, while also involving parents and teachers in the process.

#### SPARTA’s actions

SPARTA project has established contact with the following organisations to establish the national cluster for Estonia:

|  |  |
| --- | --- |
| |  | | --- | | * N/A | |

#### Future activities

### Summary Table [ALL]

The following table summarizes the current status of aggregation of the national clusters even beyond SPARTA project.

|  |  |  |  |
| --- | --- | --- | --- |
| Country/Status of national research and innovation ecosystem | Not structured / not aggregated | Structured/aggregated at informal level | Aggregated / structured at formal level |
| Austria |  | Current | Progress |
| Belgium |  |  |  |
| Czech Republic |  | Current | Progress |
| Estonia |  |  |  |
| France |  |  |  |
| Germany |  |  |  |
| Greece | Current | Progress |  |
| Italy |  | Current | Progress |
| Lithuania | Current | Progress |  |
| Luxembourg |  |  |  |
| Poland |  |  |  |
| Portugal |  | Current | Progress |
| Spain |  | Current | Progress |

## European level

SPARTA project has established contact with the following organisations to establish the European ecosystem:

* EOS (EU)
* ENLETS (EU)
* ESA (EU)
* Ministry of Internal Affairs of Ukraine (UA)
* Cysec (CY)

In addition, SPARTA contacts some international organisations to include them into its associates and friends network:

* McAfee India
* F-Secure

## Specific cooperation with EU projects [ALL partners]

### NECS

The European Network for Cyber Security (NECS) addressed the training and development of a European talent pool to help implement and support the European Cyber-security strategy as highlighted in the EC’s Digital Agenda. NeCS developed a new generation of researchers that combine a strong academic foundation with practical experiences, technological expertise with awareness of the socio-economic and legal context and conviction to furthering research with an entrepreneurial spirit. The 4-year NECS project ended in Sept 2019 and worked for a cyber-security research and training network makes a significant contribution towards meeting the increased demand of human expertise in this critical field. NECS fosters a multi-sector/multi-disciplinary approach that is absolutely necessary for tackling coherently all cyber-security needs as recognized by the Network and Information Security (NIS) platform that has been established by the EU in order to develop a public/private cooperation strategy.

NeCS winter school (https://necs-winterschool.disi.unitn.it/) has been inherited by SPARTA in cooperation with the other 3 Pilot networks and will continue as joint effort with an interesting governance model that sees equally involved all the 4 Pilot networks, in particular in the organizing committee 25% is represented by SPARTA researchers (i.e. Fabio Martinelli (CNR) and Paolo Prinetto (CINI)). The 2020 edition is described in the following brochure.



### StandICT

StandICT.eu, “**Supporting European Experts Presence in International Standardisation Activities in ICT**”, addresses the need for ICT Standardisation and defines a pragmatic approach and streamlined process to reinforce EU expert presence in the international ICT standardisation scene.  Through a Standards Watch, StandICT.eu will analyse and monitor the international ICT standards landscape and liaise with Standards Development Organisations (SDOs) and Standard Setting Organisations (SSOs), key organisations such as the [EU Multistakeholder Platform for ICT Standardisation](https://ec.europa.eu/digital-single-market/en/european-multi-stakeholder-platform-ict-standardisation) as well as industry-led groups, to pinpoint gaps and priorities matching EU DSM objectives. These will become the topics for a series of 8 Open calls focused on priority domains and a continuous cascading grants process, launched by StandICT.eu from March 2018, providing support for European specialists to contribute to ongoing standards development activities, and attend SDO & SSO meetings.

SPARTA partner Fabio Martinelli (CNR) worked on the External Advisory Group and contributed to spread the standICT opportunities in SPARTA as well as to spread SPARTA expertize in StandICT. The project coordinator of StandICT is actually also a SPARTA associate. The need to foster standardization activities is clear and well acknowledged in SPARTA.

### SAPPAN

SAPPAN is a new project and aims to develop a platform for sharing and automation to enable privacy preserving and efficient response and recovery utilizing advanced data analysis and machine learning. SAPPAN will provide a cyber threat intelligence system that decreases the effort required by a security analyst to find optimal responses to and ways to recover from an attack. SAPPAN will enable this within a single organization as well as across organisations through novel models for privacy-preserving data processing and sharing. It will enable utilizing external experts for intrusion detection and sharing of knowledge on response and recovery actions while respecting the privacy and confidentiality requirements of individuals and organizations. SAPPAN will enable a European level perspective on advanced cyber security threats detection, response, and recovery making four key contributions that go beyond existing approaches.

SPARTA partner CESNET participates in SAPPAN. At one point the project looked for a sharing platform and we presented there the results of T4.4, MISP demo, PROTECTIVE/IDEA demo, C3ISP demo during of the face to face meeting. It is worth noticing that Masaryk university (member of CONCORDIA) participates also in this project and they presented what CONCORDIA figured out to use as a sharing platform.

## Monthly workshops

<Report about the monthly workshops>

The SPARTA Spanish cluster has organized two workshops during 2019, the fist one took place in Madrid, on April 24th April in the frame of the Mundo Hacker Day, and the second one in León, on October 23rd, during the ENISE13 congress organized by INCIBE.

### SPARTA Workshop in Madrid, Mundo Hacker

The workshop was framed in the 6th edition of Mundo Hacker Day, an event organized by the popular Spanish TV show Mundo Hacker focused on the dissemination of cybersecurity in an entertaining way. Mundo Hacker Day was held at Kinepolis Madrid, on 24 April 2019. The event featured several tracks and round tables with large companies in the ICT sector where they addressed the most current issues in the digital security sector.

Bearing in mind that each year, Mundo Hacker Day brings together thousands of people, which resemble a very heterogeneous audience (cybersecurity practitioners, researchers, students, industry, etc.), and the fact that the SPARTA partner YesWeHack was going very active throughout it (as both participant and golden sponsor), they preliminarily suggested to Indra the possibility of taking advantage of this occasion to disseminate SPARTA, subsequently involving the partners Vicomtech and Tecnalia.

The activities carried out during the workshop assumed the following **objectives**:

* + To make the SPARTA project known to attendees by introducing its view for a European network of competences in cybersecurity, objectives, research programs and the challenges to be faced.
  + To acquire feedback and know the opinion of the attendees (ranging from experts to students) about the topics covered and the project approaches.
  + Since the workshop was the first SPARTA event held in Spain, it was expected to serve as a preliminarily meeting point for local partners (not excluding the rest).
  + To disseminate the possibility of cooperating as associate partners aiming on attracting the attention of new ones.

The workshop was divided into two tracks. The first of them focused on the presentation to the attendees of the overall SPARTA view, as well as the particular role/view of the attending partners. The track was coordinated by Indra (Jorge Maestre Vidal and Sebastián Laiseca Segura), which presented the project background, objectives, organization approach, roadmap and research programmes. They also introduced the Indra’s view of the project and its role. Then each attending partner (YesWeHack (Nicolas Diaz), Vicomtech (Raul Orduna Urrutia), Tecnalia (Concepcion Cortes)) presented its contribution to the project and particular view about the forthcoming work.

The second track was coordinated by YesWeHack (Nicolas Diaz), where the Coordinated Vulnerability Disclosure (CVD) process was presented and its main challenges were introduced to the attendees, covering the discussion of tools and means that facilitate CVD for a safer Internet. This facilitated the participation of the audience, triggering an open debate on various related topics of interest.

Despite the facts that the workshop was organized with short notice (due to the attempt of taking rapid advantage of the influence of Mundo Hacking Day in Spain) and that it has had little audience, it served to meet part of the established objectives. Firstly, in the context of the workshop, the project was disseminated in a public event and through social networks, thus contributing to the understanding of the SPARTA’s view for a European network of competences in cybersecurity. Second, the topics covered by the SPARTA research programme were discussed in-depth, thus facilitating the attendee participation and providing very valuable feedback. On the other hand, one-third of the Spanish partners was present, which served as preliminarily step towards triggering further joint local initiatives. Unfortunately, the workshop was not able to recruit new associated partners in situ; but the related dissemination actions in social networks and between the Mundo Hacker Day assistants may encourage new partnership requests in the short/medium term.



Figure 5. SPARTA workshop in Madrid disseminated through Tecnalia’s social network

### SPARTA Workshop in León, Mundo Hacker

The workshop was framed in the 13th edition of the ENISE congress in León (Spain), on October 23rd, and was organized by Tecnalia, Vicomtech, Eurecat and Indra. “Cybersecurity in the connected industry: from threat to opportunity” is the slogan chosen for this thirteenth edition of the International Meeting on Information Security.



Figure 6. SPARTA workshop included in the Agenda of the 13ENISE Program.

The workshop, organized with the collaboration of INCIBE that has provided the infrastructure for the event within the [ENISE 13 Concept development room](https://www.incibe.es/en/enise/13enise/program/concept-development-room), has served as an opportunity to disseminate the SPARTA objectives and results, and to connect SPARTA with other CCN pilots (CONCORDIA and CyberSec4Europe). The total number of attendees was 19, being 6 of them SPARTA partners.



Figure 7. SPARTA workshop in León (Spain).

The workshop was divided into three tracks. The first track was focused on the presentation of the objectives of the CCN and the objectives of the three pilots (CyberSec4Europe, SPARTA and CONCORDIA). The second track was dedicated to a Panel on ‘Use cases and impact for Spain’. The third track was dedicated to a panel on ‘New challenges for cybersecurity and synergies between pilots’. The agenda of the workshop is shown in the Figure 7.

****

Figure 8. Agenda of the SPARTA workshop in León (Spain).

The Spanish cluster meeting has concluded the need to identify some synergies between the 4 pilots (CONCORDIA, CyberSecurity4Europe, ECHO and SPARTA) and to work together towards the creation of a common objective: a European network of centres of cybersecurity experience.

* The creation of a **JCCI infrastructure** is present in the 4 pilots, however each pilot follows different point of view and different stages. An alignment is needed to create some interfaces because the EU has expressed the need to work together to provide a common infrastructure.
* The same applies to the **Roadmap** definition. EU’s intent is to develop a Roadmap with clear milestones to tackle cybersecurity industrial challenges in selected sectors and implement it through a complete range of activities, from research & innovation through testing, experimentation and validation to certification activities.
* The **WP Structure** is also quite similar in the four pilots, with the presence of synergies in: Governance Design; Research & Innovation, Roadmap & Demonstration cases; Education, Training and Standardization; and Communication & Community building.

During the workshop, we received an Expression of Interest to become Associate by Gradiant (<https://www.gradiant.org>). Gradiant R&D Center is a private technology centre located in Galicia (Spain). Gradiant is backed by a board foundation including representatives of the three Galician universities (Vigo, Santiago and A Coruña) and six of the most important companies working in Galicia (AAltia, Arteixo Telecom, Egatel, Indra, Plexus, R, Telefónica and Televés); and INEO business association, which represents most of ICT Galician companies.

Juan Díez (INCIBE) announced that INCIBE will manage the I+D+i of the EU Cybersecurity Competence Network. After some discussion with the CONCORDIA, CyberSec4Europe and SPARTA partners, INCIBE has decided to take the glove and organize private workshops with the Spanish partners of the four pilots, to promote the alignment of the projects, and also to have a clear vision at Spanish level of capacities, synergies, and interests.

The event was widely disseminated through the SPARTA and Tecnalia social networks.

****

****



Figure 9. SPARTA workshop in León disseminated through Tecnalia’s social network

# Clustering with other pilots [CEA]

<Description of the work done on clustering with other pilots during the first 12 months>

# Cooperation with EU and International Bodies [CNR,ALL]

SPARTA partners interacted with several EU and international bodies in several forms. We recall here some of the main organizations and EU project we cooperated with.

## Organisations

### ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State’s local, regional and national administrations, countries part of the European Economic Area (EEA) and the European Free Trade Association (EFTA) and H2020 associated countries.

SPARTA partners are fully involved in ECSO in several roles including in the Board of ECSO, e.g., CEA, CNR, Thales).

Cooperation with ECSO is at several levels, in particular, SPARTA coordinator has been invited to serve in the scientific and technical committee of ECSO. SPARTA representatives are invited in several ECSO meetings, as the ECSO WG6 ones.

The cooperation is strong and is going to be re-enforced by a MoU between SPARTA and ECSO.

### ENISA

ENISA was created in 2004 by EU Regulation No 460/2004 under the name of European Network and Information Security Agency. The Agency works closely together with the EU Members States and other stakeholders to deliver advice and solutions as well as improving their cybersecurity capabilities. It also supports the development of a cooperative response to large-scale cross-border cybersecurity incidents or crises and since 2019, it has been drawing up cybersecurity certification schemes.

ENISA assists the Commission, the member states and, consequently, the business community in meeting the requirements of network and information security, including present and future EU legislation. ENISA ultimately strives to serve as a centre of expertise for both member states and EU Institutions to seek advice on matters related to network and information security.

SPARTA partners cooperate in several forms with ENISA officers in many activities. In particular, SPARTA researchers cooperated with activities on road-mapping and certification that are currently two hot topics.

## EU Projects

### Cyberwatching

Cyberwatching aims at defining and promoting a pragmatic approach to implement and maintain an EU Observatory to monitor R&I initiatives on cybersecurity & privacy, throughout EU & Associated Countries. These initiatives will be clustered, with a cluster tool, and themes identified, leading to an online catalogue of services for cybersecurity & privacy, showcasing market uptake and advancing EU sustainable competitiveness. A supply & demand marketplace of EU cybersecurity products & services, as well as the inclusion of an end-users’ club, ensures that perspectives of SMEs as well as other relevant stakeholders are properly taken account of. Ultimately, a cybersecurity & privacy ecosystem will be created, offering prime and guided access to the cyberwatching.eu catalogue of services & marketplace & ensuring feedback in terms of effectiveness & usability of research results.

Main Outputs: Continuously updated observatory & R&I online catalogue, cluster tool, 4 concertation meetings, 4 annual workshops, 10 regional SME workshops, 10 webinars, 4 cluster reports, 2 white papers, 2 roadmaps, sustainability through cybersecurity & privacy marketplace

SPARTA project is listed among the project in Cyberwatching and SPARTA researchers are often called in meetings organized by Cyberwatching, several events were attended by CNR.

### Aegis

AEGIS aims to strengthen dialogues between Europe and the US, in order to facilitate exchange of views, policies and best practices to stimulate cooperation around cybersecurity and privacy R&I, and contribute in shaping the future global cybersecurity and privacy landscape.

AEGIS proposes a multi-stakeholder approach to engage relevant communities more actively and strategically in supporting dialogues and creating a common and orchestrated vision and strategy to accelerate EU-US cooperation in cybersecurity and privacy R&I. At the core of the AEGIS strategy is the Cybersecurity Reflection Group EU-US that will be established as a multi-stakeholder collaboration platform. The Cyber-RG EU-US, through its Working Groups, will address specific issues on international, technical trends, policy and legislation challenges in cybersecurity and privacy, and will facilitate the effective collaboration of a wide range of interested parties including policy makers, researchers, technology experts, business leaders, cyber policies experts and influencers and civil society. Under the leadership of the AEGIS consortium, these key groups will come together to decisively tackle cybersecurity and privacy related problems and to provide opinions and recommendations to policy dialogue. AEGIS will also provide a mapping of the cybersecurity and privacy landscapes in EU and US, benchmark relevant legislation and policies and promote innovation partnerships and opportunities for future EU-US cooperation in cybersecurity and privacy areas of mutual strategic interest.

The AEGIS consortium is in a privileged position to generate significant impacts in both sides of the Atlantic, by leveraging the partnership’s network multipliers with a wide-ranging access to cybersecurity and privacy stakeholders, including researchers, think tanks, business and political decision makers, and thus to contribute significantly to deepen cybersecurity and privacy R&I cooperation between Europe and the US.

### EUnity

EUNITY aims to encourage, facilitate and develop the dialogue between Europe and Japan on cybersecurity and privacy research and innovation trends and challenges, in order to foster and promote cybersecurity activities in both regions.

Among EUNITY objectives there are:

* Encourage, facilitate and support the ICT dialogue between relevant EU and Japanese stakeholders on matters relating to cybersecurity and privacy R&I trends and challenges by organizing at least two workshops, ensuring a broad participation of the relevant stakeholders (policy groups representatives, industry representatives, academia representatives) in the workshops and by feeding back the collected information into EU-based groups such as ECSO, EOS, NIS, and the CSA.
* Identify potential opportunities for future cooperation between European and Japanese R&I ecosystems and policy makers by identifying and mapping the relevant legislation, policies and cybersecurity agendas, roadmaps and timelines at the EU level (NIS platform, cybersecurity cPPP) and at the National level, as well as in Japan, clearly identifying and prioritising the joint topics in a proposed EU-Japan Cybersecurity and Privacy Strategic Research and Innovation Agenda (EUJ-C&P-SRIA) and ensuring that the collected information is made widely available through modern communication means.
* Foster and promote European cybersecurity innovation activities and increase the international visibility of EU activities in cybersecurity, by showcasing important results of projects and including key European research actors (companies and researchers) in the project’s workshops.

EUnity is managed by SPARTA partner IMT and the follow up activities of this project will be also conducted in cooperation with SPARTA.

# Summary and Conclusion

<please provide a short summary and conclusion of the deliverable, approx. ½ - 1 page>

# List of Abbreviations

|  |  |
| --- | --- |
| **Abbreviation** | **Translation** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Bibliography

[1] ...

[2] ...