SPARTA

D8.2

Intermediate results of the clustering, platforms, and ecosystems activities

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

Deliverable type	Demonstrator
Deliverable reference number	SU-ICT-03-830892 / D8.2/ V1.0
0Work package contributing to the deliverable	WP8
Due date	January 2021 – M24
Actual submission date	12th March, 2021

Responsible organisation	VICOM
Editors	Raúl Orduna
Dissemination level	PU
Revision	V1.0

Abstract	This document describes Partnership activities performed by the SPARTA ecosystem in the second 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

Raul Orduna (VICOM)

Contributors (ordered according to beneficiary numbers)

Florent Kirchner (CEA)

Christian Derler (JR)

Philippe Massonet (CETIC)

Martin Zadnik (CESNET)

Michael Meier (UBO)

Raimundas Matulevicius (UTARTU)

Athanasios Grigoriadis, Isidoros Monogioudis (KEMEA)

Cristina Martínez, Ana Ayerbe Fernandez-Cuesta (TEC)

Francesco Zola, Haizea Erostarbe, Raul Orduna (VICOM)

Joost Geurts, Thomas Jensen (INRIA)

Fabio Martinelli, Artsiom Yautsiukhin (CNR)

Bertrand Lathoud (SMILE)

Reviewers (ordered according to beneficiary numbers)

Rocco De Nicola (CINI)

Claudio Porretti (LEO)

Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

Executive Summary

This document describes partnership activities performed by the SPARTA network in the second year in different activities.

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 also finished two states of the art papers: one about federation mechanisms to design a dynamical version of the Joint Competence Center Infrastructure (JCCI) and another one about the different types of scenario that can be offered in SPARTA JCCI, in addition to the traditional "Capture the Flag" exercise. We have developed a second and distributed version of the JCCI infrastructure, 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, we also performed activities related to the consolidation of the national and European ecosystems. We have formalized the creation of the SPARTA Associates Network, selecting in a first stage a limited number (between 5 and 9) of organizations per country to facilitate the integration in the SPARTA culture, procedures and tools.

CoVID emergency and national lockdowns have impacted greatly in conducting the planned monthly workshops. Nevertheless, we have maintained the activity through on-line media closing relations between partners and associates, but also between Spartans and national or European agents, Forums and Policy Makers.

In particular 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. Each Pilot is in charge of one of this supra-project initiatives to provide the best advice and support the current and future competence 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 progress from first year and highlights the plans for the third year.

Table of Content

Chapter 1 Introduction ... 1

Chapter 2 Joint Competence Centre Infrastructure ... 2

2.1 Purpose ... 2

2.2 JCCI components ... 2

2.3 Authentication and Authorization ... 5

2.3.1 Implementation in SPARTA ... 6

2.4 Next steps ... 7

Chapter 3 Clustering activities at national, European and international level ... 8

3.1 SPARTA ecosystem ... 8

3.2 National level ... 10

3.2.1 France ... 10

3.2.2 Belgium ... 12

3.2.3 Greece ... 14

3.2.4 Austria ... 14

3.2.5 Poland ... 15

3.2.6 Germany ... 16

3.2.7 Czech Republic ... 17

3.2.8 Lithuania ... 18

3.2.9 Spain ... 20

3.2.10 Luxemburg ... 22

3.2.11 Portugal ... 23

3.2.12 Latvia ... 24

3.2.13 Italy ... 25

3.2.14 Estonia ... 26

3.3 European level ... 29

3.3.1 Cooperation with EU Projects ... 29

3.3.2 Further activities ... 30

3.4 Monthly workshops ... 31

Chapter 4 Clustering with other pilots ... 33

4.1 Federated workstreams ... 33

4.1.1 Communication and dissemination workstream ... 33

4.1.2 Cyber-ranges workstream ... 34

4.1.3 Governance workstream ... 34

4.1.4 Roadmap workstream 34
4.1.5 Education and training workstream 35
4.1.6 On legal and ethics issues 35
4.2 Atlas 36
Chapter 5 Summary and Conclusion 38
Chapter 6 Appendix – Learning Content Inventory 39
6.1 Training Contents Inventory 39
6.1.1 CEA 39
6.1.2 CESNET 40
6.1.3 INRIA 40
6.1.4 TEC 41
6.1.5 TUM 42
6.1.6 UKON 44
6.1.7 INOV 44
Chapter 7 Appendix – State of the Art for Federated Infrastructures 46
7.1 Introduction 46
7.2 Authentication and authorization 46
7.2.1 Non-web 46
7.2.2 Web 48
7.3 Shared infrastructure 52
7.3.1 Site-to-Site VPN 52
7.3.2 Remote-access VPN 53
7.3.3 SD-WAN VPN 53
7.4 References 53
Chapter 8 Appendix – Description of Potential Cyberrange Scenarios 54
8.1 Introduction 54
8.2 Cyber Range Architecture 54
8.3 War Games strategies 55
8.3.1 Capture the Flag (CTF) 55
8.3.2 King of the Hill (KotH) 57
8.3.3 Last Man Standing (LMS): 58
8.3.4 Locked Shields 59
8.4 Limitation 59
8.5 War Games proposal scenarios 60
Chapter 9 List of Abbreviations 65

List of Figures

Figure 1: JCCI Infrastructure 2
Figure 2: JCCI NEXUS on-line 3
Figure 3: Example live data........ 4
Figure 4: SPARTA official main page 5
Figure 5: FIWARE structure 6
Figure 6: SPARTA ecosystem........ 8
Figure 7: SPARTA associates/friends 9
Figure 8: SPARTA overall community 10
Figure 9: Belgian SPARTA associate workshop agenda 13
Figure 10: SPARTA monthly workshops 31
Figure 11: SPARTA monthly workshops per country........ 32
Figure 12: SPARTA presentation at Convergence 34
Figure 13: Cross-pilot workshop on ELSA in cybersecurity research........ 36
Figure 14: The Atlas portal........ 37
Figure 15: Example of CTF Jeopardy-style board 57

List of Tables

Table 1: Specifications for a War Game Scenario 60

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.

This one has been devised as a man-in-the-moon project, so policies, processes and technologies will be proposed from this Pilot to set the basis for future accurate investments in digital security, comparing and aligning the proposals with those of the rest of the Competence Centers Network (CCN) pilots underway.

In this vision, we think that the best way to achieve this goal is to maximize the impact of project's resources by establishing networking and collaborative activities, and by defining the roadmap, holding workshops, and sharing resources that SPARTA made available by partners and associates.

The three pillars that sustain the integration and clustering activities in which we organize the partnership tasks are:

- **Infrastructures**: Work is being 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 can be integrated. 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 those less represented groups in the sector. We highlight the future role of young people and women in the scientific, research and development fields because they represent the future European workforce. We aim 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 is 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

2.1 Purpose

During this year, the JCCI has been updated in order to fit the usage workflow already presented in the *Deliverable 8.1 Initial results of the clustering, platforms, and ecosystems activities.* In fact, the main idea was to create a dynamic infrastructure, in which different customers could access to a list of all available resources and in which, this information is not kept from a centralized entity but each provider it oversees its own. In fact, they must generate its contents and make then understandable to the consumer. The available resources can be separated into two categories: workbench and learning content. While the first one represents assets/products that the partners make available to the consumer, the learning content is referred to course or environment in which it is possible improve their knowledge. A detailed description about the detected learning content is presented in Chapter 6.

Furthermore, the access to these resources could be limited by an authentication process regulated by SPARTA Identity Provider.

The new JCCI infrastructure is drawn in the Figure 1.

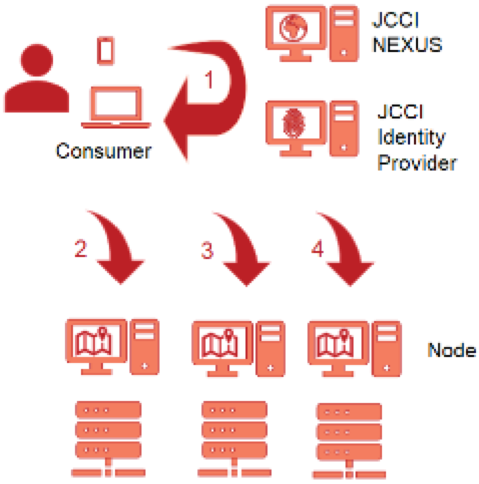
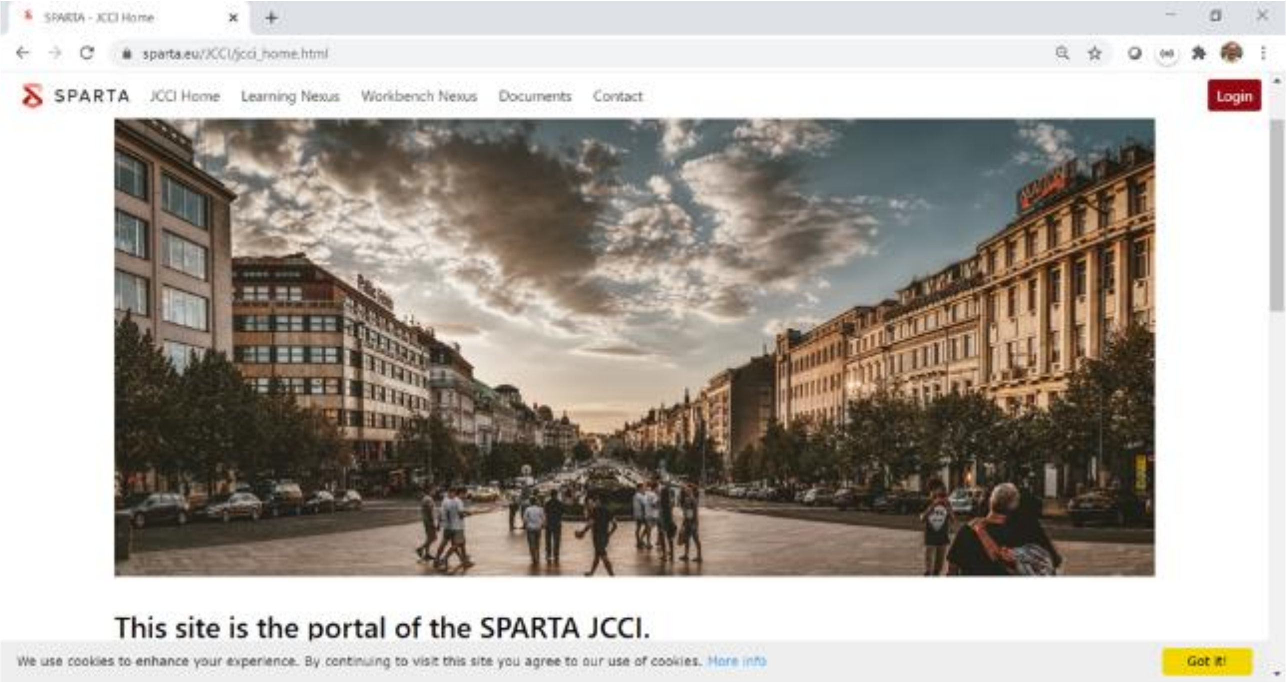


Figure 1: JCCI Infrastructure

2.2 JCCI components

In this scenario, it is possible distinguish two main entities that are called SPARTA NEXUS and SPARTA NODE. The first one represents the web part (freely available and documented[1]) that substitutes the old and static webpage. 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 also in a remote way. This embodies both the research and development aspects, and the financial and administrative ones.

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



This site is the portal of the SPARTA JCCI.

We use cookies to enhance your experience. By continuing to visit this site you agree to our use of cookies. More info

Figure 2: JCCI NEXUS on-line

The second actor represents a REST-API[2] that allow 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., NEXUS. Partners should install this rest-API to manage their own information without problem, so for example they can change it without the permission of a central unit. The static content will remain in the main page, nevertheless, for the benefit of the project 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.

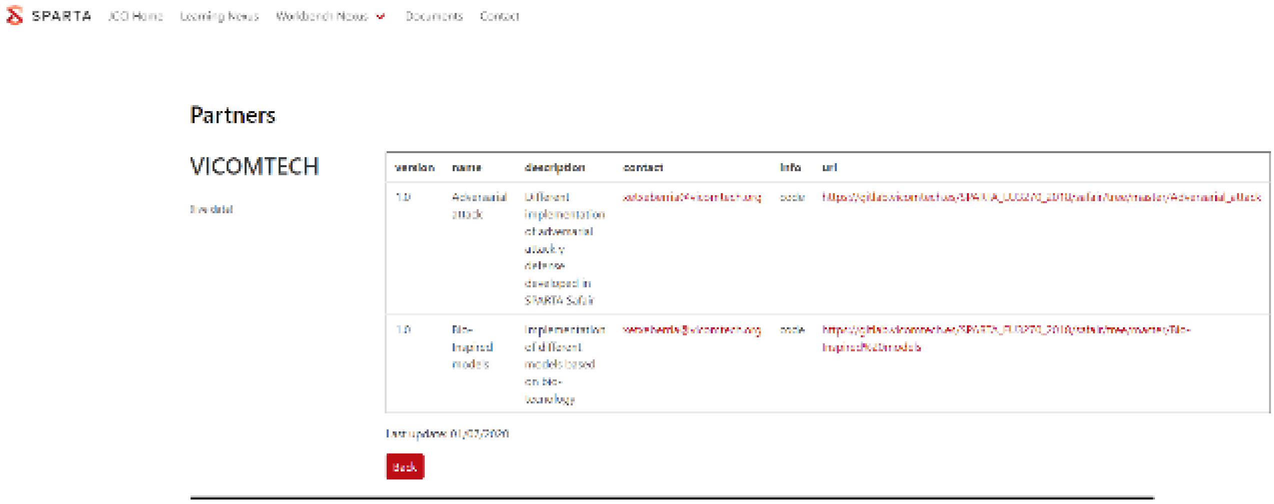
Separation and decentralization of the information allow the infrastructure to be easily updated and without causing temporary error. In fact, if a new JCCI NODE is deployed, the NEXUS just needs the new IP address (or the domain) of the node to ask and then show the information published by the novel node. In the same way, if a JCCI NODE want to leave the NEXUS, it can shutdown itself and automatically the NEXUS will not show its information without causing an error or affecting the functionalities of the others JCCI NODES.

A Service Description Language (SDL) is defined in order to establish the communication between the JCCI NEXUS and JCCI NODE. In particular, the taxonomy implemented in SPARTA JCCI, recall the structure of a Web Application Description Language (WADL), i.e., an XML vocabulary used to describe RESTful web services. In this way a generic client can load a WADL file and be immediately enabled to access the full functionality of the corresponding web service knowing, which URIs one can visit, what data those URIs expect you to send, and what data they expect in return. The Nexus can process this WADL to show directly to the user the information about the description of each partner, the information about the used dataset by each one, the developed tools, the services and so on.

According to the needs and the resources that each partner could share in the JCCI NEXUS, 5 calls are defined: getCapabilities, getData, getTools, getService and getInteraction. These calls are applied for the Learning contents as well as for the Workbench contents, in which the structure of the calls and the structure of the data are the same, however changing its contents.

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

In particular, the call getCapabilities asks JCCI NODE the description of the Company and the structure of the resource that it provides in order to know the available data, tools, services and platforms are available. Then, according to this first call, four new buttons related with the four calls getData, getTools, getService and getInteraction will be available. Each one, will be in charge to ask to the JCCI NODE the information related, and show them in a table, as presented in Figure 3.



Partners

VICOMTECH

live data

version	name	description	contact	info	url
1.0	Adversarial attack	Different implementation of adversarial attack y defense developed in SPARTA Safair	[illegible]@vicomtech.org	code	https://gitlab.vicomtech.es/SPARTA_SU8270_2010/safair/tree/master/Adversarial_attack
1.0	Bio-Inspired models	Implementation of different models based on bio-knowledge	[illegible]@vicomtech.org	code	https://gitlab.vicomtech.es/SPARTA_SU8270_2010/safair/tree/master/Bio-Inspired%20models

Last update: 01/07/2020

Figure 3: Example live data

An example of the structure of the WADL contract implemented in SPARTA JCCI is reported below. There, it is possible see that the external layers define the kind of application and where the resource is based, and so its address as well as the company that owns this service. The five functions useful for the JCCI communication between the NEXUS and the NODE, are defined inside the resource base, and for each one of them, the parameters needed for the call, as well as the respond status and the field for the result are specified.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<application>
  <resources base="URL" name="CompanyNames">
    <resource path="getCapabilites">
      <param required="true" style="template"/>
        <method name="GET" id="getCapabilities" >
          <response status="200">
            <representation mediaType="application/xml"/>
            <result></result>
          </response>
         </method>
     </resource>
    <resource path="getData">
      <method name="GET" id="getData" >
      <response status="200">
        <representation mediaType="application/xml"/>
        <result></result>
      </response>
      </method>
    </resource>
    <resource path="getTools">
      <method name="GET" id="getTools" >
      <response status="200">
        <representation mediaType="application/xml"/>
        <result></result>
```

```
            </response>
            </method>
        </resource>
        <resource path="getServices">
            <method name="GET" id="getServices" >
            <response status="200">
                <representation mediaType="application/xml"/>
                <result></result>
            </response>
            </method>
        </resource>
        <resource path="getInteraction">
            <method name="GET" id="getInteraction" >
            <response status="200">
                <representation mediaType="application/xml"/>
                <result></result>
            </response>
            </method>
        </resource>
    </resources>
</application>
```

Currently, the JCCI webpage is integrated in the main SPARTA website as shown in Figure 4. Both, the Workbench contents, and the Learning contents of the JCCI NEXUS are composed by a combination of static (or archived data) and dynamic (or live data) information. The static contents represent the old information that were available in the first centralized version of the JCCI webpage, the dynamic ones are the newest one provided by each partner through their respective JCCI NODE.

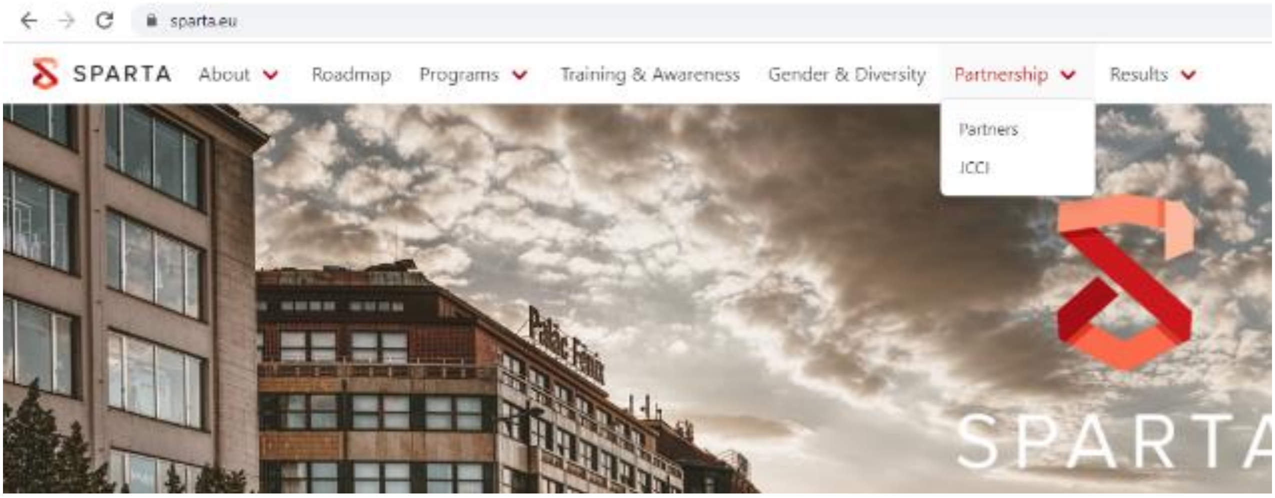


Figure 4: SPARTA official main page

2.3 Authentication and Authorization

As indicated in the *Deliverable 8.1 Initial results of the clustering, platforms, and ecosystems activities,* and shown in Figure 1, an access policy is introduced in the SPARTA JCCI flow. Before starting the implementation, a deep study about the Federated Infrastructures, as well as the authentication and authorization policies was led, and it is presented in Chapter 7. Finally, with the gathered information, the FIWARE framework is selected.

The FIWARE Authentication and Authorization framework works as follows: a website or application registers in Keyrock Identity Provider to be able to implement the login with Keyrock (like Oauth login in Google or Facebook). Once successfully registered, the user that wants to enter the web application will have to login into Keyrock (as well as register in it as a new user if it is the first time that the user tries to login). When Keyrock verifies that the password and username of the user are correct, it assigns a temporary token identifier to the user that will be transferred to the web application. Then, the latter will allow the user to enter the content of the web application.

Once the user has been authenticated in the web application, authorization policies can be configured. Keyrock is connected to AuthZForce Policy Decision Point (PDP). This module allows the framework administrator to configure the authorization policies and decide which user can access which resource.

Finally, Wilma Policy Enforcement Point (PEP) Proxy is installed in front of the protected resource so that the web application points to the PEP Proxy, instead of to the resource directly. This way, once the user has authenticated, when this user tries to access a protected resource, the web application will send a request to the proxy with the user token identifier provided by Keyrock during the login process. The proxy will redirect this information to Keyrock and AuthZForce and will then know whether the user can access the requested resource or not. If the user has permissions, the proxy will redirect the user to required resources.

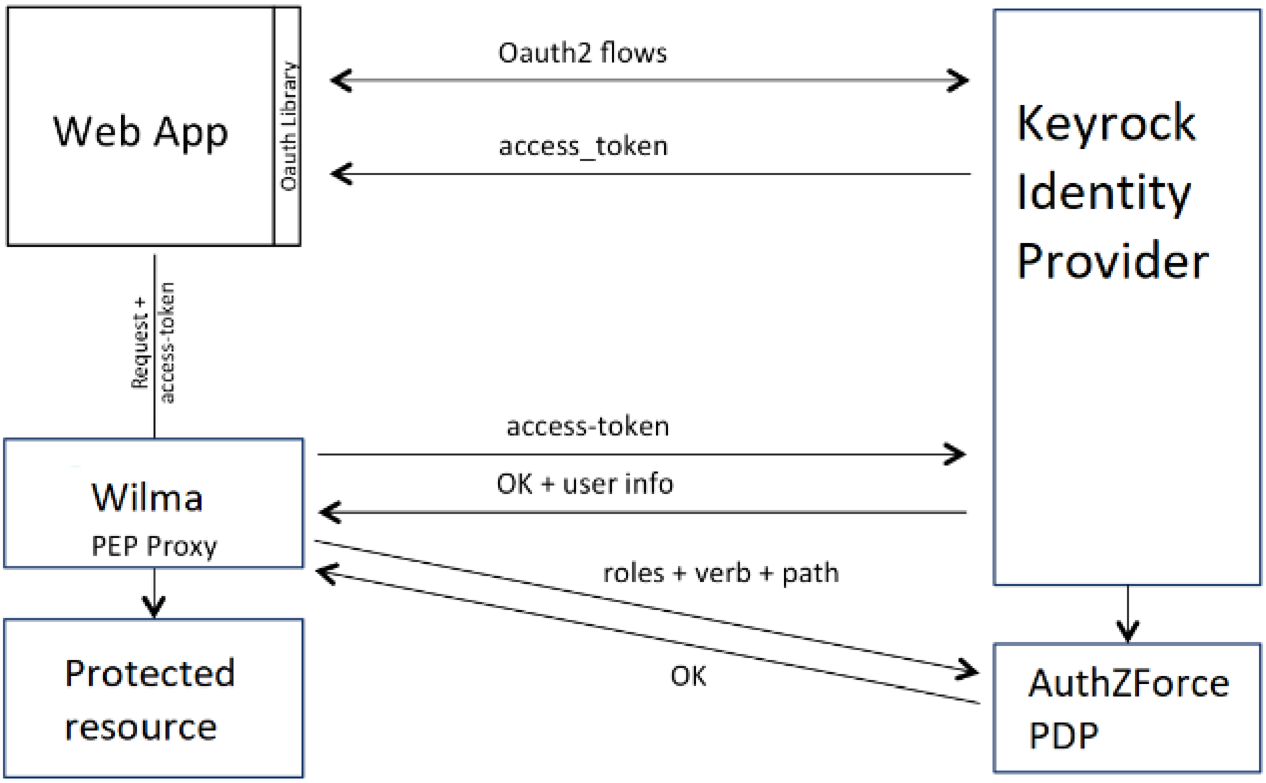


Figure 5: FIWARE structure

2.3.1 *Implementation in SPARTA*

As presented in the previous section an extra actor is added in the presented flow, a SPARTA Identity Provider (IdP). This IdP stores and manages users' digital identities to be checked via username-password combinations and other factors. Furthermore, it may simply provide a list of user identities to another service provider for him to check. Currently, in SPARTA JCCI implementation, this entity is a centralized one implemented using the Keyrock IdP developed under FIWARE initiative.

The solitary IdP is not sufficient to protect the resources in the SPARTA JCCI NEXUS, in fact, the IdP just specifies which users/profile are authorized and which are not. A proxy is needed to define an access policy to the resources. For this reason, the code of the SPARTA NODE was modified to include a proxy implementation (WILMA PEP), that can be easily modified and is already linked with the central SPARTA Keyrock IdP. The proxy acts as an intermediary for requests from clients seeking resources from servers holding them.

The proxy was included in the NODE implementation, in order to facilitate the deployment of the REST API among the partners, to facilitate its replication and at the same time to guarantee security of the deployment through an access policy.

In the basic case, all the general contents are kept public for increasing the SPARTA community and the dissemination of the results achieved in the project. Only the more critical services/applications could be protected by the proxy. Nevertheless, this decision will be taken by individual partners.

2.4 Next steps

For steering the growth of the SPARTA JCCI, our envisaged next steps are:

- Waiting for candidate's enrolment based on SPARTA available assets, increasing the number of associates working with live and dynamic information.

- Defining Cyber Range Scenarios using declared inventories and new outcomes. The definition of these scenarios will be done starting from the information that each partner uploads in the Learning and Workbench part.

- Defining the role inside the JCCI Identity Provider; several profiles with different privilege and access policies will be defined to increase the security of the available resources in the NEXUS.

Chapter 3 Clustering activities at national, European and international level

3.1 SPARTA ecosystem

SPARTA network is growing in terms of cooperation among partners and in the number of 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).

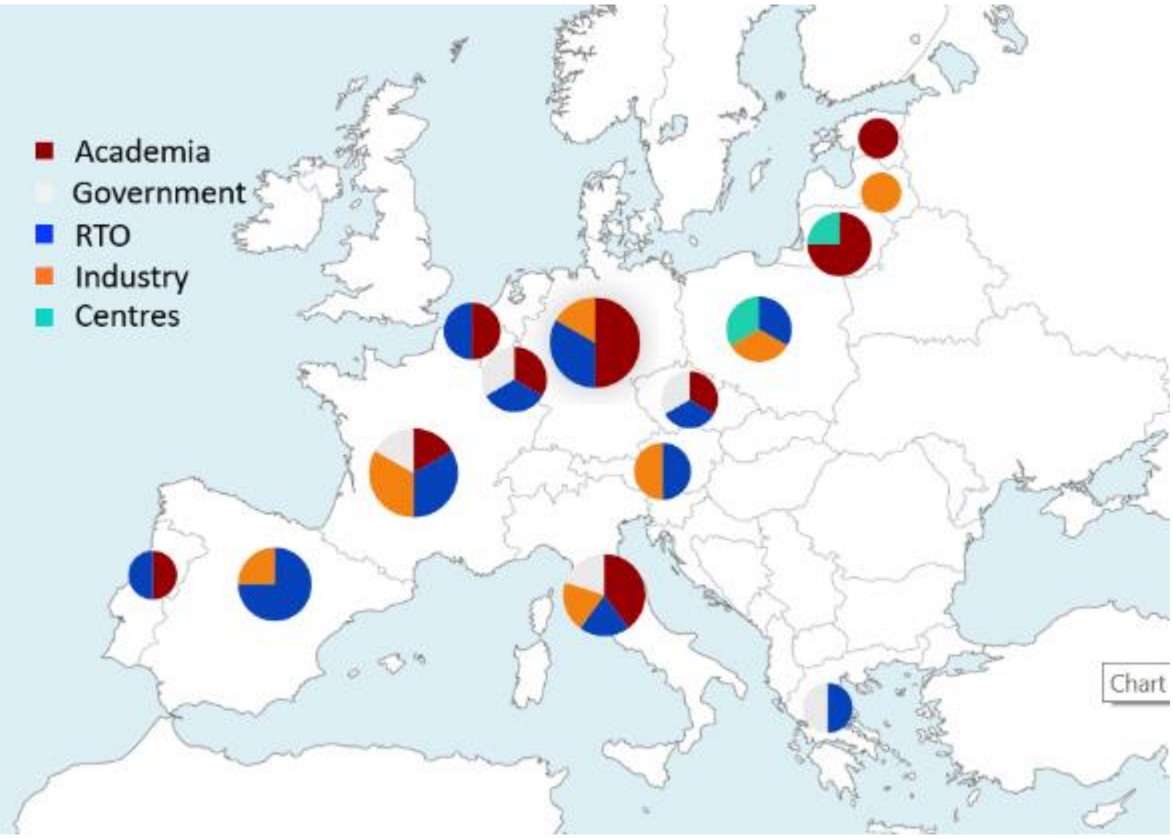


Figure 6: SPARTA ecosystem

This seems to be the optimal size w.r.t. manageability and creation of the critical mass to achieve its objectives. Being community building, one of the main goals, it is useful for several reasons to consider also other forms of involvement in the Network.

During the second year, we asked the partners to involve in their countries an increased number of organizations, to improve the local ecosystem cooperation, also with SPARTA.

In particular, we consider the notion of associates/friends, not formally bounded by the Grant Agreement, yet with the possibility to have active roles in the Network activities.

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).

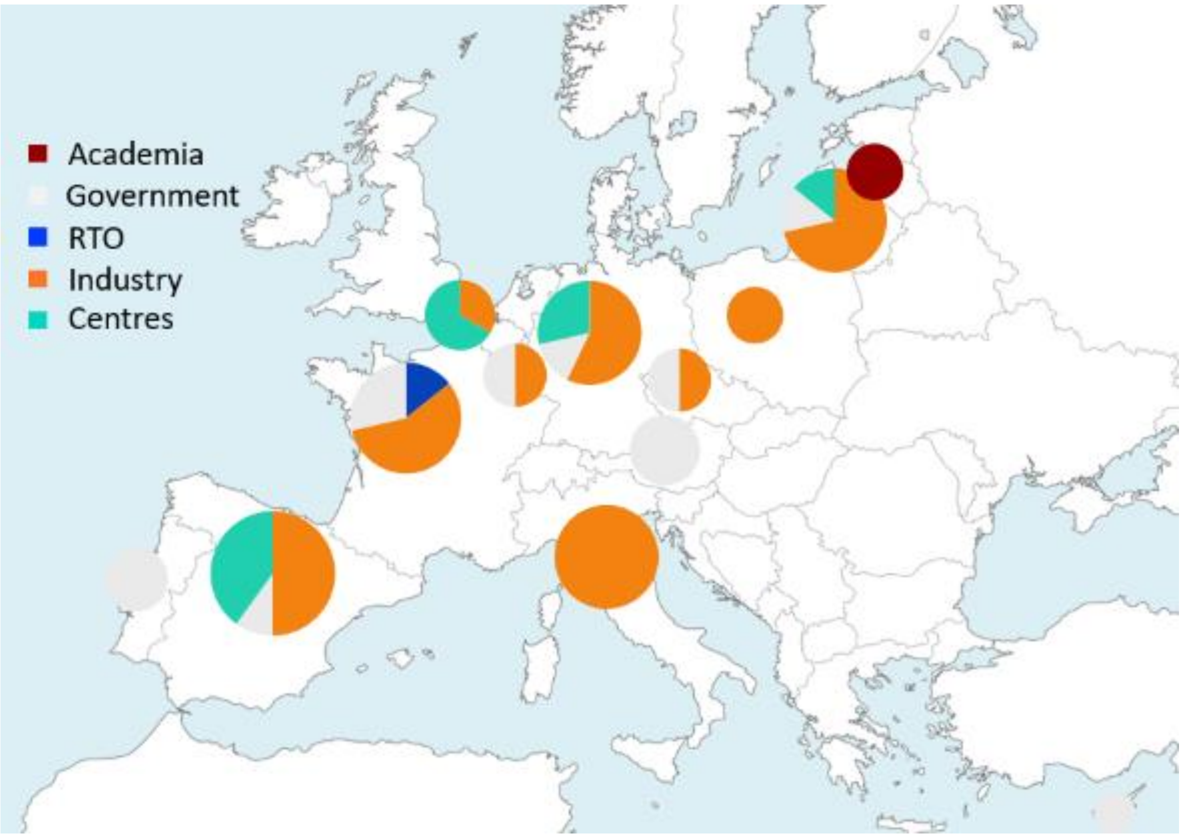


Figure 7: SPARTA associates/friends

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

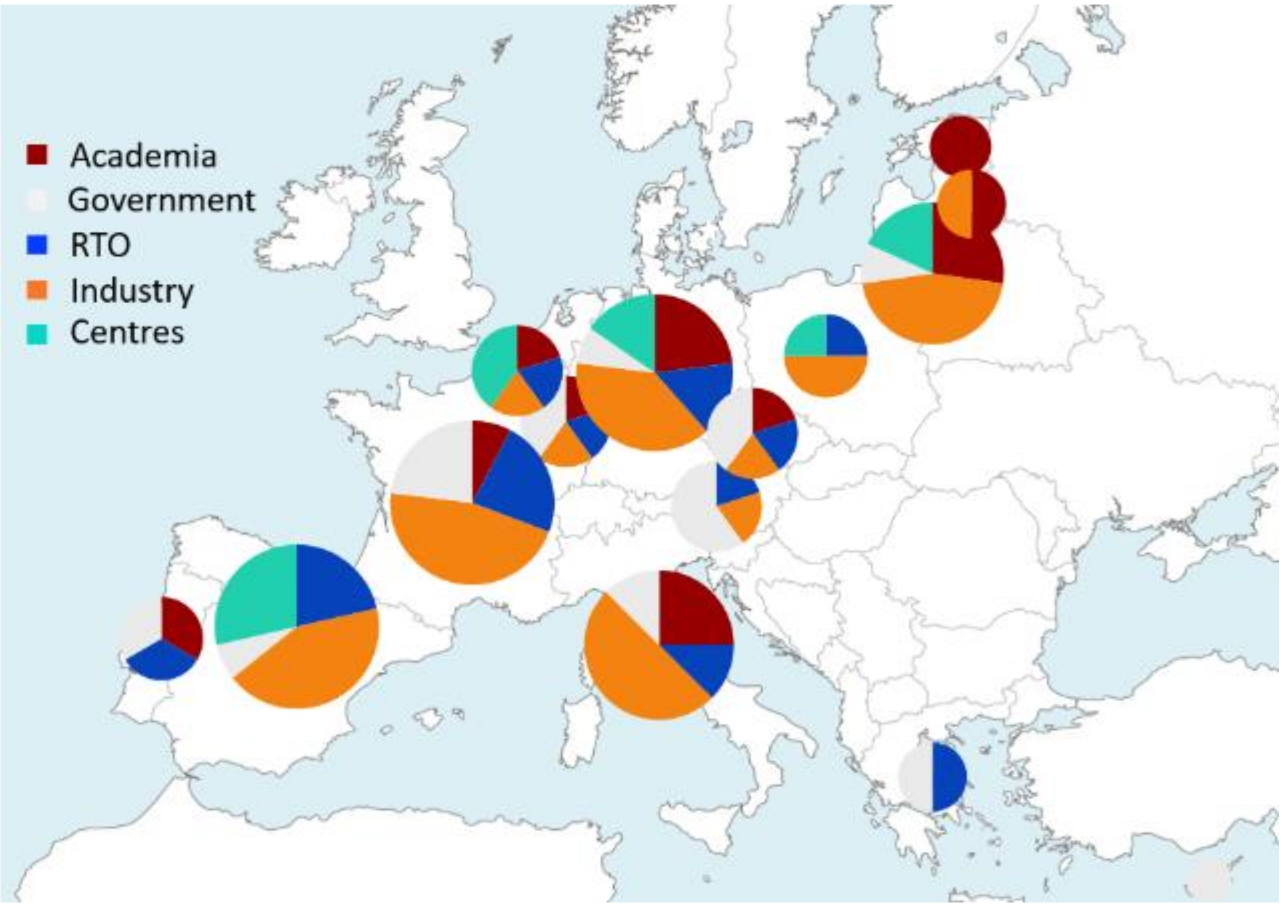


Figure 8: SPARTA overall community

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 two.

3.2.1 *France*

Current status

2020 was a cornerstone year for cybersecurity in France, with several structuring and strategic initiatives coming to fruition during this period.

- The Strategic Branch Committee (Comité Stratégique de Filière – CSF) "Security industries" was officially created in January 2020. **Under the presidency of Marc Darmon (Thales, a SPARTA Partner), it represents 4000 companies, about 130 000 jobs and a combined 28B€[3] yearly revenue**. Cybersecurity is one of the three activities covered by this branch committee: this marks a successful national-level organization of the French industrial ecosystem. Several SPARTA partners (CEA, Inria, IMT) are also members of the organization's Research and Innovation Working Group.

MICHEL VAN DEN BERGHE
CAMPUS CYBER
FÉDÉRER ET FAIRE RAYONNER L'ÉCOSYSTÈME DE LA CYBERSÉCURITÉ
Pour un nouveau centre de gravité de la sécurité et de la confiance numériques en France et en Europe.

[3] In short scale, 28 000 M€

- The French "Campus Cyber" was launched, following a report issued in January 2020. The Campus will be a totem pole for French cybersecurity that brings together the main national and international actors of the domain. It will welcome, in a common location in Paris, companies from small to large, state services, learning institutions, research organizations and associations. Of particular note, **the specific mention of SPARTA as a large-scale project, sponsored by the H2020 program, representative of dynamism in research and innovation**. The campus is scheduled to open its doors in 2021.
- The "Cybersecurity Automation Grand Challenge" made its official debut, with concrete R&I efforts launching in the final quarter of 2020, after a months-long preparation phase. Its approach was in part **inspired by the governance of SPARTA, with an expert nominated as Program Director, supported by a 30M€ budget, and guiding disruptive innovation efforts from the community**. In its initial phase, the Grand Challenge will focus on 3 opportunities: (1) dynamic networking and security models; (2) object-level detection, resilience, and trust; and (3) the protection of small entities (SMEs, associations, individuals) against cybercrime.

FAIRE DE LA FRANCE UNE ÉCONOMIE DE RUPTURE TECHNOLOGIQUE

Soutenir les marchés émergents à forts enjeux de compétitivité

Rapport aux Ministre de l'Économie et des Finances et Ministre de l'Enseignement Supérieur, de la Recherche et de l'Innovation
7 février 2020

Finally, the February 2020 report to the Ministry of Economy and the Ministry of Higher Education, Research and Innovation "Making France a Disruptive Technology Economy" places cybersecurity as the core of its "Digital sovereignty" challenge, and one of only four areas where leadership capacities exist. The document in particular argues for unified strategic and political support, across ministerial boundaries, for these areas, and underscores "the success of the French ecosystem can only be attained in European-scale synergies". The priorities and principles highlighted here will be core to the execution, in the coming months, of the French "Acceleration Strategy", and the backbone of the post-COVID stimulus plan.

SPARTA's actions in the second year

A wide variety of liaison activities have been taking place with French stakeholders throughout the pilot's second year. SPARTA and the execution of disruptive, concrete R&I activities with the mission to advance European strategic autonomy, within the scope of the Proposed Regulation, was presented to academic, institutional, and industry partners at:

- 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.
- The "Security Industries" strategic branch committee Research and Innovation working group and in particular its focus on cybersecurity, cloud and IoT
- ETP4HPC, in an effort to cross-examine strategic priorities, and with a marked interest from the HPC community in the SPARTA Roadmap.

The involvement of the general public is a key objective in SPARTA, and in the French community this has taken several forms: speaking at public events (FIC for instance), digital communications(eg, social networks[4]), and continued involvement with grassroots events. While COVID delayed the 2020 iteration of LeHack, preparations are already largely underway to make the 2021 edition a success.

[4] https://twitter.com/MaliciaRogue/status/1337348604453904384?s=19

3.2.2 *Belgium*

Current status

The current members of the Belgian cluster are the following:

Name	Type	SPARTA partner or associate
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

CCB is the Belgian national cybersecurity authority and it is responsible for supervising, coordinating, and overseeing the implementation of the Belgian cybersecurity strategy. This strategy defines the objectives and defines its different domains of action, including contributing to broadening cybersecurity expertise and knowledge. The current national cybersecurity was defined in 2012 and is currently under revision.

CCB is currently leading the implementation of the Belgian National Coordination Centre (NCC) of the future European Cybersecurity Competence Network and Centre (CCCN). It will be coordinating different cybersecurity activities that are distributed across several federal and regional ministries. It will also be involved in the community-building activities of the Competence Centre and the Network.

Currently CETIC and UClouvain are involved in NCC related meetings with CCB and the 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). As members of the SPARTA project, we are providing feedback based on SPARTA experience and results. Discussions among members of the Belgian cluster are continuous, in order to gather support for public authorities in the area of cybersecurity. This includes continuation of the “Keep It Secure” cybersecurity label for SMEs[5], and its complementary as a steppingstone to the federal Cyber Fundamentals certification scheme for SME (see [1] for a comparison).

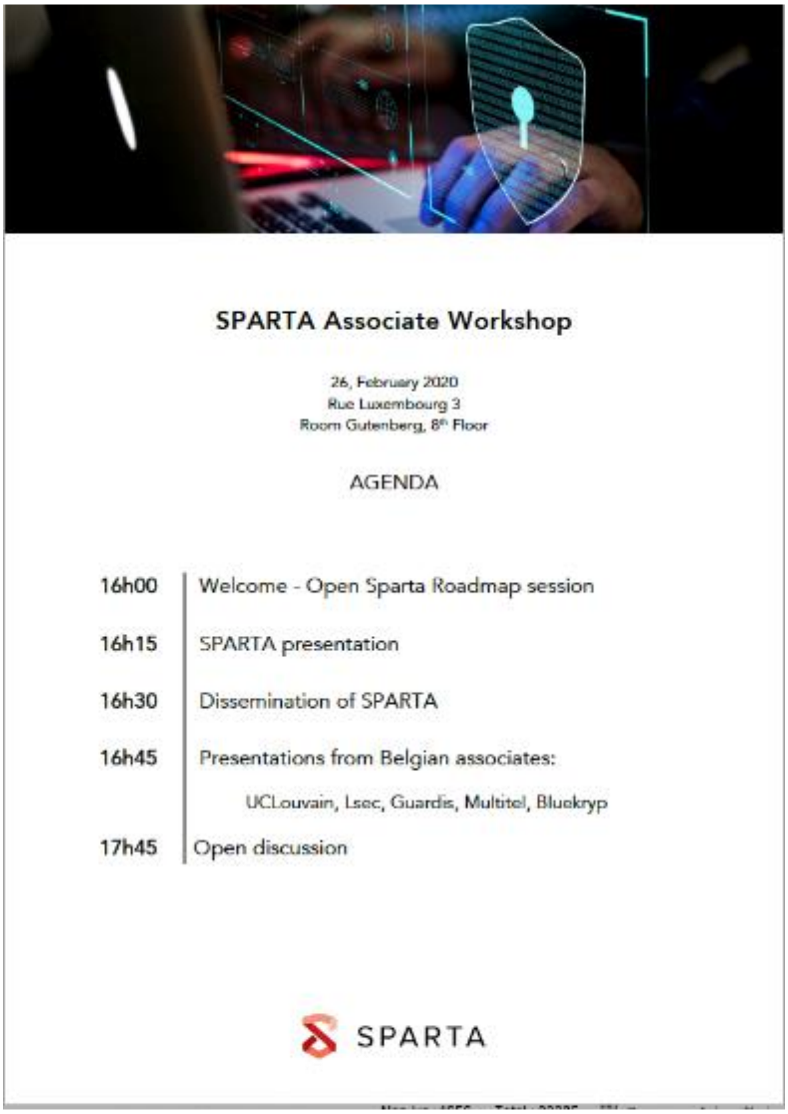
[1] Christophe Ponsard, Philippe Massonet, Jeremy Grandclaudon, Nicolas Point: From Lightweight Cybersecurity Assessment to SME Certification Scheme in Belgium. EuroS&P Workshops 2020: 75-78

[5] https://www.digitalwallonia.be/fr/publications/keepitsecure

SPARTA’s actions in the second year

Three main events occurred in the second year:

- Organisation of the Belgian SPARTA associate workshop on 26/02/2020.
- Presentation of a project idea and participation of several Belgian partners on 22/06/2020.
- Submission of a H2020 project proposal on 27/08/2020 that was presented at the brokerage event.



SPARTA Associate Workshop

26, February 2020
Rue Luxembourg 3
Room Gutenberg, 8th Floor

AGENDA

16h00	Welcome - Open Sparta Roadmap session
16h15	SPARTA presentation
16h30	Dissemination of SPARTA
16h45	Presentations from Belgian associates: UCLouvain, Lsec, Guardis, Multitel, Bluekryp
17h45	Open discussion

SPARTA

Figure 9: Belgian SPARTA associate workshop agenda

The figure above (Figure 9), shows the agenda of the Belgian associate workshop, and lists the new associate partners that made presentations about their cybersecurity activities during the event.

On 22/06/2020, several Belgian cluster members participated in the SPARTA brokerage event. CETIC presented a project idea during the event and completed the consortium with several partners that made presentations during the same brokerage event.

On 27/08/2020, CETIC submitted the ENSURE H2020 proposal on behalf of the consortium that was created as the result of the SPARTA brokerage event.

Plans for the M24-M36 period will focus on information Belgian cluster members on the progress of the Belgian NCC and the setup of the CCCN. How the community will be managed by the NCC and CCCN will be something to take into account. This will enable SPARTA partners and associate partners to join the CCCN.

3.2.3 *Greece*

3.2.3.1 Current status

In Greece, the National Cyber Security Authority (NCSA) was established in the Ministry of Digital Policy Telecommunications and Media following a Presidential Degree. The General Directorate of Cyber Security of the Ministry of Digital Government (National Cyber Security Authority) is responsible for its management Strategy and coordination of the Bodies during the implementation of the required meters. Through the Strategic Plan, the aim is to define suitable organizational, technical, and operational measures. NCSA is in the strategic level. the Cyber Defense Directorate of HNDGS (Hellenic National Defence General Staff) has the main national “technical role”, which is 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 infrastructures and the operational completion. In Greece, the Greek Cybercrime Centre is also established. 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.

For the personal data and privacy in National level there is Hellenic Data Protection Authority (HDPA) which oversees monitoring 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 in the European Union.

Other major cybersecurity pillars in National level described in the National Cybersecurity strategy are the National Telecommunications and Post Commission (E.E.T.T.) and KEMEA.

EETT is an Independent Administrative Authority. It is the National Regulator that regulates, supervises and controls:

(a) the electronic communications market: fixed and mobile telephony, wireless and internet companies and

(b) the postal market in which the supply companies operate postal services and courier services.

KEMEA. on the other hand, is a scientific, research and consulting body that its purpose is to conduct theoretical and applied research and elaboration studies, in particular at strategic level, on issues related to Security Policy, as well as the provision of services, of an advisory and advisory nature, and security issues in general.

Furthermore, there are several other cybersecurity activities such as the Annual Cyber defence national exercise “PANOPTIS” the KEMEA annual conference on CI protection, and the Hellenic Team of European Cyber Security Challenge.

3.2.4 *Austria*

Current status

Austria’s official Cyber Security strategy was developed in 2013. It defines certain processes and structures in order to ensure overall coordination of numerous stakeholders which are working individually to improve cybersecurity. On the political-strategical level, a cybersecurity Steering Group was established. Under the leadership of the Federal Chancellery, this group is responsible for preparing an annual Cyber Security Report and advising the federal government in all matters relating to cybersecurity. The Steering Group is composed of liaison officers for the National Security Council and cybersecurity experts of the ministries represented in the National Security Council.

A structure for coordination at operational level serves as platform for preparing a periodic and incident-related Cyber Security Picture and supporting the operators of critical infrastructures. It is coordinated by the Federal Ministry of the Interior supported at operational level by the Federal Ministry of Defence, which will be responsible of the coordination tasks if a cyber-defence incident occurs. Institutions dealing with security issues of computer systems and the Internet, as well as the protection of critical infrastructures, will cooperate in the framework of the Operational Coordination Structure. At state level, these organisations are in particular: GovCERT (Government Computer Emergency Response Team), MilCERT (Military Cyber Emergency Readiness Team) and the Cyber Crime Competence Center (C 4).

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.

The IKT-Sicherheitskonferenz organised every year by the Ministry of Defence is the major meeting place for members of the Austrian Cyber Security ecosystem with approximately 2000 participants in two days. SPARTA partner JR gave a speech in the 2019 conference about cybersecurity research in Europe and SPARTA's goals.

SPARTA has been promoted by JR in several more occasions such as the Graz Security Days for Industry, the FORTE and KIRAS applicant's day (National Security and Defence research programs), the Workshop on AI for LEAs at MILIPOL Paris 2019, the SMI2G Meeting 2020 and several business meetings with members of the industry or the scientific community.

SPARTA's actions in the second year

In 2020, like many other relevant events, the Austrian IKT-Sicherheitskonferenz was cancelled because of COVID-19. Nevertheless, SPARTA partner JR, was able to promote SPARTA in two online symposiums:

- Cyber Security in Österreich 2020: Ein- & Ausblicke für Studierende on May 28th and
- Cybersecurity in Finance on Oct 30th.

At the KIRAS Fachtagung (National security research program) on Sep 21st – one of the very rare physical events – JR staff used the opportunity to promote SPARTA in several business talks with stakeholders of the Austrian cybersecurity ecosystem.

3.2.5 *Poland*

Current status

The key objective of the National Framework of Cybersecurity Policy of the Republic of Poland is to expand the national cybersecurity system and ensure a consistent approach taken across the Republic of Poland. National Framework of Cybersecurity Policy requires involvement of different actors who are either public sector, telecommunications sector or Trust Service Providers and competent ministers responsible for preparing proposals of legal changes in the field of cybersecurity.

Development of the cybersecurity system at the national level also entails further development of structures dealing with cybersecurity at the operational level, including the national level CSIRTs, sectoral incident response teams (sectoral CSIRT), information exchange and analysis centres (ISAC). In order to make these developments possible, the Government introduced new legislation setting out the revised competencies of the relevant institutions. Three national level CSIRTs have been assigned to civilian, military and government sectors. The civilian sector forms the constituency of CSIRT NASK, which operates within the structures of NASK (Research and Academic Computer Network) — a SPARTA consortium member and a research institute which conducts scientific studies, operates the national ".pl" domain registry and provides advanced IT services.

CERT Polska[6] 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.

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)[7]. 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[8] is a network of integrated activities supporting and promoting companies in Malopolska Region from cybersecurity sector.

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

- AGH
- ENERGA Group
- The John Paul II Hospital in Krakow
- PKP Informatyka

SPARTA's actions in the second year

In 2020, NASK planned to organize a SPARTA workshop collocated with SECURE 2020 – one of the largest cybersecurity conferences in Poland, organized by NASK/CERT Polska. This event was expected to disseminate information about SPARTA in the cybersecurity community and lead to further growth of the cluster. Due to the COVID-19 situation, the SECURE 2020 conference was entirely remote, which limited the networking potential of such workshop. For this reason, the workshop was moved to SECURE 2021 (third year) and SPARTA participation in SECURE 2020 was limited to a presentation "European experiment in cybersecurity R+D financing ", which presented SPARTA as a new approach to building cooperation in the cybersecurity field and a wide scope of interests. The presentation was well received, and new contacts were established.

3.2.6 *Germany*

Current status

One of the players heavily shaping the Cooperation in the field of cyber security is the Cyber Security Cluster Bonn e.V. based in the geographic region of Bonn. Meanwhile the Cyber Security Cluster Bonn e.V[9]. has more than a hundred members compared to about 60 members in 2019.

As part of the nation-wide German initiative called "Nationaler Pakt Cybersicherheit" a structured overview of the cybersecurity landscape in Germany has been created and published [10]in 2020. The document covers the areas of Civil society, research and education, economy, government, NGOs, stakeholders, and initiatives. Overall, more the 1500 companies and organizations in Germany have been considered in the document.

[6] https://www.cert.pl/en/
[7] http://www.man.poznan.pl/online/en/
[8] http://cybersechub.eu/
[9] https://cyber-security-cluster.eu/en
[10]https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/it-digitalpolitik/online-kompendium-nationaler-pakt-cybersicherheit.html

SPARTA's actions in the second year

In cooperation with regional SPARTA partners and associates, in particular: Fraunhofer, German Federal Office for Information Security, City of Bonn, T-System, IHK (Chamber of Commerce) Bonn/Rhein-Sieg, Cyber Security Cluster Bonn e.V., and HiSolutions AG), UBO organized two online editions of the event format "Bonner Dialog für Cybersicherheit (BDCS)" (in German). These events comprise one or more topic-specific keynote(s) followed by a panel-audience discussion and are typically visited by about 200 attendees. The first BDCS edition of 2020 took place on May 5th, 2020 and focused the topic "Digital Self-Defence – Tomorrow is Too Late". The second BDCS editions of 2020 took place on October 29th, 2020 and covered the topic of "Usable Authentication – What Is Even Better Than a Secure Password?".

On October 1st, within the European Cyber Security Month (ECSM) partners and associates of SPARTA from the Bonn area (namely) organised an online-event called "Cybersicherheitstag" focusing on the topic "Networks Strengthen Networks – the New Work, Digital and Secure[11]".

On November 6th, SPARTA members UBO and BSI together with external partners from University Hospital Bonn (UKB) and Federal Institute for Drugs and Medical Devices (BFArm) organized an Online-Symposium on Cyber Security Aspects in the Health Sector.

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

3.2.7 *Czech Republic*

Current status

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

The private cyber security cluster operates through the Network Security Monitoring Cluster (NSM Cluster[12]) covering the region of South Moravia. In 2019, the National Cybersecurity Competence Centre (NC3) was established to connect partners from various research and industry sectors. SPARTA participates in NC3 through its members CESNET and Brno university of technology.

In 2020, the NC3 was significantly extended by new partners, including renowned universities (Czech Technical University in Prague) and companies such as UNIS, Flowmon, or Axenta.

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

[11] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Angebote/NewWork/newwork_node.html

[12] http://www.nsmcluster.com/en/

In 2020, CESNET organized its own cybersecurity workshop for its members organizations.

In 2020, Brno University of Technology, the SPARTA Training and Education WP leader, was coordinating national activities focusing on cybersecurity skills training, together with other partners involved in pilot projects. Work on a national framework for skills identification has been started. Furthermore, an inter-pilot team for an open-source Cyber Range development and testing (KYPO) has been initialized.

SPARTA's actions in the second year

CESNET organized five dedicated meetings for the Ministry of Defence and Armed Forces of the Czech Republic on various cybersecurity topics to foster further cooperation.

SPARTA member CZ.NIC, onboarded new SPARTA Associated partners, EZÚ, which is among others the CAB for eIDAS certifications as well as ISO/IEC 27001 (Information security management), ISO/IEC 12207 (Software life cycle processes) and ISO/IEC 15288 (Systems and software engineering – System life cycle processes).

Brno University of Technology cooperates with Masaryk University (member of CONCORDIA project) on their cybernetic polygon with the aim to connect the polygon to Brno University of Technology Cyber Grid and join this infrastructure into SPARTA.

Brno University of Technology cooperates with Masaryk University on the creation of a national skills framework for cybersecurity education.

In 2020, we achieved on-board National Cyber and Information Security Agency as a SPARTA Associate partner as well as other organisations that we are in touch with as SPARTA friends. To further foster the cooperation with NCISA, Brno University of Technology contributed to the standardization workshop for smart-grid technologies.

CZ.NIC also got in touch with the Czech Accreditation Institute (ČIA), which is active as a national supervisory body for various certifications, including those according to the Cyber Security Act.

Our future plan is to further develop cooperation and support of governmental cybersecurity bodies and include them into the roadmap process organized by SPARTA. Finally, we will reach out to other organizations in the Czech Republic through a SPARTA workshop, which we plan to organise together with the CESNET cybersecurity conference on the beginning of February 2021.

3.2.8 *Lithuania*

Current status

According to the National Cybersecurity Report provided by the National Cyber Security Centre under the Ministry of National Defence of the Republic of Lithuania, the dynamics of cyber incidents are changing dramatically. Cybercrimes have become more complex, more sophisticated and targeted to the wide spectrum of societal vulnerabilities, in particular threats like disinformation, and propaganda caused by Russian Federation attempts to negatively impact the political system of Lithuania has posed huge challenges to national security.

Thus, our government has invested heavily in the development of new policies, new initiatives, and international collaboration to ensure that its capabilities are sufficient to address new and emerging threats. Some of them are the transformation of the National Cyber Security Centre, the implementation of the Kaunas region Cybersecurity Cluster, the DEBUNK[13] national platform aimed

[13] https://www.economist.com/science-and-technology/2019/10/24/lithuanians-are-using-software-to-fight-back-against-fake-news

to fight disinformation, the NCSC/CERT-LT[14] measures over Health sector during the COVID-19 crisis or the formation of rapid cyber response teams under the Permanent Structure Cooperation (PESCO)[15] initiative.

Synergies between SPARTA and the national cybersecurity security strategy of the Republic of Lithuania

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

Relevance and usability of T-Shark developments (innovations) are evaluated by a group of independent experts (Arbitrage Group). Policy, Industry, Academia and End- User representatives have put significant effort into guiding efforts to respond to emerging threats, particularly those highlighted in the national cybersecurity and national security strategies.

National projects inspired by the SPARTA concept

The project “Development of the National Ecosystem for the Recognition and Analysis of the Information Effect Phenomena” (NAAS) is an excellent example of how SPARTA research results can be cascaded into national initiatives.

The NAAS project aims to create an efficient and modern R&D ecosystem enabling national research organizations to train public security practitioners and carry out research activities, including information security, information, and hybrid threat analyses, integrated (Internet and kinetic) information space monitoring and analysis of potentially criminal content. The ecosystem will integrate the SPARTA innovation governance model, methodological base, and measures to implement the vision of modern studies, thus enabling direct cooperation between national research organizations and SPARTA network partners.

New initiatives: SPARTA-REWARE

One of the examples of successful collaboration between SPARTA and pilot projects such as CONCORDIA, ECHO, CyberSec4Europe is the “Cybersecurity Skills Alliance – New Vision for Europe (REWARE) project that was developed and kicked-off by SPARTA network partners. REWARE brings together 12 education and training providers, 11 partners representing industry and certification, and two EU umbrella organisations for Vocational Education & Training from 12 EU countries to develop and implement a new sectoral approach on cybersecurity skills management including matching between cyber skills demand and available education and training programs and training providers. ERASMUS+ funding instrument was leveraged for this purpose. Funding approved by the program will support successful implementation of the REWARE project.

The synergies between SPARTA WP9 “Cybersecurity Training & Awareness” and REWARE goals and objectives will help to minimise overlaps and contribute significantly to closing cyber skills gaps at both EU and MS level.

New arenas for collaboration: SPARTA-EU-HYBNET

EU-HYBNET is a Pan-European network that unites security practitioners, stakeholders, academics, industry players, and SME actors across EU collaborating to counter hybrid threats. EU-HYBNET

[14] https://www.nksc.lt/en/reports.html
[15] https://kam.lt/en/news_1098/current_issues/eu_member_states_to_develop_european_cyber_response_force_proposed_by_lithuania.html

aims to build an empowered, sustainable network through its on-going association with a key partner, The European Centre of Excellence for Countering Hybrid Threats.

Considering that one of SPARTA research programs T-Shark has very strong synergies with EU-HYBNET and related with the technological aspects of hybrid threats, it was decided to establish collaboration in the fields that could be considered for further clustering of EU-HYBNET and SPARTA activities.

Assuming favourable outcomes over the longer term, the cross-network collaboration tested and piloted by the T-Shark Arbitrage Group might be transformed into a permanent EU body with independent professional assistance for end-users and make innovations uptake more effective.

SPARTA's actions in the second year

Recently the national agency of Science and Innovation facilitated the establishment of Digital Innovation Hubs that will play an important role in stimulating especially the uptake of Artificial Intelligence, HPC and Cybersecurity innovations by industry and public sector organizations in Lithuania.

16 Lithuanian organizations decided to unite and contribute to the EU cybersecurity market. They include Lithuanian universities, Digital Technology Centres (DTCs), associations uniting industrial and information technology companies, and private sector leaders in digital technologies. Experienced in digitization projects, they all have established the European Digital Innovation Hub (EDIH) of Central and Western Lithuania.

EDIH will operate as a one-stop-shop and provide innovation support and advisory services to businesses and public authorities. EDIH plans to assist a minimum of 500 companies in Central and Western Lithuania, so that more than 1,000 processes will be digitized, and more than 5,000 staff will be trained to use digital technologies in their working environments. Before investing, companies will be able to test the digital technologies they intend to procure and install and evaluate their performance.[16]

Towards achieving SPARTA's third objective "To build sustained collaborations with academic, industrial, governmental, and community stakeholders and engage with a wide range of cybersecurity ecosystems", L3CE facilitated discussions as to how to integrate national EDIH into the SPARTA ecosystem.

Several workshops with national EDIH and SPARTA network partners are planned for the year 2021. L3CE will assume a leading role in kick-starting discussions between Lithuanian and EU stakeholders aimed at helping to foster the collaboration between the Lithuanian EDIH and SPARTA network.

3.2.9 *Spain*

Current status

Since 2013, Spain counts with the National Cybersecurity Strategy that provides a basis for developing the provisions of the National Security Strategy (reviewed in 2017 and 2019) on the protection of cyberspace to implement cyber threat prevention defence, detection, response and recovery actions against cyber threats.

The National Cybersecurity strategy 2019[17] ,published in the BOE 30th April 2019, develops forecasts of the National Security Strategy 2017 in the field of cyber security, according to the general

[16] https://intechcentras.lt/category/dih/?lang=en
[17] https://www.dsn.gob.es/es/file/2989/download?token=EuVy2lNr

objectives, the target of area of cybersecurity and lines of action set to achieve this. Responds well to the mandate of the National security council of 16 July 2018 published in the BOE 10th August.

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

The document is structured in five chapters: cyberspace; threats and challenges in cyberspace; purpose, principles, and objectives for cybersecurity; lines of actions and measures; and cybersecurity in the National Security System.

As one of the key actions identified in the National Cybersecurity Strategy 2019, it has been created in July 2020 the “National Cybersecurity Forum”, a public-private collaboration space promoted by the National Security Board where the CCN is one of the vicechairs and INCIBE the other one. The work lines are centred in generating a cybersecurity culture, to offer support to the industry and R&D&i and an opportunity for Cybersecurity training and talent, aligned with the measures identified in the Cybersecurity National Strategy 2019.

This Forum is now part of the **Spanish Cyber Security Ecosystem** that is also formed by:

- The **CCN-CERT** is the **Information Security Incident Response Team** ensure protection from cyber-attacks on classified systems and systems belonging to Public Administrations
- **INCIBE**[18] as the **Cyber Security National Institute**
- The **National Centre for the Protection of Infrastructures and Cybersecurity (CNPIC)**[19]**.**
- The **INCIBE-CERT**[20] is the National CERT responsible for the prevention and mitigation of, and the response to, cyber-incidents in the corporate, citizen and critical infrastructure operator spheres.
- The Spanish Network of Excellence on Cybersecurity Research **(RENIC)**[21]
- The Spanish Cybersecurity Innovation Cluster **(AEI Ciberseguridad y Tecnologías Avanzadas)**[22]
- Recently it has been created **CYBASQUE** that is the Cybersecurity Industries Association of the Basque Country as well as the Madrid Cybersecurity Cluster. In Galicia, a similar public-private initiative has been recently formed under the name CIBER.GAL.
- It must be mentioned **EGIDA**, the National Network of Excellence in security and privacy technologies.
- The ecosystem is completed with regional agencies like the Basque Cybersecurity Centre[23], the Cybersecurity Agency of Catalonia and other regional agencies.

SPARTA’s actions in the second year

Different presentations and contacts have been made with different associations and companies to promote their involvement in SPARTA. It can be mentioned the presentation of SPARTA that was made in the ENISE SPIRIT 2020.

[18] https://www.incibe.es/en
[19] http://www.cnpic.es/en/index.html

[20] https://www.incibe-cert.es/en
[21] https://www.renic.es/es
[22] https://www.clustercollaboration.eu/cluster-organisations/aei-ciberseguridad-y-tecnologias-avanzadas
[23] https://www.basquecybersecurity.eus/en/

At the same time Spanish participants in SPARTA take part in the periodical meetings organised by INCIBE with the Spanish participant in the other 3 pilots.

The scheduled SPARTA workshop in the Spanish Cybersecurity Research Conference (JNIC), Ciudad Real, June 2020[24] has not been possible as the conference were postponed till 2021.

3.2.10 *Luxemburg*

Current status

In Luxembourg, the cybersecurity ecosystem has radically evolved within the last 20 years, a shift actively supported by the Ministry of the Economy, with a vision of inclusion and access to security services and products for all parties of society. The OECD papers from 2002[25] as well as the more recent one from 2015[26] significantly inspired this development.

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

The "Cybersecurity Board (CSB)", chaired by the Prime Minister and involving all relevant ministries and State bodies, represents the highest level of the Luxembourg cybersecurity public governance. On a strategic level, the "Interministerial Coordination Committee for Cyberprevention and Cybersecurity (CIC-CPCS)" strengthens, sustains, and facilitates the implementation of the National Cybersecurity Strategy (the third revision was published in May 2018[27]).

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

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

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

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

To combat cybercrime, the national prosecutor's office as well as the police forces have dedicated units to deal with « cyber » cases. They collaborate and are supported on an operational level by the CERT.LU[28] community, composed of the 5 public and 5 private CSIRTs from Luxembourg.

Finally, the national safer internet awareness centre is called BEE SECURE[29] and is dedicated to informing citizens and especially youngsters about the dangers and opportunities of the Internet.

[24] http://2020.jnic.eu
[25] https://www.oecd.org/sti/ieconomy/15582260.pdf
[26] http://www.oecd.org/sti/ieconomy/Digital-Security-Risk-Management.htm
[27] https://gouvernement.lu/fr/publications.gouv_hcpn%2Bfr%2Bpublications%2Bstrategie-nationale-cybersecurite-3%2Bstrategie-nationale-cybersecurite-3.html
[28] https://cert.lu/
[29] https://bee-secure.lu/

In addition to all this, there are several associations and clusters like CLUSIL[30], ISACA[31], CPSI[32], APDL[33], OWASP [34]… as well as the interdisciplinary institute for security, reliability, and trust (SnT) of the University of Luxembourg[35] and other research centres, dedicated to topics around cybersecurity.

SPARTA's actions in the second year

Due to the COVID19 situation, the calendar of events had to be modified. And the initially planned workshop could not take place during the Luxembourg Cyber Security Week (CSWL).

Therefore, SPARTA organized in December, a workshop aimed at the entire cybersecurity ecosystem, in order to both present the project, and engage with the different stakeholders on the benefits of participating to community related initiatives led by the future network of NCCC's.

3.2.11 *Portugal*

Current status

In Portugal, the CNCS as part of the National Security Cabinet (GNS) which depends directly on the Prime Minister office is the operational coordinator and competent authority in terms of national cybersecurity. Its mission has been established by the framework of the National Strategy for the Security of Cyberspace, approved by the Resolution of the Council of Ministers 36/2015, of June 12 of 2015 [36]:

Another highly important structure is the Portuguese National CSIRT Network (RNCSIRT), with currently 44 members, including representatives from the CNCS, military, finance, telecom, government, academia, cybersecurity national industry and cloud providers, is the main operational forum for CSIRT's in Portugal, as well as the "key" cybersecurity forum in the country. The RNCSIRT aims to build trusted, direct communication channels among its members, facilitate incident response and disseminate best practices on computer security incident handling. INOV is an active member of RNCSIRT.

The last version of the National Cybersecurity Strategy, was approved in June 2019 and define a general and specific approach, translated into six intervention axes, which form concrete lines of action aimed at reinforcing the national strategic potential in cyberspace by increasing its security, namely:

- axis 1 — Cyberspace security structure;
- axis 2 — Prevention, education and awareness;
- axis 3 — Cyberspace and infrastructures protection;
- axis 4 — Response to threats and combating cybercrime;
- axis 5 — Research, development and innovation;
- axis 6 — National and international cooperation.

Also, in 2019, CNCS published the "National reference framework for cybersecurity" and the corresponding capability maturity assessment and roadmap. So that a given organization can self-diagnose their maturity and create their internal roadmap for increasing their cybersecurity maturity.

[30] https://clusil.lu/
[31] https://www.isaca.org/chapters2/Luxembourg/
[32] https://cpsi.lu/
[33] http://apdl.lu/
[34] https://www.owasp.org/index.php/Luxembourg
[35] https://snt.uni.lu/
[36] https://www.cncs.gov.pt/

SPARTA's actions in the second year

Due to the COVID19 outbreak, the planned SPARTA cybersecurity workshop in Portugal was postponed to 2021.

3.2.12 *Latvia*

Current status

The vision of cybersecurity Latvia is a safe, open, free and reliable cyberspace that enables reliable and continuous delivery of services essential to the State and society.

Latvia needs to take advantage of the digital environment in order to ensure economic and social welfare, while reducing the overall level of cybersecurity risks, without unnecessary limitation to the flow of technology and information.

The following priorities are defined in the implementation of the cyber security policy: cyber-defence, deterrence and growth.

- Cyber-defence - developing and improving capacity, and knowledge to defend against growing cyber threats and respond effectively to cyber security incidents a protection and capacity to function.
- Deterrence – detect, investigate and stop malicious activities in cyberspace, identifying offenders and call them justice, thereby deterring others from taking such actions.
- Growth: continuous development of cybersecurity skills in different sectors and promoting specialization in cybersecurity.

While every institution in Latvia is responsible for its own part of cybersecurity in cabinet of ministers cybersecurity is represented by Minister of defence. Ministry of defence is also chairing National Cybersecurity council. As leading agency for civil defence and disaster relief Ministry of interior is coordinating Critical infrastructure protection program. National CERT team CERT.LV is located in University of Latvia in the Institute of Mathematics and informatics (LUMII) but is reporting to Ministry of Defence. Latvia has three universities active in cybersecurity area BA School of Business and Finance, Vidzeme University of Applied Sciences and University of Latvia.

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.

SPARTA's actions in the second year

SPARTA project has established contact with the following organisations:

- CERT.LV (the Information Technology Security Incident Response Institution of the Republic of Latvia)
- Vidzeme University of Applied Sciences
- PIKC SALDUS TEHNIKUMS
- NATO StratCom
- Riga Technical University
- Institute of Electronic and Computer Science

CERT.LV and Videzemes University of Applied Sciences have become members of Arbitrage Group in T-Shark WP4 program and Vidzemes University of Applied Sciences also became a Associated partner of SPARTA.

3.2.13 *Italy*

Current status

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

- CINI has set up the largest laboratory in Italy on cybersecurity (CINI Cybersecurity National Laboratory) that puts together 44 universities and collects expertise from more than 300 researchers actively working in Cybersecurity. It contributed to create the Italian Cyber security Framework[37] and several successful initiatives as CyberChallenge.IT, the Italian cybersecurity challenge.
- CNR had an interdepartmental security project and later a cyber security 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 Feb 2017 the National Committee for Research in Cyber Security under the auspices of Italian Department of the Information for Security (DIS). This is a successful example of national cooperation.

Thus, since 2017 Italy streamlined and strengthened its cybersecurity structure in order to boost its cyber capabilities, with (DIS) at the center 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.

The NSC is responsible for promoting Italy's participation in cyber activities (such as Cyber Europe organized by ENISA, the European Network and Information Security Agency) and other initiatives aimed at increasing national cybersecurity. NSC also contributed to the creation of the National Laboratory for Artificial Intelligence and Intelligent System and the Italian Industry Plan 4.0 Funding Program launched by the Ministry of Economic Development.

More recently there has been also a proposal for setting up the Italian Institute for Cybersecurity (IIC), whose creation has been also jointly advocated by CINI,CNR and CNIT.

The overall Italian strategy provides guidelines for collaboration among both private and public stakeholders, as well as with academia and research. This is clearly reflected in the current presence of SPARTA partners. These guidelines aim to:

- Strengthen Italian critical infrastructures and other strategic players' defence capabilities;
- Improve cyber actors' technological, operational, and analytic capabilities;
- Boost public-private cooperation;
- Foster cybersecurity culture;
- Support international cooperation.

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

SPARTA's actions in the second 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 cybersecurityobservatory 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 plan to have other SPARTA italian events in April and October (cybersecurity day 2021) and work to promote the presence of European Digital innovation Hubs present in Italy also in SPARTA.

3.2.14 *Estonia*

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 with regard to 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 cybersecurity.

The main areas of cyber defence developments in Estonia are (i) critical infrastructure and vital services; (ii) cybercrime; (iii) national defence[38].

Estonia has developed the third Cybersecurity Strategy for the period of 2019–2022[39].

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:

- **Cyber defence unit of the Defence League[40]**
- **International Centre for Defence and Security (**ICDS)[41].

[38] https://www.mkm.ee/en/objectives-activities/cyber-security
[39] https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf
[40] https://www.kaitseliit.ee/en/cyber-unit
[41] https://icds.ee/

- **Estonian Information System's Authority** (RIA)[42].
- **Association of Information Technology and Telecommunications** (ITL)[43].

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

- The main tasks of the **Estonian Defence Forces Cyber Command**[44].
- From the 1st of August of 2020 the HITSA have been transferred to **Education and Youth Authority** (Harno)[45].
- **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[46].
- **ISACA Estonia Chapter**[47].
- From 2016, the eGovernment Academy holds and develops the **National Cyber Security Index** database[48].
- Estonia is the host and the framework country for the **NATO Cooperative Cyber Defence Centre of Excellence** since 2008[49].
- The **Estonian Information Security Association** (EISA)[50].

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

- RIA is leads **EU CyberNet** – the EU's prime new Cyber Capacity Building Network initiative that will establish an EU-wide network of cyber security experts that can be used by the Member States and EU institutions to carry out cyber security assistance projects in third countries[51].

- RIA is member of the project **Cyber4Dev**. This is the EU Cyber Resilience for Development Project[52].

Estonia introduces its cyber security initiatives review in the book **Cyber Security in Estonia 2020** what is freely available[53].

SPARTA's actions in the second year

SPARTA workshop in Estonia. The SPARTA associate workshop in Estonia was organised virtually on the 18th of June. It was organised by the University of Tartu (UTARTU) with a very big help and support by the Lithuanian Cybercrime Center of Excellence for Training, Research and Education (L3CE). The workshop was organised in connection to the Baltic DB&IS 2020 conference, this year happening virtually in Estonia. The SPARTA workshop was advertised in the conference Website[54]. The SPARTA workshop was attended by the representatives from the Defence Leagues,

[42] https://www.ria.ee/
[43] https://www.itl.ee/en/
[44] https://mil.ee/en/landforces/cyber-command/
[45] https://harno.ee/en/
[46] https://startupestonia.ee/focus-areas/cybertech
[47] https://www.eisay.ee
[48] https://ncsi.ega.ee
[49] https://ccdcoe.org/
[50] https://eisa.ee
[51] https://www.eucybernet.eu/
[52] https://cyber4dev.eu
[53] https://www.ria.ee/sites/default/files/content-editors/RIA/cyber_security_in_estonia_2020_0.pdf
[54] https://dbis.ttu.ee/index.php?page=71

ISACA Estonia members, ISACA Lithuania members, GDPR experts from several private companies.

SPARTA workshop on Ethical, Society, and Legal Questions in Cybersecurity Research was organised on the 19th of November by the MRU (Lithuania) and the SPARTA WP2. UTARTU participated in the workshop and presented and approach for model driven GDPR compliance management in the session on Data Privacy Related Issues.

Tartu Security initiative meetings were organised on the 30th of January and 30th of October. The main goal of these meetings is to assemble the parties who are interested in the Cybersecurity research and development in Tartu (Estonia). The meeting attracted the Cybersecurity research group representatives from the University of Tartu, Startup Estonia, Defence League members, ISACA Estonia representatives and private companies (e.g., Cybernetica, Guardtime, etc.). In both meetings, UTARTU has presented the SPARTA activities and the UTARTU role and contributions in the project.

3.3 European level

ECSO

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

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

ENISA

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

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

- EOS (EU)
- ENLETS (EU)
- ESA (EU)

Also, SPARTA cooperates with ENISA for the ATLAS for collecting the knowledge about organizations involved in cybersecurity in Europe.

3.3.1 *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 is a new project that 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.

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.

UTARTU team is involved in the following EU projects:

- **Blockchain Skills for ICT Professionals** (**BLISS**)[55], Erasmus+ Strategic Partnership. Duration: 01.10.2017 – 31.03.2020 (project has ended). The project has developed the developed educational resources and materials to address existing occupational needs and mismatches and an innovative course on blockchain skills needs that could support the large-scale open access and participation in training activities for ICT professionals. The project is awarded with the **Good Practice Example** badge from the EU Commission. Project card is available[56].
- **Safeguarding against Phishing in the age of 4 Industrial Revolution** (**CyberPhish**), Erasmus+ Strategic Partnership program Duration: 02.11.2020 – 01.11.2022. The goal is to

[55] http://bliss-project.eu

[56] https://ec.europa.eu/programmes/erasmus-plus/projects/eplus-project-details/#project/2017-1-FR01-KA202-037259

develop educational material for the course on the security phishing threats. The project involves 5 European partners.

- **A Blueprint for Sectoral Cooperation on Blockchain Skill Development** (**CHAISE**), Erasmus+ Sector Skills Alliances program. Duration: 01.11.2020 – 31.10.2024. The goal is to develop the framework for the educational skills on the Blockchain technology and application. The project involves 23 partners from 15 European countries.

An ERASMUS+ Skills Alliance project REWIRE has been accepted for funding and has its aim on creating a blueprint for cybersecurity education in Europe. The project includes many partners from SPARTA, together with other pilots' members.

SPARTA WP9 Members have become members of the ENISA Cybersecurity Skills Framework working group.

SPARTA (represented by L3CE and CESNET) negotiates with the SAPPAN project regarding cooperation on comprehensive cybersecurity threat analysis and sharing.

3.3.2 *Further activities*

The 17th edition of the annual international conference DIMVA, officially sponsored by the special interest group Security Intrusion Detection and Response (SIDAR) of the German Informatics Society (GI), has been organized as ongoing online event in 2020. Several SPARTA partners (i.e., UBO, CEA, IMT) are members of the DIMVA steering committee.

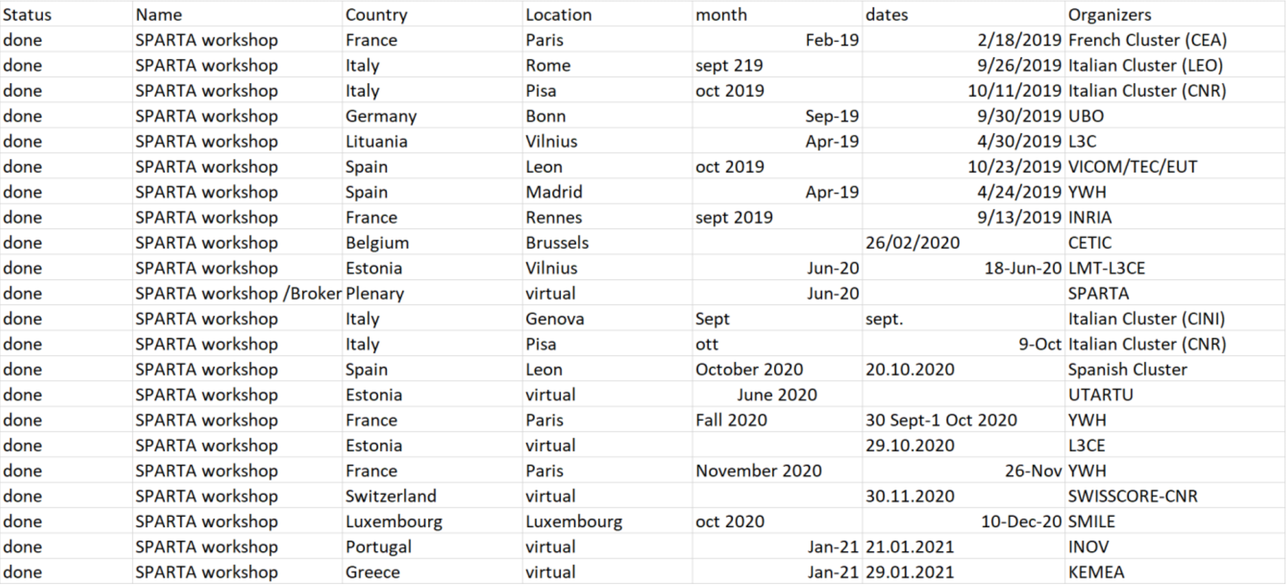
UBO and SAP published a research dataset and a paper on software supply chain attacks that triggered numerous requests by the international research community (EU, America, Asia) and fostered international research cooperation.

SPARTA partner UBO attended and participated in several international conferences: ARES, European Interdisciplinary Cybersecurity Conference (ECCI), International Conference on Information Systems Security and Privacy (ICISSP), International Conference on Trust, Privacy and Security in Digital Business (TrustBus) and Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA).

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). We created with WP12 and WP3 a handbook for running SPARTA monthly workshops as well as a report form.

In the second year we run 14 monthly workshops (listed below) and 10 are already planned for year three. We also had a major plenary event will all the associates and friends on 20 June 2020 and during this event called SPARTA brokerage event, we were able to set up several consortia for applying to the last call of H2020 in august 2020.



Status	Name	Country	Location	month	dates	Organizers
done	SPARTA workshop	France	Paris	Feb-19	2/18/2019	French Cluster (CEA)
done	SPARTA workshop	Italy	Rome	sept 219	9/26/2019	Italian Cluster (LEO)
done	SPARTA workshop	Italy	Pisa	oct 2019	10/11/2019	Italian Cluster (CNR)
done	SPARTA workshop	Germany	Bonn	Sep-19	9/30/2019	UBO
done	SPARTA workshop	Lituania	Vilnius	Apr-19	4/30/2019	L3C
done	SPARTA workshop	Spain	Leon	oct 2019	10/23/2019	VICOM/TEC/EUT
done	SPARTA workshop	Spain	Madrid	Apr-19	4/24/2019	YWH
done	SPARTA workshop	France	Rennes	sept 2019	9/13/2019	INRIA
done	SPARTA workshop	Belgium	Brussels		26/02/2020	CETIC
done	SPARTA workshop	Estonia	Vilnius	Jun-20	18-Jun-20	LMT-L3CE
done	SPARTA workshop /Broker	Plenary	virtual	Jun-20		SPARTA
done	SPARTA workshop	Italy	Genova	Sept	sept.	Italian Cluster (CINI)
done	SPARTA workshop	Italy	Pisa	ott	9-Oct	Italian Cluster (CNR)
done	SPARTA workshop	Spain	Leon	October 2020	20.10.2020	Spanish Cluster
done	SPARTA workshop	Estonia	virtual	June 2020		UTARTU
done	SPARTA workshop	France	Paris	Fall 2020	30 Sept-1 Oct 2020	YWH
done	SPARTA workshop	Estonia	virtual		29.10.2020	L3CE
done	SPARTA workshop	France	Paris	November 2020	26-Nov	YWH
done	SPARTA workshop	Switzerland	virtual		30.11.2020	SWISSCORE-CNR
done	SPARTA workshop	Luxembourg	Luxembourg	oct 2020	10-Dec-20	SMILE
done	SPARTA workshop	Portugal	virtual	Jan-21	21.01.2021	INOV
done	SPARTA workshop	Greece	virtual	Jan-21	29.01.2021	KEMEA

Figure 10: SPARTA monthly workshops

Here we see the coverage of the workshops for the countries:

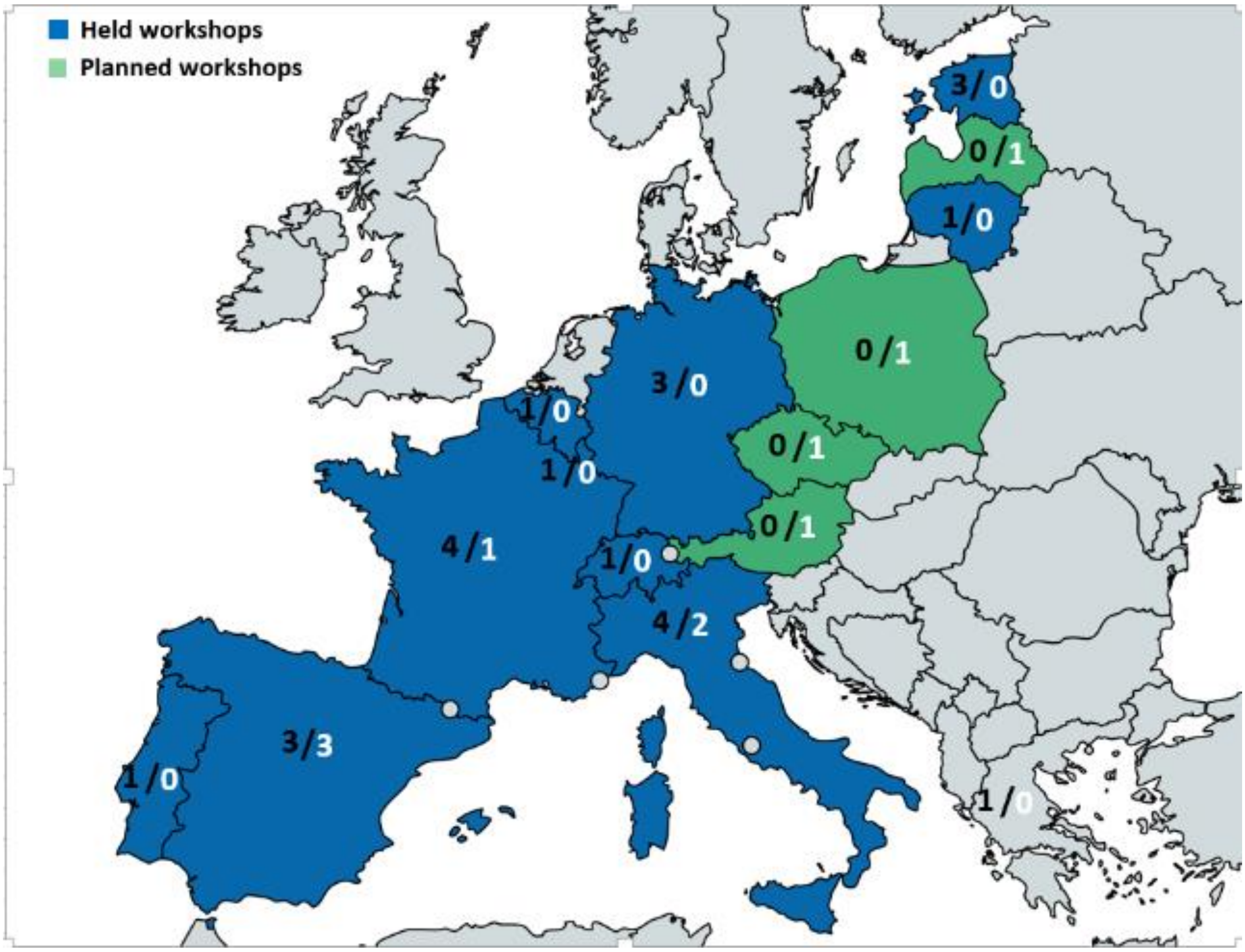


Figure 11: SPARTA monthly workshops per country

(x/y, where x stands for done and y for planned)

For the third year we plan to cover all the countries and also shift from regional based workshops to thematic ones. Indeed, all the countries of SPARTA partners will be soon covered and the strategy is to go thematic. In particular, we plan to make workshops for young people women (possibly in cooperation with ECSO).

Chapter 4 Clustering with other pilots

The SPARTA pilot explicitly allocates effort in the cooperation with the 3 other pilots to promote a truly fair cooperation across the consortia. This activity was explicitly requested by the call, sustained by the Commission, and was understood early on as instrumental for the success of the Network of Competence Centers. Empirical feedback from the community was overwhelmingly in favor of cross-pilot synchronization, with transparency and coherence being strong requirements from their part.

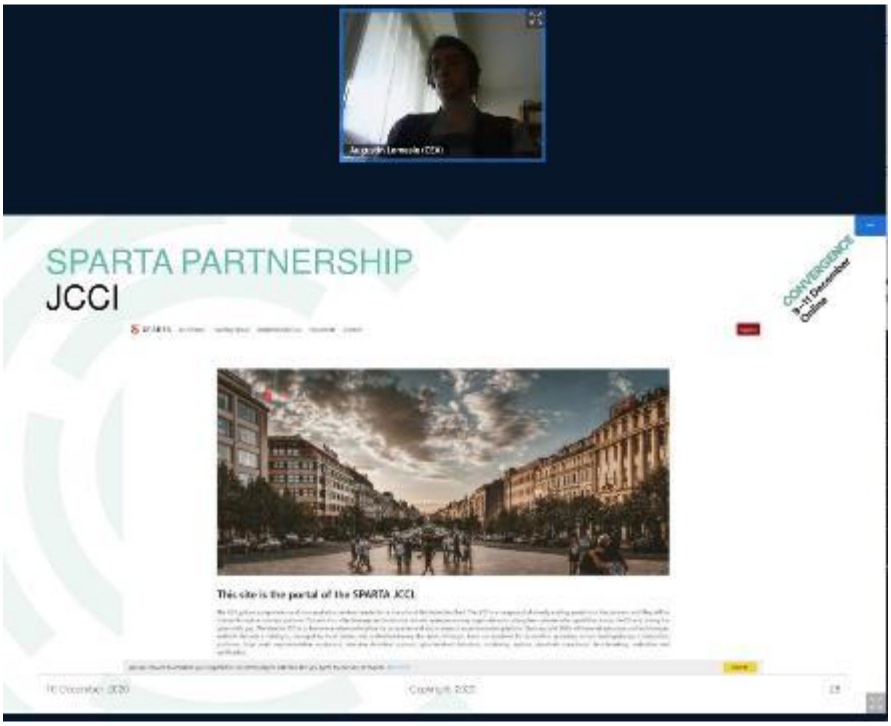
In continuation with previous efforts, coordination has been taking place with the Commission through meetings, which became bi-monthly at the start of 2020, with a larger emphasis on remote meetings. These meetings facilitated greatly the contacts with ENISA and the JRC. With the former, this was a formidable opportunity to exchange information on the new missions stemming from the application of the Cybersecurity Act. This ranged from coordinated actions on skills and training (more on this below), to sharing call for participations for ENISA's new task forces on certification. With the latter, 2020 saw intense discussions and testing of the new Atlas initiative. Through shared planning, feedback collection, workshops, and testing phases (ongoing at the time of writing), JRC and the four pilots tackled the difficult task of setting up an online repository of research actors, open but secure, wide-ranging but privacy-aware.

4.1 Federated workstreams

Cross-pilot interactions during the second year were largely structured around *federated workstream*, topical working groups constituted across the pilots with the voluntary participation of ECSO, JRC, and ENISA. Throughout 2020 participation was mostly voluntary, with a more structured and strategic approach being devised for 2021.

4.1.1 *Communication and dissemination workstream*

The Communication workstream was chaired by SPARTA in 2020 S1, resulting in a redefinition of a common communication plan, and a strong sequence across social networks. 2021 S2 was focused on the preparation of the December 2020 Concertation Meeting.



SPARTA PARTNERSHIP
JCCI

This site is the portal of the SPARTA JCCI

Figure 12: SPARTA presentation at Convergence

Communication towards European bodies included a workshop to the Council on 21 February 2020. SPARTA partners helped shape the preparatory phases and presented topics such as on “Massive IoT, integration” – Rayna Stamboliyska (YWH), and “Critical infrastructure protection and resilience“ – Emmanuel Dotaro (TCS).

4.1.2 *Cyber-ranges workstream*

The cyber-ranges workstream continued in 2020, with the involvement of Spartans despite being less of a major topic in the pilot. It was mainly host to technical discussion. The workstream seems relevant to merge with Education and training topic.

4.1.3 *Governance workstream*

A new workstream was created in May 2020 on the topic of Governance. Pilots have shared their approaches on the subject, with different alternatives and scenarios being discussed (governance and metagovernance models for instance). The difficulty here is twofold: first, to settle on a common understanding and common perimeter; second, to reconcile academic analyses with ground realities. Nevertheless, this forum has been a useful information and knowledge sharing avenue.

4.1.4 *Roadmap workstream*

Preliminary discussions on the setup of a cross-pilot workstream on Strategic Roadmapping were held in March 2020. Messages reaching out to other pilots were sent in April by the SPARTA Roadmap Committee, with encouraging replies, and follow-up teleconferences. The group drafted a clear mandate, shown below.

Very interesting insights have been gained by comparing how pilots approach their roadmap activities. For instance, the mission-oriented roadmap in SPARTA is quite different from Concordia’s focus on people, devices and network – yet the interplay has revealed key topics.

While there were challenges in communications between teams, due to a perceived competition between them, the focus on concrete scientific discussions helped smoothen the process. As an example, a collaborative approach has been implemented in structuring joint work, with questions such as:

- what should be the top priorities to strengthen sovereignty?, or
- how to structure the document to present their results to the Commission?

being submitted to scrutiny across the pilots.

4.1.5 *Education and training workstream*

The Education and Training program held fast in 2020. Contacts, in particular with ENISA, intensified, from monitoring the workstream in March 2020 to taking an active role in May 2020, and strongly inviting participation in its own Ad-hoc Working Groups in November 2020. A significant area of interest was the SPARTA Skills Framework, which was delivered early and used as a reference by the other pilots, with additional work being focused on cyber-ranges, and the mapping of existing education courses and professional training. Work in this topic has proceeded in sub-groups and workshops involving DG Connect, ENISA, ECSO and the 4 pilots (for instance in June 2020). This has allowed teams across pilots to reuse each other's results and avoid duplicating efforts. For instance, the SPARTA Skills Framework has been used across all 3 other pilots; conversely the use of Education maps from Cybersec4Europe and CONCORDIA, or of ECHO's and CONCORDIA's cyber-range developments as part of SPARTA's curricula work.

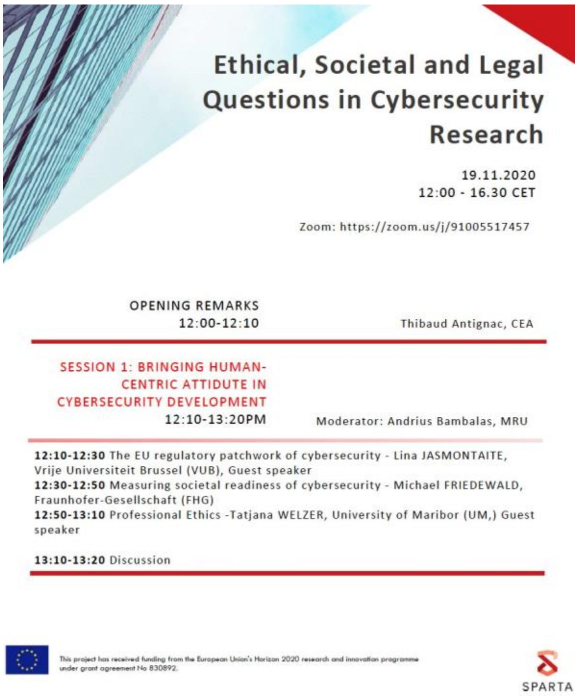
Crucially for sustainability, SPARTA has succeeded in its proposal to the Erasmus+ Skills Alliances call[57].

It should be noted that the strong involvement of the Commission and ENISA in the interpilot cooperation in general, and this workstream in particular, has very concrete and positive effects on collaborations.

4.1.6 *On legal and ethics issues*

While not defined as a cross-pilot workstream, it is really interesting to see common work and conversations on non-technical topics emerge between them. Perhaps the most telling example in 2020 was the November 2020 workshop on the topic, involving Cybersec4Europe and Concordia in addition to SPARTA.

[57] https://eacea.ec.europa.eu/erasmus-plus/selection-results/sector-skills-alliances-2020_en



Ethical, Societal and Legal Questions in Cybersecurity Research

19.11.2020
12:00 - 16.30 CET

Zoom: https://zoom.us/j/91005517457

OPENING REMARKS
12:00-12:10 Thibaud Antignac, CEA

SESSION 1: BRINGING HUMAN-CENTRIC ATTIDUTE IN CYBERSECURITY DEVELOPMENT
12:10-13:20PM Moderator: Andrius Bambalas, MRU

12:10-12:30 The EU regulatory patchwork of cybersecurity - Lina JASMONTAITE, Vrije Universiteit Brussel (VUB), Guest speaker
12:30-12:50 Measuring societal readiness of cybersecurity - Michael FRIEDEWALD, Fraunhofer-Gesellschaft (FHG)
12:50-13:10 Professional Ethics -Tatjana WELZER, University of Maribor (UM,) Guest speaker

13:10-13:20 Discussion

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

SPARTA

Figure 13: Cross-pilot workshop on ELSA in cybersecurity research

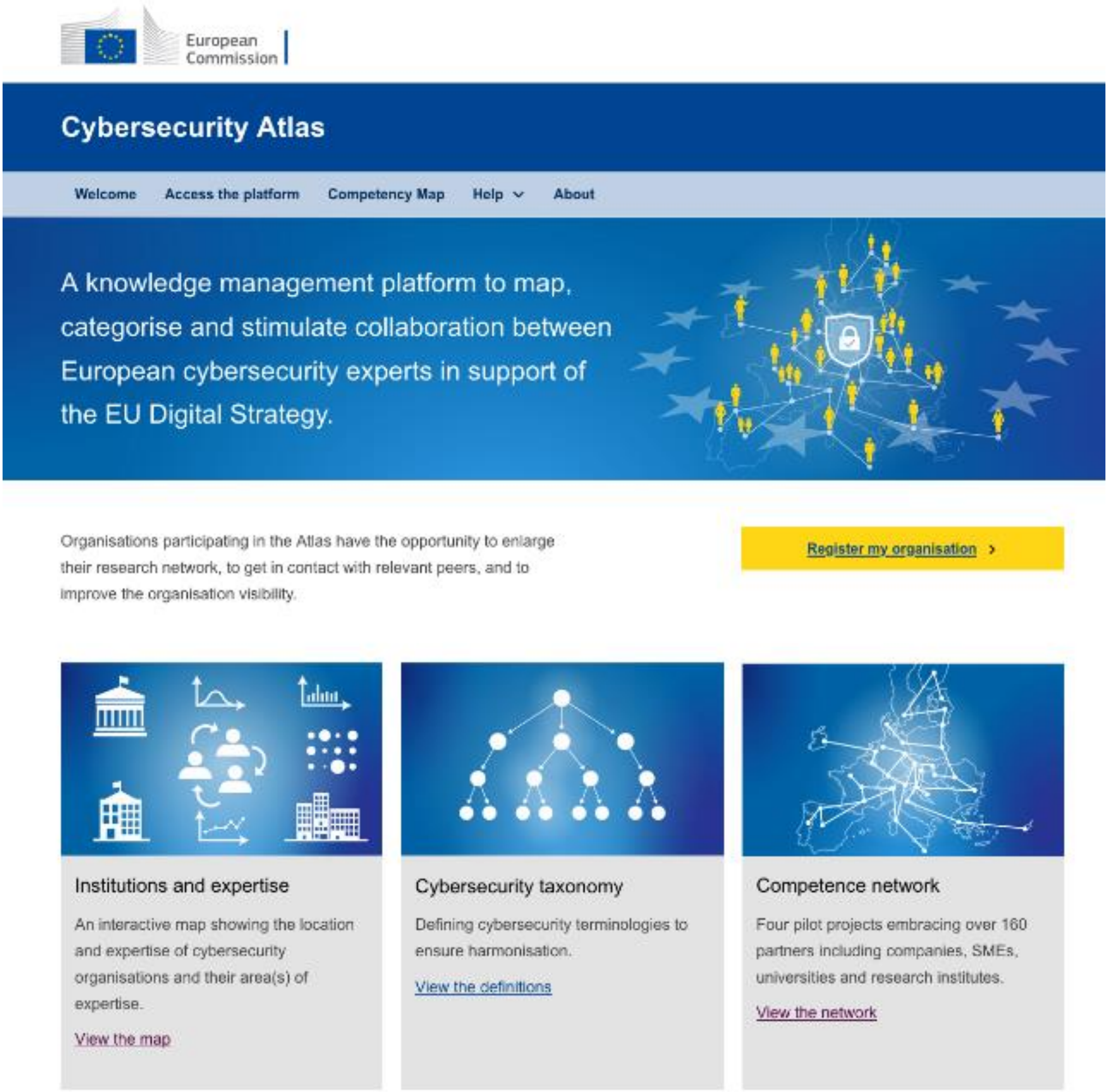
Further cross-pilot activities will be actively pursued, with support from a dedicated workstream being discussed.

4.2 Atlas

In March 2020 the Commission launched an ambitious initiative: the Cybersecurity Atlas, continuously surveying the expertise and capacities available in Europe. This digital knowledge management platform aims to map, categorize and stimulate collaboration between entities with cybersecurity expertise across Europe. The initiative, under the responsibility of the JRC, draws from the 4 pilots to help populate the Atlas with high-quality information.

SPARTA – alongside the 3 other pilots – took an active role in the preparatory phases of the Atlas, with large participations in workshops (ex. April), and constructive feedback provided on the topics of data security, integrity, sustainability, accountability, communications, organization, etc.

SPARTA has taken part in the testing phase in 2020 Q4, and in the ramp-up for the initial phase in 2021 Q1.



European Commission

Cybersecurity Atlas

A knowledge management platform to map, categorise and stimulate collaboration between European cybersecurity experts in support of the EU Digital Strategy.

Organisations participating in the Atlas have the opportunity to enlarge their research network, to get in contact with relevant peers, and to improve the organisation visibility.

Institutions and expertise

An interactive map showing the location and expertise of cybersecurity organisations and their area(s) of expertise.

View the map

Cybersecurity taxonomy

Defining cybersecurity terminologies to ensure harmonisation.

View the definitions

Competence network

Four pilot projects embracing over 160 partners including companies, SMEs, universities and research institutes.

View the network

Figure 14: The Atlas portal

Chapter 5 Summary and Conclusion

The pandemic experienced in 2020 has highlighted the importance of information systems for the development and wellbeing of modern society. The use of these systems has allowed some sectors to develop their activity using telecommunications, but the dependence that society, as a whole, has on digital technologies has also been revealed.

This dependency has been mercilessly exploited by organized groups of cyber attackers, who have put unsustainable pressure on the battered activity of organizations that have seen in digital commerce and telematic resources of collaboration, a tool for their survival, but did not have the knowledge or technology to digitalize themselves in a safe way.

The SPARTA Partnership program is committed to collaboration and teamwork as a fundamental support mechanism for people and organizations in Europe. The focus of the work is to support the European ecosystem, collaborating between 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 the level of security in Europe to the next level.

Through a shared commitment to SPARTA's values, each national cluster of partners has been tasked with identifying and selecting the best candidates to grow the network in an orderly and balanced way. These national groups of partners will oversee coordination and represent the network in events, both at the regional and national level, as well as looking for balance in the public-private weight of the national cluster. Finally, increasing the coverage of the innovation value chain, starting from the universities, passing through the RTOs and ending in organizations that offer services to the end user.

These organizations, linked and committed to the objectives of the Pilot, participate in the common tools and infrastructures as SPARTA Associates, showing in practice the benefits of the federated management of the assets that each organization has contributed separately to the network. Their participation in JCCI links them directly to activities, accessing digital resources made available by partners or other associates.

Based on a demonstration of technical feasibility, in this second year, a set of modules have been made available to the partners that make up a platform for accessing relevant information in the scope of the project, starting with the technological resources that partners provide, and adding those developed throughout the project lifetime in the four technical programs contemplated within SPARTA.

In this second year, a great effort has been made in collaboration and alignment with other Pilots, as well as with the new strategies set by organizations such as ENISA or ECSO in the strategic planning of the security technologies that must be developed in the upcoming years. The year has been strange, including general lockdowns, curfews, and the cancellation of many events, but work has always been done supporting the European and National institutions in the implementation of technical and organizational initiatives with the aim of protecting European society and advance in the achievement of a Digital Strategic Autonomy.

Currently, organizations have learning tools, as well as analysis and experimentation laboratories, but present some deficiencies in terms of training tasks and resources. For the most part, they have not yet been seen as a key enabler to join technological and personal efforts, as well as to introduce more active dynamics of response against cyber-attacks.

For these reasons, the final year of JCCI development will be dedicated to the consolidation and deployment of a distributed network of nodes offering resources. The focus will also be on the location, promotion, and publication of training scenarios, being the purpose to offer varied services and possibilities to the different types of users of the project to the European CCN.

Chapter 6 Appendix – Learning Content Inventory

6.1 Training Contents Inventory

The purpose of this chapter is to provide a template in which to reflect the main characteristics of the candidate assets to be part of the SPARTA Virtual Learning Center.

The information provided will be used as a basis to establish, in the first place, which assets will be part of the SPARTA Virtual Learning Center.

6.1.1 *CEA*

Organization	CEA
Point of contact	Florent Kirchner
Location	Saclay, France
Asset objectives	Learning vectors for software analysis and verification.
Technological Areas of Work	Software security, Software assessment

Online courses

None.

In-person courses

Description	Hours	Level	Public/private	Price	How to attend
Software verification with Frama-C: positioning and usage	22.5	Master	Private	17,000€	On-demand
Introduction to Frama-C	11	Master	Private	8,000€	On-demand
Platform virtualization and UNISIM-VP	45	Master	Private	34,000€	On-demand

Hands-on labs (hackathons, competitions, cyber-range, etc.)

Description	Public/private	Price	Based on which tool	How to obtain access
Frama-C Hackathon	Private	8,000€	Frama-C	On-demand

Knowledge management

None.

6.1.2 *CESNET*

Organization	CESNET
Point of contact	Andrea Kropáčová <andrea@cesnet.cz>
Location	Prague, CZ
Asset objectives	-
Technological Areas of Work	-

Online courses

None.

In-person courses

None.

Hands-on labs (hackathons, competitions, cyber-range, etc.)

Description	Public/private	Price	Based on which tool	How to obtain access
Capture the flag competition on forensic analysis	Public	Free of charge	None	Registration here: www.thecatch.cz

Knowledge management

None.

6.1.3 *INRIA*

Organization	Inria
Point of contact	Frédéric Beck < frederic.beck@inria.fr >
Location	Villers-les-Nancy, France
Asset objectives	-
Technological Areas of Work	-

Online courses

Description	Hours	Level	Public/private	Price	Based on which tool (sharepoint, joomla, etc)
MOOC « Code-Based Cryptography »			Public	Free of charge	https://learninglab.inria.fr/en-mai-sur-fun-le-mooc-code-based-cryptography-session-2/
MOOC “Protection de la vie privée dans le monde numérique”		All	Public	Free of charge	https://www.fun-mooc.fr/courses/course-v1:inria+41015+session03/info https://learninglab.inria.fr/mooc-protection-de-la-vie-privee-dans-le-monde-numerique/

Description	Hours	Level	Public/private	Price	Based on which tool (sharepoint, joomla, etc)
Various other MOOC			Public	Free of charge	https://learninglab.inria.fr/cours/
Class'Code		All	Public	Free of charge	https://project.inria.fr/classcode/

In-person courses

None.

Hands-on labs (hackathons, competitions, cyber-range, etc.)

None.

Knowledge management

None.

6.1.4 *TEC*

Organization	Tecnalia
Point of contact	maite.alvarez@tecnalia.com
Location	Parque Tecnológico de Bizkaia Calle Astondo bidea, Edificio 700 E-48160 Derio - Bizkaia (Spain)
Asset objectives	Training modules
Technological Areas of Work	Cybersecurity and Blockchain

Online courses

None.

In-person courses

Description	Hours	Level	Public /private	Price	How to attend
Training modules on cybersecurity: • General knowledge and good practices in cybersecurity. • Review of cybersecurity technologies applied to the development, deployment and operation of SW/ HW systems (Web, IoT, CPS, …) • General knowledge about cybersecurity in the industrial and business field	20	Elementary	Public	9,000 € (8/10 persons)	Tecnalia /customer premises. Remote

Description	Hours	Level	Public /private	Price	How to attend
• Standards, regulations and regulation in cybersecurity					
General knowledge of tools used in cybersecurity: OSSIM Vault, PKI, Security in Mobiles, Pentesting ...	10	Intermediate	Public	4,500 € (8/10 persons)	Tecnalia /customer premises
Training modules on blockchain for developers: • Introduction to blockchain • General features and deployment in Ethereum, Quorum and Hyperledger • Development in Ethereum and Hyperledger • Interaction of Blockchain and Smart contracts	22	Upper Intermediate	Public	10,500 € (8/10 persons)	Tecnalia /customer premises
Training modules on blockchain for developers: • Ethereum specialist	12	Upper Intermediate		5,400 € (8/10 persons)	Tecnalia / customer premises
Training modules on blockchain for developers: • Hyperledger specialist	12	Upper Intermediate		5,400 € (8/10 persons)	Tecnalia /customer premises

Hands-on labs (hackathons, competitions, cyber-range, etc.)

None.

Knowledge management

None.

6.1.5 *TUM*

Organization	TUM
Point of contact	norouzian@sec.in.tum.de
Location	Boltzmannstraße 3 85748 Garching Germany
Asset objectives	Teaching and learning modules
Technological Areas of Work	IT Security

Online courses

None.

In-person courses

Description	Hours	Level	Public/private	Price	How to attend
Secure mobile systems: Security architectures and protocols for secure wireless and mobile communication technologies (GSM, UMTS, WLAN, Bluetooth) Smart Cards and other security tokens Current uses cases like: security problems of the Myfair Chip, security mechanisms of the German electronic identity card (ePA), and the German electronic health card (eGK) Secure wireless sensor networks: Problems and solutions RFID technology: applications scenarios, security requirements and solutions (e.g. EPCglobal supply chain)	40	intermediate	public	0	Register at TUM registration course system
IT Security: Basic terms, vulnerabilities and attacks, security mechanisms (e.g., cryptography, signature), security models, authentication, smartcards & trusted computing, access and usage control, network security, application-level security, security engineering	60	Elementary	public	0	Register at TUM registration course system

Hands-on labs (hackathons, competitions, cyber-range, etc.)

Description	Public/private	Price	Based on which tool	How to obtain access
Rootkit programming: This Praktikum will allow the students to get a hand on feeling for Linux kernel rootkit programming	Public	0	Linux	TUM Lecturer
Binary Exploitation: This practical course teaches various techniques for exploiting buffer overflow vulnerabilities. Starting with the basics of buffer overflows the students will learn ways of executing shellcode.	Public	0	Linux	TUM Lecturer

Based on this knowledge we will explore protection mechanisms against shellcode execution, and we will work on advanced methods for bypassing them.				

Knowledge management

None.

6.1.6 *UKON*

Organization	University of Konstanz
Point of contact	Eren Ccakmak
Location	Konstanz, Germany
Asset objectives	Visualization for Cyber Security
Technological Areas of Work	Data Analysis and Visualization

Online courses

None.

In-person courses

None.

Hands-on labs (hackathons, competitions, cyber-range, etc.)

Description	Public/ private	Price	Based on which tool	How to obtain access
Vast Challenge	Public	0	Challenge	http://www.vacommunity.org/About+the+VAST+Challenge

Knowledge management

Name	Description	Public/private	Price	Based on which tool
VisSec Papers	A visual overview of all VizSec (IEEE Symposium on Visualization for Cyber Security) papers - see https://vizsec.dbvis.de/	Public	0	-

6.1.7 *INOV*

Organization	INOV
Point of contact	Filipe Apolinário
Location	Lisbon, Portugal
Asset objectives	Incident Detection for cybersecurity monitoring
Technological Areas of Work	Intrusion detection systems

Online courses

Description	Hours	Level	Public/private	Price	Based on which tool (sharepoint, joomla, etc)
Web seminar: Configuration and Operation of BP-IDS	1		Public - Consortium only	Free of charge	Zoom

In-person courses

None.

Hands-on labs (hackathons, competitions, cyber-range, etc.)

None.

Knowledge management

None.

Chapter 7 Appendix – State of the Art for Federated Infrastructures

7.1 Introduction

In our case, we are looking for best practices to connect elements from our future shared JCCI workbench. For that end, it is necessary to have a common index, allow federated authentication/authorization mechanisms and digital identity, as well as having a shared infrastructure among the organizations.

The subsections of this chapter will go through the state of the art and best practices regarding these matters and the different approaches will be overviewed, to help reach a decision on the final solution to be used when connecting workbenches and resources in a federated way.

7.2 Authentication and authorization

Authentication ensures that an identity of a subject (user or smart object) is valid, i.e., that the subject is indeed who or what s/he/it claims to be. It allows binding an identity to a subject. The authentication can be performed based on something the subject knows (e.g., password), something the subject possesses (e.g., smart cards, security token) or something the subject is (e.g., fingerprint or retinal pattern). An authentication component enables authenticating users and smart objects based on the provided credentials. The credential can be in form of login/password, shared key, or digital certificate. As a result of the authentication process, an assertion is generated to be used afterwards, in order to declare that a specific subject was authenticated successfully by the Issuing authority.

Once authenticated, **authorization** defines the set of actions that the identity can perform after gaining access to a specific part of the infrastructure.

Authentication and authorization can happen in web environments or non-web environments, and each has its advantages and disadvantages.

7.2.1 *Non-web*

Kerberos

Kerberos is a computer-network (non-web) authentication protocol that works based on tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner[58]. It is open source, and it uses the AES encryption protocol. It requires a trusted third party and the server and user have a mutual authentication.

The different entities that take part in Kerberos are the client/user, the application server (AS) who offers the service, and the Key Distribution Center (KDC) who issues the mentioned tickets. Kerberos makes Single Sign-on (SSO) more usable because the client/user proves their identity once, and then it passes the ticket granting ticket (TGT) to others as proof of their identity.

7.2.1.1 Kerberos advantages:

- Every authenticated domain entity can request tickets from its local Kerberos KDC to access other domain resources. Due to its ticketing system (they are considered access permits and

[58] https://en.wikipedia.org/wiki/Kerberos_(protocol)

they can be used more than once, cached on the client side), Kerberos does not need pass-through authentication.

- It supports mutual authentication. The client authenticates to the service and the service authenticates to the client.
- It is an open standard.
- It has support for authentication delegation, that is, the service can access remote resources on behalf of the user.

7.2.1.2 Kerberos disadvantages:

- There is a single point of failure, as it requires continuous availability of the central server.
- There are strict time requirements because the clocks of the hosts must be synchronized.
- The administration protocol is not standardized.
- Impersonation can be attained by compromising the KDC.
- Users cannot connect to unknown or untrusted clients.
- Attacks can be performed: pass-the-ticket, golden ticket, silver ticket, credential stuffing and brute force, encryption downgrade (if there is admin access) and DCShadow attack.

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a non-web networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service. It is a client/server model and runs on the application layer. It uses UDP port 1812 for authentication and 1813 for accounting. It is often used by Internet service providers (ISPs) and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services due to it being ubiquitous and having broad support. It is based on an IEEE standard for authenticated network access to wired Ethernet networks and wireless 802.11 networks.

Regarding authentication and authorization, the user or machine sends a request to a Network Access Server (NAS) to gain access to a network resource using access credentials and these are passed to the NAS device via the link-layer protocol. Then, the NAS sends a RADIUS Access Request message to the RADIUS server, requesting authorization to grant access via the RADIUS protocol.

This request includes access credentials, typically in the form of username and password or security certificate provided by the user. Additionally, the request may contain other information which the NAS knows about the user and information regarding the user's physical point of attachment to the NAS.

Then, the RADIUS server checks that the information is correct using authentication schemes. The user's proof of identification is verified, along with, optionally, other information related to the request, such as the user's network address or phone number, account status, and specific network service access privileges. RADIUS servers can either check the user’s information against a locally stored flat file database, or can refer to external sources—commonly SQL, Kerberos, LDAP, or Active Directory servers—to verify the user's credentials.

7.2.1.3 RADIUS advantages:

- Enhanced security, if implemented correctly.
- Restrictions on specific classes of users (user groups can be directed into a User Profile based on LDAP membership and/or RADIUS attributes.
- Reporting and tracking based on client usernames.
- Individual sessions with a service set identifier (SSID) using RADIUS are encrypted uniquely between the user and access point.
- A single user or device can be de-authorized easily by disconnecting them, without having to change the key for everyone.

- VLAN, firewall policy and other network permissions can be assigned within a user profile having a pre-shared key. Different permissions can be assigned based on attributes returned from the RADIUS server.

7.2.1.4 RADIUS disadvantages:

- It is traditionally implemented on-premises, and maintenance can be difficult and time-consuming for this type of hardware.
- Initial setup is difficult. Complex configuration process due to the wide range of different protocols and compatibility issues.
- Susceptible to eavesdropping attacks. It uses UDP between the NAS and the authentication server, so the only encrypted part between the two is the password. All the rest is sent in clear text.

7.2.2 *Web*

Regarding SPARTA's JCCI, we need to connect workbenches across organizations in Europe. There exist several ways to federate workbenches, by managing the identity and different types of access and authorization from the organizations. This subsection will focus on identity management federation.

Over the past several years, web applications have evolved from simple content delivery applications into sophisticated productivity tools and a mechanism for application integration within and across organizations. This has also allowed for making it possible to federate different organization's assets to share resources and computing power. The matters of importance here are:

- Should there be only one IdP managing all the identities, or a trust relationship between different IdPs?
- Organizations need a way to securely find the right workbench asset of another organization, and the workbench providers need to securely identify the requestors and authorize whatever is needed.
- We need a standard way for allowing organizations to directly provide services for others. Within a federation of services, an organization can get trusted information about a user from the user's home organization (or information-providing service). The organization does not need to register and maintain that user's identity, and the user is spared from having to get and remember a new login in order to interact with the workbench.
- We need cross-organization trust in a standardized way.
- We need a federated identity and attribute mapping: mechanisms and procedures for mapping trusted information about an external user (e.g., users from partner organizations) into authentication and authorization information usable by an organization's existing services.
- We need to enable secure and reliable transactions: A standard way to exchange messages in a secured, reliable, and traceable context.

WS-federation

WS-Federation defines mechanisms for allowing different security realms (security domains) to broker information on identities, their attributes and authentication. It gives a Federated Identity architecture with a separation between trust mechanisms, security token formats, and the protocol for obtaining those tokens. This architecture enables a reusable security token service model and protocol to address the identity requirements of both web applications and web services in a variety of trust relationships [1].

In this context, a federation is a collection of realms that have established relationships for securely sharing resources. A Resource Provider in one realm can provide authorized access to a resource it manages based on claims about an identity (or other distinguishing attributes) that are asserted by an Identity Provider (or any Security Token Service) in another realm.

A Relying Party can use an established context to grant/deny access to a resource. Establishing a federation context when Identity and Resource Providers operate in different realms requires agreement between these parties on what claims are required and on mechanisms for securely transporting those claims over unprotected networks. This provides the basis for interoperability.

A variety of Federation Services (e.g., Authentication, Authorization, Attribute and Pseudonym Services) can be developed as variations of the base Security Token Service from WS-trust. Managing, discovering, and accessing such services are dramatically simplified when they are all based on a common processing model and speak the same base protocols.

The features of WS-Federation can be used directly by SOAP clients and web services. WS-Federation also defines syntax for expressing the WS-Trust protocol and WS-Federation extensions in a browser-based environment. That way, a common model for performing Federated Identity operations for both web services and browser-based applications can be provided.

WS-Security, WS-Trust, and WS-SecurityPolicy provide a basic model for federation between Identity Providers and Relying Parties. These specifications define mechanisms for codifying claims (assertions) about a requestor as security tokens which can be used to protect and authorize web services requests in accordance with policy. WS-Federation extends this foundation by describing how the claim transformation model inherent in security token exchanges can enable richer trust relationships and advanced federation of services. This enables high value scenarios where authorized access to resources managed in one realm can be provided to security principals whose identities and attributes are managed in other realms. WS-Federation includes mechanisms (extensions to the Security Token Service model) for brokering of identity, attribute discovery and retrieval, authentication and authorization claims between federation partners, and protecting the privacy of these claims across organizational boundaries. Moreover, these mechanisms are mapped onto HTTP to leverage WS-federation with web browsers.

Security Token Services can broker the establishment of a trust relationship between a Resource Provider and other service providers (Identity Providers for example), that are prepared to vouch for the identity, pseudonyms, or other attributes which they have associated with a specific principal. In order for a security token from an Identity Provider realm to be useful in a Relying Party realm, the following items are required:

- Trust relationship between the realms.
- Agreement upon the syntax and semantics of security tokens.
- Endpoints for obtaining policy requirements and requesting security tokens.

WS-Federation does not restrict users to a specific security token format. Instead, WS-Federation builds on the WS-Trust encapsulation mechanism, the RST/RSTR, which allows protocol processing to remain agnostic of the type of token being transmitted. This enhances the interoperability.

OpenID

OpenID Connect (OIDC) is a group of lightweight specifications that afford a framework for transmitting digital identity via RESTful APIs. OpenID Connect is seen as the evolution of OpenID 2.0, and is built as a profile of OAuth 2.0 rather than a completely distinct protocol foundation. It is just another identity layer on the top of the OAuth 2.0 protocol. It facilitates clients to confirm the identity of the user depending on the authentication made by an Authorization Server, in addition to acquire simple profile information about the user.

It uses two main types of tokens: an access token and an ID token. The ID contains information about the authenticated user, and it is a JWT (JSON Web Token). This token is signed by the identity provider and can be read and verified without accessing the identity provider.

OIDC assumes five key roles in any authentication and authorization process: End User, Relying Party (RP), Authorization Endpoint (AE), Token Endpoint (TE) and User-Info Endpoint (UIE):

- End User: user of the application and owner of the information.
- Relying Party (RP): application which makes API request to get protected resources on behalf of the end user.
- Authorization Endpoint (AE): only endpoint where the end-user needs to interact if they are not already logged in. It validates the identity of the end-user and obtains the consent and authorization from the end-user if the client has not been pre-authorized. It returns an authorization grant to the end-user or client depending on the use case. Sometimes, this authorization grant can then be passed in a request by the client to the token endpoint in exchange for an ID token, access token, and refresh token.
- Token Endpoint (TE): handles requests for retrieving and refreshing access tokens, ID tokens, refresh tokens, and other variables. It accepts a request from the client that includes an authorization code that is issued to the client by the authorization endpoint directly or via end user. When the authorization code is validated, the appropriate tokens are returned in response to the client.
- User Info Endpoint (UIE): OAuth 2.0 protected resource that the client application can retrieve consented claims, or assertions, about the authenticated end user. The client should present a valid access token to retrieve only those User Info claims that are scoped by the presented token.

OpenID also offers some flexibility in the implementation; however, it standardized many parameters such as instance scopes, endpoint discovery, and dynamic registration of clients, which were left up to implementers in the OAuth 2.0 implementation.

7.2.2.1 OpenID advantages:

- Time and effort savings of developing and maintaining a log-in system, along with corresponding error-handling and security checks.
- It is open source.
- It is single sign-on. Moves trust from multiple parties to only one.
- Delegation.

7.2.2.2 OpenID disadvantages:

- Privacy: the OpenID provider can track the user's habits by all the authentication requests.
- Many cases of OpenID providers move the password in clear text.

SAML

Security Assertion Markup Language (SAML) [9] defines a standard for facilitating AA information between an identity provider and a service provider via a principal (a user/subject). The standard includes:

- Specification of assertion content, the assertion is an XML containing identification of a principal, info about the principal, information about the identity provider, etc.
- SAML protocol schema
- Protocol bindings (e.g., HTTP)
- Profiles (rules describing how to embed SAML assertion into a given protocol)
- Definition of extensible metadata format - to support agreements among entities (e.g., SSO Identity provider) regarding identifiers, binding support and endpoints, certificates, keys, etc. in a standardized way.
- Authentication context schemas.
- Conformance requirements with SAML (mandatory and optional features).

SAML primarily focuses on web based SSO. The principal requests a service (to access a web) from the service provider. The service provider responds with a SAML request and the principal with the

SAML request is redirected to the identity provider. The identity provider authenticates the principal (any authentication mechanism may be used between the principal and the identity provider, i.e., SAML does not define it), processes the SAML request and responds with its SAML response (SAML assertion about the principal). The principal sends the SAML response to the service provider who validates it and grants the principal the access to the service.

7.2.2.3 SAML advantages

- Open-source project Shibboleth.
- Large working instances such as eduGAIN.
- Supports federations, there can be multiple services and multiple identity providers.
- Since the identity provider does not communicate with the service provider directly, there is a possibility to prevent tracking of what services are being accessed by the identity provider.

7.2.2.4 SAML disadvantages

- Web-based only
- Not a leading edge

OAuth2

OAuth is a scalable delegation protocol (i.e., the user delegates someone to do something with somebody on his/her behalf). OAuth allows a user to permit access to an application to accomplish authorized tasks on behalf of the him/her [2]. Therefore, it allows a third-party program to gain restricted access to an HTTP service. This API authorization process can be securely implemented by a range of desktop, web, and mobile applications. It introduces the concept of an authorization token that states the right of the client application to access authorized services on the server. Access to authorized services on the server is controlled using an authorization token. Nonetheless, it does not override any access control decisions that the server-side program may make.

OAuth assumes four key roles in any authorization process: Resource Server (RS), Resource Owner (RO)/User, OAuth Consumer/Client (OC) and Authorization Server (AS):

- Resource Server (RS): hosts user data that is protected by OAuth.
- Resource Owner (RO)/User: user of the application and owner of data.
- OAuth Consumer/Client (OC): application which makes an API request to get protected resources on behalf of the resource owner.
- Authorization Server (AS): authorizes the consumer after getting permission from resource owner and issues access token to the consumer for accessing protected resources available on the resource server.

OAuth offers the flexibility and leaves it up to server implementers to decide how the actual authentication and authorization are to be done.

7.2.2.5 OAuth2 advantages:

- Flexible protocol that relies on SSL to save user access tokens.
- Allows limited access to the user's data.
- Authorization tokens expire.
- Convenient for different applications within the same organization: the user can log in in one application with user and password (the OAuth 2.0 based service provider), and in all the other applications the user is simply redirected to the provider and confirms that he/she wants to be authorized (tokens are stored instead of passwords).
- Access tokens can be invalidated if there is any issue.

7.2.2.6 OAuth2 disadvantages:

- Depends on the central hub.
- Can be easily attacked if not configured properly.

- There are extension points in the specification that complicate the implementation for interoperability.
- The specification does not require SSL/TLS, so it is up to the developer to implement it instead of by default.

7.3 Shared infrastructure

The main goal of the JCCI is to share a workbench with computing resources, and that requires a secure and efficient way of connecting the partaking organizations. There exist various approaches, differing mainly in cost and performance, that will be described in the upcoming subsections.

7.3.1 *Site-to-Site VPN*

A site-to-site (S2S) VPN allows organizations in multiple fixed locations to establish secure connections with each other over a public network (e.g., the internet). S2S VPN extends the organization's network, making computer resources from one location available to partners at other locations. In sum, it is connecting two or more LANs in different locations. It is generally enabled through a VPN gateway device. The main setback from using them is the cost of creation and maintenance, and most companies that use them have the service set up by specialized business security solutions companies. There are two types of S2S VPNs: intranet-based and extranet-based.

- **Intranet-based** S2S VPNs are appropriate to be used within one organization that has offices in different locations, so that each separate LAN can be connected to a single WAN. This allows for making computer resources at one location available to employees at other locations.
- **Extranet-based** S2S VPNs are appropriate to be used when an organization has a close relationship with another. This way, the VPN can connect the organizations' LANs in a way that the partners can work in a secure, shared network environment while preventing access to their separate intranets.

Moreover, there are three techniques to establish a S2S VPN:

- **Internet VPN method**: it uses the organization's existing network, together with the public internet infrastructure. For that, a VPN gateway is needed at both sites to encapsulate and encrypt all outbound data traffic from one site and send it through a VPN tunnel over the internet to a peer VPN gateway on the other site. Upon reception, the peer VPN decrypts the content and relays the data onto the second organization's LAN.
- **MPLS (Multiprotocol Label Switching) VPN method**: the VPN connection is established by connecting to a carrier-provided MPLS cloud instead of to public internet. Thus, the infrastructure belongs to the VPN provider and not the organization using it. To configure it, a provider creates virtual connections between the client organization's sites across the MPLS network. It sends data and network traffic along the most efficient routes, which may be predetermined and are communicated using labels. Packets are carried on predetermined routes along point-to-point connections through label switch routers (LSRs) until they arrive at their destination. Its main advantage is ease of deployment and optimal network performance, while its disadvantage is the cost (particularly for international connections).
- **VPLS (Virtual Private LAN Service) VPN method**: it uses MPLS and VPN to securely connect multiple LANs over the Internet, making them appear as if they were all on the same LAN. VPLS enables a service provider to extend a Layer 2 network across geographically dispersed sites using a shared core network infrastructure. VPLS works by creating a virtualized Ethernet switch at the provider's edge to link remote sites. VPLS sits at Layer 2, and the carrier builds out the network, but the customer can do their own routing if they wish. This approach is convenient for corporations that have multiple data center footprints and office or remote locations that require low-latency connections between sites.

7.3.2 *Remote-access VPN*

A simpler and cheaper approach for connecting organizations is using remote-access VPN, that is, connecting individual computers to a LAN. To set it up, each device must have VPN client software installed, or the user must have access to a web-based VPN client. Whenever the device sends data, the VPN client software encapsulates and encrypts that traffic, and then sends it over the internet to the VPN gateway for the organization's LAN. When the VPN gateway receives the encrypted transmission, it decrypts and relays the traffic onto the organization LAN, like the site-to-site VPN gateway.

This solution can be appropriate if the number of users using the VPN is small, as it involves speed and network performance compromises.

7.3.3 *SD-WAN VPN*

SD-WAN (software-defined wide area network) is an alternative technology that is more dynamic than remote-access VPN. It simplifies the management and operation of a WAN by separating the networking hardware from its software. This solution stemmed from most business applications being nowadays hosted in the cloud, and WANs struggling to keep up with the amount of data being transmitted.

A good implementation of a SD-WAN VPN combines the cost benefits of internet-based S2S VPNs with the performance and agility of MPLS VPNs. With it, organizations can replace some of their high-priced MPLS circuits with economical internet connections. The optimization and multi-path capabilities of an SD-WAN ensure performance stays high enough for each location's workload. Moreover, SD-WAN products can be physical appliances or virtual appliances.

7.4 References

[1] M. Hondo, A. Nadalin, and M. Mcintosh, "Understanding WS-Federation," pp. 1–49, 2007.

[2] I. E. T. F. (IETF), "OAuth." [Online]. Available: https://oauth.net/.

[3] Internet Engineering Task Force (IETF), "The OAuth 2.0 Authorization Framework," 2012. [Online]. Available: https://tools.ietf.org/html/rfc6749.

[4] Gemalto, "Digital identity - 5 forces that shape 2019-2020," 2019. [Online]. Available: https://www.gemalto.com/govt/identity/digital-identity-services/trends.

[5] Sovrin Foundation, "Sovrin™: A Protocol and Token for Self- Sovereign Identity and Decentralized Trust," *Whitepaper*, no. January, pp. 1–41, 2018.

[6] V. C. W. G. Charter, "W3C," 2017. [Online]. Available: https://www.w3.org/2017/vc/charter.html.

[7] M. Team, "Introduction to Self-Sovereign Identity and Its 10 Guiding Principles," 2019.

[8] Microsoft, "Decentralized Identity," 2018.

[9] "SAML Specifications" [Online]. Available: http://saml.xml.org/saml-specifications

Chapter 8 Appendix – Description of Potential Cyberrange Scenarios

8.1 Introduction

Many organisations are unable to forecast and/or estimate the impacts of a cyber-risk. This often results in insufficient and/or irrelevant investments to ensure a more secure cyber environment. Moreover, in this environment, the human factor is underestimated although statistics show it is frequently the weakest asset.

New technologies and their novel combinations require innovative ways to implement security measures and to make new security-related assumptions and managing cyber risks. Cybersecurity experts and professionals need to continuously adapt their expertise to a constantly evolving landscape with increasingly sophisticated and novel cyber-attacks, a widening surface of exposed ICT systems and services and a set of relevant changing legislation. Moreover, the threats related to industrial networks and operation technologies (OT) have surpassed widely the number of vulnerabilities found in internet technologies (IT), requiring high velocity in the identification and mitigation of "zero-day" or potential unknown vulnerabilities, forecasting new threats (plus their cascading effects) and emerging attacks.

In order to provide a realistic training environment and to practice the entire chain of cyber defence, an introduction about the Cyber Range architecture is given. Then, a set of War Game strategies are presented.

8.2 Cyber Range Architecture

A cyber range is a virtual environment that companies can use for training/testing, evaluation, and simulation experiments [18]. In fact, this platform allows to evaluate concrete assets by stressing them; simulate behaviours of malwares or infections in a global network system analysing their diffusion rate and their global effects, and train experts' skills to defence network infrastructures and detect product vulnerabilities.

The users of a Cyber Range can be divided in at least three groups [19]: white team, blue team, and red team. In standard definition, white teams are extremely important, they are in charge to implement and launches cyberattack scenarios defining the objective of the training. Furthermore, they can monitor the traffic, the success or failure of the blue team in terms of incident handling and scenario response. Red teams and blue teams represent, respectively, attacker and defender of the network. In fact, meanwhile the red teams act as malicious user in order to compromise the server/network, the blue teams have the task to apply countermeasures like network operations centre.

Most of the Cyber Ranges use either emulation or simulation.

- **Emulation**: Cyber Ranges map desired experimental network topology and software configuration onto the physical infrastructure. The main advantages of emulating Cyber Ranges are the ability to create a representative environment for training and testing, and the ability to perform high fidelity and repeatable experiments. However, a disadvantage is their high cost due to the large infrastructure requirements. This cost can be reduced through virtualisation or resource sharing.

- **Simulation**: Cyber Ranges make use of software models of real-world objects. This allows large simulations to be run on relatively modest hardware. In this sense, simulation Cyber Ranges are highly scalable, flexible, and low cost. Their main disadvantage is that it is hard to verify their reflection of reality accurately [2].

In this document, a taxonomy regarding different types of scenarios that can be easily deployed in a Cyber Range architecture is presented. These scenarios, also known as War Games, represent cybersecurity challenges in which players must compete to reach a fixed goal. In computer security, several wargames are developed and implemented, and in this document, we present four classes of them. Each class can include difference War Games joined by their common aim. After a brief introduction and a description of the chosen class strategies, real-world use cases where such strategies can be applied are drawn.

8.3 War Games strategies

War Game, is a strategy game, often used in military operations, for simulating warfare, training the troops, and evaluating the response capabilities. This game allows to analyse the dynamic decision of the humans and allows to appreciate the consequences of their choices [5].

Over the years, with the increase of the information technology and the digitalization of the industry processes, the need to have cybersecurity experts able to react and mitigate any kind of predictable situations has arosen. In this scenario, the implementation of cyber wargames (or cybersecurity exercises CSXs) was chosen to evaluate companies' capabilities to respond to a range of cyber incidents, thereby helping them to improve their resilience when inevitable cyber-attacks occur [5].

The War Game implementation starts from the analysis of a real-world situation, and its implementation in a controlled environment. This operation aims to identify what is going on in the business context, who the adversary is, what assets are targeted, and what the purpose is. This way, it is possible to define a scenario as much as possible similar to the real one once it is defined and the problems to address are detected, the War Game can start. These games represent perfect tools for teaching offensive and defensive cybersecurity techniques, and they allow users to test themselves and their knowledge considering different scenarios.

In this document four strategies/classes of War Games are presented, in which several scenarios are joined by their final goal. In particular, we consider Capture the Flag (CTF), King of the Hill (KotH), Last Man Standing (LMS) and the Locked Shield strategies.

8.3.1 *Capture the Flag (CTF)*

Capture-the-Flag is a kind of information security competition that challenges contestants to solve a variety of tasks to get a fixed item called flag. This flag often represents a piece of text that may be hidden on the server or behind a webpage. The CTF setup introduces the concept of a flag to monitor the status of each participant. In fact, the goal is to provide objective measure of proficiency, and a guided exercise needed to evaluate the performance of trainees.

The first cyber security CTF was developed (and hosted) in 1996 at DEFCON[59] in Las Vegas, Nevada. DEFCON is the largest cybersecurity conference in the United States. Since then, CTF competitions have become popular and global, and are now the most used strategy for implementing cybersecurity exercises. In [4], a description of a DEFCON CTF implemented in 2003 is presented.

[59] https://www.defcon.org/

In several research, the Capture the Flag strategy is used for testing frameworks functionalities and planning new approach. In [7] it is used for deploying and testing a toolkit for designing an action hierarchy and in [8] the games is studied and resolved as a zero-sum differential game. In [10] a learning system based on CTF is implemented to educate the students to act like crackers and find new vulnerabilities in existing systems (data, files, devices, …).

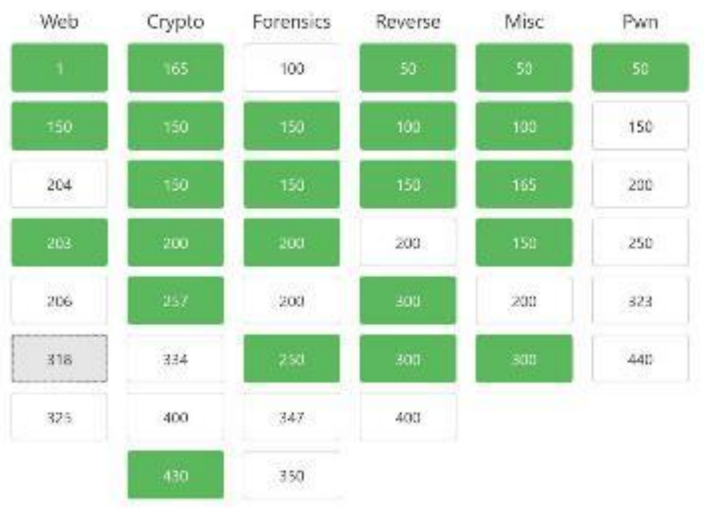
Usually, the CTFs are divided into two formats: ***Attack/Defend*** and ***Jeopardy-style,*** however in this deliverable, to clarify some implementation aspects, we specify two more categories: ***Attack/Defend individually*** and ***Treasure Hunt***. The presented division is performed by analysing the goals, architecture, and limitations of the challenges.

Attack/Defend: this format is an *interactive* competition game that involve at least two teams; each one equipped with identical machines with the same vulnerable services. The main goal is to defend its own flag (text files, folders, archive, etc.), while trying to conquer (or corrupt) the flags of as many of the other teams [3]. In this scenario, teams need to identify their vulnerabilities, patch them without breaking the service's functionality, make sure all passwords are strong, checking the user privilege, and all the allowed operations for increasing the security of their system. At the same time, they must exploit the acquired knowledge to attack and penetrate to the other machines and get the other flags. If there is any rule violation, the team could incur in a penalty or could be disqualified. In [9] an implementation of interactive teaching techniques based on Attack/Defend strategy is described, as in [15] where the experiences of ten years in running CTF are joined to create a unique framework.

Attack/Defend singularly: this format is a variation of the Attack/Defend strategy. Nevertheless, in this case, the challenge starts by dividing participants exactly into two teams: attacker team (red) and defender team (blue), and the flag (text files, folders, archive, etc.), is assigned just to the blue team. The task of the read team is to detect and exploit blues' vulnerabilities to conquer the flag. On the other hand, the blue team must resist and mitigate the reds' attacks applying countermeasures. In this scenario, when the clock runs out, the final result will be getting the flag (red wins) or retaining the flag (blue win). Usually, two rounds are planned in which the two teams switch their "colours" and their attack/defend roles. If there is any rule violation, the team could incur in a penalty or could be disqualified. In [13] a training system that implement several attack and defence scenarios is presented. Such system is used to train students divided into two teams with separate attack/defence tasks.

Jeopardy-style: this format is a *challenge-based* competition like the actual Jeopardy game with different categories and point values. This scenario is one of the most common, very easy to setup and deploy since it does not provide a competition for the same resources. In fact, the game consists in earning as many points as possible before the clock runs out. More than two teams can be involved, and each one starts by choosing a challenge from the board. When they find the solution of the chosen challenge (find the required flag), they submit it to the scoring system for the evaluation. If the answer is correct the score of the team is updated and the system allows the team to move on the next challenge in the board, otherwise they keep going to resolve the challenge. The team with the highest score in the end wins. In the Jeopardy-style, in each round, the participants can choose freely the task to deal with. Nevertheless, if this decision is restricted, the participants must address one particular challenge in order to unlock and earn the access to the next one. The format took the name of **Treasure Hunt**. In [14] a training system based on Treasure Hunt is presented, meanwhile in [11] a Jeopardy-style strategy is used for creating realistic scenarios and teaching high school students cybersecurity's notions. The good results presented in [17], where a CTF Jeopardy framework is implemented, has led the authors to create an online platform called PicoCTF[60].

[60] https://picoctf.com/



Web	Crypto	Forensics	Reverse	Misc	Pwn
1	165	100	50	50	50
150	150	150	100	100	150
204	150	150	150	165	200
203	200	200	200	150	250
206	257	200	300	200	323
318	334	250	300	300	440
325	400	347	400		
	430	350			

Figure 15: Example of CTF Jeopardy-style board

In Figure 15 can be seen that usually the challenges in the Jeopardy-style are divided into categories and ordered by the degree of difficulty. In this deliverable we propose several common categories (only a small selection):

- *Web*: finding and exploiting the vulnerabilities in web application (or find the hidden flag).
- *Cryptography (Crypto)*: decrypting or encrypting a piece of data.
- *Forensics*: data analysis and investigation, like a packet analysis on .pcap file, memory dump analysis, etc.
- *Reverse*: reverse engineering or exploiting a binary file.
- *Miscellaneous (Misc)*: miscellaneous challenges relevant to Information Security.
- *Pwn*: exploiting a server to find the flag.
-

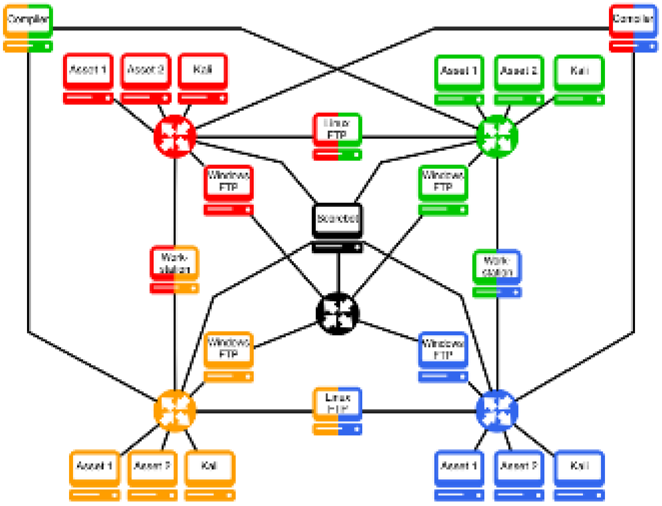
8.3.2 *King of the Hill (KotH)*

Although in several works the King-of-the-Hill strategy is considered a variation of the attack-defend CTF, in this document we consider it as a standalone, separated War Game strategy. This is because, considering the goal of each strategy, we want to remark the difference between the CTF and KotH. In fact, while in the CTF (and its subversions) the aim is to conquer a flag, in KotH the main goal is to prove the capability to impersonate as users, or more generally, to execute processes in the target device. In this document, we divide the strategy into two formats according to the initial architecture: ***SafeHole KotH*** and ***NoHole KotH***.

In both, participants are divided into teams, and their objective is to take the control off of as many possible servers as available in the training field. Nevertheless, in **SafeHole** format the initial machine given to the participant can be considered as a safe space, i.e., it is not in the battlefield, meanwhile in **NoHole** format the initial resource belong to the battlefield and so it is possible that the user is kicked out from the CDX.

Although the scoring is calculated differently, in both formats when the clock runs out, the team that has the highest number of resources wins the competition. In this scenario, members of a team have to work together for attacking, controlling and defending as many servers on the training field as possible. In fact, when teams take control of a machine, they also take on the responsibility of running its critical services and defending it against other teams [4]. This challenge allows to know and exploit strength and weakness of each team, increasing the communication among teammates.

Teams earn points keeping critical services up-and-running on the machines they control. The training field can be populated with any kind of resources, from isolated virtual environment, including vulnerable Linux and Windows virtual machines of various builds, embedded systems, industrial systems etc. all spread across multiple partially interconnected subnet, pushing the teams to use pivoting techniques. Usually, a scorebot is available in the network that scans all the critical ports of all the machines in the network map, and awards points to the team who has claimed each service or machine.



8.3.3 *Last Man Standing (LMS):*

This CSX is inspired by a game mode very popular in many shooter and real-time strategy (RTS) videogame, in each of which is named differently, but the aim is clearly the same: be the last man standing. In this document we present two formats of this strategy easily applicable to War Games: ***Classic*** and ***Infection***.

Classic LMS: This format recalls some concept described in the survival mode of the game Alien vs Predator (AvP), in which the players are marines with the aim to fight against a never-ending wave of Alien controlled by the system. Each wave represents a new level of the game, passing the level means increase the complexity of the scenario, in fact more numeric and stronger hordes of Alien appear. Furthermore, the weapons are also conditioned by the game level. The game ends only when all marine players have been killed. These guidelines can be used to implement a new War Game strategy named classic LMS. The CSX starts by assigning the same resources to each participant, which have the aim to defend them against a batch of cyberattacks executed by the controller (or an external team). The challenge is divided in levels, in each of which the degree of difficulty and the complexity of the scenarios increases. In fact, in each level a new sophisticated attack is executed and less permissions are given to the participants. The last participant that remains in control of its machine is the winner closing the challenge. This CSX is suited for training and testing the defensive skills of the cybersecurity experts. A similar strategy is used during the National Collegiate Cyber Defense Competition CCDC[61], where participant teams are asked to

[61] https://www.nationalccdc.org/

manage an existing network (each one with identical set of hardware and software) and to mitigate “external threat” provided by a volunteer red team. Each defender decision is evaluated by a scoring engine that determine the points.

Infection LMS: Also, this format is based on a game mode available in the Alien vs Predator game and called Infestation. In this mode, one player among others starts the match as Alien and all the rest starts as marine (the selection is made randomly). The Alien player must hunt and kill the marines, and when it happens the killed marines reborn as Aliens. The game ends when everyone has been killed and turned into one of the Alien hives. Following the AvP Infestation rules, it is possible to define a new War Game strategy. This new format, called Infection LMS, starts by assigning the same resources to each participant and select one of them to be the attacker (red team) while all the others represent the defender team (blue). If the attacker obtains the access to one blue resource, the machine is considered infected and the owner (participant) is converted into an attacker. The scores are computed analysing the number of conquered resources and the applied countermeasures. The game ends when the attacker has infected all the blue team or when the clock runs out.

8.3.4 *Locked Shields*

Locked Shields challenges arise from the need of having a timely response to cybersecurity threat in critical infrastructures. In fact, in modern era, more and more societies depend on a set of critical infrastructures (automotive, energy supply, etc.) exposed to cyberattack due to digitalization of the processes. In this kind of scenario, it is essential to have cybersecurity experts trained to react as fast as possible in order to mitigate attacks and protect their assets. This strategy is promoted by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) [12], that every year sets up a real-world scenario inviting over 1,000 cyber experts to participate. This event is considered the world’s largest and most advanced international network defence exercise.

The Locked Shields exercise involve two teams: an attacker team (red) and a defender team (blue). The aim of this second group is to quickly respond to, resist to and mitigate the reds’ attacks which target everything from communication networks to infrastructure. The design of this strategy is particularly suited for the defender team, in which the participant learns how to manage the realistic cyber incidents. The blue team needs to practice and improve important skills such as teamwork for handling external pressure. In fact, in this scenario communication and coordination among teammates is essential. Furthermore, in the case deployed by the CCDCOE, the red ream contains experts from various private firms that support the exercise, like Siemens AG and Cisco, allowing these companies to improve their own services and systems. In [13] an exercise using the Locked Shield strategy is implemented to validate a new feedback tool, meanwhile in [18] a dataset extracted from the real Locked Shields organized by the CCDCOE is used to evaluate team learning utilizing natural language processing methods.

We propose to use this strategy to train and improve the information available for the white team (organizer/controller). In particular, the ability to collect CDX information about the dynamics in the Locked Shield among the red team and blue team, could be used to increase the expertise of the controller.

8.4 Limitation

War Games represent an excellent way to test the skills of the cybersecurity expert and to training them using real-world scenarios. These challenges can be also used to improve the knowledge about novel threats and the routine to be followed to timely mitigate cyber-attacks effects. Nevertheless, also War Games implementations present some limitations:

- Since they are deployed in a controlled environment, they cannot mimic perfectly real-life incidents. In fact, some actions, situations and events may be quite different. For the same reason, is difficult to calculate and demonstrate the real system overload, since production system are (of course) not involved in the simulation.
- Not all the threats and malware available on the real-world can be tested or addressed, such as nation-state-sponsored military or terrorist level capabilities not commonly available through malware marketplaces.
- It Is not possible to fully evaluate the ability of the participants to react to unexpected situations that could happen during a crisis, emergency, or security warfare. Particularly it is difficult to preview cascading effects that happens in the real world (see de CoVid-19 case).

8.5 War Games proposal scenarios

In this section, several potential examples of scenarios that can be deployed in the Vicomtech JCCI asset, part of Basque Digital Innovation Hub (BDIH), are presented. These descriptions represent suggestions and guidelines in order to draw and implement the CDXs exploiting the laboratories of the involved partners.

Each War Game scenario drawn and described follow the specifications presented in Table 1.

#	STEP	DESCRIPTION
1	Strategy	Indicate the War Game strategy among those presented in this document
2	Objectives	Describe the goals of the scenario (Attacks vulnerability, Recovery file, Corrupt DB, etc.)
3	Tasks and Phases	Describe the phase in which the scenario is divided; each phase can be composed by several task to be addressed
4	Architecture	Describe the architecture of the scenario, and how the different resources (hosts, networks, embedded systems, etc.) are connected.
5	Software and Hardware	Describe the different resources Hardware and Software that are involved in the scenario
6	Parameters	Define the variable parts of the scenario (user passwords, IP addresses, etc.)
7	Scoring	Define the scoring rules used for determining the winner

Table 1: Specifications for a War Game Scenario

List of possible scenarios:

- **Scenario 1.** This scenario is drawn as a *CTF Jeopardy-style* with challenges suited to run into a supercomputer (High-Performance Computing or HPC). A board with different tasks regarding cryptography and forensics operations will be implemented to test the knowledge and skills of the participants. In the first phase, the participants must analyse a .pcap file to find some breadcrumb that can help to find the flags for addressing several board challenges. In the second phase, the flags are hidden into ciphered files, each one encrypted with a different key (using dictionary, short random characters, mix of both, etc.). The participants are called to apply different decryption techniques as dictionary attack, brute force, rainbow table, etc. and earn the solutions. For each correct answer (flag), participants receive a pre-determined score, and at the end, who has reached the major total score will be the winner. For this scenario, several decryption software and algorithms are requested like John the Reaper, Hash tables, etc. An important feature is represented by the key size, in fact its maximum will be fixed. A different scenario based only on the cryptography can be planned to use the *CTF Attack/Defend* strategy.

- This **Scenario 2** is composed by a training field with several encrypted data (text file, image, video, etc.) in which known flags are hidden. The aim of the participants is not only to use different decryption techniques to get the hidden flags and reclaim the property of the data (as in the Scenario 1), but also, once the ownership is owned, they must defend the flags by changing its encryption key or even encryption technique. When time runs out (120 minutes), the team with the highest number of flags will be the winner. For this scenario, a combination of good encryption/decryption software, as well as coding/decoding skills are necessary. The maximum size of the allowed key will be fixed as feature of this scenario, as well as a list of the admitted encryption algorithms.

- **Scenario 3** can be defined by using the *Classic LMS* strategy. In this new CDX, the same resource (text file, image, video, etc.) is given to each participant, which have the task to quickly encrypt it. At the same time, an automatic system starts to use decryption techniques to achieve the participant data. Every 15 minutes, the level goes up, and the automatic system increases its “knowledge” using new complex and sophisticated decryption algorithms and increasing its speed or computation power. Once the participant file is decrypted by the automatic system, the owner of the file is out of the game (dead). The participants still in the game can change the encryption key at the beginning of each level as many times as he/she wants, always respecting the game rules. The game ends when only one participant remains in the game or after 180 minutes. The maximum allowed size of the key will be fixed as feature of this scenario.

- **Scenario 4.** This scenario is based on the *CTF Jeopardy-style* strategy. It involves training and testing challenges regarding the analysis of the vulnerabilities in electronic systems. The game starts showing a board with different challenges to be addressed by the participants in order to get the point. These challenges aim to find vulnerabilities in the available electronic system using pre-determined software. Each encountered vulnerability is considered as a flag, and its detection correspond to the solution of a challenge. The vulnerability detection process is considered more complicated, so more points are assigned to that challenge. The team that reaches the highest score when the clock runs out, will be the winner. The electronic devices used, as well as the list of the permitted software, are given as parameters of the scenario.

- Another interesting scenario, **Scenario 5**, is based on exploiting the vulnerabilities in electronic devices. It can be implemented recalling some concept of the *Locked Shield* strategy. The idea is to involve the participants to attack and exploit the vulnerabilities of several electronic devices with the aim to take their controls. In this case all participants take part at the CSX as red team, meanwhile static countermeasures defined in the deployment phase represent the blue team (there will not be an actual live team). When the clock runs out, if the red team reached the control of most of the available devices will be the winner. All the operations will be recorded to evaluate and improve the characteristics of the used devices. A manual of technical specifications of each device is given as parameters for this exercise.

- **Scenario 6.** This scenario is defined as a *CTF Jeopardy-style* with tasks and challenges focused on blockchain analysis. In this case, the control board can offer deanonymizing tasks regard on-line and off-line transactions, user tracking between blocks, ownership of particular contract, temporal analysis of abnormal transactions, and so on. All the solutions of these challenges represent the flags to be indicated in the control board for resolving the related task. According to each task's difficulty, different score points are assigned. When the clock runs out, the participant with the highest number of points will be the winner. The blockchain service can be used also to define a new scenario.

- **Scenario 7**, drawn by following the *CTF Attack/Defend individually* strategy. In this new context, the participants are divided into two teams: an attacker (red) and defender (blue) team. In this CDX, the aim of the red team is to attack the blockchain service, in order to make it unavailable, for example performing a flooding transaction attack. On the other hand, the blue team need to figure out how mitigate this kind of attack, keeping alive the service. The team that achieves its goal when the time runs out, will be the winner.

- A version slightly different of the presented scenario, in which the main goal is to take the control of the available resources *(SafeHole KotH)* can be used to implement the **Scenario 8**. In this new CDX, all participants belong to the red team, and have the aim to attack and take the control of the given blockchain. The red team must attack the integrity of the blockchain by directly attacking the miner node or generating new ones until reaching the full control of the network. In this case, they prove the solution of the task by re-writing a block's data. The game ends when the red team achieves the re-writing of a block in the blockchain (red wins) or when the time expires (blue wins).

- **Scenario 9.** This scenario is planned to follow the *CTF Jeopardy-style* strategy. The challenges described in the board involves the analysis of the communication between model cars and the analysis of their settings. In the first phase, the participants must collect flags hidden in the configuration of the model cars fleet. In the second phase, they need to capture, analyse, and localise flags in the communication protocol between the fleet. Each task varies its score according to its degree of complexity. When the clock runs out, the participants who reach the highest score will be the winner. A list of the specification of the cars model and the communication protocol is given as feature.

- A different scenario (**Scenario 10**), based on automotive model car control, can be drawn following the *SafeHole KotH* strategy. This new strategy defines the new goal into take the control of model cars fleet. This CDX can be divided in four levels each one with a different level of complexity. In each level, the participants start with the same resources with the aim of taking and holding the control of the fleet. Nevertheless, what is different is the definition of the control action. In a first level of complexity, the control can be taken by avoiding cars receiving messages (DoS or jamming). In the second level, in order to take the control, the participants need to inject command through the normal messages (using Sabotage Fault Injection Framework). In the third level, the participants must obtain an interactive session, for example opening a reverse shell. In the most complex case, the fourth level, an administrator session for executing new process or creating new hosts is requested. When the clock runs out, the team that has the control of most of the fleet, will be the winner. A list of the technical specification of the model cars is given as feature.

- **Scenario 11.** This scenario is based on the *CTF Jeopardy-style* strategy. The idea is to train and test the skills of the participants in both attack and defence operations regard a critical sector as it is the electrical supply. In the first phase, the teams are called to retrieve flags in the network using the SecureGrid Hacking Tool Box (HTB). The flags can be identified through an open port, fingerprinting, configuration, etc. In the second phase, the defence skills are tested by using the SOTER tool trying to address challenges regarding detection or countermeasures. Each task in the control board has score points assigned basing on its complexity. The teams need to resolve the major number of the tasks in order to gain the reward points. When the clock runs out, the team with the highest number of points will be the winner. A user guide regarding the functionality of both the HTB and SOTER is provided to start this CDX.
- **Scenario 12.** This scenario is implemented as a *CTF Attack/Defend individually* exercise. The participants are divided into two teams, an attacker team (red) and defender team (blue). The aim of the first group is to exploit the vulnerabilities in the SmartGrid network (open ports, bad configuration, etc.) in order to collect or corrupt several hidden flags. The attacker can count with the help of the SecureGrid Hacking Toolbox (HTB). On the other hand, the blue team can use the SOTER tool to detect the threats and apply countermeasures in order to mitigate the attacks. The CDX ends when the red team conquers all the flags (attacker wins) or when the time runs out (blue wins). A user guide regarding the functionality of both the HTB and SOTER is provided to start this CDX.
- **Scenario 13.** This scenario is planned to follow the *SafeHole KotH* strategy. The same resources, and the same tools are assigned to each participant, which have the goal to take and hold the control of as many as possible elements available in the training field. Each one can use the SecureGrid Hacking Toolbox (HTB) to attack and exploit the detected vulnerabilities using for example DoS, or exploit for execute piece of code, etc. The training field is composed by several embedded systems, real and simulated (SCADA, router, switch, etc.). When the clock runs out, the participant that have the control of the majority of the elements will be the winner.
- **Scenario 14.** This scenario is drawn as *CTF Treasure Hunt* exercise, implemented by using a smart factory testbed. This CDX is suited for training and testing the knowledge of the participants over several levels of cybersecurity, from IT concepts until the most complex OT. Using the Treasure Hunt strategy, all the challenges (or levels in this case) are related among them, and it is possible to reach a new one, only when the previous ones are resolved, like following a guided path. In fact, each flag detected in a level is a trail to address the next one, and of course each one is related with a score point. When the clock runs out, the participant that has achieved the highest score will be the winner.
- The smart factory testbed could be used also for creating the battlefield of a new scenario, **Scenario 15,** based on *SafeHole KotH* strategy. In this CDX, the participants are separated into teams, with the aim of finding and exploiting the vulnerability of the resources available in the battlefield to take their control. These resources are related with parts or devices of the smart factory testbed. The teams not only have to take the control of the factory but also, they also must defend their ownerships from the adversarial attack. When the clock runs out, the team that has the control of the major number of devices in the battlefield will be the winner. The description of the battlefield and the used device/protocol will be provided as parameters of this CDX.

- **Scenario 16.** This scenario is planned to follow the *Classic LMS* strategy. In this case the participants must implement a decision model with the aim of protecting fixed assets (from a company, a service, application, etc.). The game starts attacking these implemented models with an automatic system that with time it increases its “knowledge” of the models and it increases its power of attack. For each decision/answer computed by the model the team will receive points. When an attack results successful, i.e., information is found about the asset, the team owner of the model will out of the CDX. The game ends when only one team remains or when the clock runs out. In this second case, the winner will be the team with the highest score.
- A similar scenario can be implemented with the aim of attacking several decision-maker models. In this new scenario, **Scenario 17**, all the participants belong to the red team with the aim to attack the models and extract information about their key assets. All the attack-defence processes are recorded to use the historic information for training the white team, following the *Locked Shield* strategy. In this CDX the blue team is a not a live team, which means that static countermeasures are set to react to several reds ‘attacks. If the red team achieves the asset’s information from most of the models, it will be the winner. All the information about the attacks used and strategies, and about the decisions taken by the model in the CDX will be recorded and used to analyse and perform an optimization in both attack/defence scenario.
- **Scenario 18.** This scenario is based on the *Infection LMS.* All participants receive the same amount of computational power, and among them, one user is randomly chosen to be the attacker (red team), meanwhile all the others are chosen to be the resistance (defender or blue team). All the resistant users receive a file that must be protected by using several available algorithms. The aim of the attacker is to collect those files by resolving the protection puzzles. Once he/she decodes them and gets access to the file, the owner of the file is considered infected and must change the team, becoming an attacker. The game ends when all the defender team is infected (so all are converted into attackers) or when the clock runs out (180 minutes). In this second case, the team with the highest number of users is the winner. A list of the admitted protection algorithms is given as feature of this CDX.

Chapter 9 List of Abbreviations

Abbreviation	Translation
AAA	Authentication, Authorization, and Accounting
AI	Artificial Intelligence
API	Application Programming Interface
AS	Application Server
BOE	Spanish Official State Gazette
CAB	Conformity Assessment Body
CCB	Center for Cyber Security Belgium
CCCN	European Cybersecurity Competence Network and Centre
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CCN	National Cryptology Centre
CDTI	Centre for Industrial Technological Development
CDX	Cyber-Defense Exercise
CNCS	Portuguese National Cyber Security Center
CNI	Spanish National Intelligence Centre
CNPIC	National Centre for the Protection of Infrastructures and Cybersecurity
CSIRT	Hellenic National Computer Security Incident Response Team
CTF	Capture the Flag
DTCs	Digital Technology Centres
E.E.T.T.	National Telecommunications and Post Commission
ECSM	European Cyber Security Month
ECSO	European Cyber Security Organisation
EDIH	European Digital Innovation Hub
ENISA	The European Union Agency for Cybersecurity
EZÚ	Electrotechnical Testing Institute

Abbreviation	Translation
GDPR	General Data Protection Regulation
HNDGS	Hellenic National Defence General Staff
HTTP	Hypertext Transfer Protocol
HW	Hardware
ICT	Information and Communication Technology
IdP	Identity Provider
IEEE	Institute of Electrical and Electronics Engineers
INCIBE	Spanish Cyber Security National Institute
IoT	Internet of things
ISPs	Internet service providers
IT	Information Technology
JCCI	Joint Competence Centre Infrastructure
KDC	Key Distribution Center
KotH	King of the Hill
LDAP	Lightweight Directory Access Protocol
LEA	Law Enforcement Agency
LMS	Last Man Standing
NAAS project	Development of the National Ecosystem for the Recognition and Analysis of the Information Effect Phenomena project
NAS	Network Access Server
NASK	Research and Academic Computer Network
NATO	North Atlantic Treaty Organization
NC3	National Cybersecurity Competence Centre
NCC	Belgian National Coordination Centre
NSM Cluster	Network Security Monitoring Cluster
PDP	Policy Decision Point
PEP	Policy Enforcement Point

Abbreviation	Translation
PESCO	Permanent Structure Cooperation
RADIUS	Remote Authentication Dial-In User Service
RENIC	Spanish Network of Excellence on Cybersecurity Research
REST(ful)-API	Representational State Transfer Application Programming Interface
RIA	Estonian Information System's Authority
RTO	Research and Technology Organisations
S2S	Site-to-Site
SAML	Security Assertion Mark-up Language
SDL	Service Description Language
SME	Small and Medium-sized Enterprises
SOAP	Simple Object Access Protocol
SPW	Service Public de Wallonie
SSID	Service Set Identifier
SSO	Single Sign-on
SW	Software
TGT	Ticket Granting Ticket
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
VLAN	Virtual local area network
VPLS	Virtual Private LAN Service (aka Transparent LAN Service)
VPN	Virtual Private Network
w.r.t	With respect to
WADL	Web Application Description Language

References

[1] H. Dong, F. Khadeer Hussain, and E. Chang, “Semantic Web Service matchmakers: state of the art and challenges,” Concurr. Comput. Pract. Exp., 2012.

[2] Davis, J. and Magrath, S., 2013. *A survey of cyber ranges and testbeds* (No. DSTO-GD-0771). DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION EDINBURGH (AUSTRALIA) CYBER AND ELECTRONIC WARFARE DIV.

[3] Cowan, C., Arnold, S., Beattie, S., Wright, C. and Viega, J., 2003, April. Defcon capture the flag: Defending vulnerable code from intense attack. In *Proceedings DARPA Information Survivability Conference and Exposition* (Vol. 1, pp. 120-129). IEEE.

[4] Bock, K., Hughey, G. and Levin, D., 2018. King of the Hill: A Novel Cybersecurity Competition for Teaching Penetration Testing. In *2018 {USENIX} Workshop on Advances in Security Education ({ASE} 18)*.

[5] CASANO, F. and COLOMBO, R., 2019. Wargaming: The Core of Cyber Training. *Next Generation CERTs*, *54*, p.88.

[6] https://deloitte.wsj.com/cio/2014/09/22/an-introduction-to-cyber-war-games/

[7] Atkin, M.S., Westbrook, D.L. and Cohen, P.R., 1999. Capture the Flag: Military simulation meets computer games. In *Proceedings of AAAI Spring Symposium Series on AI and Computer Games* (pp. 1-5).

[8] Huang, H., Ding, J., Zhang, W. and Tomlin, C.J., 2011, May. A differential game approach to planning in adversarial scenarios: A case study on capture-the-flag. In *2011 IEEE International Conference on Robotics and Automation* (pp. 1451-1456). IEEE.

[9] Vigna, G., 2003. Teaching network security through live exercises. In *Security education and critical infrastructures* (pp. 3-18). Springer, Boston, MA.

[10] Eagle, C. and Clark, J.L., 2004. *Capture-the-flag: Learning computer security under fire*. NAVAL POSTGRADUATE SCHOOL MONTEREY CA.

[11] Ford, V., Siraj, A., Haynes, A. and Brown, E., 2017, March. Capture the flag unplugged: an offline cyber competition. In *Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education* (pp. 225-230).

[12] NATO Cooperative Cyber Defence Centre of Excellence. 2017. Cyber DefenceExercises. (2017). http://ccdcoe.org/event/cyber-defence-exercises.html

[13] Vykopal, J., Ošlejšek, R., Burská, K. and Zákopčanová, K., 2018, February. Timely feedback in unstructured cybersecurity exercises. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education* (pp. 173-178).

[14] Roschke, S., Willems, C. and Meinel, C., 2010, June. A security laboratory for CTF scenarios and teaching IDS. In *2010 2nd International Conference on Education Technology and Computer* (Vol. 1, pp. V1-433). IEEE.

[15] Vigna, G., Borgolte, K., Corbetta, J., Doupe, A., Fratantonio, Y., Invernizzi, L., Kirat, D. and Shoshitaishvili, Y., 2014. Ten years of ictf: The good, the bad, and the ugly. In *2014 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*.

[16] Chapman, P., Burket, J. and Brumley, D., 2014. PicoCTF: A game-based computer security competition for high school students. In *2014 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*.

[17] Maennel, Kaie & Kim, Joonsoo & Sütterlin, Stefan. (2019). Team learning in cybersecurity exercises.

[18] Neville, S.W. and Li, K.F., 2009, May. The rational for developing larger-scale 1000+ machine emulation-based research test beds. In *2009 International Conference on Advanced Information Networking and Applications Workshops* (pp. 1092-1099). IEEE.

[19] Davis, J. and Magrath, S., 2013. *A survey of cyber ranges and testbeds* (No. DSTO-GD-0771). DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION EDINBURGH (AUSTRALIA) CYBER AND ELECTRONIC WARFARE DIV.