SPARTA

D8.3

Final 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	41 months
Programme	H2020-SU-ICT-2018-2020

Deliverable type	Demonstrator
Deliverable reference number	SU-ICT-03-830892 / D8.3 / V1.0
Work package contributing to the deliverable	WP8
Due date	June 2022 – M41
Actual submission date	14th September, 2022

Responsible organisation	CNR
Editor	Fabio Martinelli
Dissemination level	PU
Revision	V1.0

Abstract	This document describes Partnership activities performed by the SPARTA ecosystem in the final year.
Keywords	Clustering, community building, Joint Competence Centre Infrastructure

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

Editor

Fabio Martinelli (CNR)

Contributors (ordered according to beneficiary numbers)

Florent Kirchner (CEA)

Christian Derler (JR)

Philippe Massonet (CETIC)

Martin Žádník (CESNET)

Jan Hajný (BUT)

Marc Olm, Michael Meier (UBO)

Raimundas Matulevicius (UTARTU)

Panagiotis Douris (KEMEA)

Ana Ayerbe Fernandez-Cuesta, Cristina Martínez (TEC)

Francesco Zola, Raúl Orduna (VICOM)

Fabio Martinelli, Artsiom Yautsiukhin (CNR)

Egidija Versinskiene (L3CE)

Bertrand Lathoud (SMILE)

Armands Meirāns (LMT)

Michal Choras (ITTI)

Nelson Escravana (INOV)

Reviewers (ordered according to beneficiary numbers)

Augustin Lemesle (CEA)

Elisabete Carreira (INOV)

Disclaimer

Executive Summary

This document describes partnership activities performed by the SPARTA network in the final year of the project.

We promoted the gathering, identification and homogenization of learning contents from participants contributing to build an initial catalogue of the courses, virtual learning platforms or hands-on-labs.

In this sense, we have currently identified 15 courses and 6 hands-on-labs. We have developed and distributed a second version of the JCCI, providing the JCCI Nexus and JCCI Nodes as open-source code paving the ground to a migration of the Inventory Asset developed during the first year of the project.

Despite the health situation caused by the CoVID pandemic, we also performed activities related to the consolidation of the national and European ecosystems.

CoVID emergency restrictions and national lockdowns have impacted greatly in conducting the planned monthly workshops. Nevertheless, we have maintained the activity through on-line media fostering relations between partners and associates, but also between the SPARTA partners and national or European agents, Forums and Policy Makers. Overall, the respective KPIs have been achieved.

A strong collaboration has been established between the other fellow pilot projects of the competence network, setting meetings, coordinating results and sharing approaches through formal and controlled channels following management best practices, but also fostering the direct collaboration between partners sharing common goals, like the creation of a Cyber Range workgroup, or the alignment of research roadmap, management of the activities and consolidation of the practitioners network.

On the other hand, the collaboration with other EU organizations and EU projects has been reduced with respect the expected activities planned a year ago, although we have tried to support the new initiatives and support in CoVID management in the realm of the SPARTA network.

In summary, this document reports the status of the networking and JCCI activities in the final year.

Table of Content

List of Figures

List of Tables

Chapter 1 Introduction

The goal of SPARTA partnership activities is to foster and consolidate the cybersecurity ecosystems, creating and supporting links at local, national, European, and international level.

Another objective is to pave the ground, at technological and relational levels, to promote European Digital Strategic Autonomy, supporting and bringing together the communities and assets of its Member States.

SPARTA has been devised as a “man-on-the-moon” project, so policies, processes and technologies proposed from this Pilot are the basis for future accurate investments in digital security, comparing and aligning the proposals with those of the rest of the Competence Centres Network (CCN) pilots underway. SPARTA considered the best way to achieve this goal by maximizing the impact of project's resources by establishing networking and collaborative activities, and by defining a roadmap, holding workshops, and sharing resources that SPARTA made available to partners and associates.

Thus, the three pillars that sustained the integration and clustering activities are:

- **Infrastructures:** Work has been done on the roadmap for the creation, recruitment, and demonstration of a Joint Competence Centre Infrastructure (JCCI) in which the tools available through SPARTA partners and associates. Its objective is to optimize research and innovation in cyber security, by creating new services or extending those that are currently provided by third parties, and by offering learning, training, and experimentation resources. Those singular assets can be accessed and used in similar ways to those of a Digital Innovation Hub.
- **People:** We favour integration and promote inclusive initiatives for the less represented groups in the sector. We highlight the future role of young people and women in the scientific, research and development fields as they are the future European workforce by promoting join PhD school with the other pilots, and many other specific events. We aimed at a collaboration that stems from local communities, is channelled into national clusters, and is added at a European level through integrated ecosystems. The inclusion of Associates and Friends in the project has been a key factor for the growth of communities, people, and organizations, that will provide resilience to the technological infrastructure.

Network: Creating a dynamic community requires SPARTA-related organizations to be part of broader networks, by connecting with the network created in the other pilots and interacting with national, European, and international stakeholders. The collaboration is developed through existing organizations, especially ENISA, ECSO and the national hubs that bring together the main actors of each member state, involving both institutions, industry, academia, and users, in an organized and incremental way.

Chapter 2 Joint Competence Centre Infrastructure (JCCI)

2.1 Purpose

In the second year, the JCCI was re-organized in order to decentralize the shown information, as presented in the *Deliverable D8.2 – Intermediate results of the clustering, platforms, and ecosystems activities* and described in Figure 1. In fact, the main idea was to create a dynamic infrastructure, in which different customers could access a list of all available resources and where this information would not be stored in a centralized entity but each provider oversees its own. Each partner must generate its contents and make them understandable to the consumer. Furthermore, the access to these resources could be limited by an authentication process regulated by SPARTA Identity Provider.

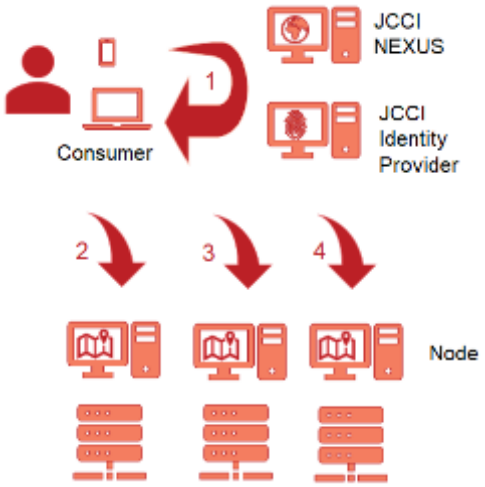


Figure 1: JCCI

In the third year, the main goal was to involve more SPARTA partners, associates, and friends in deploying their own JCCI node, in order to take part directly in the JCCI. In this sense, dissemination activities (news, meeting, e-mail, and so on) were achieved for sharing the JCCI main goals and showing the actual "new" architecture. During this year two versions of the JCCI landing host were implemented and shared with the SPARTA community. The idea behind the JCCI Landing host was to give the possibility to each partner to share the resources of their labs in an interactive way to all the JCCI partners.

2.2 Description

2.2.1 JCCI components

As already described in previous deliverables, the JCCI is formed by 3 main components: a workbench for a shared and distributed testbed where computation and communication resources can be shared, a virtual learning centre to share and spread knowledge for learning purposes, and a federated cyber range with different scenarios to gain skills in cyber-attacks and defences (Figure 2). This section updates on the previous deliverables on the JCCI components.

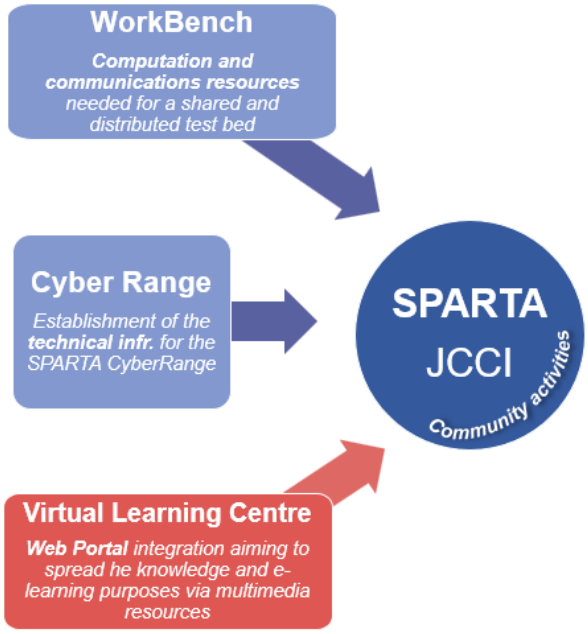


Figure 2: Components of the Joint Cybersecurity Centre Infrastructure

2.2.1.1 Work Bench

The WorkBench gathers computation and communication resources needed for a shared and distributed test bed. As mentioned before, the WorkBench is a compound of already existing assets from the partners, which are offered through a common platform. So far, **17 partners have contributed 30 assets' information** to the common asset inventory. 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.

2.2.1.2 Virtual Learning Centre

The Virtual Learning Centre is a web portal integration aiming to spread the knowledge and e-learning purposes via multimedia resources.

So far, **10 partners** have contributed their learning contents to the common learning catalogue. Among the learning contents, there are online courses, in-person courses, hackathons, contests and practical courses, which will offer a variety of resources available to share or access under certain conditions.

2.2.1.3 Cyber Range

Based on the asset inventories, and once the WorkBench is outlined, it will be possible to select a subset of the testbed to be included in the Cyber Range category 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 Centre, 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 particularly all the testbeds that include [not exclusively] an instance of KYPO Cyber Range developed in the framework of the Cybersecurity Competence Network pilots.

2.2.2 Usage workflow

The three components of the JCCI are available through a web application that can be accessed by any organization – the JCCI NEXUS detailed in the next section. The usage workflow of this web

application can be found on Figure 3. Different customers (either partners or external organizations) can access a list of all available resources. This index is available through SDLs that return the existing labs and learning equipment, contents, and datasets, as well as workbench resources and how to access them. These either are directly accessed or the site redirect the organization to the corresponding place.

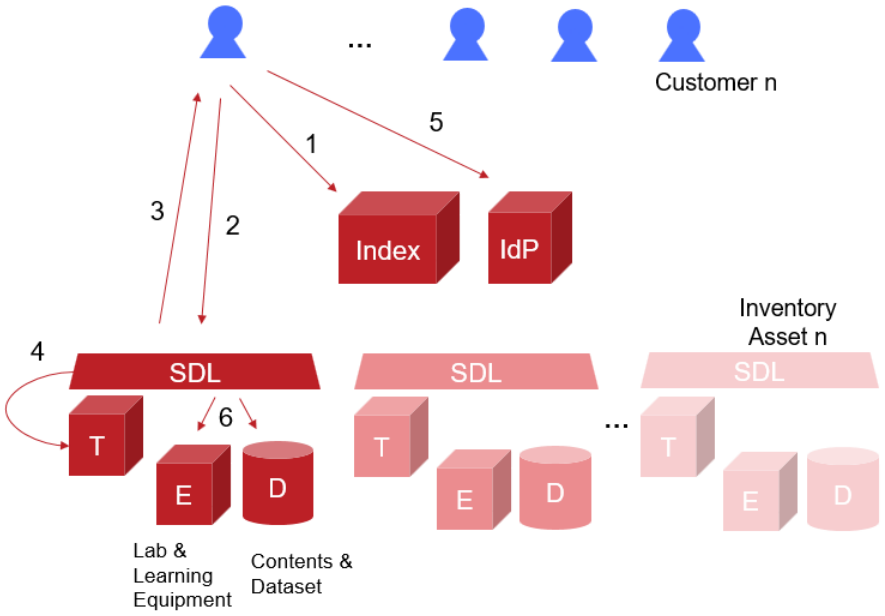


Figure 3: Usage workflow. IdP = identity provider, SDL = service description language

2.2.3 JCCI NEXUS and NODE

As introduced in the *Deliverable D8.2 – Intermediate results of the clustering, platforms, and ecosystems activities*, it is possible, in the JCCI, to distinguish two main entities that are called "SPARTA NEXUS" and "SPARTA NODE". The first one represents the web part (freely available and documented[1]). NEXUS is a Marketplace devoted to the identification of the main facilities that the SPARTA JCCI provides in order to improve the collaboration among SPARTA partners as well as to allow sharing of facilities with external organizations. In general, it creates a common working environment that enables the sharing and collaboration among partners in a remote way. This implies both the research / development aspects and the financial / administrative ones.

[1] https://github.com/tv-vicomtech/SPARTA_JCCI_OFFICIAL_NEXUS

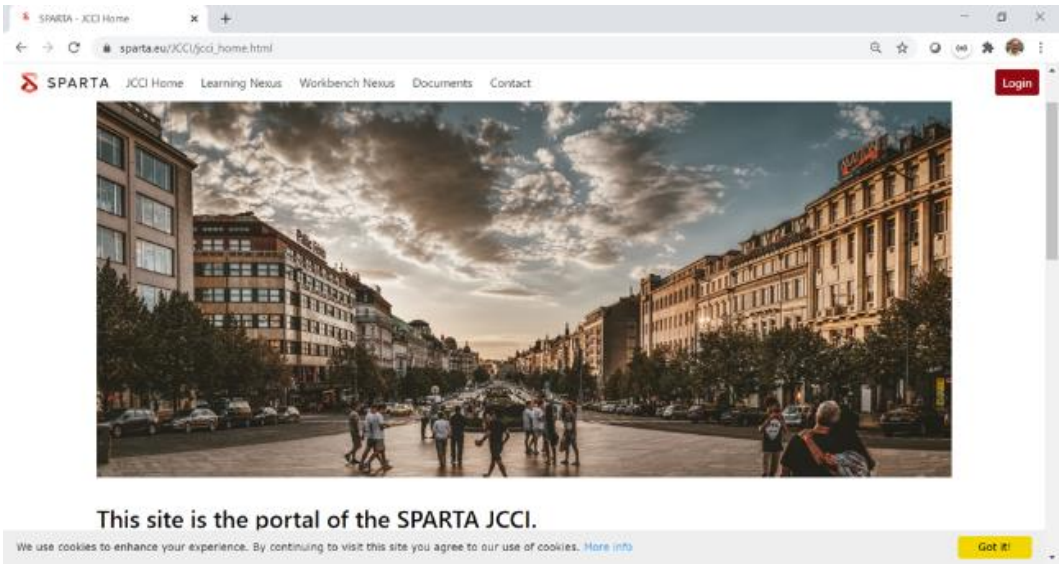


Figure 4: JCCI NEXUS online

The second actor represents a REST-API[2] that allows each partner to communicate with the NEXUS and provide its own information to all the customers. This REST-API is used to dynamically update the information in the SPARTA JCCI webpage, i.e., the JCCI NEXUS. Partners should install this REST -API to manage their own information without problem, so for example they can make modifications it without the permission of a central unit. Nevertheless, the static content will remain on the main page for the benefit of the project and the partners that cannot provide dynamic services over the Internet. However, it is strongly recommended to install this REST -API. The REST -API is developed in a docker container in order to increase its usability and facilitate its deployment among all the SPARTA partners and associates.

In the third year of SPARTA, we worked on implementing and perfecting a new actor called “JCCI Landing host” which is used for sharing interactive services. In particular, this actor allows the partners to share a hands-on lab and to access that service through the JCCI Nexus, as shown in Figure 5. In this sense, the JCCI Landing host can be deployed in order to give them access in two different ways, through the “traditional” terminal (we referred to this implementation as ShellInABox or SIAB), or through the graphical interface (we referred to this implementation as Virtual Network Computing or VNC). In both cases, the code was implemented using a docker container in order to facilitate the deployment to all the partners and it was published in a public repository.

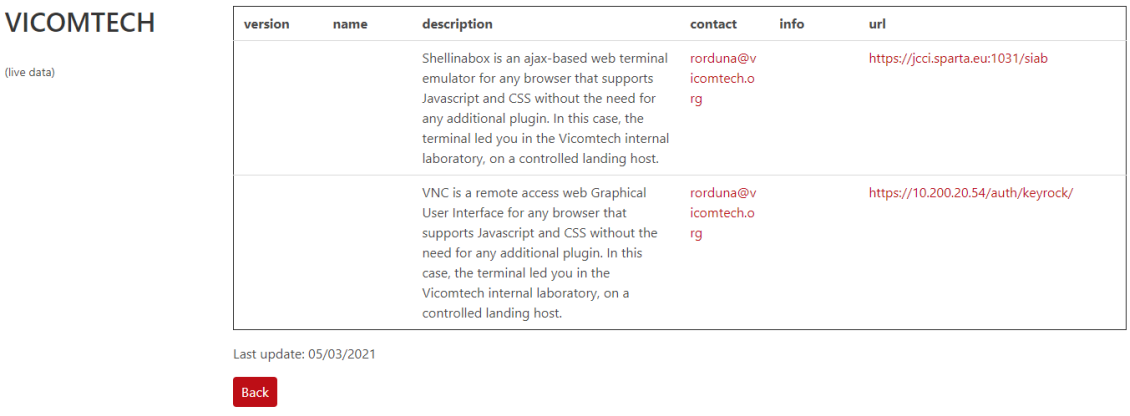


Figure 5: Example of Interactive services

[2] https://github.com/tv-vicomtech/SPARTA_JCCI_NODE

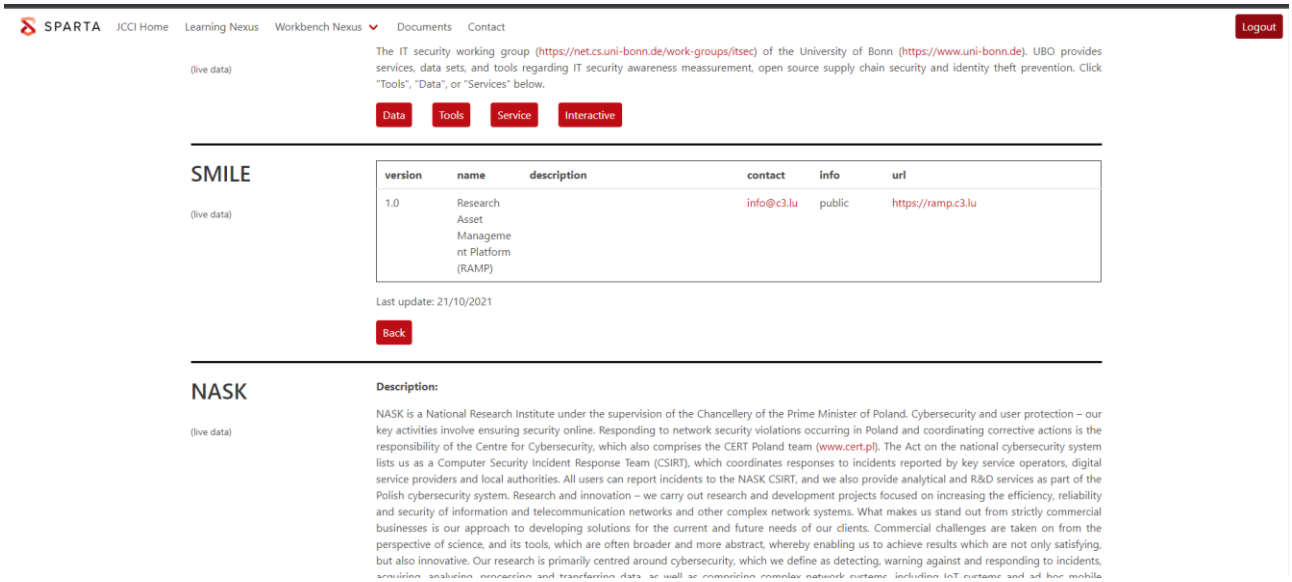


Figure 6: Example of live data

SIAB[3] is a tool that allows sending SSH commands directly using HTTPS protocol, in fact, it implements a web server that can export arbitrary command-line tools to a web-based terminal emulator. This emulator is accessible to any JavaScript and CSS-enabled web browser and does not require any additional browser plugins (Figure 8). In our specific implementation[4], the SIAB was improved by regulating how access to the service and how commands were sent through HTTPS. More specifically, in order to increase the security and the protection of the hand-on lab, our implementation provides the deployment of a proxy directly connected with the SPARTA IdP which is in charge of checking all the commands sent to the SIAB letting pass only the one received by authorized Sparta user (as similarly for the proxy built the in JCCI NODE and introduced in Deliverable D8.2). As shown in Figure 9, when a user tries to access the service without being authenticated in the SPARTA IdP, an error is shown that claims a missing token. For more details about the deployment, the public code has a small guide for helping the users.

[3] https://github.com/shellinabox/shellinabox
[4] https://github.com/tv-vicomtech/SPARTA_JCCI_SIAB_PROXY

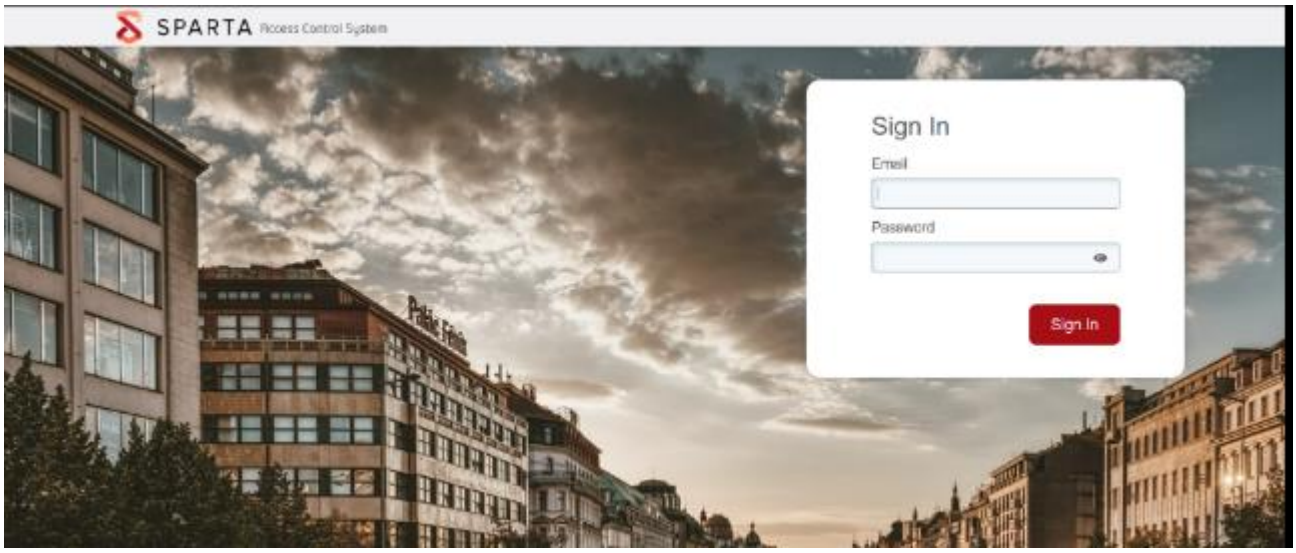


Figure 7: Fiware Identity provider (IdP) deployed in SPARTA

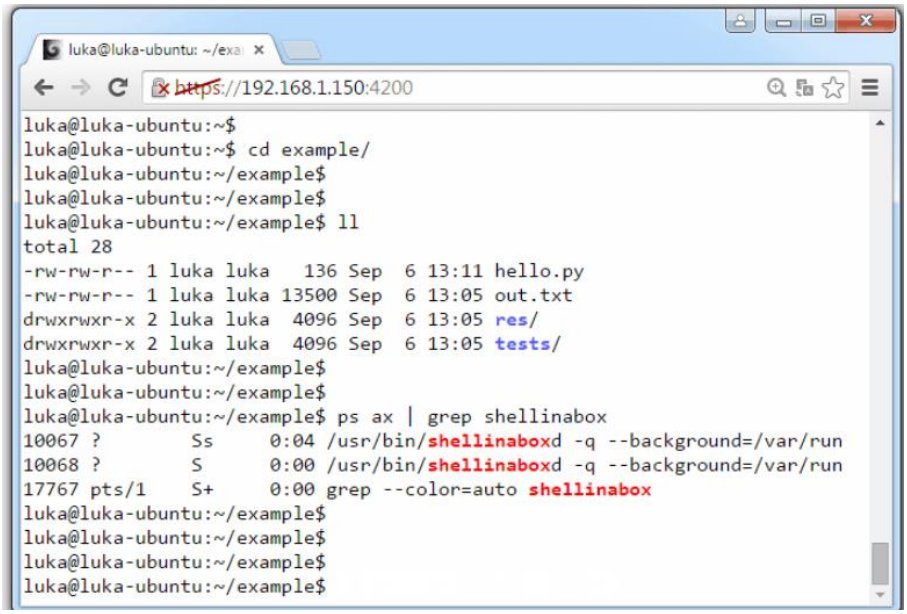


Figure 8: Example about ShellInABox (SIAB) service

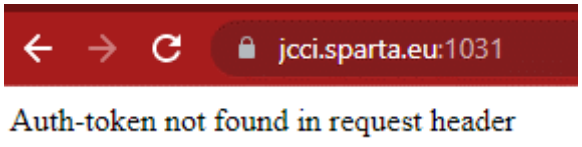


Figure 9: No authenticated user error

Another way to provide a hands-on lab is based on the VNC system, which is able to display the visual desktop display of another computer and control that computer over a network connection. More concretely, the noVNC[5] client, an open-source VNC client is used. noVNC is both a VNC client

[5] https://novnc.com/info.html

JavaScript library as well as an application built on top of that library. noVNC runs well in any modern browser including mobile browsers. In particular, in our implementation, the noVNC[6] is deployed into a docker which contains the virtual machine that we want to control and of which we want to show the graphical interface. Once again, in order to protect this service and regulate who can access it, a proxy linked to SPARTA IdP is deployed. The aim of the proxy is again to check that all the commands, instructions, and communication to the noVNC container are from authenticated and authorized SPARTA users. In Figure 10, an example of access to the noVNC hands-on lab is reported.

Figure 10: Example about noVNC service

2.3 JCCI disseminations

In the third year of SPARTA, we have also worked in disseminating and presenting the JCCI functionalities and potentialities to all the SPARTA partners, associates, and friends, in order to involve them in deploying JCCI NODE and Landing host. For this reason, we have organized several one-to-one calls showing them how JCCI works and how easy it was to deploy a new instance. Moreover, we have shared this information also with news on the SPARTA web page. For example on date 31st January 2021, we talked about which is the mission of a Join Competence Centre Infrastructure (https://sparta.eu/news/2021-01-19-the-mission-of-a-joint-competence-centre-infrastructure.html), and which are the benefit of having decentralized information. On 7th February 2021, we presented an article about the importance of the Hands-on lab and how they can be used for deploying Cyber Range scenarios (https://sparta.eu/news/2021-01-19-federated-infrastructure-hands-on-labs-and-cyberranges.html).

Finally, on 27th September 2021, we showed the update about the partners that had already a JCCI NODE deployed, and how the presence of National Clusters pushed the JCCI growth, especially presenting the Spanish one as success case through the integration in JCCI of the Spanish Security Competence Network "EGIDA" (https://sparta.eu/news/2021-09-27-national-clusters-pushing-the-jcci-joint-competence-centre-infrastructure-growth.html) and promoting the adoption in other national clusters of reference, like the French, Italian and German.

[6] https://github.com/tv-vicomtech/SPARTA_JCCI_VNC

Chapter 3 Clustering activities at national, European and international level

3.1 SPARTA ecosystem

SPARTA network is an established cooperation means among consortium partners and several external organizations comprising the ecosystem, namely the SPARTA Associates and Friends.

In most of the 14 countries represented in SPARTA, we ideally collected a core set of partners from research (RTO), academia, governmental agencies, and industries.

The picture below describes the partners in SPARTA (per country, per typology, size is proportional to number of partners).

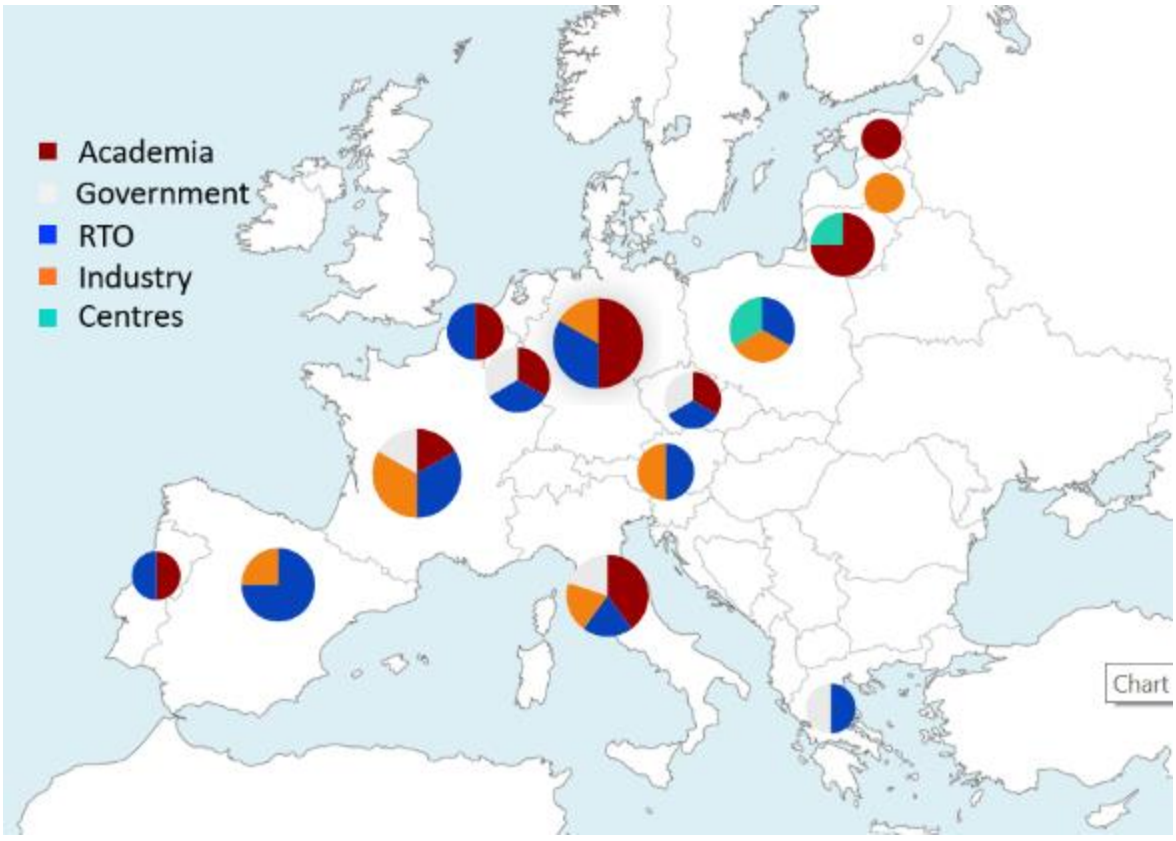


Figure 11: SPARTA ecosystem

During the third year, we mainly consolidated the existing network built during the first and the second years of the project.

In the following figure, we show the current associates and friends that were enlarged during the second year. Each country followed its own strategy to involve new associates and friends (size is proportional to number of associates/friends).

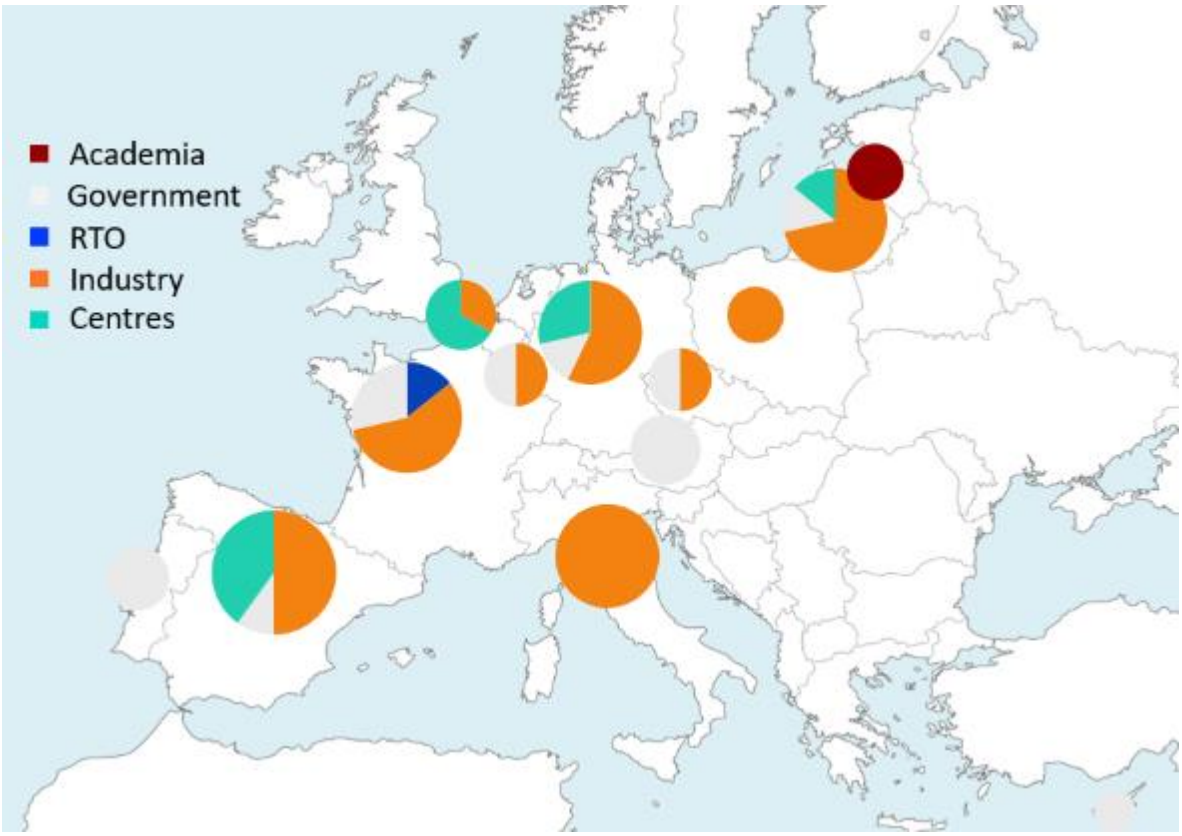


Figure 12: SPARTA Associates/Friends

And the following picture shows the overall community (size is proportional to community size):

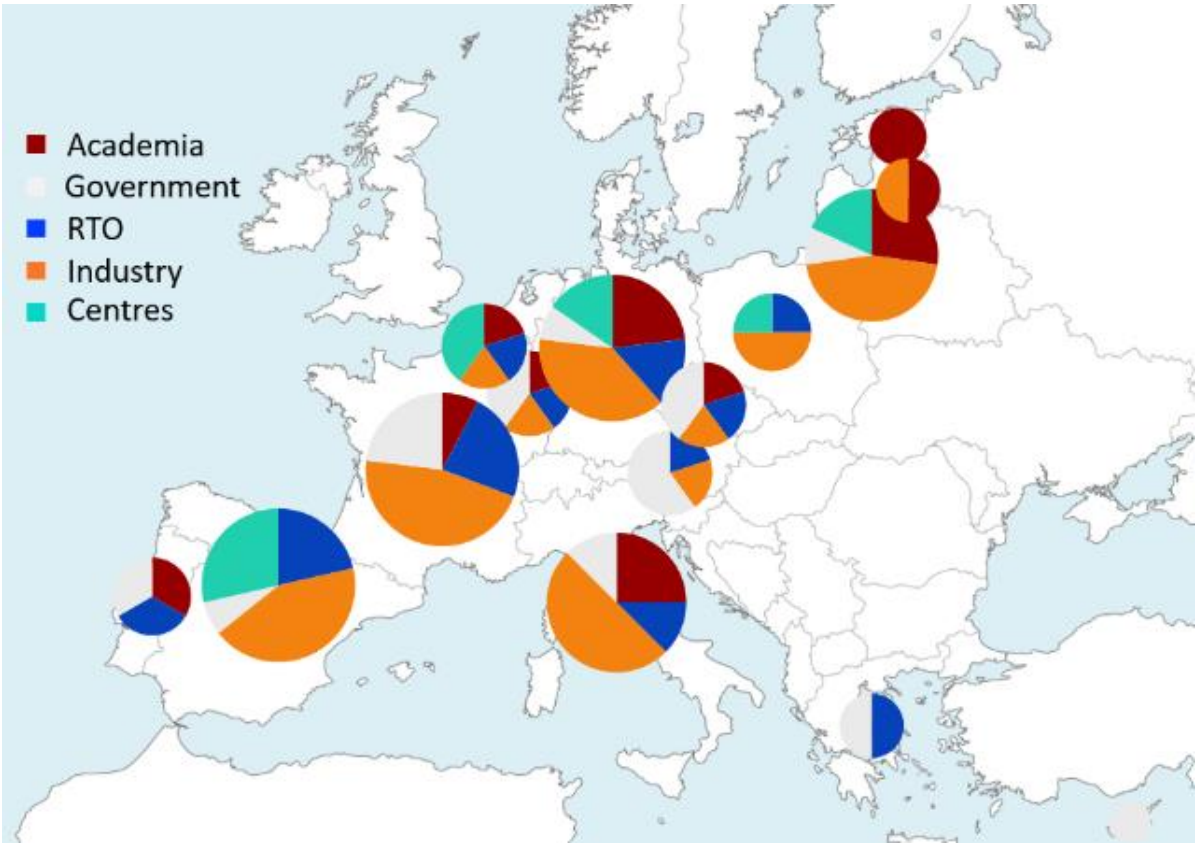


Figure 13: SPARTA overall community

3.2 National level

This section describes the situation at national level after two years of SPARTA and highlights some specific SPARTA actions taken in year three.

3.2.1 France

3.2.1.1 Current status

2021 and 2022 were very active years for cybersecurity in France, building on the structuring and strategic initiatives launched in 2020.

- The Strategic Branch Committee (Comité Stratégique de Filière – CSF) "Security industries" continues to lead the national-level organization of the French industrial ecosystem. Marc Darmon (Thales) is the president of this Committee, and several SPARTA partners (CEA, Inria, IMT) are members of the organization's Research and Innovation Working Group.
- Following the successful launch of the French "Campus Cyber", many actors of the ecosystem have taken possession of the location. The Campus leverages multiple tools to bring together its community: working groups on Education, Innovation, Anticipation, Dissemination and awareness, etc. have been operating, animated by experts of the field, and producing reports and recommendations. Events and conferences are being hosted on topics that range from European geopolitical topics to hackathons: SPARTA has led the way here, with YesWeHack successfully organizing the "Hack me I'm famous" competition, involving 3 European Unicorns, the hacker community, and SPARTA's scientific expertise. The event was attended by France's Grand Challenge Director and representative to the ECCC Governing Board, and by the Director of ANSSI.

- The "Cybersecurity Automation Grand Challenge" reached the end of its first phase, yielding concrete R&I results in the summer of 2022. It's been expanded by a full-blown Cybersecurity Acceleration Strategy, rooted in the February 2020 report to the Ministry of Economy and the Ministry of Higher Education, Research and Innovation "Making France a Disruptive Technology Economy", and clearly integrated in the France 2030 investment program. Topics of interest include :
  - innovation in critical technologies,
  - the support of cyber startups,
  - expert-led priority research investments,
  - a joint data-sharing platform,
  - the transposition of national certificates into the European Cyber Act,
  - securing regional territories,
  - the creation of a skills observatory and the reinforcement of education offers.
- The launch of the French NCC has been initiated, with ANSSI teams working on establishing the foundations for this new way of operation.

3.2.1.2 SPARTA's actions in the third year

Liaison activities have been extended from the second year into the third, including with :

- Allistene, the consortium of public research institutions in informatics, and regular status updates within its Cybersecurity working group.
- Systematic and its Cyber and Security Hub, one of France's largest ecosystem with upwards of 225 members spanning start-ups, SMEs, academia, public administrations, and large industries.
- The Ministry of Research and Higher Education, with opportunities to structure SPARTA-based competence centres as a support to the French research planification.

New, additional activities have taken place too: the above-mentioned hackathons and participation in the Campus Cyber working groups have brought SPARTA, its scientific policy model, and its achievements to the attention of new partners. Liaison and dissemination events around the Slovenian and French presidencies have been a successful part of their communication sequences. Numerous exchanges have also taken place with the French NCC, spanning topics from roadmapping to lessons learnt to operational recommendations.

3.2.2 Belgium

3.2.2.1 Current status

The members of the Belgian cluster are the following:

Name	Type	SPARTA partner or associate
Centre of Excellence in Information and Communication Technologies (CETIC)	RTO	partner
Université de Namur/CRIDS	Academic	partner
Center for Cyber Security Belgium (CCB)	Public body, national cybersecurity authority	associate
Infopole Cluster TIC	Public, cybersecurity network	associate
UCLouvain	Academic	associate
Guardis	Industry	associate
Multitel	RTO	associate
Bluekrypt	Industry	associate
Leaders In Security (LSEC)	Industry (cluster)	associate

The Belgian cluster is composed from entities of the three regions of Belgium with most partners coming from the French speaking regions. The two partners of the SPARTA project are CETIC, an applied ICT research centre focusing on software, and the CRIDS which is the Research Centre in Information, Law and Society of the University of Namur. The Belgian national cybersecurity authority (CCB) is responsible for supervising, coordinating, and overseeing the implementation of the Belgian cybersecurity strategy. A new department of CCB is now responsible for the National Coordination Centre (NCC) and they participate in the EU Governing Board (GB) meeting of the European Cybersecurity Competence Network and Centre (ECCC). CCB organises regular meetings of the Strategic Board where federal and regional authorities (Service Public de Wallonie (SPW) and Agence du Numérique (ADN) that are responsible for public cybersecurity strategy and funding at the regional level) participate. CCB is responsible for managing the national cybersecurity community. The Belgian SPARTA cluster has been providing continuous feedback based on SPARTA experience and results to CCB. In the following, some info in its members.

Infopole cluster TIC among its different responsibilities is managing the regional cybersecurity network. UCLouvain has participated as associate in several SPARTA brokerage events and has

led the creation of a regional cybersecurity initiative described in the next sub-section. GUARDIS is an SME that has been developing expertise in the area of cybersecurity testing of cyber physical systems. Multitel, which is an applied ICT research center focused on hardware, has been participating in the regional cybersecurity initiative. Bluekrypt is an SME that provides services in the area of security of information systems and their management. LSEC is a Belgian based internationally renowned Information security cluster founded by the University of Leuven (K.U. Leuven). LSEC includes members from all regions of Belgium. LSEC is an associate member of SPARTA and have been involved via the SPARTA associate communication channels. With LSEC the Belgian cluster covers all regions of the country.

3.2.2.2 SPARTA's actions in the third year

Actions in the third year have mostly consisted in:

- Submission of the AIDE H2020 project proposal to call "HORIZON-CL3-2021-CS-01-03: AI for cybersecurity reinforcement" on the 21st of October 2021, that was presented at the SPARTA day and brokerage event on the 12th of April of the same year.
- Supporting the setup of the Belgian NCC
- Initiating a strategic initiative in cybersecurity for the Walloon region of Belgium called "Cybersecurity for Wallonia" (CyberWal).

SPARTA PARTNERSHIP

SPARTA DAY &
BROKERAGE EVENT

12 APRIL 2021 9H00 - 17H30

AGENDA

Link for connection to SPARTA Day

09.00-11.00 SPARTA DAY OPEN SESSION

SPARTA WELCOME and SPARTA NETWORK (CEA)
SPARTA ROADMAP (INRIA)
SPARTA RESEARCH PROGRAMS: CAPE (IMT), T-SHARK (L3CE), HAIIT (CINI) and SAFAIR (ITTI)
SPARTA PARTNERSHIP (CNR)
SPARTA JCCI (VICOMTECH)
SPARTA EDUCATION and TRAINING (BUT)

SPARTA Brokerage link
11.15-13.00 SPARTA BROKERAGE EVENT for EDIH
EDIH CALL PRESENTATION (Region Bretagne & Pôle Images & Réseaux)
NATIONAL CONSORTIUM PRESENTATIONS (currently BUT, CETIC, CINI, CS4.0, CNIT, INRIA, INOV, JR, KTU, LDO, L3CE, ...)

LUNCH BREAK

14.00-14.40 SPARTA ASSOCIATE Plenary and COOPERATION with INSTITUTIONS/PROJECTS/ASSOCIATIONS
ECSO, TRUST-IT, IMT, U. LAUREA, Bologna A.,

14.45 -17.30 BROKERAGE EVENT for HEU/DEP
OPEN CALLS PRESENTATION

CONSORTIUM PROPOSALS (CETIC, CNIT, CNR...)
AND
COMPETENCE PRESENTATION FROM PARTNERS/ASSOCIATES/FRIENDS
(INOV, ADACORE, ATOS, Brescia U., CUBIT, CCI-ES, DITECTFER, EZU, F-SECURE, KTU, INMARK, IKERLAN, Lux. U., L3CE, Mondragon U., TECNALIA, TECHNIKON...)

17.30 CONCLUDING REMARKS

FOR REGISTRATION SEND AN EMAIL TO
SPARTA_PARTNERSHIP@IIT.CNR.IT

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

Figure 14: The Brochure of SPARTA Day and Brokerage event.

The AIDE proposal consortium included SPARTA partners CETIC, CNR, and Tecnalia and associate partner UCLouvain. The proposal aimed at extending work on cybersecurity assessment carried out in SPARTA, with various AI based techniques coordinated by a federated learning process.

With respect to setting up the Belgian NCC, feedback from the Belgian members, as well as feedback on the global operation of SPARTA has been communicated to CCB. Support from the SPARTA experience has been provided by CETIC during the regular NCC Strategic Board meetings. Since CCB is a SPARTA associate member there have been some audio conferences on the status of the SPARTA project and the other pilot projects. An important subject of discussion is the organisation of the national cybersecurity community.

Based on experience in the SPARTA project and in preparation of the ECCC, UCLouvain and CETIC have set up a strategic innovation initiative in cybersecurity in the Walloon region called CyberWal. CyberWal aims to coordinate cybersecurity research, training (non-university) and innovation at the regional level. CyberWal groups research entities and public entities (e.g., CCB) with cybersecurity responsibilities. Companies are closely involved in accompanying the process via the reseau LIEU that is responsible for connecting business to research. CyberWal is open to all companies interested in cybersecurity research, innovation and training. The CyberWal initiative is tightly coordinated with CCB, responsible for cybersecurity at the federal level, Agence du Numérique (ADN) and “SPW Économie, Emploi, Recherche”. A first project funded by the SPW recherche in the context of CyberWal started in january 2022 and is called CyberExcellence. CyberWal is carrying out fundamental research on the following topics: (1) making systems resilient to cyberattacks during design, (2) sensing, response, reaction during execution, (3) security by design for GDPR and Open data, (4) data protection and sharing at the heart of concerns, (5) experimentation, validation and training laboratories (cyber range), and experimentation in the factory and industrial research challenges.

3.2.3 Greece

3.2.3.1 Current status

The Hellenic (Greek) cluster includes the National Cyber Security Authority (NCSA), established in the Ministry of Digital Policy Telecommunications and Media, following a Presidential Degree. It is the responsibility of NCSA to coordinate all competent Ministries as well as independent Greek authorities, with the aim to take all the steps, which are necessary for a secure Cyber space in Greece. The General Directorate of Cyber Security of the Ministry of Digital Government (National Cyber Security Authority) is responsible for its management Strategy as well as for coordinating the Bodies during the implementation of the required measures. Indicatively, by means of the Strategic Plan, the main goal lies in the definition of suitable organisational. Technical as well as operational measures. NCSA is in the strategic level. The Cyber Defence Directorate of HNDGS (Hellenic National Defence General Stuff) possesses the main national “technical role”, be it the Hellenic National Computer Security Incident Response Team (CSIRT) on the response to incidents in the military sector – cyber defence (military CSIRT), the response of incidents to critical infrastructure as well as the operational completion. Additionally, the National CERT and National Cyber Security Incident Response Team (NCSIRT also constitutes the Cyber Defence Directorate of the Hellenic Armed Forces) closely cooperate with NCSA towards the purpose of handling all national critical incidents. Moreover, the NIS directive is in effect in Greece. Nevertheless, there are a lot of mandatory steps, which need to be completed, such as the identification of essential services. Furthermore, there exists a published National Cyber Security Strategy, and this refers to the establishment of a national incident notification procedure and legislation, as far as rules and penalties are concerned. In addition, the Greek Cybercrime Centre (GCC) has been established. Amongst other activities, the Centre (www.cybercc.gr/en/) deals with the DG-HOME funded project, which primarily aims at the improvement of research and education, maintained by the Center for Security Studies as well as the Hellenic Police. Therefore, GCC has the following objectives:

- The advancement of cyber security training and University education in Greece
- The improvement of research in focused areas of cybersecurity and crime
- The mobilisation of the Greek constituency in cyber security and crime, and
- The collaboration with similar centres to maximise the uptake of results

The mission of the Cybercrime Directorate includes prevention, investigation and suppression of crimes or anti-social behaviour, committed via the internet or other electronic means of communication. Besides, there are various other cyber security activities, such as the Annual Cyber Defence national exercise, called “PANOPTIS”, the KEMEA annual conference on CI protection as well as the Hellenic Team of European Cyber Security Challenge.

Concerning the personal data and privacy at the National level, there exists the Hellenic Data Protection Authority (HDPA), which oversees the monitoring of the implementation of the provisions of the EU General Protection Regulation Data Law and GDPR, with a view to protecting fundamental rights and freedoms of individuals versus the processing of data that also facilitate the free movement of data inside the European Union.

Other major pillars at the National level, as described in the National Cybersecurity strategy, are the National Telecommunications and Post Commission (E.E.T.T.) and KEMEA. EETT constitutes an Independent Administrative Authority; it is the National Regulator, regulating supervising and controlling the following:

- The electronic communications market: fixed and mobile telephony, wireless and internet companies
- The postal market, in which the supply companies operate postal and courier services

KEMEA is a scientific, research and consulting body. Its purpose is to conduct theoretical research, applied research and elaboration studies, particularly at strategic level, on issues related to Security Policy as well as to provide services of an advisory nature and on security issues, in general.

3.2.4 Austria

3.2.4.1 Current status

Austria adopted a new Cyber Security strategy in 2021 (OSCS 2021) which is a further development of ÖSCS 2013, which defined certain processes and structures in order to ensure overall coordination of numerous stakeholders, which are working individually to improve cybersecurity. With ÖSCS 2021, the federal government adopted a renewed, comprehensive and proactive concept for the protection of cyber space and people in virtual space. The ÖSCS 2021 therefore forms the foundation of national cooperation in this area. With the Austrian Strategy for Cyber Security, an operational cyber coordination structure was established at national level, which contributes to the long-term creation of a secure cyber space as a contribution to increasing the resilience of Austria and the European Union through a national approach.

The ÖSCS 2021 pursues the following goals:

- Austria has sufficient financial and human resources to prevent cyber threats and incidents, to recognize them as such, ward them off and to prosecute such attacks;
- Austria has the ability to protect and defend its critical information systems and infrastructure in the event of a crisis;
- In Austria, cyber security is perceived as a joint task of society, business and the state; Responsibilities and competencies are clearly defined and lived by all those involved;
- Austria has a nationwide picture of the cyber situation; Cyber security skills are strengthened and promoted in all areas of society, life and work, and awareness is created;
- In Austria, secure participation in social and political life in cyberspace is possible for citizens;
- Austria has clear legal and operational options to offer a secure and attractive business environment in cyber space and to ensure adequate criminal prosecution if necessary;
- Austria is actively involved in the cyber area and works intensively with all stakeholders at national, European and international level;
- In cooperation with the EU, Austria can guarantee its digital sovereignty and contribute to the strategic autonomy of the EU;
- In Austria there is a coordinated and networked research and development landscape in the field of cyber security;

- Austria is training enough cybersecurity professionals to increase cybersecurity resilience, meet labour market demand and fight cybercrime in a sustainable manner;
- Austria makes an active contribution to the application and strengthening of international standards for cyberspace;
- In a nationwide approach, Austria is constantly working on the further development of its legal basis to increase cyber security and combat cybercrime.

The National Cyber Security Coordination Center in Austria is a cooperation between the Federal Chancellery (BKA) and FFG (The Austrian Research Promotion Agency) and, as part of the EU-wide network of national coordination centers, forms together with the European Competence Center for Cyber Security (ECCC) the new European framework to support innovation and industrial policy in the field of cybersecurity.

The Austrian Cyber Security Platform (CSP-AT) was established as a public-private partnership to facilitate ongoing communication with all stakeholders of the administration, economy, and academia. It organises regular general meetings twice a year, which became a forum for information exchange between stakeholders of the Austrian Cyber Security ecosystem. SPARTA partner JR participates in those meetings regularly and promotes the SPARTA network and its activities.

3.2.4.2 SPARTA's actions in the third year

SPARTA has been promoted by JR in several more occasions such as the EDIH Brokerage event of SPARTA Day, at the CONECT Business Academy, at the DIH Süd information event at FH Joanneum, at the Silicon Alps webinar "Cybersecurity Insights: Emerging Threats in Europe", at Trend-Radar: "Digitalisierung und Automatisierung für Energiegemeinschaften", at the Silicon Alps Cluster event series "Spotlight Cybersecurity", at the CONECT Informunity Security Trends Online Round Table and in several business meetings with members of the industry or the scientific community.

3.2.5 Poland

3.2.5.1 Current status

The core element of the cybersecurity in Poland at national level is the National Framework of Cybersecurity Policy of The Republic of Poland for 2017-2022. The Polish cybersecurity strategy identifies the scope of the National Framework of Cybersecurity Policy and vision, main goals and specific objectives in the cybersecurity context at the national level. Defined strategic objectives with sets of sub-objectives address such challenges as increased capacity for actions to prevent, detect, combat and minimise the impact of security incidents, enhanced capacity to counter react to cyber threats, increasing the national potential and competence in the area of security in cyber space, and building international position of Poland in this area.

Since 2021 in Poland there is also implemented National Cybersecurity System. In fact, it entered into force on August 28, 2018 as the act on National Cybersecurity System, but in order to fully implement the NIS Directive in Poland, it was necessary to adopt additional regulations as executive acts. Within the National Cybersecurity System, NASK which is one of the SPARTA partners is one of three national level CSIRTs. NASK handles, analyses and coordinates responses to incidents related to civil cyberspace security in Poland.

CERT Polska[7] is a core part of CSIRT NASK and the oldest CERT in Poland. Since its creation in 1996, 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, supported by the research staff of the institute, particularly the Network and Information Security Methods Team.

[7] https://www.cert.pl/en/

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

Poznan Supercomputing and Networking Center (PSNC)[8] – since 1993, integrating and developing the information infrastructure for science has been the mission of PSNC affiliated with the Institute of Bioorganic Chemistry at the Polish Academy of Sciences.

CYBERSEC HUB[9] is a network of integrated activities supporting and promoting companies in Malopolska Region from cybersecurity sector.

In Poland, there are also at least two governmental clustering initiatives launched in last years. PWCyber – Program Współpracy w Cyberpezpieczeńswie (eng. Cybersecurity Cooperation Program) is focused on raising the competences of the entities of the national cybersecurity system in terms of awareness of threats, methods of attacks in cyberspace as well as legal, organizational and technical skills to counteract threats in ICT systems and networks[10].

Governmental cybersecurity cluster #CyberMadeInPoland[11] was established as a platform for cooperation and promotion of the Polish cybersecurity industry. Its goal is to define directions and develop safe cyberspace in Poland and to promote Polish companies abroad. The cluster also stimulates the cooperation of the sector with scientific institutions, public administration entities, international corporations, industry and trade, and other partners.

Among newly established initiatives, it is worth to mention also the Maritime Cybersecurity Center – a think tank operating within the Command and Naval Operations Department of the Polish Naval Academy. The main focus is put on management of cybersecurity, cybercrime and securing maritime and space infrastructure. Prof. Michał Choraś from ITTI is involved in this initiative.

3.2.5.2 SPARTA's actions in the third year

- NASK was among the founders of the macrocluster - Technologies in Public Safety,
- NASK was established cooperation with the Global Cyber Alliance,
- NASK organized Internet Governance Forum 2021 and 2022,
- In October 2021, NASK co-organized SECURE conference with a special track dedicated to the SPARTA project,
- NASK was involved in information hub "PoLAND of IT Masters" focused on promotion of Polish achievements in the area of IT (also cybersecurity),
- PPBW together with #CyberMadeInPoland cluster was institutional partner of CyberSec Forum/EXPO 2022.

3.2.6 Germany

3.2.6.1 Current status

UBO and partners are actively participating and hosting the events as already listed previous deliverables. Thus, the next chapter will give a brief overview of actions carried out in the final year of SPARTA.

3.2.6.2 SPARTA's actions in the third year

The event format "Bonner Dialog für Cybersicherheit (BDCS) (in German)" (https://www.fkie.fraunhofer.de/de/Veranstaltungen/bonner-dialog-fuer-cybersicherheit.html) has

[8] http://www.man.poznan.pl/online/en/
[9] http://cybersechub.eu/
[10] https://www.gov.pl/web/cyfryzacja/program-wspolpracy-w-cyberbezpieczenstwie-pwcyber--partnerstwo-publiczno-prywatne-na-rzecz-krajowego-systemu-cyberbezpieczenstwa
[11] https://cybermadeinpoland.pl/

been successfully continued as series of online editions which were moderated by Prof. Dr. Michael Meier from SPARTA partner UBO:

- The 16th edition took place on March 17 2021 and was dedicated to the topic "Corona 2020 – Was sonst noch geschah: IT-Gesetzgebung in außergewöhnlichen Zeiten (in German)". Following a keynote given the Federal Commissioner for Data Protection and Freedom of Information Prof. Ulrich Kelber, he and the further panelist Dr. Ulf Buermeyer (Head and Legal Director of Society for Civil Rights e.V. (Gesellschaft für Freiheitsrechte e.V. or "GFF")), Dr. Sven Herpig (Head of International Cyber Securiy Policy at Stifung Neue Verantwortung), Dr. Dennis-Kenji Kipker (University of Bremen) and Andreas Könen (Director General CI – Cyber- and Information security in the German Federal Ministry of Interior) discussed recent IT and Cyber Security related regulations created during the Corona pandemic. This event attracted about 400 participants. Video recording is available here: https://www.youtube.com/watch?v=-0B4N8Hvh68
- The 17th edition on October 27 2021 focussed the topic "Wem gehört die digitale Welt oder wie souverän sind wir noch? (in German)". The panellists Ann Cathrin Riedel (LOAD e.V.), Dr. Patrick Breyer (Member of the European parliament), Klaus Landefeld (Association of the Internet Industry) and Anke Domscheit-Berg (member of the Bundestag) discussed about digital sovereignty. Video recording: https://www.youtube.com/watch?v=zg_6-eyeYg4
- The 18th edition took place as hybrid event at the University of Bonn and was on the topic of Ransomware. After a keynote given by Michael Daum (Senior Underwriter Cyber at Allianz Global Corporate & Specialty SE) he and the further panelists Heimo Krum (deputy CIO Funke Mediengruppe), Uli ten Eikelder (Head of Security Awareness and Communication, Deutsche Telekom Security GmbH) and Dr. Christian Nawroth (Federal Office for Information Security) discussed the threat of ransomware as well as preventive and reactive means. Video recording: coming soon.

Under the umbrella of the "Allianz für Cybersicherheit (in German)" numerous online networking events took place during the pandemic. The following Cyber Security Web Talks were organized:

- 12.04.2022 - Cyber-Sicherheits-Web-Talk “Unternehmen im besonderen öffentlichen Interesse (UBI) der Kategorie 1 (AWV-UBI)”
- 29.03.2022 - Cyber-Sicherheit in der Hotellerie
- 22.03.2022 - Schwachstellen-Management als präventive Maßnahme für mehr IT-Sicherheit
- 08.12.2021 - Unternehmen im besonderen öffentlichen Interesse (UBI)
- 01.10.2021 - Digitale und sichere Identitäten: Auf dem Weg zu mehr Cyber-Sicherheit!
- 20.05.2021 - Datenretten: Auf das Backup kommt es an
- 23.04.2021 - Kritische Infrastrukturen schützen! – Gemeinsam für mehr Cyber-Sicherheit
- 11.03.2021 - Virtuelle Versammlungen und Abstimmungen: Herausforderungen und Chancen
- 27.01.2021 - Warum Pentesting erfolgsrelevant ist: Erfahrungen aus der Praxis
- 03.12.2020 - Cyber-Sicherheit und Einfachheit: eine unmögliche Balance?

The cooperation between SPARTA partners and the cybersecurity training and educations initiative "Lernlabor Cybersicherheit" operated by Fraunhofer and several universities of applied sciences, was continued and further strengthened.

SPARTA partners are continuously involved in the preparation and execution of European research projects. SPARTA partner UBO was involved in the preparation of one project proposal with 29 European partners and in the preparation of another project proposal with 10 partners. Furthermore, UBO is currently planning a new project proposal together with SAP and further partners.

3.2.7 Czech Republic

3.2.7.1 Current status

In the Czech Republic, the National Coordination Centre for Cyber Security Research and Development (hereinafter "the Centre") was established by Regulation 2021/887 of the European Parliament and of the Council in May 2021, establishing a European Industrial, Technological and Research Centre for Cyber Security Competences and the network of national coordination centres (hereinafter "Regulation 2021/887").

This initiative aims to promote coordination in cyber security R&D at international level (between the Member States of the European Union and the European Union institutions - the European Commission, the European Cyber Security Agency and the European Cyber Security Competence, Technology and Research Centre), creation of national professional communities (consisting of state administration institutions, academia and the private sector), ensuring effective communication between the European Union institutions and entities at the national level, as well as strengthening existing regional cooperation or finding new ways to establish it. The Czech Republic will thus have the opportunity to more effectively manage the funds allocated under the European Union programs (Digital Europe, Horizon Europe and possibly others) both for the Centre's activities and to support related activities of other entities at the national level. The National Office ensures the establishment of the Centre in the Czech Republic for Cyber and Information Security which will be the primary contact point for communication with the European Union and, at the same time, the coordinator of cooperation at the national level.

3.2.7.2 SPARTA's actions in the third year

The Centre was established by the SPARTA associate, the Czech NCISA, and all the Czech SPARTA partners, CESNET, BUT and CZ.NIC were involved in the initial as well as subsequent development of the Centre. Especially, the partners actively participated in the meetings of the Platform for research and development in cyber and information security. The Platform gathers representatives of the public, private and academic sectors to identify their research needs and possibilities for cooperation. The platform currently has 22 members and continues to grow. The first meeting took place in June 2021 online. The second meeting took place physically on November 12, 2021 at the Brno University of Technology. The third meeting was also held physically, on March 31, 2022 in the premises of TACR in Prague.

Additionally, CESNET organised three dedicated meetings for the Ministry of Defense and Armed Forces of the Czech Republic on various cybersecurity topics to foster further cooperation.

Furthermore, Brno University of Technology is the founding member of the Cybersecurity Hub[12], an institute founded in 2020. This joint activity with Masaryk University and Czech Technical University aims at coordination of national activities in cybersecurity and supporting the Centre in its activities.

3.2.8 Lithuania

3.2.8.1 Current status

Considering the deteriorating landscape of cyberthreats as well as the growing number and complexity of incidents, Lithuanian government invested significant resources in strengthening the state's cyber security and defence capabilities. The Lithuanian government undertook the following initiatives:

- Implemented new legislation preventing unreliable manufacturers from participating in the development of critical infrastructure, and the removal of equipment manufactured in unfriendly countries from critical infrastructures and public service
- Development of cyber security and defence capabilities to increase the resilience of national institutions
- Strengthening international collaboration with NATO and EU

[12] https://www.em.muni.cz/en/news/13454-cybersecurity-hub-a-new-centre-for-cooperation-on-cybersecurity

- Development of the Regional Cyber Defence Centre as the main platform for innovations development and specialist training in cybersecurity domain.

It is important to note, that Baltic States are under constant and multi -vector attacks from Russia. Attempts to influence policy actors, disinformation campaigns, large scale cyber-attacks and persistent hybrid threats remain a crucial aspect of Baltic States security.

There is growing understanding, that security and defence practitioners must be supported with the latest technologies to enhance their ability of timely detection and awareness of potential threats.

National Information Impact Identification and Analysis Ecosystem (NAAS)

Mykolas Romeris University (MRU) and General Jonas Žemaitis Military Academy (LKA) jointly implemented a project aimed to establish a National Information Impact Identification and Analysis Ecosystem (NAAS). Innovative technological platform is procured under the rules of precommercial procurement, which allows collaborative development of technologies that are not yet available in the market.

The technological solution created during the project, will allow to conduct research, test national and EU funded innovations, support and facilitate innovations uptake by security and defence practitioners.

NAAS ecosystem will become a marketplace to help various stakeholders from academia, SMEs, RTOs, to showcase their solutions to security practitioners, generate new research ideas, make new contacts and foster cooperation and collaboration between innovation developers and potential users.

Innovations developed by SPARTA research programs will be evaluated by NAAS team of researchers and will create opportunities to showcase innovation to security practitioners.

DI4 LITHUANIAN ID:

To achieve significant breakthrough in digital innovations the Lithuanian government supported the establishment of national cluster DI4 LITHUANIAN ID (Digital Innovation for Lithuanian Industrial Development) that will supply services for the digitalisation and progress of industries in Western and Central Lithuania. DI4 LITHUANIAN ID unites 14 organizations that have outstanding achievements in the fields of:

- High-Performance Computing
- AI
- Cybersecurity
- Training and Education

The concept and latest developments of National DIH were introduced during SPARTA brokerage event as a perfect place to showcase latest achievements, make new contacts, develop new project ideas and foster collaboration between SPARTA community and national clusters.

Missions

To boost innovation ecosystems that address the most critical societal challenges Lithuanian government issued a mission-based science and innovation program.

The missions aim to strengthen research, experimental development, and innovation (R&D&I) capacities, foster targeted interdisciplinary research and innovation activities to address specific societal challenges, develop innovative technologies and solutions, and foster the country's competitiveness through innovation.

The government seeks to make the missions specific enough, but not too narrow, to ensure that the missions are horizontal, interdisciplinary and that the mission challenge is fully addressed.

The missions are expected to be carried out by research and business consortia composed of research and study institutions and business entities. Consortia will be selected through an open and fair competition.

First missions (2022–2026) will be funded under the New Generation Lithuania plan. The Government plans to allocate 63.7 million euros for the implementation of the missions.

Non-refundable grant will fund the following activities:

- research and experimentation
- development and implementation of innovations
- commercialization of research results
- protection of intellectual property
- certification,
- infrastructure development
- participation in international networks.

Recently LT government announced the shortlist of preselected project ideas.

The idea: “Strengthening Lithuania's cyber resilience in the context of the digital society” made it to the shortlist from six ideas submitted to the mission call. The consortium that leads the mission has strong links with SPARTA community.

3.2.8.2 SPARTA’s actions in the third year

National Coordination Centre (NCC)

Recently Lithuania established its National Coordination Centre that is designed to support innovation and industry policy in the cybersecurity domain and establish strong collaboration links with European Cybersecurity Competence Centre.

The NCC will play a key role in delivering cybersecurity objectives of the Digital Europe Programme with a strong focus on innovations development, uptake and dissemination in cybersecurity domain.

It is expected that SPARTA will become a trusted partner for Lithuanian NCC by sharing the knowledge and results developed during the implementation of the project.

After the several workshops organised by SPARTA network members (L3CE, LKA) following collaboration directions have been identified:

Awareness and skills

- Education
- Training

Sustainable collaboration links with national and EU stakeholders:

- International networks of cybersecurity community
- Digital Innovation Hubs
- ECSO
- 4Pilots – (SPARTA, ECHO, CONCORDIA, CyberSec4Europe)

Human and social perspective and European values

- Ethics
- Privacy
- Identity management
- Liability and accountability.
- Openness and transparency.
- User aspects.

Supply-chain resilience and cybersecurity

- Risk assessment and mitigation.
- Incident detection, analysis and sharing
- Standardisation and certification

SPARTA could serve as a reference point for Lithuanian NCC by integrating Lithuanian cybercommunity into SPARTA ecosystem. The most significant results achieved by SPARTA in the areas would be reused to the development of ambitious innovations program in the cybersecurity domain and establish well-functioning national ecosystem:

- WP2 innovation: Ethical, Legal and Societal Aspects
- WP3 Roadmap design
- WP9 Training and Education
- WP10 Sustainable exploitation& IPR
- WP11 Certification organization and support

Next steps towards SPARTA- LTNCC integration:

- Engagement of SPARTA network members and Associates in the national innovation's development projects
- Exploitation of SPARTA ecosystem to dissemination of LT made innovations
- Integration of LT NCC with SPARTA JCCI
- Involve SPARTA stakeholders in the development of national competences and capabilities

3.2.9 Spain

3.2.9.1 Current status

The Spanish Cybersecurity Strategy has had a special push this year with the approval of the Cybersecurity National Plan the 29th March 2022. This plan has as its main objective the definition of specific actions and projects to put into action the measures defined in the Cybersecurity National Strategy defined in 2019. The plan is for the next 3 years and has more than 130 actions with a budget of 1000 million euros. Many of the actions are related to the Recovery, Transformation and Resilience Plan[13].

The Spanish Cybersecurity Ecosystem continues to grow with the Spanish "National Cybersecurity Forum", in which SPARTA partners like GRADIANT and TECNALIA take part, having published its first results[14] and continue its work in it in the area related to R&D and the development of a Spanish Cybersecurity Strategic Research Agenda aligned with EU´s cybersecurity strategy.

Trying to push forward the creation of the Spanish Cybersecurity Community, it has been presented a proposal to obtain financial support for its research and networking activities to the public consultation asked by INCIBE. While periodic meetings with INCIBE and the Spanish members of the four pilot continue.

It must be mentioned that INCIBE will be the Spanish national coordination centre of the Network of National Coordination Centres (NCC) of the European Cybersecurity Competence Center (ECCC).

3.2.9.2 SPARTA's actions in the third year

Contacts with different associations and companies to promote their involvement in SPARTA have go on during this last year. Some examples are the presentation of SPARTA made by TECNALIA in the Spanish Chapter of the Women4Cyber and the presentation of SPARTA under the title " Escenario de seguridad digital en Europa: el caso Sparta " in the event "Encuentro sobre Ciberseguridad Y Protección De Datos", organised by Fundecyt-Parque Científico y Tecnológico de Extremadura and the "Secretaria General de Ciencia, Tecnología, Innovación y Universidad de la Junta de Extremadura".

[13] https://www.dsn.gob.es/es/actualidad/sala-prensa/plan-nacional-ciberseguridad-0
[14] https://foronacionalciberseguridad.es/index.php/publicaciones

3.2.10 Luxemburg

3.2.10.1 Current status

SMILE is in the process of reorganizing its activities, with the purpose of better supporting the growth of the Cybersecurity Ecosystem. There are now more than 300 companies having some level of security services or products in their offer in the country.

SMILE is now in charge of the national portal on Cybersecurity ("Cybersecurity Luxembourg"), and coordinating the different stakeholders to ensure that the country's citizen and organisation can get the right level of support or services with regards to their security needs. For doing so, it deployed and actively maintains a website at this address: https://www.cybersecurity.lu/

Finally, SMILE is becoming the National Coordination Centre (NCC) in the framework of the Regulation of the 20th of May 2021 on the ECCC. It is actively involved in the network build-up, along with other NCC's. It did also define five areas of priority, in order to fulfil its obligations as part of the regulation, but also to support effectively the European Centre (ECCC).

1. Education and Training, Assistance, Vulgarisation (Competence)
2. Research, Innovation, Industrialization (Industrial Capability)
3. Community Animation and Evaluation (Ecosystem)
4. Coordination, administration, liaison ECCC
5. Funding programs management (In close cooperation with the Ministry of Economy)

The ongoing reorganisation is done in a way that will support these domains of activity with high priority.

3.2.10.2 SPARTA's actions in the third year

As part of the WP10 activities, SMILE kept developing the RAMP platform. It is still aimed at improving the re-use of research outcomes from previous EU funded research programs. It is also designed to support smaller entities in their compliance and reporting obligations when participating to EU funded projects, as the "administrative overhead" was identified as being a roadblock to the participation of such entities to research projects.

The RAMP Platform was also deployed on the JCCI, in order to make it more accessible, but also to increase the overall usage value of the JCCI.

As part of the preparation of Deliverable D10.5, SMILE ran two hackathons focused on generating business initiative from SPARTA research products. The first one took place in 28 to 30 of January, 2022 and was mostly online. Six teams participated. The second one happened in 20 to 22 of May, 2022 in Luxembourg, and involved 7 teams. As a consequence of both events, three teams were selected for mentoring activities. Two of them are mature enough for generating a start-up project if the teams decide to do so once the mentoring activities are over.

SMILE also supported the outreach to the Commission and the ECCC through WP1 related activities, and in particular the Executive Boards and Strategic Direction Boards that took place during the extension period.

3.2.11 Portugal

3.2.11.1 Current status

C-Hub, the Portuguese Digital Innovation Hub on cybersecurity created in 2021, led by the National Cybersecurity Centre (CNCS), with participation of INOV has been recognized in 2022 as a European Digital Innovation Hub.

Since 2021, Portugal implemented the Digital maturity seal on Cybersecurity, as part of the Digital Transaction Action Plan, allowing SMEs to assess and be certified, regarding their Cybersecurity Digital Maturity resorting to a scale of Bronze, Silver and Gold.

Beginning of 2022 CNCS has published the Cybersecurity Competence Framework, which builds on top of the National Cybersecurity Framework and the Roadmap for Minimum Capabilities in Cybersecurity, and inspired by the National Initiative for Cybersecurity Education (NICE) of the US National Institute of Standards and Technology (NIST) and the Singapore Skills Framework.

3.2.11.2 SPARTA's actions in the third year

A SPARTA cybersecurity workshop was developed in Madeira University, with the goal of providing the necessary means for the creation of a cybersecurity curriculum, ensuring that students at the university level have access to education on cybersecurity, a subject of growing critical importance. The workshop was organised by INOV and led by the Brno University of Technology and L3CE.The University of Las Palmas de Gran Canaria showed a keen interest in establishing a Cybersecurity bachelor degree, in a collaborative effort with SPARTA project.

3.2.12 Latvia

3.2.12.1 Current status

With recent activities in Ukraine and Latvia's support to Ukraine in ongoing war, there have been increased cyber activates within Latvia cyberspace. This has sparked and improved collaboration between Latvian national bodies and critical infrastructure, as well as initiated / speed up new plans to improve national cyber space.

The Latvian government has approved the development of new, National cybersecurity centre in 2023. The goals of new cybersecurity centre will be to increase cybersecurity level in all government entities. It will also improve coordination and review of national cybersecurity projects, ensuring similar approach across government sector. Ministry of Defence will oversee the new cybersecurity centre, which will integrate existing CERT.LV unit.

CERT.LV, together with NATO experts from Canada are improving cooperation and testing Latvian national government system vulnerabilities, improving existing cooperation procedures on real examples.

To take advantage of new technologies, the Ministry of Defence has signed an agreement of cooperation with LMT to future improve and develop military 5G test site Adazi military base. The 5G test base in Adazi, Latvia, was one of first military 5G test sites in Europe, when it opened in 2020. It has been proven as place to test and develop new technologies and have raised interest in other NATO countries as well.

Latvia has developed cybersecurity industry ranging from hardware producers at Mikrotikls to communication security products to different cybersecurity services including e-signature and digital id services from LVRTC to NOTAKEY.

NGO and civic activity field in cybersecurity is well developed as there are active local and international NGO like ISACA, United cyber-defence league, LIKTA, NETSAFE active in country.

Latvia has four universities active in cybersecurity area BA School of Business and Finance, Vidzeme University of Applied Sciences, University of Latvia and Riga Technical University.

3.2.12.2 SPARTA's actions in the third year

LMT researched possible 5G impact on election process as part of T-SHARK program. During the research LMT used 2021 Latvian municipal elections as case study to show, how mobile networks can be used to detect election interference. LMT also looked at other benefits and possible risks of 5G features to publish research paper "5G network and elections: pros and cons". Research was published in SPARTA webpage https://sparta.eu/news/2022-05-25-5g-elections.html.

3.2.13 Italy

3.2.13.1 Current status

The Italian community started already some 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 collects expertise from more than 300 researchers actively working in Cybersecurity. It contributed to create the Italian Cybersecurity Framework[15] and several successful initiatives as CyberChallenge.IT, the Italian cybersecurity challenge.
- CNR had an interdepartmental security project and later a cybersecurity one putting together the expertise 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 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 in SPARTA.

CINI, CNR and CNIT created on February 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.

Thus, since 2017, Italy streamlined and strengthened its cybersecurity structure to boost its cyber capabilities, with DIS at the centre of the Italian cybersecurity ecosystem's governance, acting as:

- Supporting body for the Prime Minister and the Inter-Ministerial Committee for the Security of the Republic (CISR) on cyber issues.
- Chair of the Cybersecurity Management Board – Nucleo Sicurezza Cibernetica (NSC) an interagency and intergovernmental operational body within the DIS tasked with cyber crisis prevention, preparation and management.
- European Point of Contact under the Network and Information Security (NIS) directive.

In 2021, the Italian agency for cyber security (ACN) has been established taking expertise from DIS and other ministries as MISE. This is a main activity at the Italian level in cyber security, and a cornerstone of the Italian architecture for cybersecurity.

3.2.13.2 SPARTA's actions in the third year

The SPARTA clustering is thus representative of the Italian Cybersecurity ecosystem and the clustering activities of SPARTA in the sector. Nevertheless, the aim is to enlarge also to other partners especially in vertical/applicative sectors. Indeed, as mentioned above the Italian presence in SPARTA already collects the main public and research stakeholders, including the national industry champion i.e., LEONARDO.

SPARTA partnership has been thus enriched with several organizations representing industry and end users. Several new end-users joined the community and participated to joint projects and activities.

CNR and CINI collaborated to Tuscan Cyber security centre (involving the Tuscany Region) and are working to cooperate with SPARTA activities (also through the cybersecurity observatory of the Tuscan region, also provided as part of JCCI).

The plan is to continue to work at SPARTA project level as well as at national one in a linked manner.

We had to have other SPARTA Italian events in October 2021 and in June 2022 (cybersecurity day 2021) and work to promote the presence of European Digital innovation Hubs present in Italy also in SPARTA.

[15] https://www.cybersecurityframework.it/

The Italian partners as LEONARDO, CINI, CNR, MISE are explicitly mentioned in the cybersecurity strategy recently promoted from ACN.

More recently CINI, CNR and CNIT together with LEONARDO and other assciates/friends in Italy made a successful proposal for a public private partnership (Partenariato Esteso 7 Cyber) that will be granted an amount of 100ME in three years (25 Italian partners). This stemmed from the SPARTA core Italian partners.

3.2.14 Estonia

3.2.14.1 Current status

Estonian Government Security Committee is responsible to analyse and assess the national security situation and coordinate the activities of authorities of executive power regarding planning, developing, and organisation of national defence. In 2009, the Cyber Security Council was established at the **Government Security Committee**. The **Cyber Security Council** is the strategic level coordination unit between various institutions, which conducts the implementation of the Estonian Cyber Security Strategy. The Council is chaired by the Secretary General of the Ministry of Economic Affairs and Communications. Ministry of Economic Affairs and Communications is the leading ministry in the area of cyber security.

Estonia has developed the third Cybersecurity Strategy for the period of 2019–2022 (https://www.mkm.ee/media/703/download).

The Cybersecurity Strategy lays down four important objectives:

- Estonia is a sustainable digital society relying on strong technological resilience and emergency preparedness.
- Estonian cybersecurity industry is strong, innovative, research-oriented and globally competitive, covering all key competences for Estonia.
- Estonia is a credible and capable partner in the international arena.
- Estonia is a cyber literate society and ensures sufficient and forward-looking talent supply.

The Ministry of Economic Affairs and Communications implements the cyber security strategic objectives with the cooperation of other ministries and in close co-operation with the following partners:

- **Estonian Information System's Authority** (RIA) – Co-ordinates the development of information systems, maintains the state network, develops, and supports the implementation of national information security standard (https://eits.ria.ee/), coordinates the critical information infrastructure (CII) protection by advising and providing them pen testing services. In the composition of RIA is the CERT-EE/CSIRT. CERT monitors the Estonian computer network and solves cyber incidents. RIA conducts the cyber security awareness campaigns and trainings, coordinates the safe implementation of IT infrastructures important for the state and conducts supervision. RIA is also a national contact point for international cooperation in the field of IT security and collaborates with private and public sector IT staff to keep contacts with experts (exercises, trainings, information sharing). (https://www.ria.ee/).
- **Cyber defence unit of the Defence League** – is a voluntary organisation aimed at protecting Estonian cyberspace in the time of crisis. Cyber defence unit is a national collaboration model for cyber security professionals and technology experts, structurally integrated into Estonia's voluntary National Defence organisation (https://www.kaitseliit.ee/en/cyber-unit)
- **International Centre for Defence and Security** (ICDS) – Research and analysis in the field of NATO and EU security and defence (https://icds.ee/).
- **Association of Information Technology and Telecommunications** (ITL) – non-profit association uniting information and communication technology (ICT) companies and organisations (https://www.itl.ee/en/) to improve the cooperation between the private and public sector.

There are several other organizations supporting wide range cyber security objectives. Next are mentioned some of them.

Foundation CR14 "was established by the Estonian Ministry of Defence on the 1st of January 2021 and is based on more than 10 years of military-grade cyber range experience in cybersecurity training, exercises, testing, validation, and experimentation. CR14 is a government-owned and operated entity, which offers cybersecurity-related research and development for domestic and international; private and public sector partners" (from https://cr14.ee/).

"The main tasks of the **Estonian Defence Forces Cyber Command** are to organise operations in cyberspace, managing the information and communication technology in the area of responsibility of the Ministry of Defence, ensuring cyber security in the domain, providing Headquarters support for the Joint Headquarters, preparing and forming wartime and reserve units, leading and coordinating the development of cyber and management support capabilities, supporting the strategic communication of the Defence Forces and organising information operations" (from https://mil.ee/en/landforces/cyber-command/).

From the 1st of August 2020 the HITSA (formerly known as the Tiger Leap Foundation) have been transferred to **Education and Youth Authority** (Harno). Harno among other tasks develops and manages educational information systems, e-services, and ICT infrastructure (https://harno.ee/en/).

Startup Estonia is a governmental initiative which works closely together with the different Estonian ministries and stakeholders with the aim of connecting different sectors with the startup community. One of the StartUp Estonia focus area is CyberTech. "The goal of CyberTech focus is to strengthen the local CyberTech startup ecosystem, grow the number of new CyberTech startups and support the development of existing startups in the sector" (https://startupestonia.ee/focus-areas/cybertech). StartUps are also supported by accelerator programs. Startup Wise Guys conducts the **CyberNorth programm** which takes place in Tallinn, Estonia (https://startupwiseguys.com/cyber/).

ISACA Estonia Chapter is the Estonians ICT auditors and IT professionals' community, a voluntary organisation, which has monthly meetings to keep strong network between the members for more than 20 years. Also, the chapter has network with other ISACA chapters all over the world (https://www.eisay.ee).

From 2016, the eGovernment Academy holds and develops the **National Cyber Security Index** database. The NCSI measures "the preparedness of countries to prevent cyber threats and manage cyber incidents. The NCSI is also a database with publicly available evidence materials and a tool for national cyber security capacity building" (https://ncsi.ega.ee). Estonia is in fifth place in the ranking of NCSI countries.

Estonia is the host for the **NATO Cooperative Cyber Defence Centre of Excellence** since 2008. As the NATO-accredited cyber defence hub, it supports its members nations and NATO with unique interdisciplinary expertise in the field of cyber defence research, training and exercises covering the focus areas of technology, strategy, operations, and law. To name only some of NATO CCD CoE provided products or events like Tallinn Manual, Locked Shields international cyber defence exercise, the annual International Conference on Cyber Conflict CyCon gives an idea of the impact and scope of the activities (https://ccdcoe.org/).

The **Estonian Information Security Association** (EISA) was founded in 2018 to advance cross-sectoral cooperation in Estonia between the private sector, academia and government. The joint effort intends to formalise the existing ties between the cybersecurity partners in Estonia, boost collaborative participation, as well as look at and influence the European and international policies on cybersecurity. EISA intends to enhance R&D activities in the information security and cyber security field in Estonia (https://eisa.ee/).

Estonian Republic participates in the international cyber security projects. Some of them are EU CyberNet and Cyber4Dev.

Since 2019, RIA is the host and lead of **EU CyberNet**, which bridges the expertise across the European Union (EU), establishes a network and a practical learning platform for strengthening cybersecurity globally. The insights promoted by contributing experts shape the development and

execution of the EU policies towards partner countries within the field of cybersecurity. EU CyberNet is set to achieve four major deliverables: building a network of cybersecurity experts and stakeholders, developing a technical platform, providing training and assistance and becoming a knowledge hub of EU's external cyber engagements. (https://www.eucybernet.eu/).

Also, RIA is the member of the project **Cyber4Dev**. This is the EU Cyber Resilience for Development Project. It aims to increase cyber security in Africa, Asia, Latin America, and the Caribbean through topical training programs (https://cyber4dev.eu).

Estonia introduces its cyber security initiatives review in the book **Cyber Security in Estonia 2022** what is freely available at https://www.ria.ee/sites/default/files/content-editors/kuberturve/kuberturvalisuse_aastaraamat_2022_eng.pdf.

3.3 European level

3.3.1 Cooperation with EU Organisations

3.3.1.1 ECSO

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

3.3.1.2 ENISA

TECNALIA is part of the "Stakeholder Cybersecurity Certification Group" and several partners contributes to the Ad Hoc working groups, including the ones on label for certification.

3.3.1.3 ERCIM

Partners as CNR and INRIA are main players in ERCIM and in its Security and Trust WG. For the edition of the 2022 of the STM workshop, the co-chair is University of Luxemburg. Also, CNR and other SPARTA partners run the award for the best PhD thesis in the field.

3.3.1.4 IFIP

CNR and other partners support the FOSAD PhD school, promoted also by the IFIP WG1.14 on secure engineering. The 21st edition has been held in Sept. 2022 in cooperation also with CS4E pilot and the E-CORRIDOR project.

3.3.2 Cooperation with EU Projects

MEDINA - Security framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme (H2020-SU-ICT-2019)

"MEDINA proposes a framework for achieving a continuous audit-based certification for CSPs based on EU CSA's scheme for cloud security certification. MEDINA will tackle challenges in areas like security validation/testing, machine-readable certification language, cloud security performance, and audit evidence management. The MEDINA consortium is composed of academic and industrial partners, which play key roles in the EU cloud security certification ecosystem (e.g., research, cloud providers/customers, and auditors). MEDINA will provide and empirically validate sustainable outcomes in order to benefit EU adopters."[16]

SPARTA partners TECNALIA and CONSIGLIO NAZIONALE DELLE RICERCHE collaborate in this project and will try to establish collaborations between this project and the certification activities of SPARTA.

[16] MEDINA's objectives https://cordis.europa.eu/project/id/952633

AI4CYBER, Trustworthy Artificial Intelligence for Cybersecurity Reinforcement and System Resilience

The objective of AI4CYBER is to create an Ecosystem Framework of next-generation trustworthy cybersecurity services that leverage AI and Big Data technologies to support system developers and operators in managing robustness, resilience, and dynamic response against cyberattacks based on AI. In this project collaborates TECNALIA and THALES.

EUROBIN, European ROBotics and AI Network

The objective of euROBIN is to create a European ecosystem of robots that share their data and knowledge to learn to perform the different types of tasks that can be found in the environment in which humans work. euRONBIN wanst to advance in AI enabled robots that are accessible, usable and trustworthy. SPARTA partners like CEA, TECNALIA, INRIA and Fraunhofer FhG are taking part in this network

SPARTA T-SHARK programme cooperated with the H2020 project SAPPAN No 833418. “SAPPAN 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.”[17] Especially, the cooperation with SPARTA was performed in the field of privacy preserving sharing and collaborative learning.

Furthermore, SPARTA WP9 intensively collaborated with ERASMUS+ project REWIRE (Cybersecurity Skills Alliance – A New Vision for Europe, # 621701-EPP-1-2020-1-LT-EPPKA2-SSA-B). Representatives of REWIRE were involved in the CCN Education Focus Group, where all pilots meet on the subject of cybersecurity education and training and coordinate their activities. In fact, REWIRE may be considered a follow-up project where results achieved in SPARTA, such as good-practices for curricula design and tools produced are further used. CCN Education Focus Group was active during the whole lifetime of SPARTA and was one of the most active cooperation activities where all CCN pilots (CONCORDIA, Cybersec4Europe, ECHO and SPARTA) were represented.

SPARTA cooperated with **SecurIT** for launching Open Calls with the main objective of revolutionising the new global competitive security industry (product & service) by supporting a better integration of innovative security systems, in particular:

- supporting the development and integration of innovative security solutions in a new industrial value chain (and services);
- co-financing and supporting the development of collaborative projects allowing the prototyping and experimentation of technological solutions in the field of security, taking into account the ethical, legal and societal challenges of this sector;
- promoting cross-border cooperation between SMEs and other innovation actors in this sector.

Cooperation with the **NeCS** EU project community continued through the NeCS PhD winter school organized in Jan. 2022 that will have a follow up as SPARTA event also in Jan. 2023 (in cooperation with the other 3 Pilots). This is a major result of cooperation among the pilots in terms of formation of young PhD students from all the pilots that can work together in the future by exploiting the ties created during these events.

In addition the NeCS project has a joint PhD community with SPARTA of near 500 subscribers and contribute to the overall SPARTA partnership:

[17] SAPPAN’s objectives https://cordis.europa.eu/project/id/833418

Figure 15: NECS PhD Winter School

3.4 Monthly workshops

SPARTA workshops have the goal to integrate associates and the wider SPARTA and national communities. The information flow is bidirectional from SPARTA to attendees and from attendees to SPARTA, mainly related to Roadmaps, Research programs and community-based activities (partnership and JCCI). WP8 created with WP12 and WP3 a handbook for running SPARTA monthly workshops as well as a report form.

In the third year, 18 workshops were organised (listed below). Also, other events have been planned after the formal end of the project that since the SPARTA network will survive to SPARTA project, in particular the FOSAD phd school in Sept. 2022 and the Cyber Security Day in Italy (Oct. 2022).

done	SPARTA workshop	Czech Republic	Prague	Feb-21		CESNET
done	SPARTA workshop	Latvia	virtual	Mar-21		LMT
done	SPARTA workshop	Luxembourg	virtual	Jun-21		SMILE
done	SPARTA day/brokerage		virtual	Apr-21		ALL
done	SPARTA workshop -transpo	Italy	Bertinoro/hybrid	Sep-21		CNR+IMT
done	SPARTA workshop - Fosad	Italy	Bertinoro/hybrid	Sep-21		CNR+IMT
done	SPARTA workshop	Italy	Pisa	Oct-21		CNR
done	SPARTA workshop	Luxembourg	virtual	Nov-21		SMILE
done	SPARTA workshop	Baltic countries	virtual	Nov-21		L3CE (baltic coutries)
done	Cybersecurity Awareness	Caldas da Rainha	virtual	Oct-21		INOV
done	Cybersecurity Awareness	Maderia	virtual	Jul-21		INOV
done	Cybersecurity Awareness	La Reunion	virtual	Nov-21		INOV
done	SPARTA Hackathon I	Luxembourg		Jan-22		SMILE
done	SPARTA day		virtual	Mar-22		TUM
done	Hacker day	France	hybrid/Paris	Apr-22		YWH
done	SPARTA Hackathon II	Luxembourg		May-22		SMILE
done	SPARTA day	France	virtual	Jun-22		CEA
done	Convergence 2022	Belgium	Bruxelles	Jun-22		CEA

Figure 16: SPARTA monthly workshops in third year.

3.4.1 An example: the event organized by YesWeHack community in April in Paris.

To show the diversity and inclusiveness of the SPARTA approach, we consider here the event organized by YesWeHack community of ethical hackers where several SPARTA results and achievements were highlighted.

Location:	*Paris, France*	**Date and Time:**	13 & 14 April 2022 10h – 17h
Attachments:	Attendees list, presentations	**Organized By**	YesWeHack in cooperation with Doctolib, Malta, Blablacar

3.4.1.1 Agenda of the day

Welcoming remarks 13 April, 10h00

- Florent Kirchner, Strategic Director at SPARTA
- Guillaume Vassault-Houlière, CEO at YesWeHack
- Evangelos Kantas, Cybersecurity Expert at ENISA
- Cedric Voisin, Group CISO at Doctolib

The ethical hackers community: Challenges and opportunities to increase the cybersecurity readiness in Europe 13 April, 10h30

Moderated by Moderated by Nina Olesen, Head of Sector, Applications & Human Factors, ECSO

- Csaba Virag, Director of Capacity Building at Talgen Cybersecurity
- Evangelos Kantas, Cybersecurity Expert at ENISA
- Fabio Martinelli, Research director at CNR
- Ludovic Mé, Deputy Scientific Director at Inria
- Mario Trinchera, Technical Coordinator at CERTFin

Visit cyber campus 13 April, 15h00

- Keynote of William Lecat, Coordinator of the National Cybersecurity strategy and French representative at the Governing Board of the European Cybersecurity Competence Center
- Introduction to the Cyber Campus by, Alexandre Hamilton-Clark, Project Manager
- Demo of the "Bounty Hunter" Virtual Reality Game developed by YesWeHack

Apero & dinner 13 April, 17h00

- Drink station and foodtruck

Nominee announcement 14 April, 16h by Cedric Voisin, Group CISO at Doctolib

3.4.1.2 Main outcomes

This SPARTA monthly workshop consisted of two events. YesWeHack, in partnership with Doctolib, Blablacar, Malt and the cybersecurity network SPARTA, organised the first live Bug Bounty event dedicated to European scale-ups and unicorns and gathered high-level speakers to discuss policy issues related to the ethical hacker's community.

The live bug bounty: YesWeHack called on 40 of the best European hackers to come and challenge the information systems of Doctolib, Blablacar and Malt. For more than 30 hours, day and night, the hunters were busy to find vulnerabilities in the partners' information systems.

For corporate security teams, it has been a unique and invaluable opportunity to discuss their findings with researchers, and better understand security bugs.

During these 30 hours of hacking at Campus Cyber, 109 vulnerabilities have been reported!

SPARTA Monthly Workshop

Alongside the live Bug Bounty, a dedicated workshop of the SPARTA project, of which YesWeHack is a member, took place on the first day of the event. The workshop gathered the European ethical community, SPARTA partners and decision makers (including the representative from the French

cybersecurity directorate) to spread the SPARTA result and get feedbacks on the SPARTA Roadmap and programs by the specific audience of ethical hackers. In addition to that, the workshop aimed to discuss the current and future contribution of ethical hackers to the European cybersecurity.

The main outcome is grounded to further continue the collaboration between ethical hackers and European policy makers to give more legal protection to ethical hackers and to contribute to the works of the EU cybersecurity community to support the ECCC as well to ENISA works on the vulnerability management.

A wrap-up video (https://www.youtube.com/watch?v=_ukBP-3F31Q) was developed and published on SPARTA social media channels.

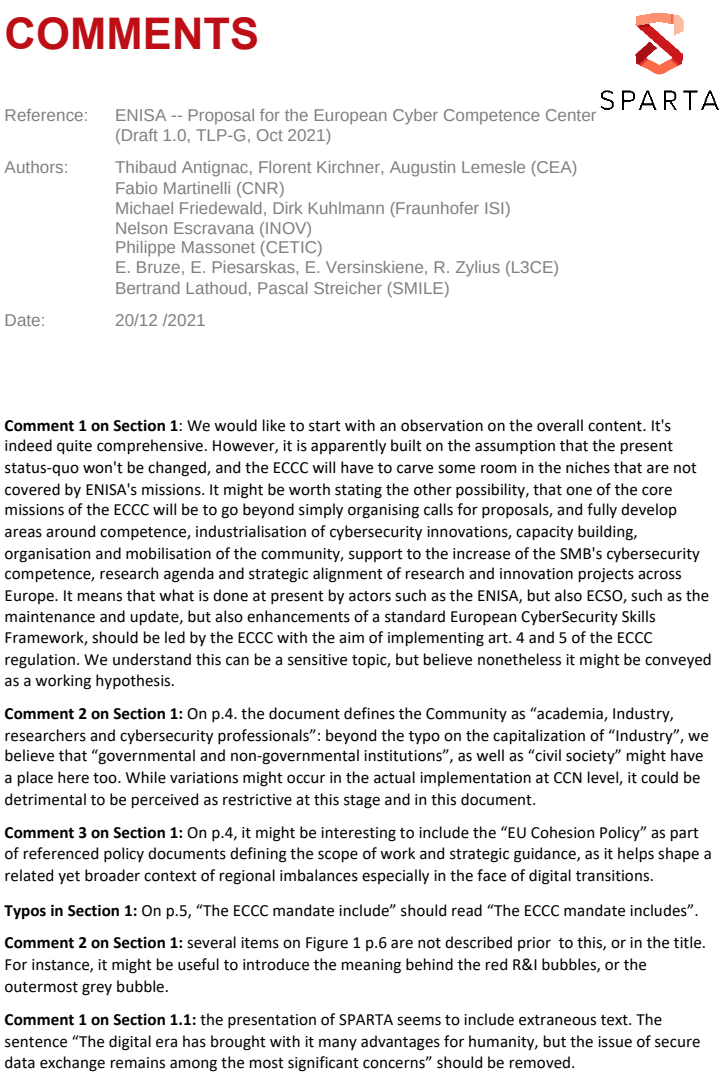
Chapter 4 Clustering with other pilots

As with previous years, the SPARTA pilot has explicitly allocated effort to the cooperation with the 3 other pilots, ECSO, and the Commission. In continuation with previous efforts, coordination has been taking place with the Commission through remote meetings, greatly facilitating the contacts with ENISA and the JRC, and extending the work started in 2020 on the Cybersecurity Act.

4.1 Federated workstreams

As for the second year, cross-pilots interactions during the final year were largely structured around *federated workstream*, topical working groups constituted across the pilots with the voluntary participation of ECSO, JRC, and ENISA. Since 2021, a structured approach of the workstreams was articulated, with direct inputs from the pilots, consolidating their approaches, achievements and upcoming work. This synthesis, formulated by ENISA, benefitted from significant comments and feedback from SPARTA. It was also provided for input to the ECCC.

Figure 17: Proposals for the European Cybersecurity Competence Center by ENISA



COMMENTS

SPARTA

Reference: ENISA -- Proposal for the European Cyber Competence Center (Draft 1.0, TLP-G, Oct 2021)

Authors: Thibaud Antignac, Florent Kirchner, Augustin Lemesle (CEA)
Fabio Martinelli (CNR)
Michael Friedewald, Dirk Kuhlmann (Fraunhofer ISI)
Nelson Escravana (INOV)
Philippe Massonet (CETIC)
E. Bruze, E. Piesarskas, E. Versinskiene, R. Zylius (L3CE)
Bertrand Lathoud, Pascal Streicher (SMILE)

Date: 20/12 /2021

Comment 1 on Section 1: We would like to start with an observation on the overall content. It's indeed quite comprehensive. However, it is apparently built on the assumption that the present status-quo won't be changed, and the ECCC will have to carve some room in the niches that are not covered by ENISA's missions. It might be worth stating the other possibility, that one of the core missions of the ECCC will be to go beyond simply organising calls for proposals, and fully develop areas around competence, industrialisation of cybersecurity innovations, capacity building, organisation and mobilisation of the community, support to the increase of the SMB's cybersecurity competence, research agenda and strategic alignment of research and innovation projects across Europe. It means that what is done at present by actors such as the ENISA, but also ECSO, such as the maintenance and update, but also enhancements of a standard European CyberSecurity Skills Framework, should be led by the ECCC with the aim of implementing art. 4 and 5 of the ECCC regulation. We understand this can be a sensitive topic, but believe nonetheless it might be conveyed as a working hypothesis.

Comment 2 on Section 1: On p.4. the document defines the Community as "academia, Industry, researchers and cybersecurity professionals": beyond the typo on the capitalization of "Industry", we believe that "governmental and non-governmental institutions", as well as "civil society" might have a place here too. While variations might occur in the actual implementation at CCN level, it could be detrimental to be perceived as restrictive at this stage and in this document.

Comment 3 on Section 1: On p.4, it might be interesting to include the "EU Cohesion Policy" as part of referenced policy documents defining the scope of work and strategic guidance, as it helps shape a related yet broader context of regional imbalances especially in the face of digital transitions.

Typos in Section 1: On p.5, "The ECCC mandate include" should read "The ECCC mandate includes".

Comment 2 on Section 1: several items on Figure 1 p.6 are not described prior to this, or in the title. For instance, it might be useful to introduce the meaning behind the red R&I bubbles, or the outermost grey bubble.

Comment 1 on Section 1.1: the presentation of SPARTA seems to include extraneous text. The sentence "The digital era has brought with it many advantages for humanity, but the issue of secure data exchange remains among the most significant concerns" should be removed.

Figure 18: Comments from SPARTA on the ENISA proposal

4.1.1 Roadmap workstream

The workstream has produced a remarkable compilation of the 4 pilots and ECSO's research and innovation priorities, ranging over four main topics: Governance and Capacity-building, Trustworthy Ecosystems of Systems, Trust Building Blocks, and Disruptive and Emerging Developments.

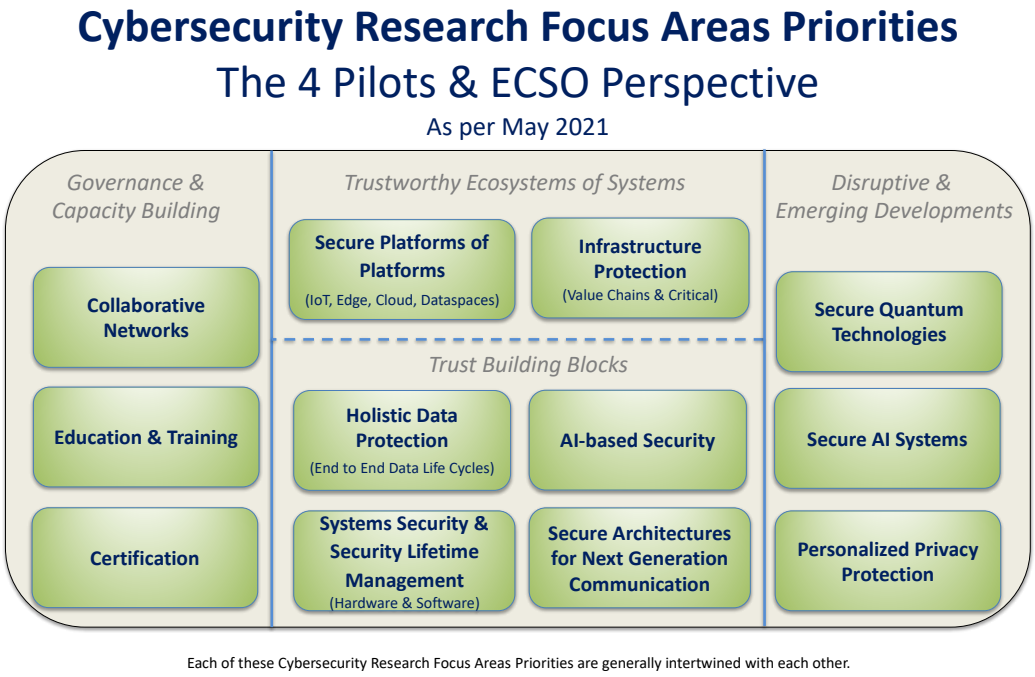


Figure 19: Cybersecurity Research Focus Areas Priorities

4.1.2 On legal and ethics issues

Further cross-pilot activities have been actively pursued such as the ones on legal, ethics and societal issues, unfortunately without the support from a dedicated workstream.

Chapter 5 Summary and Conclusion

The SPARTA Partnership program is committed to collaboration and teamwork as a fundamental support mechanism for people and organizations in Europe. This has been particularly useful during the first two years of the pandemic. The focus of the work is to support the European ecosystems, the collaboration among the driving organizations of each Member State, both public and private, so that people and technical resources can get in touch to extract their maximum potential. Education, training, and experimentation are three of the main factors that will raise security in Europe to the next level.

Through a shared commitment to SPARTA's values, each national cluster of partners increased their cooperation level and experienced the creation of the location national coordination centres and other significant initiatives.

SPARTA partners, associates, and friends, linked and committed to the objectives of the Pilot, participate in the common network activities. Through the mobilization of national and European communities the SPARTA partners can benefit the enlarged European cyber security ecosystem.

The final year of JCCI development has been dedicated to the consolidation and deployment of a distributed network of nodes offering resources as well as spreading the monthly workshops.

In this third year, a great effort has been made in collaboration and alignment with other Pilots, as well as with the new strategies set by EU and other organizations such as ENISA or ECSO in the strategic planning of the security technologies that must be developed in the upcoming years.

Chapter 6 Appendix – JCCI Business Models Analysis

6.1 Introduction

This document provides an overview of different business models and pricing strategies that might apply to SPARTA's aims of offering cloud infrastructure and software services to users, primarily partners and external organizations. Here, we review the principal ideas contained in several scholarly papers that cover available alternatives, best practices and various conceptions of business models and pricing schemes that could be considered as candidates for incorporation, in whole or in part, into the JCCI framework. The areas covered in our preliminary literature review are revealed in the titles of the papers we examined. Consider the entries listed below, for which full citations are provided in the footnotes that follow later on in our review:

- 'Business Models of Platform as a Service (PaaS) Providers: Current State and Future Directions'
- 'The NIST Definition of Cloud Computing'
- 'Success-driving business model characteristics: IaaS and PaaS Providers'
- 'The Business Model Canvas: A shared language for describing, visualizing, assessing, and changing business models' (In Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers)
- 'Semantic Web Service matchmakers: state of the art and challenges'
- 'Web 2.0 Business Models as Decentralized Value Creation Systems' (In Web 2.0: The Business Model)

We anticipate that the SPARTA JCCI will provide a pleasant and productive collaborative environment among SPARTA partners, with a focus on the integration of existing means for carrying out research, as well as allowing external organizations to share its facilities.

In addition, we have identified several criteria that have been drawn from internal project discussions and from advice provided by our project experts that may lead to an understanding of how the different approaches to business model creation and/or adaptation may result in the adoption of one or more of the possible approaches that would best serve the needs of stakeholders. A concluding shortlist of possible pricing schemes may also be of help in this process.

When reviewing our discussion of various business models and pricing schemes, the reader should keep in mind the following criteria:

- The model should have the flexibility to allow for early adoption but be able to sustain itself and the viability of JCCI over the long term by means of appropriate revenue streams. Developers of intellectual products or services in any form (tools, methodologies, reports, etc.) should be induced to become an integral part of the system by offering them or their organizations some form of financial remuneration for their efforts; and the resulting products/services should be offered at a reasonable price so that users would enthusiastically engage the review and sharing of these.
- The model should support different levels of involvement by stakeholders, made up of partners, associated partners, friends, supporters, members of the Arbitrage group, and various institutions, all of whom would take part in structured interactions with the various participants of the SPARTA project. In this respect, the model should support a multi-level membership structure.
- The model should remain easily understood, accessed, and used, despite the complexity of content provided by the system and the multi-layered structure of stakeholders.

Different business models and pricing schemes can address these criteria, but the principal aim is to eventually construct a model that best meets the needs of JCCI.

This document aims to serve as a basis for further discussion and for determining the best fit for the needs of JCCI. Summary statements should be considered as suggestions and not as definitive conclusions. We emphasize that no final conclusions have been drawn at this point, and there has been no effort expended on developing or recommending any particular model.

6.1.1 Methodology

The approach used to search for the best solution for the JCCI case include a few steps.

First, the main principles are described. The principles are needed to describe the general view on the JCCI case and why relevant business, and pricing models are analysed. Principles are extracted from internal project discussions and provided by project internal experts.

Then, the main alternatives business and pricing models are described. They all are presented to give readers the opportunity to understand their characteristics and how they serve the needs of organizations in different situations. Those activities were based on a literature review. No intention to develop any novel model was considered at this point. Our analysis has taken into account key papers[18] and several blogs and websites.

At this point, we do not aim to provide a final conclusion and propose a single final model. This document is aimed as a base for further discussions and search for the best-fit approach and provided summary statements should be considered as suggestions to evaluate and adapt to the final instance of European Cybersecurity Network of Competences deployed in Europe.

6.2 Guiding principles

It is planned, that the SPARTA JCCI should provide easy collaboration among SPARTA partners as well as for allowing sharing of facilities with external organizations.

It meant to integrate the existing means of the partners. Parts of the Lab should be also available to external organizations.

While setting up the business model and defining pricing, a few aspects, shaping the choice, should be considered:

- Model should sustain viability of the JCCI. This attributes both: developers of intellectual products in any form (tools, methodologies, reports, etc.) should be motivated to become part of the system. Users of such products should be interested to visit, review, share and uptake materials on supply. This principle at the first stage imposes the flexibility and easy adaption of the model.
- Model should consider the different levels of involved stakeholders. There are partners, associated partners, friends, supporters, members of the Arbitrage group and other types of institutions, having structured interactions with the SPARTA project. In this respect, the model should support a multi-level entrance structure.
- Model should provide motivation for suppliers of intellectual products. Financial motivation is at the centre of that principal, conditioning that the access to material provided should not be

[18] *'Business Models of Platform as a Service (PaaS) Providers: Current State and Future Directions' [provide full citation information]; https://www.researchgate.net/publication/329400820_Success-Driving_Business_Model_Characteristics_of_IaaS_and_PaaS_Providers; H. Dong, F. Khadeer Hussain, and E. Chang, "Semantic Web Service matchmakers: state of the art and challenges," Concurr. Comput. Pract. Exp., 2012.*

https://pdfs.semanticscholar.org/66a1/2e6e12e542a65be806e29863c1827c116ec6.pdf

completely free. Another principal – the model should be able to sustain the system – also adds to the paid content supporting model development.

- Model should remain simple. It is assumed, that despite the complexity of content provided in the system and multi-layer structure of stakeholder, the model still needs to remain simple to understand, access and use.

Different business and pricing models can meet the principles listed to a certain level, but the aim is to construct one, best meeting criteria, described as principles.

6.3 Analysis of business models

In the paper on 'Business Models of Platform as a Service (PaaS) Providers: Current State and Future Directions'[19] the authors review the current state of affairs regarding three principal cloud services: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). As the authors write in their opening abstract, these services are:

> "… completely changing the way software is produced, consumed, and distributed. In particular new PaaS business models have a disruptive effect on existing business models and require thorough business model innovation in the software industry. Despite their impact, PaaS business models have not been considered in a sufficient manner in literature yet."[18]

The paper attempts to provide "a systematic literature review, a classification model of existing PaaS business models based on case studies, and an overview of the current state and future development directions of PaaS."

Although most of the paper focuses on PaaS, it does so within a context that in part takes into account SaaS and IaaS, and takes its lead in defining these services from the definition of cloud computing by NIST.[20] These definitions are described like this:

Software as a Service (SaaS)

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Infrastructure as a Service (IaaS)

IaaS generally refers to online services that provide high-level APIs used to dereference various low-level details of underlying network infrastructure like physical computing resources, location, data partitioning, scaling, security, backup etc. NIST describes IaaS as allowing the consumer "to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)."

Platform as a Service (PaaS)

For PaaS, the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-produced or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has

[19] Andrea Giessmann and Katarina Stanoevska-Slabeva, 'Business Models of Platform as a Service (PaaS) Providers: Current State and Future Directions,' *Journal of Information Technology Theory and Application*, Volume 13, Issue 4, pp. 31-55, December 2012.

[20] Mell, P. and Grance, T. (2011), "The NIST Definition of Cloud Computing", NIST, Gaithersburg, USA.

control over the deployed applications and possibly configuration settings for the application-hosting environment.

Now, the PaaS paper treats these three services as business models in their own right, which differs from the way in which business models are defined in two other papers that we have examined.

First, in the paper by Floerecke and Lehner on 'Success-driving business model characteristics: IaaS and PaaS Providers,'[21] the category of business model is described as part of an ecosystem in this way:

> "A business ecosystem represents a pertinent scope for systemic innovations, where different interrelated and interdependent companies cooperate to deliver full-scale customer solutions. Compared to traditional linear and customer-focused value chains in IT service provision, the value creation is not an exclusively linear process with upstream and downstream actors anymore. Value is, instead, created in a network of companies with many both vertical and horizontal relations. The cloud ecosystem's core consists of providers of the three basic service layers – IaaS, PaaS, and SaaS. IaaS supplies infrastructural resources (compute, storage, and network). PaaS allows users to develop and deploy applications by offering a software development environment with programming languages, libraries, and tools. SaaS refers to providing on-demand applications. Building upon these three consecutive and interrelated service layers, a multitude of further ecosystem roles, such as aggregators, integrators, and marketplace operators, has evolved. (p. 2)"

In this context, a business model, can be defined as a detailed specification of how ecosystem roles are realized by individual companies. As each occupied ecosystem role must be implemented in the form of (at least) one business model, a firm can employ several business models simultaneously. Although designing and running such a business model portfolio might be challenging, it nevertheless offers the great potential to exploit synergies.

Significantly, business models in this interpretation are not standalone conceptions. They are subject to the demands of a wider conception that includes the following key aspects. A business model is:

- a system comprising a set of interrelated components or partial models for depicting, implementing and evaluating the business logic of a company;
- an intermediary between a company's strategy and its business processes;
- the conceptual and architectural implementation of a business strategy;
- the foundation for the realization of business processes.

Figure 20 summarizes the relationship between a cloud provider, its ecosystem roles, their instantiated business models, their components, and their multiple design options for component-specific business model characteristics:

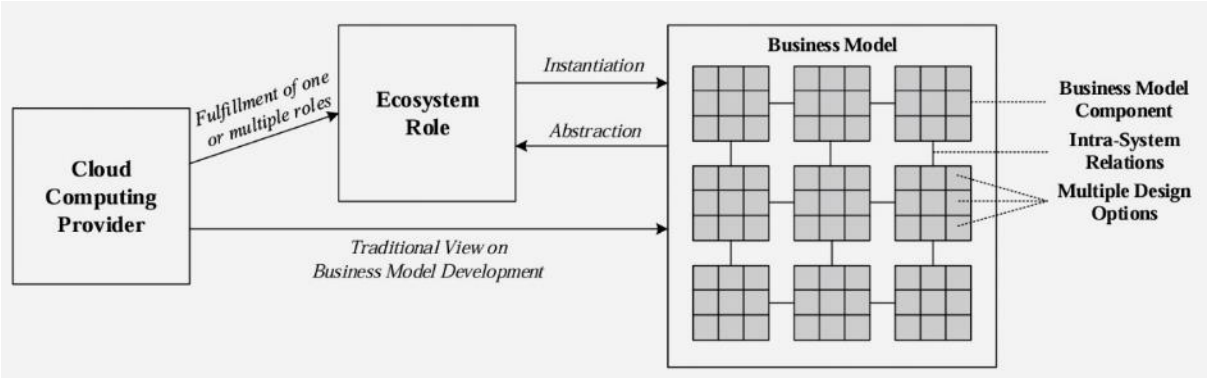


Figure 20: The Connection between Cloud Providers, Ecosystem Roles and Business Models

[21] Sebastian Floerecke and Franz Lehner, SUCCESS-DRIVING BUSINESS MODEL CHARACTERISTICS OF IAAS AND PAAS PROVIDERS, *International Journal on Cloud Computing: Services and Architecture (IJCCSA)* Vol. 8, No.6, December 2018, DOI: 10.5121/ijccsa.2018.8601.

Floerecke and Lehner set the stage for their discussion by introducing the comprehensive and widespread cross-industry framework called the Business Model Canvas.[22] This framework comprises the following nine components: customer segments, value propositions, channels, customer relationships, revenue streams, key resources, key activities, key partnerships, and cost structure.

In the Business Model Canvas, these 9 Building Blocks (pp. 16-17) are described in this way:

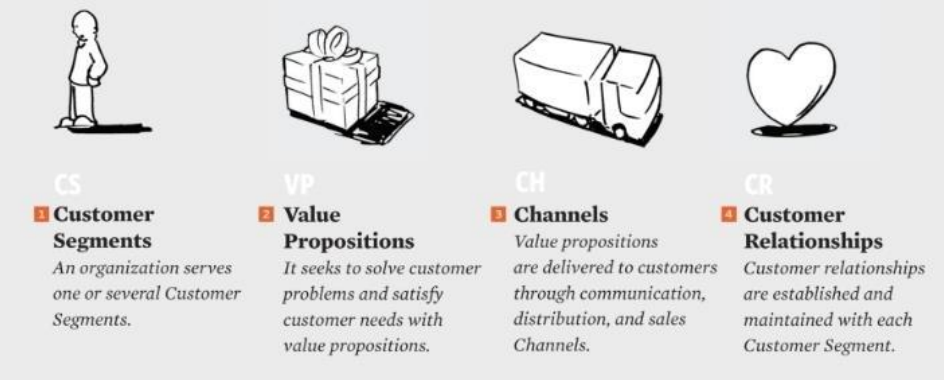


Figure 21: Cross-industry framework - Business Model Canvas (1-4 Building Blocks)

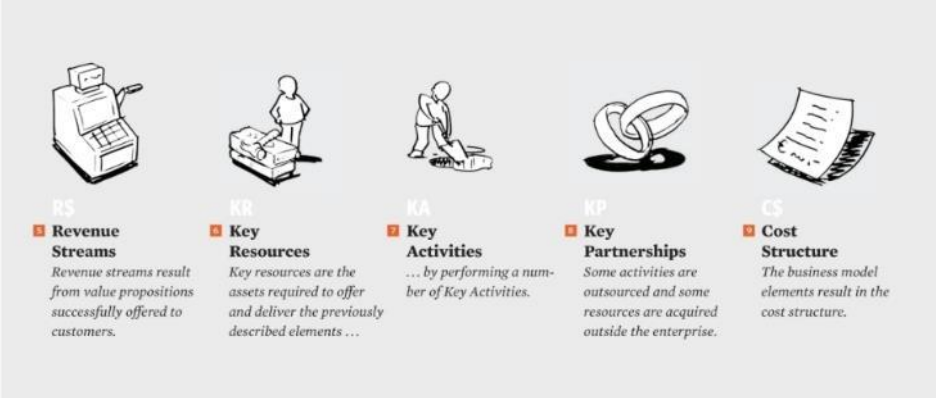


Figure 22: Cross-industry framework - Business Model Canvas (5-9 Building Blocks)

About 'Business Models of Platform as a Service (PaaS) Providers: Current State and Future Directions,' (hereafter referred as the JITTA paper); although this paper defers to Osterwalder's 'Business Model Canvas,' it only acknowledges or treats five of the nine categories or building blocks that make up the definition of a business model. These are:

[22] 'The Business Model Canvas: A shared language for describing, visualizing, assessing, and changing business models.' In Osterwalder, A. and Pigneur, Y. (2010), *Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers*, 1. ed., New Jersey: John Wiley & Sons.

Business Model Building Block	Description
Value Proposition	Gives an overall view of a company's bundle of products and services
Customer Segment	Describes the segments of customers a company wants to offer value to
Customer Relationship	Explains the kind of links a company establishes between itself and its different customer segments
Channel	Describes the various means of the company to get in touch with its customers
Revenue Stream	Describes the way a company makes money through a variety of revenue flows

Table 1: Business Model Building Blocks based on Osterwalder et al (2005)

The JITTA paper omits the following: key resources, key activities, key partnerships, customer relationships, and cost structure.

Again, we emphasize that the JITTA paper treats the PaaS conception, along with SaaS and IaaS, as business models within a framework of cloud computing, and what is more ties these services closely to the associated pricing schemes. The authors write: "Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms, and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the infrastructure provider by means of customized SLAs [service level agreements]."

These cloud services can also be identified with a wide range of vendors in the following way:

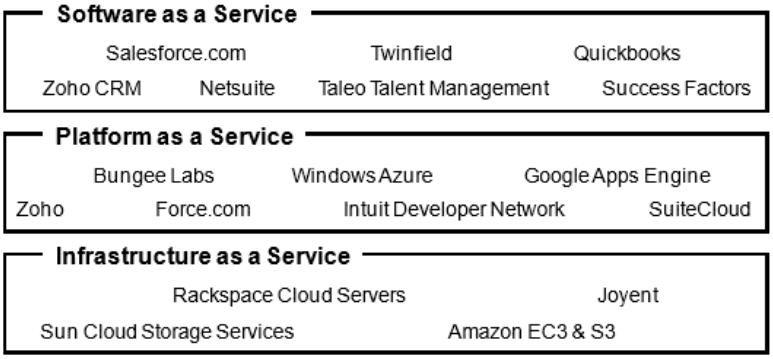


Figure 23: The three layers of cloud computing: SaaS, PaaS, IaaS

The authors of the JITTA paper go on to discuss the relationship between these services within the context of the most cited architectural concepts for clouds and cloud computing. In Figure 23 PaaS is the middle layer connecting the IaaS and the SaaS layer of clouds. The IaaS layer offers computing resources such as processing, storage, networks, and other fundamental computing resources that can be obtained as a service. The SaaS layer is the most visible service of cloud computing, since the software applications are accessed directly by the end-users. As is well known, these applications are deployed and executed in cloud systems and can be accessed from various client devices through a thin client interface, i.e., a Web browser.

The JITTA paper goes on to suggest that, according to the well-known consultants at Gartner, the PaaS offerings will at some point be broken down further into the following sub-categories of service offerings:

- aPaaS—application platforms for hosting and managing individual application services and data;

- iPaaS—integration platforms for integration and intermediation of applications services;
- kPaaS—knowledge platform for access and analysis of broad data resources in context;
- uxPaaS—user experience platforms for multichannel, multi-device user-facing applications;
- dPaaS—data platforms for hosting and serving data.

The authors also include the ideas of researchers who have identified ten general 'essential' cloud characteristics of viable cloud services, namely: User Friendliness, Virtualization, Internet Centric, Variety of Resources, Automatic Adaptation, Scalability, Resource Optimization, Pay per Use, Service SLAs, and Infrastructure SLAs. However, they also suggest that since PaaS, defined as an execution environment where external developers deploy and run their components, have further distinguishing characteristics in addition to the essential characteristics of cloud computing. These are:

Essential characteristics:

- Accessibility by external developers
- Ease of deployment and execution
- Automated resource management

Significant characteristics:

- Availability of a development environment
- Testing and simulation facilities
- Administration and management
- Knowledge management

The bottom line by the author is that: "PaaS is a software platform, which is opened toward external developers, in order to develop, deploy, and run their components. A PaaS platform abstracts from the hardware resources demanded for the execution of the components. Developers no longer have to manage or control the underlying infrastructure, including network, servers, operating systems, or storage; these resources are managed automatically by the platform. While the openness toward external developers, deployment, execution, and automated resource management are essential characteristics, PaaS also has specifically identified several additional characteristics of significance listed above."

"PaaS platforms facilitate developers to administrate their applications themselves by providing management tools to start, stop, configure, and/or backup their applications and data. In addition to this, PaaS platforms usually encourage an interactive exchange of knowledge between developers by providing knowledge management facilities. Knowledge management in this context comprises several practices used to identify, create, distribute, and share insights and experiences concerning development in general and the platform in particular." PaaS will facilitate the development, testing, deployment, execution, and management of software components, as well as the exchange of knowledge between developers.

The JITTA paper also attempts to strengthen its arguments through several case studies, the most important of which is that of Facebook, to which we will turn after our discussion of the importance of Web 2.0 and semantic web technologies in order to provide the listed characteristics.

6.3.1 Web 2.0 and the Semantic Web

The article on 'Semantic Web Service matchmakers'[23] is of interest and relevance, but would be difficult to make use of, unless 'experts' in the field of the Semantic Web were to be enlisted, as it deals primarily at a 'META' level in terms of Semantic Web services. The authors deal with Semantic Web Services and Semantic Web Service discovery, which make use of the Semantic Web technologies; and the Semantic Web Service matchmakers are the programs or frameworks designed to implement the task of Semantic Web Service discovery.

[23] Dong, H., Hussain, F.K. and Chang, E. (2013), Semantic Web Service matchmakers: state of the art and challenges. Concurrency Computat.: Pract. Exper., 25: 961-988. doi:10.1002/cpe.2886.

In simplified terms, the authors conduct a survey of the contemporary Semantic Web Service matchmakers in order to obtain an overview of the state of the art in this research area. The survey involves 34 typical SWS matchmakers and the identification of six major dimensions for analysing the technical features of the matchmakers. These were:

- SWS description languages
- SWS discovery mechanisms
- SWS discovery architecture
- SWS matching approaches and degrees
- SWS matching parameters
- Test platforms for evaluating SWS matchmakers

Further, the SWS matchmakers were divided up into four groups on the basis of the manner in which they used the SWS description languages, namely: DAML-S/OWL-S, WSMO, and WSDL-S/SAWSDL. The authors then compared the features of the matchmakers in each group on the basis of the six dimensions and explored the potential research issues in each dimension.

At a much higher level, but still within the domain of the Semantic Web, is the important study entitled *Web 2.0: The Business Model,* which deals with crucial themes such as 'Learning and Knowledge Communities,' 'Large Online Communities,' and 'Web Communities of Practice.'

As described in the Forward section of the book, the authors suggest that Web 2.0 is one of the hottest topics nowadays in Information Systems and stress the importance of analysing the business models and business perspectives of the new generation web, and its implications regarding business value.

The book is a collection of essays, the most relevant of which is the chapter by Christian Briggs on 'Web 2.0 Business Models as Decentralized Value Creation Systems.'[24]

Web 2.0, refers to a perceived or proposed second generation of Internet-based services such as social networking sites, wikis, communication tools, etc., that emphasise ways for groups to collaborate and share information. In addition, Web 2.0 fosters social norms that allow large groups of scattered people in space and time to self-organize and to co-create value in a decentralized manner. "Consequently, new business models have begun to emerge that leverage this tendency toward decentralization to varying degrees and in different ways."

The essay on 'Web 2.0 Business Models as Decentralized Value Creation Systems' opens by stating that the advent of Web 2.0 has brought with it new business models that are serious departures from anything that may have preceded these before, and focuses on the problem of formulating a value creation system, for the purpose of understanding the practical implications and opportunities of these models for current and future web-based businesses.

Briggs defines 'Value creation' as the formulation of the relative worth, utility or importance in a product or service such that these aspects can then be exchanged within a market for some sort of gain. Value can be inherent in the product itself for can be viewed as a system of relations around the product. The author uncovers the fact that there is a strong connection between an organization's conception of value and its business model of choice. Significantly, nowadays, the value does not stand on its own – it is a system of relations.

The paper looks at business models through the lens of:

1. The Locus of Value – where the value of a product is believed to exist
2. The Creator of Value – who or what is believed to be the agent of value creation
3. The Scarcity of the Product – how much of the product is produced and reproduced.

Recent social and technological developments have shifted the locus of value creation in new business models away from the product itself, and toward the relationships that the product has with the consumer and with other products. These shifts have also implicated the relationships that

[24] Christian Briggs, 'Web 2.0 Business Models as Decentralized Value Creation Systems.' In Miltiadis D. Lytras, Ernesto Damiani and Patricia Ordóñez de Pablos, *Web 2.0: The Business Model* (Boston, MA: Springer US, 2009), DOI: 10.1007/978-0-387-85895-1.

people around a product established with each other. Moreover, products or services that were previously considered scarce were now becoming ever so more abundant.

The two figures below depict the differences between the pre-Web ways of looking at value in relation to the product itself; versus the ways in which value became a system of relations.

Pre-Web context of value:

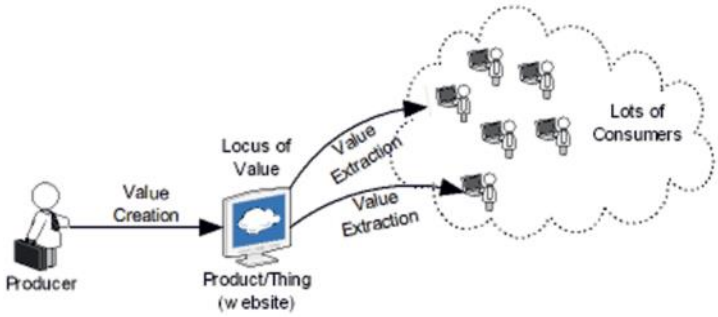


Figure 24: The Web 1.0 Value Chain Looked a Lot Like its pre-web Predecessor

The modern conception of value as a system of relations between people and product(s):

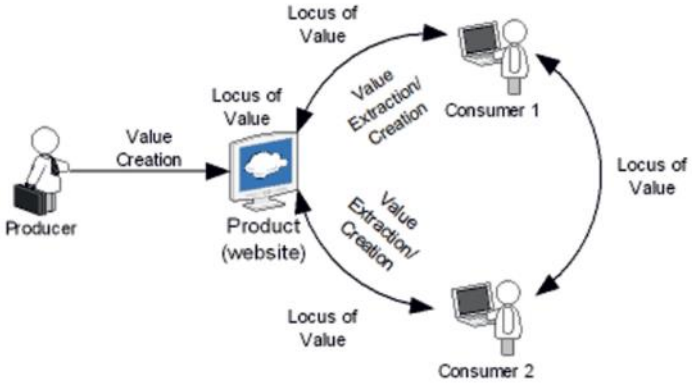


Figure 25: The modern conception of value as a system of relations between people and product(s)

The examples provided by major web-based services such as MySpace or Facebook are instructive in this context. Both are highly-decentralized value creation systems, in other words, they are highly decentralized value networks. We can test this by taking away one or another of the elements that make up the system. If we remove any of the pieces of the value creation system, we would significantly lessen its value. For example, if we remove the users from the value creation system, its value will decrease significantly since in both cases the users create all of (or most of) the relevant content. Similarly, if we remove the web pages from the value creation system, the value of the system would be meaningless, since millions and millions of users would have no way to connect with each other within their respective cyberspaces. In either case, the value resides in the relations between the company, the technology and the users, but that value is created mainly outside of the company by the users, whose content and actions provide value to each other and to the company. In this context, it would make no sense to charge users for setting up an account.

Both the MySpace and Facebook examples demonstrate that their value is manifested by being a major component of a system, and as such, the respective business models must properly account for the creation of that value if these companies are to survive.

Table 2 below summarizes some of the ways in which decentralizing Web 2.0 is included in the models of several companies.

Company	Description of Means
Twitter, Yahoo!, Google, YouTube	Have released API's which allow outside commercial and non-commercial developers to execute functions as well as to pull and push data to and from their systems.
Facebook, Salesforce, MyS-pace	Have created platforms which allow outside commercial and non-commercial developers to build entire applications within the sys-tem.
Digg, OhMyNews, Wikipedia	Have allowed users to create a large amount of the content within the system
CrowdSpring, Threadless, Widgetbox	Have allowed users to self-organize to create products individually or in groups through the system

Table 2: Current means of Decentralizing Web 2.0 Value Chain

Now, let us return to the JITTA paper which introduced our analysis at the beginning of this review, and have a look at the case study on FACEBOOK. The example is instructive.

The Facebook Developer platform offers development tools and an execution environment for the social network of Facebook. It enables enterprises and individual developers to integrate its applications and services with the Facebook website, gaining access to millions and millions of potential users. Facebook is not only a PaaS, but it is also a distribution channel where developers can find their potential users. However, as the JITTA authors point out, Facebook does not offer application hosting and, hence, does not also support automated resource management.

Developers can work in three directions: integration of Facebook in websites, integration of Facebook in mobile applications, or integration of applications into Facebook. The main components of the Facebook Developers platform offer are:

- The Graph API, a RESTful API that allows developers to read and write data to Facebook and manage the Facebook Social Graph, its objects (e.g., people, photos, pages, etc.), and connections between them;
- The Social plugins that allow the easy integration of Facebook features into any Web page. In addition to this, Facebook provides SDKs for several programming languages like JavaScript, PHP, Python, iOS for iPhone and iPad and Android.

From our 'Business Model Canvass' discussion before, here we have:

Business Model Building Block	Description

Value Proposition	▪ Access to world's largest social network Facebook
	▪ Development tools and execution environment for Facebook apps.
	  ▪ Read and write data to Facebook
	  ▪ The Social plugins for easy integration of Facebook features
	  ▪ Advanced APIs: Graph Realtime API, Facebook Query Language (FQL), Facebook Markup Language (FBML)
	▪ High reach of Facebook application marketplace
	▪ Broad linking possibilities

Customer Segment	▪ Facebook social network users ▪ Software vendors ▪ Individual developers
Customer Relationship	▪ Facebook developer Web page ▪ Online documentation ▪ Forum, blogs, and showcases
Channel	▪ On demand
Revenue Stream	▪ Advertisement ▪ Revenue sharing—usually Facebook takes ca. 30% revenue share of applications.

Table 3: Case Study- Facebook Developers

The revenue of Facebook is mostly based on advertisement and revenue sharing with Facebook developers. Facebook introduced a virtual currency within their platform and offers an API for service providers, which enables developers to use so-called credits as a method for purchasing digital and virtual goods within their application (transaction-based or based on upgrades within the applications). Service providers can redeem credits received at a certain rate, minus a service fee per credit redeemed.

As can be seen, the revenue/pricing model for Facebook is relatively straight forward. However, if we take into account the more broadly defined concept of business models, we see that there are other aspects to consider.

As we saw earlier, the JITTA paper omits the following business model building blocks: key resources, key activities, key partnerships, customer relationships, and cost structure.

The Revenue Streams building block of the 'Business Model Canvas' represents the cash a company generates from each Customer Segment (costs must be subtracted from revenues to create earnings, or break-even, if appropriate). "If customers comprise the heart of a business model, Revue Streams are its arteries." It goes without saying that 'cost reduction' is of paramount importance in this context.

But "what are customers/clients willing to pay?". Successfully answering that question allows the organization to generate one or more Revenue Streams from each Customer Segment. Each revenue stream may have different pricing mechanisms, such as fixed list pricing, bargaining, auctioning, market dependent, volume dependent, or yield management.

A business model can involve two different types of revenue streams:

1. Transaction revenues resulting from one-time customer payments;
2. Recurring Revenues resulting from on-going payments (either by delivering a Value Proposition to customers or providing post-purchase customer support).

Revenue Streams can be generated in several ways through:

- brokerage fees (intermediary services performed on behalf of two or more parties, e.g. credit card merchants/customers; real estate agents match buyer/seller);
- advertising (product, service, or brand);
- asset sales (physical products);
- usage fees (charges for use of a particular service);
- subscription fees (generated by selling continuous access to a service);
- lending/renting/leasing (temporarily granting someone the exclusive right to use a particular asset or service for a fixed period at no charge or in return for a weekly/monthly/yearly fee – implies recurring revenues);
- licensing (customers have permission to use protected intellectual property in exchange for a licensing fee);

In the last two cases, then, customers would avoid one-time costs of purchasing an asset; and rights holders of IP could generate revenues without having to manufacture a product or commercialize a service. A somewhat different perspective is offered by the 'Business Model Canvas.' There, Revenue Streams are classified according to two main types: fixed and dynamic pricing.

In general, offering products or services of similar value at a lower price, or at no charge initially, is a common way to satisfy the needs of price-sensitive Customer Segments (e.g., certain no-frills airlines, or lower-priced cars like the Nano in India, or free service offerings for the first month, etc.).

6.3.2 Pricing models

There are different approaches of setting the price for the services provided. They might be focused on costs, simplicity, consumer behaviour and other aspects. Having a full spectrum of available

pricing alternatives would help to make a choice for JCCI pricing strategy. This section provides a short outline of main pricing models used by similar platforms. These include:

- Flat rate (single product, a single set of features, and a single price, usually billed monthly);
- usage-based (or pay as you go), pay for what you use (e.g., Amazon Web services);
- tiered strategy (offer multiple packages with different combinations of features at different price points (Software examples – Adobe, MS, etc. – basic, pro, enterprise offerings);
- per user (per seat, or per active user) – Mathematica, other software offerings;
- per feature (separates out different pricing tiers according to the functionality available in each);
- free service offerings (free to use products offered, supplemented by paid add-on features; or a certain number of months free, then you pay).

An extensive study of the seven key SaaS pricing model can be found here and we refer the reader to it for complementary information on each of them with their advantages and drawbacks. Nevertheless, selection of pricing model depend on the number of features. For the complex, diverse service, and multi-layer user structure platforms, like JCCI, the mixed approach combining some pricing models should be applied. This is also encouraged by the different nature of agents in the network. JCCI ecosystem includes Academia, non-profit organizations, and companies. Those different profiles have different economic models and financial goals. So, each one should decide which model fits better with their own revenue system.

At this point, available proposition would be to define the most suitable pricing models for higher level groups of services available on JCCI. Based on this the core model can be selected, while other models still can be applied for certain groups of services.

6.4 SPARTA JCCI External Economy Model

JCCI can be described as a business platform, providing an access to a complex set of resources of different nature. Different platforms provide different value for their customers, meaning they should be operated and priced in a different way.

Following John Hagel[25] classification, the JCCI is to be considered as the aggregation platform, having features of mobilization and learning platforms. It is also characterized as having at least few layers:

- General – how customers (SPARTA partners, project related organizations and external organizations) access the structured content of the platform. There are few alternatives, this can be accessed free, on the subscription or freemium models.
- Component layer – how customers access the resources available at the JCCI component level. Business model at this layer start to differ, so can pricing model and parameters used for them.
- Resource layer – how customers can use each of instruments, training and other available resources. At this level pricing becomes very individualized and presumably each resource owner should be free to choose own pricing model.

Guiding principles, business model (incl. sub-model) and pricing models set the motion for the external economy model, presented in the following table.

[25] *"Harnessing the Full Potential of Platforms" – John Hagel*, *http://www.marketingjournal.org/john-hagel-harnessing-the-full-potential-of-platforms/*

	Business Model	Sub-model	Pricing Strategy	Delivery organization	Key outputs, VP
JCCI General	PaaS	Aggregation platform	Free access		
JCCI WorkBench	PaaS	Aggregation platform	Resource layer pricing		
JCCI Virtual Learning Centre	PaaS	Learning platform	Freemium (Resource layer pricing)		
JCCI Cyber Ranges	PaaS / IaaS	Aggregation platform Mobilisation platform	Active user / feature-based pricing		