Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D9.14
Exploitation Strategy Report 1

Document Identification	
Due date	31 January 2021
Submission date	04 March 2021
Revision	1.0

Related WP	WP9	Dissemination Level	PU
Lead Participant	TDL	Lead Author	David Goodman
Contributing Beneficiaries	ATOS, JAMK, SINTEF	Related Deliverables	D9.19, D9.27

Abstract: This is the first in a series of three reports identifying the exploitation of the CyberSec4Europe results at a consortium and individual partner level relating to assets developed or enhanced during the course of the project, as well as a sustainability strategy in the context of the establishment of a cybersecurity competence centre and network.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

This is the first in a series of three reports identifying the exploitation of the CyberSec4Europe results at a consortium and individual partner level relating to novel cybersecurity products and services developed or enhanced during the course of the project. These assets may have been exploited either within or during the course of the project, or for which partners plan future exploitation after the completion of the project. We look at the responses from individual partners broken down by organisational sector as well as a series of criteria for categorising assets, their benefits and exploitable potential.

We also identify the sustainability strategy of the CyberSec4Europe framework in the context of building a network of competence centres in Europe beyond the completion of the project, in collaboration with the other three pilots and ECSO, the European Commission and the recently announced Competence Centre in Bucharest.

Finally we consider the patents and the generation of intellectual property. In conclusion, we acknowledge that this is going to be a living document over the rest of the project and give indicators of proposed next steps over the coming twelve months.

Document information

Contributors

Name	Partner
Aida Omerovic	SINTEF
Aljosa Pasic	ATOS
David Goodman	TDL
Elina Suni	JAMK
Gencer Erdogan	SINTEF
Jani Paijanen	JAMK
Karin Bernsmed	SINTEF
Per Meland	SINTEF
Shukun Tokas	SINTEF

Reviewers

Name	Partner
Mark Miller	CONCEPT
Pasquale Annicchino	ARCH

History

Version	Date	Authors	Comment
0.1	30 October 2020	David Goodman	First draft
0.2	29 January 2021	David Goodman	Second draft
0.3	15 February 2021	David Goodman	Third draft
0.4	18 February 2021	David Goodman	Fourth draft
1.0	02 March 2021	Ahad Niknia Kai Rannenberg	High-level review and preparation for submission

Table of Contents

List of Tables

List of Acronyms

A	**AI**	Artificial Intelligence
C	**CESM**	Centre d'Expertise en Sécurité Métier
	CHECK	Community Hubs of Expertise in Cybersecurity Knowledge
	CHECK-T	Community Hubs of Expertise in Cybersecurity Knowledge – Toulouse
	CONCORDIA	Cyber security cOmpeteNCe fOr Research anD InnovAtion
D	**DG CONNECT**	Directorate-General for Communications Networks, Content and Technology
	DoA	Description of the Action
E	**ECHO**	European network of Cybersecurity centres and competence Hub for innovation and Operations
	ECSO	European Cyber Security Organisation
	EHR	Electronic Health Record
	eIDAS	Electronic IDentification And trust Services
	ESSoS	International Symposium on Engineering Secure Software and Systems
	ETSI	European Telecommunications Standards Institute
G	**GDPR**	General Data Protection Regulation
H	**H2020**	Horizon 2020
	HPC	High Performance Computing
I	**IdM**	IDentity Management
	IoT	Internet of Things
	ISO/IEC	International Organization for Standardization and the International Electrotechnical Commission
	JRC	Joint Research Centre
J	**JTC**	Joint Technical Committee
L	**LPA**	Local Public Administration
M	**MOOC**	Massive Open Online Course
	MPC	Multi Party Computation
N	**NIS**	Network and Information Security
O	**OBSIDIAN**	Open Banking Sensitive Data Sharing Network For Europe
	OLYMPUS	Oblivious identitY Management for Private and User-friendly Services
R	**RGCE**	Realistic Global Cyber Environment
S	**SC27**	Standardization Committee 27
	SDVA	Social Driven Vulnerability Assessment

	SFI-NORCICS	Sentre for forskningsdrevet innovasjon Norwegian Center for Cybersecurity in Critical Sectors
	SME	Small to Medium-sized Enterprise
	SPARTA	Strategic Programs for Advanced Research and Technology in Europe
T	**TCG**	Trusted Computing Group
	TRL	Technology Readiness Level
U	**UN INFO**	United Nations Information
V	**VDES**	VHF Data Exchange System
W	**WP**	Work Package

List of CyberSec4Europe Partners

A	**ABI**	ABI Lab
	AIT	Austrian Institute of Technology
	ARCH	Archimede Solutions SARL
	ATOS	Atos
B	**BBVA**	BBVA Group
	BRNO	Masaryk University
C	**C3P**	University of Porto
	CNR	Consiglio Nazionale delle Richerche
	CONCEPT	CONCEPTIVITY
	CTI	Computer Technology Institute and Press “Diophantus”
	CYBER	Cybernetica
D	**DAWEX**	Dawex
	DTU	Technical University of Denmark
E	**ENG**	Engineering Ingegneria Informatica S.p.A
F	**FORTH**	Foundation for Research and Technology Hellas
G	**GEN**	Comune di Genova
	GUF	Johann Wolfgang Goethe-Universität Frankfurt
I	**I-BP**	Informatique Banques Populaires
	ICITA	International Cyber Investigation Training Academy
	ISGS	Intesa Sanpaolo
J	**JAMK**	JAMK University of Applied Sciences
K	**KAU**	Karlstad University
	KUL	KU Leuven
N	**NEC**	NEC Laboratories Europe GmbH
	NTNU	Norwegian University of Science and Technology (NTNU)
O	**OASC**	Open and Agile Smart Cities
P	**POLITO**	Politecnico di Torino
S	**SIE**	Siemens
	SINTEF	SINTEF
T	**TDL**	Trust in Digital Life
	TLEX	Timelex
	TUD	Delft University of Technology
U	**UCD**	University College Dublin & LERO
	UCY	University of Cyprus
	UM	University of Maribor
	UMA	University of Malaga
	UMU	University of Murcia
	UNILU	University of Luxembourg
	UNITN	University of Trento
	UPRC	University of Piraeus Research Center
	UPS-IRIT	Université Toulouse III Paul Sabatier – Institut de Recherche en Informatique de Toulouse
V	**VAF**	VaF
	VTT	VTT Technical Research Centre of Finland

List of Countries

A	**AT**	Austria
B	**BE**	Belgium
	BL	Bulgaria
C	**CH**	Switzerland
	CY	Cyprus
	CZ	Czech
D	**DE**	Germany
	DK	Denmark
E	**EE**	Estonia
	ES	Spain
F	**FI**	Finland
	FR	France
G	**GR**	Greece
H	**HR**	Croatia
	HU	Hungary
I	**IE**	Ireland
	IT	Italy
L	**LU**	Luxembourg
N	**NL**	Netherlands
	NO	Norway
P	**PL**	Poland
	PT	Portugal
S	**SE**	Sweden
	SI	Slovenia
	SK	Slovakia

1 Introduction

According to the DoA (Description of the Action), the role of task 9.4 is to:

> *... identify the exploitation of the CyberSec4Europe results at a consortium and participant level, relating to the comprehensive suite of novel cybersecurity products and services as well as the implementation of a common cybersecurity research and innovation roadmap also taking into consideration advice from the advisory board.*[1]

This document, the first in a series of three, reviews the objectives of a CyberSec4Europe exploitation strategy and reports on the status quo, from the perspective of the individual partners and the project as a whole.

2 Exploitation Strategy

One of CyberSec4Europe's main challenges is to scale up and use the power of community-based collaboration and cooperation in order to improve the transtion from research to market and to make a lasting impact on the Digital Single Market, the digital transformation of the European economy and in particular the EU's industrial strategy for Europe.[2]

2.1 Test and validate exploitation methodology

The nature of this pilot makes the development of an exploitation strategy different from other H2020 projects, as CyberSec4Europe must also test and validate the procedures and operational setup for the better exploitation of cybersecurity research, which will later serve the Cybersecurity Competence Network and Centre.

Organisations benefit greatly when they are part of a larger community, whether it is in their own value chain, with early clients who want to test solutions, or cross-domain, where the sharing of best practices and lessons learnt can take place. By its very nature, CyberSec4Europe plays a brokering role and brings together research and industry, both demand and supply side. Co-creation might especially help promote local and small organisations improve their reach; so the exploitation strategy should acknowledge this with specific tactical choices and priority settings.

2.2 Attention to non-tangible results

CyberSec4Europe has a collection of competences that span different types of research excellence, technical expertise and vertical sectors, added to which not all of the project results are of a technical nature. Take, for example, the research roadmap, which has a very important outcome for EU policymakers but also has exploitation potential. Other exploitable non-tangible activities that could live after the project ends are raising awareness (e.g., the annual CONVERGENCE conference), security assurance services or maturity assessment, demonstration and best practice documents, the process of knowledge and technology transfer.

[1] DoA Annex 1 (part A) p.50
[2] https://ec.europa.eu/info/sites/info/files/communication-eu-industrial-strategy-march-2020_en.pdf

2.3 Synchronisation and prioritisation milestones

When it comes to the timing of activities, the exploitation strategy should be synchronised with the progress and activities of the individual work packages. CyberSec4Europe's technical workpackages follow an iterative development methodology, with at least two development and evaluation cycles over the course of the project. Synchronisation points are also good opportunities for exploitation-related activities so as to consolidate around determining what the key exploitable results are, as well as to prioritise and focus resources.

2.4 Support for SME and start-up growth

The project exploitation strategy should support companies, especially SMEs and start-ups, organisations and public administrations, to become more competitive.

In the DoA, it mentions that:

> *CyberSec4Europe will offer possibilities to SMEs to exploit new services to deliver custom applications that, only a few years ago, demanded independent software vendor involvement in million-euro projects.*[3]

In other words, CyberSec4Europe is developing a series of basic building blocks that could serve as a catalyst for start-ups and SMEs and enable these stakeholders to develop and integrate innovative services without having to design specialised functionalities from scratch.

Open architectures and solutions from the project could foster SME competitiveness, while enabling transformation in vertical sectors. Here, an exploitation strategy would align with "test before invest" or "try before buy", where start-ups and/or SMEs would get free or heavily discounted cybersecurity services.

Examples include helping SMEs to make use of the cybersecurity testing facilities or services (e.g. free pentesting), use of cybersecurity services from the cloud, datasets and algorithms that are relevant for their needs, risk assessment and security audits, training, demand placement and business opportunities etc

As many SMEs carry out research and development work without being involved in a wider community, an important strength of the burgeoning European cybersecurity network will be to enable SMEs to participate more than they do today in pan-European research activities.

2.5 Connecting EU ecosystems

CyberSec4Europe is not the only community in the EU. Besides the other pilot projects supporting the Cybersecurity Competence Centre, there are established communities in other IT domains, such as Industry 4.0, AI or high-performance computing (HPC). An exploitation strategy should also look at external ecosystems, with the aim of identifying innovation opportunities.

This includes the expansion of CyberSec4Europe community, opening new markets, developing cross-domain value chains (including cybersecurity data sharing), creating new business opportunities for CyberSec4Europe partners or helping to commercialise earlier project results.

[3] DoA Annex 1 (part B) p.28

Furthermore, given the extensive connections between CyberSec4Europe and ECSO, we see the clear connection with this significant cybersecurity community.

In this aspect, the exploitation strategy should link to community building activities in the project, especially when it comes to the detection of gaps whether they be geographical, technological, sectorial focus, etc.

2.6 Living document

During the project this exploitation strategy, tactical choices, path or activities described above will be refined and adapted to trends and developments occurring both inside and outside the project, resulting in a final exploitation plan that includes agreements on the sustainable exploitation of the project results.

3 Methodology

The approach adopted in this report is based on the commitments made in the project proposal and contained in the DoA[4] under the headings:

- *Individual Exploitation*
- *Exploitation by the consortium as a whole*
- *Innovation Management*

The primary information gathered to demonstrate both the individual and joint exploitation plans and ambitions came from the individual partner activity files that are stored centrally within the project. It is the responsibility of each partner to manage and maintain their own activity file based upon the common template provided. Each of these files contains six tabs, including one entitled 'Exploitation Plans' the details of which are contained in the next section.

All partners completed the exploitation tab irrespective of how developed their exploitation plans for beyond the end of the project have been formulated. As indicated above, this is a 'living document' and it is anticipated that many partners' plans will mature during the later stages of the project.

To provide some initial context, we have included a brief description of each partner's role in the project as well as the benefits expected, in their own words, from prior to the project start as described in the Description of Work. In a later report in this series, we will canvas all partners to consider and compare their organisations's intitial exploitation expectations with how those expectations have (or have not) been met.

4 Individual Exploitation

CyberSec4Europe comprises diverse organisations, large and small from software vendors to corporate businesses, universities and research institutes, SMEs, legal and consultancy firms, and not for profit organisations. This diversity is expected to *enable efficient exploitation of results*

[4] DoA Annex 1 (part B) pp.33-34

across a number of avenues in line with the needs and opportunities for each type of consortium partner.[5]

4.1 Exploitation and Business Plans

All partners are expected to develop their own clear ideas on how to exploit their achievements and to contribute to their own exploitation goals, enabling implementation of the project results through various disciplines and stakeholder types.

To assist with achieving a degree of uniformity in their responses, partners were offered a pre-defined set of headings to describe their plans and to maintain independently throughout the course of the project.

The category headings are:

- Type of exploitation
  - technical component,
  - complete product or solution,
  - service,
  - education course,
  - research proposal,
  - marketing,
  - internal processes
- Pre-existing status of asset:
  - an update of a pre-existing asset
  - an update of pre-existing open source
  - a new exploitable result
  - not applicable
- Exploitation period:
  - within the project: asset used in ongoing CyberSec4Europe project work
  - during the project: assets to be exploited before the end of CyberSec4Europe
  - after the project: assets to be exploited after the end of CyberSec4Europe
- Description
- Anticipated benefits, including for example:
  - scale
  - audience
  - geography
- Ownership: is there associated with the asset
  - a patent
  - proprietary IPR
  - open source
  - another kind of licence type
  - not applicable
- Associated work package or task

[5] ibid

- Collaboration with other partners

At this stage, individual partner exploitation plans are not carved in stone but at least provide an indicator of direction that will be refined over the rest of the project and updated in later iterations of this report series at M36 (January 2022) and M42 (July 2022).

The split of CyberSec4Europe project partners more or less follows the categories originally outlined in the Description of Work[6]:

- **Associations** (4.1.1) will expect to:
  - improve and extend their networks
  - extend the scope of cybersecurity coverage and activity
- **Businesses** (4.1.2) will:
  - improve the security of their IT systems
  - adopt secure and privacy-preserving practices to customers and participants
- **Legal and consultancy firms** (4.1.3) will be able to:
  - improve and extend their consulting services
  - establish leadership in cybersecurity practices
- **Local government** (4.1.4) will:
  - improve the security of their IT systems
  - adopt secure and privacy-preserving practices to employees and citizens
- **Research institutes** (4.1.5) will be enabled to:
  - build partnerships with other research institutions and facilitate collaboration with industry
  - raise their profile both nationally and internationally
  - participate in standardisation activities
- **Software vendors** (4.1.6) will benefit by:
  - increasing their technology readiness levels based on the set of roadmaps developed from the outcomes of each of the industrial challenges
  - bolstering their thought and market leadership in cybersecurity
  - improving and extending their consulting services
  - participating in standardisation activities
- **Universities** (4.1.7) will seek to:
  - expand the scope of post-graduate course and research offerings
  - develop specialist summer schools with a focus on cybersecurity topics
  - collaborate with other research and academic institutions industry

4.1.1 Associations/Networks

4.1.1.1 Open and Agile Smart Cities (OASC)

Not for profit network organisation, Belgium

[6] ibid

Role in project: OASC will act as a demonstration case and impact participant for the smart cities domain. OASC will deploy prototypes addressing key cybersecurity challenges and provide a dedicated environment for exchanging ideas, needs, and best practices in and between cities.

Expected benefit: The project will allow OASC to increase the focus of its members on cybersecurity through pilots, working groups, and communication.

4.1.1.1.1 Marketing

Description: OASC will offer the CITYxCITY catalogue featuring operational solutions. OASC will ensure that solutions piloted in T5.7 will be featured on the catalogue after the project ends for replications and scale
Audience: Cities and communities linked, but not limited to, the OASC network
Geography: Global
Context: To be used after the project
WP: WP5/T5.7

4.1.1.2 Trust in Digital Life (TDL)

Not for profit membership association, Belgium

Role in project: TDL is responsible for co-ordinating the demonstration use case on the security issues associated with the deployment of PSD2 (and GDPR) and for developing and implementing a cybersecurity roadmap in this domain. TDL also has responsibility for leading WP9 on Dissemination, Outreach, Spreading of Competence, Raising Awareness, with specific responsibility for leading the individual tasks associated with both dissemination and exploitation.

Expected benefit: The benefits TDL anticipates accruing from its participation in the project are to be in a strong position to create and disseminate awareness about au courant state of the art issues relating to cybersecurity, both to its existing members as well as to the wider industrial and research community in Europe.

4.1.1.2.1 Marketing

Description: Based on its participation in CyberSec4Europe, TDL will seek to extend the scope and range of its membership in the context of cybersecurity and open banking in particular.
Audience: Industry, SMEs, knowledge institutes
Geography: Europe
Context: To be developed during the project and continued afterwards
WP: WP5 / T5.1 and all

4.1.1.2.2 Internal processes

Description: Based on its CyberSec4Europe experience, TDL will seek to extend the scope and range of activities with its member organisations
Audience: Industry, SMEs, knowledge institutes
Geography: Europe
Context: To be developed during the project and continued afterwards
WP: WP5 / T5.1 and all

4.1.1.2.3 Research proposal

Description: Usage of the project's results for further research proposals in the area of cybersecurity and open banking
Geography: Europe
Context: To be developed during the project and continued afterwards
WP: WP5 / T5.1 and all

4.1.1.2.4 Research Proposal

Description: SC1-PHE-CORONAVIRUS-2020-2B Medical technologies, Digital tools and Artificial Intelligence (AI) analytics to improve surveillance and care at high Technology Readiness Levels (TRL). Support market innovation (from lab-to-fab) for further developing and maturing innovative solutions that have already been validated in lab environments (TRL 6-7 or higher) with the aim to help accelerate developments and achieve conformity assessment (CE marking) (type 2).
iP3Health: Interoperable Privacy-Preserving Personal Health Technologies with Tracking and Tracing (not granted)
Geography: Europe
Partners: AIT, CONCEPT, CYBER, GUF, VTT
Context: Developed during the project
WP: All

4.1.2 Businesses (Banks)

4.1.2.1 BBVA Group (BBVA)

Bank, Italy

Role in project: BBVA's role is to provide user validation of CyberSec4Europe results especially in respect to the financial sector demonstration use case in respect of incident resilience and security intelligence as well as to link with different working groups in Europe.

Expected benefits: BBVA seeks to enhance the financial sector ability to cope with mandatory incident reporting and to foster a voluntary info-sharing and threat intelligence mechanism, in order to be better prepared towards the implementation of the blueprint to responding to large scale cyber incidents and crisis management.

4.1.2.1.1 Product

Description: BBVA will use the Incident Reporting Platform that is being developed in WP5 / T5.4. The objective of the Incident Reporting Platform is to enable financial institutions to fulfil the mandatory incident reporting requirements according to the different procedures and methods specified by applicable regulatory bodies (such as PSD2 and the ECB Cyber Incident Reporting Framework). The platform covers from the collection of the data related to a security incident detected until the generation of the mandatory reports that have to be sent to the competent authorities. The Incident Reporting Platform will address the common need for standardized and coordinated cybersecurity communication cooperation and could also pave the

way towards a public and private cooperation to reach the common goal of an enhanced cyber resilience across Europe and beyond the EU borders.

Benefits: Currently, there are no standards defined for mandatory incident reporting and each Supervisory Authority, both at EU and national level, defines the relevant impact assessment criteria, thresholds, timing, dataset, procedures and communication means that must be followed. All these different criteria and patterns cause fragmentation into the overall incident reporting operation for the affected financial entities and are to be managed along the critical path of managing the incident itself. This implies time-consuming reporting processes for the incident management and reporting teams and can even lead to potential faster propagation of threats.

Additionally, in the overall context of incident reporting, there is an increasing importance given to cooperation and threat intelligence data sharing among all the different stakeholders to improve the capacity and resilience of the European cyber environment and give a more efficient and quick answer to the new cyber security threats.

A further listing of the main benefits of the Incident Reporting Platform is at section 7.1.2.3

Ownership: To be discussed during the current phase of the development of the Incident Reporting Platform.
Partners: Atos, Intesa Sanpaolo
Context: The Incident Reporting Platform is a new asset and will be used by BBVA after the project, once the development and testing of the platform has been finished.
WP: WP4 / T4.7 and WP5 / T5.4

4.1.2.2 Informatique Banque Populaire (I-BP)

Bank, France

Role in project: The CESM's missions gives it an in-depth knowledge of security challenges in banking applications and systems in a digital economy, given that these applications and systems are the central assets of bank digital strategy, and the security inside these assets is the critical part to ensure customers trust their bank services. Thanks to i-BP IT and security skills and expertise, CESM will contribute to the Open Banking demonstration use case (T5.1), from specifying in detail use cases maximising the business value of project work, to community building solutions.

Expected benefits: Offering competitive services thanks to their value in terms of trust and contributing to definitely make the European digital and security ecosystem a world leader

4.1.2.2.1 Service

Description: Converting the OBSIDIAN prototype into a commercial service delivered to banks and other banking partners including payment service providers, financial transfer software editors et al.
Further descriptions of OBSIDIAN may be found at section 7.1.2.3
Benefit: Fraud loss decrease by a minimum of 4%
Context: A new asset, to be piloted during the project and to be commercialised afterwards
Partners: ABI Lab, CAIXA, POSTE, TDL
WP: WP5

4.1.2.3 Intesa Sanpaolo Group Services (ISGS)

Bank, Italy

Role in project: ISGS role is to provide user validation of CyberSec4Europe results especially in respect to the financial sector demonstration use case in respect of incident resilience and security intelligence, as well as to link with different working groups in Europe.

Expected benefits: Intesa Sanpaolo seeks to enhance the financial sector ability to cope with mandatory incident reporting and to foster a voluntary info-sharing and threat intelligence mechanism, in order to be better prepared towards the implementation of the blueprint to responding to large scale cyber incidents and crisis management.

4.1.2.3.1 Complete product or solution

Description: After the end of the project, we will update the available prototype with possible new regulatory frameworks, insert the classification functionality, if not available, and use it within the Group and when possible also with external stakeholders.
Geography: Europe
Ownership: Not yet decided
Partners: Atos, BBVA
Context: New asset, to be used and commercialised after the project
WP: WP5 / T5.4

4.1.3 Legal and Consultancy Firms

4.1.3.1 Archimede Solutions SARL (ARCH)

Consultancy, Switzerland

Role in project: Archimede Solutions contributes to the following tasks:

- T3.7 Regulatory sources for citizen-friendly goal
- T7.3 Certification
- T8.1 Maintaining contacts with the Europeans SDOs and the relevant cybersecurity community
- T8.2 Linking the technical work of the project to standards and standards to the project
- T9.6 Policy recommendations

Expected benefits: Archimede Solutions aims at enhancing its positioning in the research of solutions for cybersecurity, data protection and certification. The participation to this research project will be a key step towards this goal.

4.1.3.1.1 Research proposals

Description: Use of project's research results to further increase our R&D capacity and participation to research call on cybersecurity
Geography: Europe
Context: Update of existing asset, to be developed after the project
WP: All

4.1.3.1.2 Research proposals

Description: Use of project's research results to further increase our R&D capacity and participation to research call on data protection and certification
Geography: Europe
Context: Update of existing asset, to be developed after the project
WP: All

4.1.3.1.3 Educatioal course

Description: Use of project's result to contribute to education and training initiatives in the field of data protection
Geography: Europe
Context: New asset, to be developed after the project
WP: All

4.1.3.2 CONCEPTIVITY (CONCEPT)

Micro-SME security think tank and government advisory, Switzerland

Role in project: CONCEPTIVITY leads WP10 (including concertation activities) as well as leading task 2.5 (WP2) and task 8.1 (WP8).

Expected benefits: Opportunities to expand the client base with respect to cybersecurity studies, cybersecurity certification support and government and private sector advisory activities.

4.1.3.2.1 Research proposals

Description: Usage of the project's results for further research proposals in the area of cybersecurity
Geography: Europe
Context: To be developed during the project and continued afterwards
WP: All

4.1.3.2.2 Service

Description: Usage of the project's results for advisory and consulting opportunities in policy and regulatory recommendations, cybersecurity certification, SME specific elements
Benefits: Client expansion
Geography: Europe
Context: To be developed during the project and continued afterwards
WP: All

4.1.3.2.3 Service

Description: Usage of the project's results for further research studies and for the benefit of European Governments and European Institutions clients
Geography: Europe
Context: To be developed during the project and continued afterwards
WP: All

4.1.3.2.4 Marketing

Description: Based on its participation in CyberSec4Europe, CONCEPT will seek to extend the scope and range of its client base
Audience: European governments, international organisations, European institutions
Geography: Europe
Context: To be developed during the project and continued afterwards
WP: All

4.1.3.3 International Cyber Investigation Training Academy (ICITA)

Consultancy, Bulgaria

Role in project: ICITA's experience in building successful partnerships, initiatives and projects with government organizations, academic institutions and industry adds value to the project by engaging ICITAs community of stakeholders to participate in surveys, mapping exercises and assessment activities. It also adds value in the development of certification program by taking part in methodology development. ICITA distributes the outcomes of this project to all its partners and will involve them in the development cycle as needed.

Expected benefits: By participating in this project ICITA will be able to benefit from next generation industrial and civilian cybersecurity technologies applications and services. This will enable us to address the current cyber threats in a more efficient manner and provide us the necessary tools to tackle the future threats in order to protect the European citizens.

4.1.3.3.1 Research proposals

Description: Usage of CyberSec4Europe results, capabilities, and networking assets for further European, regional and national public and industry projects
Geography: Bulgaria, Balkans, Europe
Context: Update of a pre-exsiting asset, to be developed during the project and continued afterwards
WP: All

4.1.3.4 Timelex (TLEX)

Law firm, Belgium

Role in project: Timelex is in charge of legal aspects related to cybersecurity.

Expected benefits: Timelex wishes to be involved in advanced European expert networks and innovation actions to remain updated on the latest developments in order to provide better legal services to its clients.

4.1.3.4.1 Service

Description: TIMELEX will combine its legal capabilities with the experience of several IT cybersecurity partners. The objective is to offer a holistic approach consisting of (1) legal, (2) IT, (3) insurance, and (4) communication.
Geography: Belgium, Europe
Context: Developed during the project
WP: All

4.1.3.4.2 Research Proposal

Description: SU-FCT01-2018-2019-2020 –
Rayuela: Development of a serious game environment with interactive and interwoven storylines on cybercrime especially designed for children and youngsters, and the definition of appropriate methodologies to analyse the data of youngster and children playing this game. This will allow the project to model in a friendly and non-invasive manner, online habits and user profiles related to cybersecurity and cyber criminality based on a large and diverse sample covering the most representative geographical areas in Europe, identifying the factors that make children likely to become a victim of a cybercrime (e.g. cyber bullying, online grooming) or to become an offender themselves (e.g. a cyber bully, a hacker). (granted)
Geography: Europe
Context: Developed during the project
WP: All

4.1.3.4.3 Research Proposal

Description: ICT-40-2020: Cloud Computing
Reyna: towards a smart cloud computing continuum.
Geography: Europe
Context: Developed during the project
WP: All

4.1.3.4.4 Research Proposal

Description: SU-BES03-2018-2019-2020 (sub-topic 1) Demonstration of applied solutions to enhance border and external security –
Emerald: Remotely piloted aircrafts and underwater autonomous platforms to be used from on-board offshore patrol vessels. (not granted)
Geography: Europe
Context: Developed during the project
WP: All

4.1.3.4.5 Research Proposal

Description: SU-DS03-2019-2020 –
Cyberangel: Securing the Cyber Space for SMEs through a global and multi-purpose solution that monitors and reports on cyber intrusion attempts. (not granted)
Geography: Europe
Context: Developed during the project
WP: All

4.1.3.4.6 Research Proposal

Description: SU-DS02-2020, subtopic (d) –
DIPIMIS: DIstributed Privacy-preserving Trusted ID Management for IoT-based Services (not granted).
Geography: Europe
Context: Developed during the project
WP: All

4.1.3.4.7 Research Proposal

Description: SU-INFRA02-2019 –
iFOCUS: augmented inFOrmation eCosystems for enhanced Urban Security (not granted)
Geography: Europe
Context: Developed during the project
WP: All

4.1.3.4.8 Research Proposal

Description: SU-DS05-2018-2019 b) Digital security, privacy and personal data protection in healthcare ecosystem –
CIRCLE: A collaborative privacy aware platform for assessing and sharing cybersecurity risks in the healthcare ecosystem (not granted)
Geography: Europe
Context: Developed during the project
WP: All

4.1.3.4.9 Research Proposal

Description: DT-TDS-05-2020 –
INCISIVE: A multimodal AI-based toolbox and an interoperable health imaging repository for the empowerment of imaging analysis related to the diagnosis, prediction and follow-up of cancer. The project will generate a pan-European repository of medical images that can be used for ML-based training for various types of cancer. Inevitably, the project will also deal with data privacy and security implications of such a repository and toolbox. (granted)
Geography: Europe
Context: Developed during the project
WP: All

4.1.3.5 VaF (VAF)

Micro-SME consultancy, Slovakia

Role in project: VaF acts as an internal reviewer

Expected benefits: VaF expects to benefit from participation in the project by improving its knowledge and skills.

4.1.3.5.1 Service

Description: Experience in CyberSec4Europe helps to improve the quality of (consulting) services provided to VaF's clients as well as our reviews of various (conference/journal) papers, project proposals, etc. in the future
Geography: Europe
Context: Developed during the project and continued afterwards
WP: All

4.1.4 Local Government

4.1.4.1 Comune di Genova (GEN)

Local public administration, Italy

Role in project: The city of Genoa focuses on the action on the Smart City demonstration case, focusing in particular on services related to mobility, tourism and civil protection according to the fragile characteristics of the territory.

Expected benefits: include:

- to strengthen and make more uniform the protection of personal data in the municipal processes,
- to simplify the process of managing data processing by standardizing the procedure.
- to help reduce overall data security management costs.

4.1.4.1.1 Internal Process

Description: This exploitation aims at supporting ENG cybersecurity offer
Geography: Italy
Ownership: Apache License 2.0
Partners: ENG
Context: Update of pre-existing asset, improved during the course of the project for exploitation after the end of the project
WP: WP5 / T5.7

4.1.4.1.2 Marketing

Description: This exploitation aims at supporting the ENG commercial proposition
Geography: Italy
Partners: ENG
Context: A new exploitable result, developed during the project
WP: WP5 / T5.7

4.1.5 Research Institutes

4.1.5.1 ABI Lab (ABI)

Research and innovation centre, Italy

Role in project:

- **Use Case Execution:** ABI Lab delivers the execution of the PSD2 related use case with regard to the security considerations in realising PSD2.
- **Specific research for the use case execution:** Moreover, threat intelligence and hunting activities delivered by the Italian Financial CERT, operated by ABI Lab Consortium, also supports the realisation of the cyber threat landscape, specific for the open banking scenario, that will support PSPs to define the adequate preventive and corrective measures.
- **Interaction with banking and financial operators:** A specific group of banks are invited to concretely participate in the analyses provided in the WP. The participation is on a voluntary basis and coordinated by ABI Lab with an internal “call of proposal”. Specifically, info sharing activities is activated within the community to collect real open issue in security that has to be addressed. Moreover, ABI Lab together with the project

participants, aggregates and leads a community of open banking platform providers to assess and verify the identified threats and security countermeasures. Open banking platform providers and banks that have developed their own platform are identified and contacted in all the European countries involved in the project. Regular meetings and workshops are organized to discuss about the state-of-the-art of the activities carried out during the WP and receive feedback from the various outcomes arising from the studies.

- **Dissemination, Communication & Exploitation activities:** The European added-value of ABI Lab activity includes the fact that key results and outcomes of the EU projects where ABI Lab has been involved, are always planned to be disseminated European-wide with an extensive geographical coverage of the banking and financial networks & communities.

Expected benefits: The digital transformation of modern society has created great opportunities for EU citizens and companies: services and information can be accessed 24/7, instantaneously and at global level. We are rapidly moving toward a paradigm in which embedded systems will be highly interconnected and pervasive in nearly every aspect of our lives. Cyber attacks are particularly challenging for several reasons: they rapidly increase in sophistication and complexity; they are persistent; they exploit both technological and human weakness and vulnerabilities; the entry points can be external to the organisation. **The financial and banking sector is one of the most targeted**. In line with the overall objectives of CyberSec4Europe, ABI Lab expects to highlight and stress the importance of innovating the way to create, analyse and take advantage from the knowledge base incoming from cyber security analysis manifested in the cyber landscape along all the execution of the project with a big impact at EU level.

The main benefits ABI Lab is expected to obtain from participation in the project are:

1. to increase the capabilities of the banking and financial EU networks by demonstrating it as a critical sector;
2. to raise awareness through the conduction of workshops, exercises and simulation sessions in the cybersecurity fiancial & banking domain;
3. to increase the level of collaboration and information sharing among among banks, CERTS, LEAs and related regulatory bodies;
4. to respond to the Eurosystem's need for a common framework for simulation and testing activities in the security domain;
5. to contribute to the sustainability of the Digital Single Market in terms of reliability and trustworthiness;
6. to safeguarde the trust of EU citizens in the financial system and its network and services;
7. to raising the awareness and improve the level of readiness of the EU financial sector.

4.1.5.1.1 Research proposal

Description: ABI Lab wishes to find the ways in which it would be possible to strengthen the logic of collaboration with structures similar to CERTFin in the context of info sharing activities, also in order not to lose the relationships built during the project.
Partners: Any other partner similar to a CERTFin
Context: To be used after the project
WP: Possibly all

4.1.5.2 Austrian Institute of Technology (AIT)

Research institute, Austria

Role in project: AIT actively contributes to work packages WP3, WP5, WP8 and WP9. Within WP3, AIT will contribute to the research performed in T3.2 on privacy-preserving authentication and data processing; the developed solutions are then also integrated and demonstrated in WP5 in T5.3. Regarding standardization, AIT contributes to WP8 within T8.1, specifically with regards to ETSI and ISO/IEC. Finally, the team contributes to the dissemination activities within WP9 mainly in T9.3, e.g., through research publications or summer schools.

Expected benefits: AIT expects to benefit from its participation to CyberSec4Europe in various ways, including, research, education, and community building. Concerning research, AIT plans to actively contribute to the scientific progress being made and produce high quality results published in renowned conferences and journals in order to gain visibility also beyond the project. Regarding education, the involved research group at AIT aims to foster collaborations with the involved universities in order to find efficient means to host MSc and PhD students which are externally supervised by partner institutions. Finally, concerning community building, AIT expects to strengthen its relations with other universities, research centers and industrial participants and to improve its coordination with the other participants in novel research, innovation and development activities in cybersecurity.

4.1.5.2.1 Research proposal

Description: Use of CyberSec4Europe results, capabilities and networking for further national and European projects and project proposals
Geography: Austria; Europe
Partners: Proposals have already been submitted together with, e.g., GUF, TDL, CYBER, and CONCEPT
Context: To be used during the project
WP: Mainly WP3 and WP5

4.1.5.2.2 Research proposal

Description: Usage of the project's results for further research proposals in the area of cybersecurity
Geography: Austria; Europe
Context: To be used after the project
WP: Mainly WP3 and WP5

4.1.5.2.3 Technical component

Description: Existing knowledge and assets, for example, on anonymous credentials or secure multi-party computation will be extended by project results and integrated into prototypes and products with customers and commercialisation partners in the mid future
Benefits: Increased functionality and higher security guarantees for existing prototypes and demonstrators, increasing the chances for successful commercialisation
Ownership: Dual licence agreement
Context: Update of pre-existing asset, to be exploited after the project
WP: WP3 and WP5

4.1.5.3 Computer Technology Institute and Press "Diophantus" (CTI)

Research and technology organisation, Greece

Role in project: CTI participates in task T5.3, Trustworthiness in Digital Life (Privacy-preserving Identity Management for public sector including e-Government and higher Education), based on the expertise explained below.

CTI's expertise in Attribute Based Credentials are brought to the project as a demonstration case within the context of WP5 in the field of IdM (Identity Management) with privacy preserving properties.

Expected benefits: Among the major goals of CTI is its involvement in security and privacy services for the state and its governmental institutions. Currently, CTI acts as security advisor for the Greek Ministry of Education while it offers penetration testing and security analysis services based on it Security Division personnel. CTI will deploy the expertise from its participation in the project to enhance its expertise in cybersecurity services through information exchange with other participants as well as hands-on experience with the rest of the demonstration cases in WP5.

4.1.5.3.1 Educational course

Description: Use project's identity management platform for the omprovment of courses in the area of PETs
Geography: Greece
Partners: Proposals have already been submitted together with, e.g., GUF, TDL, CYBER, and CONCEPT
Context: Update of pre-existing asset, to be used after the project
WP: Mainly WP3 and WP5

4.1.5.3.2 Educational course

Description: CTI team members give ICT security and privacy courses which they will enhance using material from deliverables and the projects' results.
Audience: All students (approx 600) from the Department of Informatics and Telecommunications of the University of Ioannina and the Business Administration Department, University of Patras
Geography: Greece
Partners: Mainly WP5 partners
Context: Update of pre-existing asset, used during the project
WP: All, but especially WP5 pilot services

4.1.5.3.3 Research proposal

Description: Use of CyberSec4Europe results, capabilities and networking for further national and European projects and project proposals
Geography: Greece; Europe
Context: Update of pre-existing asset, to be used after the project
WP: WP3 and WP5

4.1.5.3.4 Research proposal

Description: CTI will investigate the possibility of submitting a new proposal within the Cybersecurity/ICT Security fields
Geography: CTI
Context: New asset, to be used after the project
Partners: All project partners, potentially but mainly GUF and WP5 partners.
WP: WP3 and WP5

4.1.5.3.5 Technical component

Description: Improving the identity management demonstrator in order to be applicable to other domains except the education sector like monitoring activity report systems etc
Benefits: Increased functionality and higher security guarantees for existing IdM demonstrator, increasing the chances for successful commercialisation
Context: Update of pre-existing asset, developed during the project and to be commercialised after the project
Partners: AIT, UMU
WP: WP5 / T5.3

4.1.5.3.6 Technical component

Description: Adapting to the developed demonstrator various services like cloud deposit for credentials or integration with other security mechanisms
Benefits: Increased functionality and higher security guarantees for existing IdM demonstrator, increasing the chances for successful commercialization
Context: Update of pre-existing asset, developed during the project and to be commercialised after the project
Partners: AIT, UMU
WP: WP3 and WP5

4.1.5.3.7 Service

Description: CTI will exploit, mainly WP5 results but also all project results, to enhancing its penetration testing methodology which it provides as a service in Greece.
Benefits: All Greek organisations (private and public sector alike).
Context: Update of pre-existing asset, to be commercialised after the project
Partners: CTI team members mainly
WP: WP5 and all

4.1.5.3.8 Internal processes

Description: CTI will incorporate components developed within WP3 in its position application submission portal in order to enhance it with privacy preserving and anonymity features.
Benefits: All potential applicants for positions within CTI, from all over Greece
Context: Update of pre-existing asset, to be used during and after the project
Partners: WP5 / T5.3 partners
WP: WP5

4.1.5.4 Consiglio Nazionale delle Richerche (CNR)

Research institute, Italy

Role in project: CNR is mainly active in: WP3 to identify, develop and integrate the security techniques and methodologies needed by CyberSec4Europe, coherently with the expertise and experience listed below. In particular CNR is active in tasks 3.2, 3.3, 3.4, 3.5, 3.6 and 3.7, addressing and encompassing all methodologies and approaches, also on their development and mutual integration side. In WP5, task "Smart Cities" has been selected to demonstrate what is done in WP3 in a challenging environment, where all security requirements in the broader sense present.

Expected benefits: CNR will have benefits from CyberSec4Europe along three main axes: increase of its knowledge in cyber security, both in terms of technologies and methodologies, and also in terms of their implementation and management; increase and make stronger its network of contacts and relationship with European entities and institutions involved in cyber security research and development: cyber security is a global challenge, requiring coordinated and distributed answers. Last but not least, the dissemination of the project results in university and PhD courses, as long as, in consultancy to companies.

4.1.5.4.1 Technical component

Description: **GENERAL_D** (Gdpr-based EnforcemeNt of pERsonAL Data)
Geography: Italy; Europe; sometimes global
Ownership: Not yet defined
Context: New asset, developed further during the course of the project
WP: WP3/T3.2, WP4/T4.10 and WP5/T5.7

4.1.5.4.2 Research proposal

Description: Usage of CyberSec4Europe results, capabilities, and networking assets for further European and national public and industry projects
Geography: Italy; Europe; sometimes global
Context: Update of pre-existing asset, developed further during the course of the project
WP: All

4.1.5.5 Fondazione Bruno Kessler (FBK)

Research institute, Italy

Role in project: FBK is a third party partner of the University of Trento

4.1.5.5.1 Research proposal

Description: Exploit the improvement on existing assets carried out within the CyberSec4Europe project to propose added-value tools for further European and national public and industry projects
Geography: Italy, Europe; sometimes global
Ownership: Apache 2.0 licence
Context: Update of pre-existing asset, developed further during the course of the project and afterwards
WP: WP3 / T3.4

4.1.5.5.2 Research proposal

Description: Usage of the collaborative research on adversarial machine learning initiated in CyberSec4Europe for further European and national public and industry projects
Geography: Italy, Europe; sometimes global
Partners: KUL
Context: A new asset, to be used after the project
WP: WP3 / T3.4

4.1.5.6 Foundation for Research and Technology Hellas (FORTH)

Research institute, Greece

Role in project: FORTH leads WP4 Research Roadmap.

Expected benefits: By participating in the project FORTH expects to contribute its expertise in the area of cybersecurity, road-mapping, and policy making. At the same time, FORTH will significantly increase its expertise in this area and will have the opportunity to make an impact. In this capacity, FORTH will be able to help at various Strategic Committees on planning and policy making both in Europe and in Greece.

4.1.5.6.1 Research proposal

Description: Usage of the project's results for further research proposals in the area of cybersecurity
Geography: EU
Context: To be used after the project
WP: All

4.1.5.6.2 Service

Description: Use project's results in the preparation of policy documents in the area of cybersecurity and privacy
Geography: EU
Context: To be used after the project
WP: All

4.1.5.6.3 Education course

Description: Use project's cyber ranges for the improvement of courses in the area of experimental security
Audience: 50-100 students
Context: To be used after the project
WP: All

4.1.5.7 SINTEF (SINTEF)

Research institute, Norway

Role in project: SINTEF is focused mainly on WP3, in a task on secure software development (T3.3), in WP5 on maritime cyber security (T5.5) and in WP9 on dissemination and exploitation activities.

Expected benefits: SINTEF's interest in the results of the project are two-fold:

(1) extending its competence in the field of cybersecurity and ist practical application. Its basic research activities in the area will be validated internally and with the other organisations involved in this project, opening up more business opportunities for contract research for Norwegian and international customers;

(2) the opportunity to use project results to develop technology and services in the wider area of cybersecurity, which is gaining more importance within the research foundation.

4.1.5.7.1 Technical component

Description: Our tool-supported methods **CORAS** and **Bowtie+** will be adapted to be used in a smart city case, thus extending the usage domains of our approaches.
Benefits: Consolidated software development lifecycle
Audience: The software development / software security community
Partners: DTU
Externals: Kongsberg Seatex, Navtor, Kongsberg Defence and Aerospace, The Norwegian Maritime Authority and The Norwegian Coastal Administration.
Context: Update of pre-existing asset, developed further during the course of the project
WP: WP3

4.1.5.7.2 Technical component

Description: Implement and test our VDES radio solution for secure communication (ship-to-shore and ship-to-ship communication) in a real (production) maritime environment.
Benefits: Strengthened secure communication for the maritime sector
Partners: CYBER
Externals: Kongsberg Seatex, Navtor, Kongsberg Defence and Aerospace, The Norwegian Maritime Authority and The Norwegian Coastal Administration.
Context: Update of pre-existing asset, developed further during the course of the project
WP: WP5

4.1.5.7.3 Marketing

Description: Publish scientific papers based on the experiences gained from improving and using **Bowtie+**, **CORAS**, and secure maritime communication.
Benefits: Publicity in the scientific community and the industry gaining potential customers for future projects
Partners: CYBER
Externals: Kongsberg Seatex, Navtor, Kongsberg Defence and Aerospace, The Norwegian Maritime Authority and The Norwegian Coastal Administration.
Context: New development, developed further during the course of the project
WP: WP3 and WP5

4.1.5.7.4 Research proposal

Description: Use the competence gained via the literature survey on indicators for risk assessment to develop new projects addressing identified challenges/gaps.
Benefits: Research proposals accepted by the Research Council of Norway and the European Commission

Externals: Kongsberg Seatex, Navtor, Kongsberg Defence and Aerospace, The Norwegian Maritime Authority and The Norwegian Coastal Administration.
Context: Developed during the course of the project
WP: WP3

4.1.5.8 VTT Technical Research Centre of Finland (VTT)

Research centre, Finland

Role in project: VTT leads several tasks, for example task 3.6. "Usable Security", which focuses on using automation and artificial intelligence to support the end users in their normal work as well as providing tools for users to improve their security.

4.1.5.8.1 Technical component

Description: Cryptovault is an application for managing private keys in trusted execution environment. Cryptovault provides secure method for key backup.
Benefits: More reliable and independent account back-up method compared to current user-controlled back-up methods
Context: Update of pre-existing asset, developed further during the course of the project and to be commercialised afterwards
WP: WP3 / T3.2

4.1.5.8.2 Technical component

Description: **EEVEHAC** (End-to-End Visualizably Encrypted and Human Authenticated Channel) combines human authenticated key exchange and visualizable encryption into a single, human understandable system.
Benefits: Enhancing user understanding on the security status of their digital life. Exploring new research directions in the scientific community.
Partners: UPS-IRIT
Context: New asset, developed further during the course of the project and to be commercialised afterwards
WP: WP3 / T3.6

4.1.5.8.3 Research proposal

Description: Usage of CyberSec4Europe design of education and professional framework for further European and national public and industry projects and collaboration
Geography: Europe
Partners: Possibly
Context: To be developed after the end of the project
WP: WP6 / T6.2

4.1.6 Software Vendors

4.1.6.1 Atos Spain

Software vendor/consultancy, Spain

Role in project:

- Technology provider (cybersecurity, cloud-supporting security mechanisms, and security information sharing).
- Commercialisation and delivery to market of CyberSec4Europe results.
- Leader of two demonstration cases T5.4 Incident Reporting and T5.6 Medical Data Exchange, being the main link with end customers and with different working groups in Europe.

Expected benefits: Atos seeks to enhance its delivery of solutions to its customers in Financial Services, by means of improved protection of the infrastructures that Atos delivers or manages for our customers.

4.1.6.1.1 Product

Description: The Threat Intelligence Integrator (**TIE**) is able to correlate static and real-time information, associated with the monitored infrastructure, with cybersecurity related data coming from external OSINT sources, through a heuristic.
Benefits: Cost and time savings: less time wasting for IoC assessment and management
Ownership: Proprietary licence
Context: An existing Atos asset, improved during the course of the project
WP: WP3/T3.4 and WP5/T5.4

4.1.6.1.2 Product

Description: **DANS** is an anonymisation service based on the data anonymization Java tool that provides different privacy models to enable the application of certain privacy criteria over a specific dataset.
Benefits: Compliance
Ownership: Open source
Context: Improved during the course of the project
WP: WP5/T5.6

4.1.6.1.3 Product

Description: **SPEIDI** is a connectivity eIDAS-based solution intended to provide a hub or proxy service between the private service provider domain and the European national eIDAS nodes.
Benefits: Cost and time saving during the integration of online service providers (OSP) with eIDAS infrastructure
Ownership: Open source
Context: Improved during the course of the project
WP: WP5/T5.6

4.1.6.1.4 Product

Description: The Atos Incident Reporting Engine (**AIRE**) is a tool that will help in the mandatory incident reporting to different Supervisory Authorities. It will receive in real-time incidents to be reported and user, depending on his/her role, will be able to classify them, to confirm the classification (managerial judgement) and carry out the reporting process to the competent authorities selected.

Benefits: Compliance, cost and time saving
Ownership: Open source with some proprietary code. Developed by Atos with background knowledge from partners. Ongoing discussion with partners
Partners: BBVA, Intesa Sanpaolo
Context: Developed during the course of the project
WP: WP3/T3.4 and WP5/T5.4

4.1.6.2 Cybernetica

Software vendor/consultancy, Estonia

Role in project:

- Cybernetica leads WP8 – Standardisation. It has had the same role in previous FP7/H2020 funded projects. It maintains close connection with the Estonian Centre for Standardisation, facilitating the translation of international standards into Estonian, and thereby promoting Estonian-language terminology in the area of information systems' security. Cybernetica has also been active in ISO, leading the standardisation efforts in privacy area.
- Cybernetica participates in the maritime transportation security demonstration case. This fits perfectly with Cybernetica's business activities in the area of maritime surveillance and communications systems. Cybernetica also participates in other demonstration cases that can use its research results, mostly in the area of privacy-preserving computation.
- Cybernetica participates in WP3, and leads Task 3.8. It performs research in areas where it has experience (privacy-preserving computations, blockchain, security and privacy analysis and measurement of systems).
- In detail, CYBER participates in WP3 (Tasks 3.2, 3.3, 3.8), WP5 (Task 5.5) and WP8 (Tasks 8.1, 8.2, 8.3)

Expected benefits:

- Cybernetica will perform research it considers commercially relevant for itself, including privacy-preserving computations, long-term integrity preservation, maritime security.
- Cybernetica will make contacts, and work together with potential users of its technologies. It will also receive validation to its technologies through the project, which will allow it to widen its commercial reach.

4.1.6.2.1 Product

Description: Using the Sharemind asset for privacy-preserving machine learning of Rescue Board and National Census data.
Benefits: The asset will be tested whether using secure multi-party computation for privacy-preserving machine learning is feasible on these data.
Audience: Government institutions, industry, scientists.
Geography: Currently national (Estonia)
Ownership: Academic licence
Context: Update of pre-existing asset, improved during the course of the project
WP: WP3/T3.2

4.1.6.2.2 Service

Description: Privacy-enhanced business process models for use cases in tasks 5.5 and 5.6
Benefits: Leakage analysis was performed on the use cases defined in tasks 5.5 and 5.6.
Audience: Project partners, product owners, industry.

Geography: EU
Ownership: Open source licence
Partners: UPRC and Atos
Context: Update of pre-existing asset, used within the project
WP: WP3/T3.3, WP5/T5.5 and WP5/T5.6

4.1.6.2.3 Product

Description: Using the Sharemind asset for privacy-preserving detection of money laundering
Benefits: Implementing a prototype for privacy-preserving analysis of money laundering data at the Global Anti-Money Laundering and Financial Crime TechSprint.
Audience: Industry.
Geography: EU
Ownership: Academic licence
Partners: UPRC and Atos
Context: Update of pre-existing asset, used within the project
WP: WP3/T3.2 and WP5/T5.1

4.1.6.3 Dawex (DAWEX)

Software vendor / data marketplace exchange, France

Role in project: Dawex works on the 5.6 medical demonstration case, by providing its global data marketplace to the project. It defines the requirements to develop the solutions addressing cybersecurity challenges, and integrate them in the platform. In a second phase, it will enable medical data exchange using these innovations, to test them, gather feedbacks from the data providers and data suppliers, and improve the outcomes of the project.

It also brings its business, technical and legal expertise on data exchange (mainly in WP3) to ensure the innovations remain in line with what the market expects. Finally, Dawex contributes to the other WPs depending on the needs of the project

Expected benefits: Dawex will benefit from the innovations developed during the project funding; we will have the possibility to integrate in our platform the solutions the Consortium will build to address the cybersecurity challenges identified. It will allow us to improve our resilience, the level of security of our solution, by implementing the most innovative technologies. Doing so, Dawex will increase trust among the companies using our platform, which is a key factor of success in our market.

4.1.6.3.1 Internal processes

Description: Exploitation of user feedback gathered during the T.5.6 pilot. Very useful insights to better understand challenges and expectations of this kind of user (in the medical area) that is for now quite far from Dawex's main value proposition
Benefits: Improve user experience in Dawex solutions and help to penetrate the health data market
Ownership: None
Context: Update of pre-existing asset, improved during the course of the project
WP: WP5/T5.6

4.1.6.3.2 Service

Description: DANS service (data anonymisation) developed by Atos. A new service that can be provided to Dawex clients before they want to commercialise or exchange data on our platform
Benefits: Enlarge the scope of services offered to Dawex clients
Ownership: None
Partners: Atos
Context: A new asset, used during the project
WP: WP5/T5.6

4.1.6.4 Engineering Ingegneria Informatica S.p.A (ENG)

Software vendor / consultancy, Italy

Role in project:

- Technology provider (cybersecurity risk assessments, social engineering cyber-security solutions, GDPR solutions for citizens and public administrations, Open Innovation for city cybersecurity strategy co-design).
- Link with public administrations and with different working groups in Europe.
- Link with OASC (Open Agile Smart Cities).

Expected benefits: ENG benefits deriving from the CyberSec4Europe participation include:

- Carry over the CyberSec4Europe results to be included in its overall security services offering, combining it with other existing services (ENG offers cybersecurity services transversally through a dedicated business unit, D.HUB and vertically through sector focused business units)
- The improvement of its offer concerning privacy and GDPR–compliant tools and services addressing Smart City domain. In particular, the results of CyberSec4Europe will be passed to Municipia Spa, the company of the Group that addresses the public sector market

4.1.6.4.1 Service

Description: This exploitation aims at enlarging the ENG cybersecurity offer through the inclusion of additional services that are based on the prototypes validated by the activities of CyberSec4Europe
Benefits: The main channel for this transversal exploitation is the business unit dedicated to cybersecurity, Cybertech, which will get the opportunity to evolve the CyberSec4Europe outcomes to a full-fledged Social Driven Vulnerability Assessment (SDVA) thus enlarging its offer for the assessment and management of the cybersecurity risks. CyberTech is a large organisation with a large customer base and sites in seven EU countries
Geography: Italy, Germany, Norway, Serbia, Sweden, Spain and Switzerland
Ownership: Apache License 2.0
Partners: GEN
Context: Update of pre-existing asset, improved during the course of the project for exploitation after the end of the project
WP: WP5/T5.7

4.1.6.4.2 Marketing

Description: This exploitation aims at reinforcing the ENG commercial proposition by providing successful case studies to ENG customers in the public administration, as well as to help in the acquisition of new ones

Benefits: The main channel for this vertical explotation is represented by Municipia, the ENG company that supports local public administrations (LPAs) in their digital transformation process. In particular, the SDVA campaign conducted in Genova as part of the CyberSec4Europe activities could be used by Municipia as a success case when interacting with its customer base.

Scope: With its 15 operational sites, Municipia currently provides its services to around 1,000 Italian municipalities.

Audience: It provides a relevant channel for the exploitation of CyberSec4Europe's results to Italian LPAs.

Partners: GEN

Context: A new exploitable result, developed during the project

WP: WP5/T5.7

4.1.6.4.3 Research Proposal

Description: To build partnerships with other research institutions and facilitate collaboration with industry

Partners: UMU, UNITN and FORTH

Context: To be leveraged after the project

WP: WP5

4.1.6.5 NEC Laboratories Europe GmbH (NEC)

Industry, Germany

Role in project: NEC is involved in securing a blockchain platform for relevant use cases and on device security to devise TEE-based solutions to ensure high performance privacy processing over encrypted data. NEC also works on use cases for financial and supply chain management to provide relevant requirements for the technologies to be developed.

In WP3 of the project, NEC works on security and privacy enablers related to public and private blockchain advancements based on its experience in previous projects in applying these to storage, financial and supply-chain application areas. In addition, NEC builds on its experience in device security to contribute to securing devices based on secure hardware as well as attestation of properly running critical software.

Within WP5, besides leading the overall work package, NEC specifically contributes to the demonstration case for supply-chain management using its experience in applying blockchain to this domain. NEC further contributes with its security experience to new financial applications related to the PSD2 Directive.

Expected benefits: NEC is interested in devising, analysing, and implementing secure blockchain technologies, with the aim of offering differentiating services for its customers.

NEC plans to use the project outcomes to enhance current products in this area by focusing on production-ready components, thereby making them more attractive and competitive in the market.

4.1.6.5.1 Technical component

Description: Distributed protocol enabling participating users to reach consensus on a shared ledger of transactions, despite Byzantine failures, in permissioned and permissionless settings.
Audience: Global applicability: any group of organisations or stakeholders who are working together and do not rely on a trusted third party
Ownership: Proprietary
Context: New asset, used within the project and afterwards
WP: WP5 / T5.1 and T5.2

4.1.6.5.2 Product / Solution

Description: Ready-to-use platform for instantiating blockchain protocols and related applications.
Audience: Global applicability: across several industries including but not limited to finance, banking, supply chain and identity management
Ownership: Proprietary
Context: Update of pre-existing asset, used within the project and afterwards
WP: WP5 / T5.1 and T5.2

4.1.6.6 Siemens AG (SIE)

Industry, Germany

Role in project: Siemens provides challenges, problems and partially solutions to the "Security and Integrity of the Supply Chain" use case. Siemens also revises proposed solutions of the participants and evaluates them according to the requirements that are being defined within the project.

Expected benefits: As systems become more complex and the pressure to use standard communication protocols, the attack surface is increasing. The main benefit will be to develop techniques and expertise to counter these developments. Since the design, development and operation of critical infrastructures is increasingly a distributed process, it is necessary to develop a strong technical working platform with the different security centers to understand and manage the emerging risks. We expect from this project also a strengthening of our security network.

4.1.6.6.1 Product / Solution

Description: Workflow compliance
Benefits: Siemens are developing a language and tools to specify and enforce distributed workflows. We see company internal use case that can/will make use of this technology.
Ownership: Open source with some proprietary code
Partners: NEC, University of Malaga
Context: An existing asset, being used during the project
WP: WP5/T5.2

4.1.6.6.2 Product / Solution

Description: Workflow compliance accountability

Benefits: Siemens are developing a protocol for secure 'blaming' in case of disputes. In the context of CyberSec4Europe we will (together with NEC) evaluate conflict resolution techniques which are benefitial/required for distributed supply chains.
Ownership: Open source with some proprietary code
Partners: NEC, University of Malaga
Context: To be exploited after the end of the project
WP: WP5/T5.2

4.1.7 Universities

4.1.7.1 Johann Wolfgang Goethe-Universität Frankfurt (GUF)

University, Germany

Role in project: GUF, with its experience in successful coordination of EU projects, is the coordinator of the CyberSec4Europe project. In addition, GUF will participate in all work packages. In particular, it leads the design of the governance structure in T2.3 and the assessment of the appropriateness of existing standardisation procedures for the cybersecurity goals in T8.3. In work package 3, it participates in the research and integration on cybersecurity enablers and underlying technologies (T3.2), in usable security (T3.6), regulatory sources for citizen-friendly goals (T3.7), in continuous scouting (T3.9) and the impact on society (T3.10). Then, it participates in maintaining contacts with European standards developing organisations (T8.1), certification (T8.3), and all three tasks connected to work package 10.

Expected benefits: GUF expects benefits through research opportunities, actively contributing to academic research and produce scientific literature based on the findings. Furthermore, being responsible for project management, GUF plans to sharpen its profile as a central institution at the cutting edge of European cybersecurity and privacy.

4.1.7.1.1 Educational course

Description: Use of CyberSec4Europe results in Master and Bachelor courses e.g. on business informatics, information and communications security, privacy, mobile communications, and their applications
Audience: Depending on course between 10 and 350 students per course
Geography: Frankfurt, including short and long term guest students from all over the world
Context: Update of pre-existing course, used during and after the project
WP: All

4.1.7.1.2 Research proposal

Description: Usage of CyberSec4Europe results, capabilities, and networking assets for further European and national public and industry projects
Geography: Germany, Europe, also global
Context: Update of pre-existing proposal, used during and after the project
WP: All

4.1.7.2 JAMK University of Applied Sciences (JAMK)

University, Finland

Role in the project: JAMK participates in the development work in following WPs:

- WP3 T3.6 Usable security
- WP4 T4.7 Roadmap for industrial challenge 5.4
- WP5 T5.4 Incident Reporting, T5.6 Medical Data Platform
- WP6 T6.1 University Education, T6.3 Virtual Education
  T6.4 Cyber ranges as platform for education, training and exercises
- WP7 T7.1 Open tools and common portable virtual lab
  T7.2 Federated cyber range infrastructures for testing, validation and certification
- WP9 T9.1 Dissemination activities & reporting; T9.3 Spreading of excellence;
  T9.4 Raising cybersecurity awareness; T9.5 Exploitation & Sustainability

Expected benefits: Both scientific and technological benefits are anticipated through participation in the project. The network will be the base for long-lasting EU-wide co-operation in cybersecurity-related research in the future. Also technological benefits will be achieved by using the RGCE Cyber Range as a demonstration, exercise or education platform in the project. There is also commercial potential for the cyber range.

4.1.7.2.1 Educational course

Description: Flagship 1 exercise content and concept
Benefits: A remote cybersecurity exercise content and concept for English-speaking participants
Geography: Online
Ownership: Proprietary
Partners: BRNO, GUF, TDL, UNITN
Context: A new asset, used within the project
WP: T6.4

4.1.7.2.2 Educational course

Description: Massive Online Open Course (MOOC) on basic digital forensic investigation
Benefits: Experience on planning and conducting a free MOOC on cybersecurity that has a cyber range component included, available globally for English-speaking attendees. Also it was a preliminary task for Flagship 1
Geography: Online
Ownership: Proprietary
Partners: BRNO, GUF, TDL, UNITN
Context: A new asset, used during the project
WP: WP6

4.1.7.2.3 Technical component

Description: Flagship 1 technical solution
Benefits: The enviroment to implement a remote cybersecurity exercise utilising D7.1 requirement specification, built on top of RGCE
Geography: Online
Ownership: Proprietary
Partners: BRNO, GUF, TDL, UNITN
Context: Update of pre-existing asset, used within the project
WP: T7.1

4.1.7.2.4 Product / Solution

Description: Infocards for awareness raising
Benefits: Infocards about cybersecurity for English-speaking persons
Ownership: Currently proprietary
Partners: TDL
Context: Update of pre-existing asset, used during the project
WP: WP9

4.1.7.2.5 Marketing

Description: Flagship 1 event website page
Benefits: Awareness raising on cyber security exercise benefits
Ownership: Proprietary
Partners: GUF, TDL
Context: A new asset, used during the project
WP: WP9

4.1.7.3 Karlstad University (KAU)

University, Sweden

Role in project: KAU contributes to cybersecurity research and development in WP3, with a focus on T3.6 on usable security. It also contributes to WP6 with a focus on the development of MOOC on cybersecurity and to the vertical stakeholders engagement in WP4.

Expected benefits: KAU will benefit by increasing its research excellence and cooperation in areas such as usable security and privacy and with expanding MOOCs offered in cybersecurity for internal and external students including part-time industrial students.

4.1.7.3.1 Educational course

Description: Improvements and update of KAU's MOOCs, especially the one on "Privacy by Design", in compliance with the Cybersecurity MOOC quality criteria
Benefits: Improved quality of our MOOC
Geography: Online
Context: Update of pre-existing asset, used during the project and afterwards
WP: WP6

4.1.7.3.2 Educational course

Description: Use of the online cyber range course elements for a new "Ethical Hacking" course at KAU
Benefits: New education of high interest, also for local industry in Karlstad
Geography: Online
Partners: JAMK
Context: A new asset, used during the project and afterwards
WP: WP6

4.1.7.3.3 Technical component

Description: Use of anonymous credentials for pseudonymously answering data subject requests for pseudonymous data
Benefits: A new privacy-preserving application that will be especally useful for medical applications
Partners: AIT
Context: A new asset, used during the project
WP: WP3 and WP6

4.1.7.4 KU Leuven (KUL)

University, Belgium

Role in the project: The DistriNet reseach group of KUL contributes in WP3 its security analytics and (adversarial) machine learning expertise in the area of behavioral authentication and security incident analysis, as well as its knowledge on the secure software development life-cycle. Given its know-how, KUL leads Task 3.4 on security intelligence. KUL contributes to the strategic roadmaps in WP4 with a particular focus on incident reporting as the industrial challenge (task 4.7). Additionally, as a university, KUL participates in education and training, targeting both academic and professional audiences, thereby contributing to WP9, for example, through the SecAppDev event. It collaborates in the spreading of excellence in task 9.3, not only through dissemination of research results in top security conferences and journals, but also through the organisation of international security events, such as ESSoS.

Expected benefits: KUL will benefit from its participation in the project by enhancing its security knowledge and expertise, and will be able to advance its research roadmap through collaboration with its industrial and academic project participants. The project will most likely lead to a more intensive and innovative exploitation.

4.1.7.4.1 Research proposal

Description: Usage of the project's results for further research proposals in the area of cybersecurity
Geography: Belgium; Europe
Context: Update of pre-existing asset, to be continued after the project
WP: WP3/T3.4

4.1.7.4.2 Technical component

Description: **TATIS** software asset for enhanced threat intelligence sharing
Geography: Belgium; Europe
Ownership: Not yet defined
Context: Update of pre-existing asset, used within the project
WP: WP3/T3.4

4.1.7.5 Masaryk University (BRNO)

University, Czech Republic

Role in project: BRNO is leader of WP7: Open tools and infrastructures for certification and validation; in particular Masaryk University leads T7.1 on open tools. Furthermore, MU provides the open cyber range with selected tool for specific training uses for T6.4, is involved in activities

of T7.2, select example tools for one certification showcase and suggests tools and cyber ranges in T7.3 and examines the exploitation of open tools for standardization procedures and related activities in T8.3.

Expected benefits: Exposing the recent research outcomes to the wide community and namely to the industry, where we focused mainly on national partners so far. With the proposed project, our objective is to take this further, and to build on very recent experience, e.g., assistance to national security teams and e-ID providers in Estonia, Slovakia and other countries with the ROCA vulnerability discovered at our institution.

4.1.7.5.1 Educational course

Description: Use of CyberSec4Europe results in Master and Bachelor courses e.g. on business informatics, information and communications security, privacy, mobile communications, and their applications
Audience: Depending on course between 10 and 350 students per course
Geography: Brno, including short and long term guest students from all over the world
Context: Update of pre-existing course, used during and after the project
WP: All

4.1.7.5.2 Research proposal

Description: Usage of CyberSec4Europe results, capabilities, and networking assets for further European and national public and industry projects
Geography: Brno, Europe, also global
Context: Update of pre-existing proposal, used during and after the project
WP: All

4.1.7.6 Norwegian University of Science and Technology (NTNU)

University, Norway

Role in the project: The NTNU team provides expertise in cybersecurity, education and security awareness to the project. Furthermore, NTNU contributes in areas related to open tools and infrastructure for certification and validation, as well as activities related to dissemination and spreading of competence. NTNU participates in the following tasks:

- WP3 / T3.1 Common framework design; and T3.10 Impact on society
- WP4 / T4.8 Roadmap for industrial challenges (maritime transport)
- WP9 / T9.1 Dissemination activities and reporting; T9.3 Spreading of excellence; T9.4 Raising cybersecurity awareness; and T9.6 Policy recommendations

Expected benefits: Scientific, technological and societal benefits are anticipated through the participation in theproject, which will be projected on a national, regional, and European scale. The network will facilitate the long-lasting EU-wide co-operation in cybersecurity related research, and the establishment of the required communication channels for competence development and dissemination of expertise.

4.1.7.6.1 Educational course

Description: The security awareness measures, processes, and relevant experience that are developed within the WP9 are curently utilized to enhance educational activities that are offered by the department to relevant actors within the Norwegian industry
Audience: The primary audience of the related course consists of SMEs and corporations within the Norwegian industrial complex.
Geography: The material, although in Norwegian, is available and accessible online.
Context: Update of pre-existing course, used during the project
WP: WP3 and WP9

4.1.7.6.2 Service

Description: The security awareness measures, processes, and relevant experience that are developed within WP9 are curently utilised to enhance educational and research activities that are developed both within the Norwegian Cyber Range and the SFI-NORCICS for the establishment of education and training offerings within Norway
Audience: The aforementioned projects are national initiatives: thus the audience is primarily Norwegian actors.
Geography: Norway
Context: Update of pre-existing course, used during the project
WP: WP4 and WP9

4.1.7.6.3 Educational course

Description: Usage of CyberSec4Europe results in Master and Bachelor courses on information and communications security
Audience: Depending on course between 10 and 350 students per course
Geography: Norway
Context: Update of pre-existing course, used during the project and afterwards
WP: WP3, WP4 and WP9

4.1.7.6.4 Research proposal

Description: Usage of CyberSec4Europe results and capabilities further European and national public and industry projects
Geography: Norway; Europe
Context: Update of pre-existing proposal, used during the project
WP: WP3, WP6 and WP9

4.1.7.7 Politecnico di Torino (POLITO)

University, Italy

Role in project: POLITO is mainly active in:

- WP3 for the analysis and development of various cybersecurity techniques, and will lead task 3.9 (continuous scouting);
- WP4 to create the cybersecurity roadmap for supply chain and medical applications, given its involvement in these sectors, and leads T4.2 (legal and regulatory requirements);
- WP6 for curricula development and development of training material; and

- WP8 for standardisation activities with national (UN INFO) and international bodies (ETSI, TCG).

Expected benefits: POLITO will benefit from the outputs of the project in scientific terms (better knowledge in various cybersecurity areas and networking with major actors in the field), as well as technological (acquisition of better technologies for teaching and training about cybersecurity topics, e.g. cyber-ranges) and commercial (improved offer for strategic consultancy to companies and continuous education and training).

4.1.7.7.1 Educational course

Description: Use of CyberSec4Europe results in Bachelor, Master, and PhD courses e.g. on cybersecurity, business informatics, innovation management and their applications. Particular interest for the cyber range, with application both to technical and management tracks (e.g. we are currently discussing to use of the Flagship 1 exercise for short training courses for people already employed.
Audience: Depending on course between 10 and 200 students per course
Geography: Torino, (and rest of Italy via distance learning) including short and long term guest students from all over the world
Context: Update of pre-existing course, used during and after the project
WP: All

4.1.7.7.2 Research proposal

Description: Usage of CyberSec4Europe results, capabilities, and networking assets for further European and national public and industry projects. The most promising use cases are those related to open banking, supply chain security, and smart-cities as they are hot topics in Italy.
Geography: Torino (and rest of Italy), Europe, also global
Context: Update of pre-existing proposal, used during and after the project
WP: All

4.1.7.8 Delft University of Technology (TUD)

University, The Netherlands

Role in project: The TUD team leads WP2 and contributes to WP5.6. The team provides its expertise in cybersecurity and privacy technology and governance to the project. In particular TUD has expertise related to all elements of the classic feedback control loop that underlies all governance models: measure, decide, act & repeat. It has researched quantitative risk assessment, quantitative security metrics and internet measurement. It has developed cyber risk management methods and tools, security incentives and security governance policies. It has studied the impact of interventions and controls, method to increase user awareness, and usability for admins, users and providers. Regarding the technology, TUD has researched privacy enhancing technologies that is used in WP5.6.

Expected benefits: TUD expects to benefit from its participation in the project by being able to share research data more efficiently and more widely with EU Participants. It also expects to be able to conduct cutting edge research based on industry data from real-world settings.

4.1.7.8.1 Educational course

Description: Usage of CyberSec4Europe results in a Master course "Cybersecurity governance"
Audience: Depending on the enrolment, 50-100 students
Geography: Delft and Twente, with addition of short and long term guest students from all over the world)
Context: Update of pre-existing course, used during the project
WP: WP2

4.1.7.9 Technical University of Denmark (DTU)

University, Denmark

Role in project: DTU contributes to WP3 with research on proactive security, focusing on early stages of secure software development and secure-by-design principles, through the application and extension of formal methods for security. This is mostly reflected in DTU's leading role in task 3.3. DTU also contributes to security intelligence research in task 3.4 with a focus on intruder detection systems and log mining techniques. DTU also provides contributions to task 3.2, in particular related to identity management, cryptograpy and cryptanalysis, IoT, and Fog/Edge computing. DTU helps integrate WP3 results in the medical exchange demonstration (task 5.6) of WP5. DTU also leads task 9.3 on spreading of excellence to help promoting research results, technologies and best practices in cybersecurity. DTU also facilitates the collaboration between WP3 and WP4 (task 4.2) in the identification of research challenges to be addressed in the context of the project and beyond (in future larger programmes). Within WP6, DTU provides a review of existing Cyber Security MSc programmes in Europe for task 6.1, with a focus on Central Europe (DK, NL, DE, PL), and will be responsible for the process for Continuing Education courses of task 6.3.

Expected benefits: DTU will benefit from collaboration with strategic partners in the area of cybersecurity to become one of the leading research centers in Europe. Dissemination and collaboration will also help increase the impact of DTU's research in cybersecurity, in particular through publications in top-level venues. We also expect to enrich our education programmes in cybersecurity by establishing collaborations such as exchange and joint programs that will foster the mobility of students and teachers.

4.1.7.9.1 Research proposal

Description: National project on Security by Design
Benefits: Dissemination and exploitation of CyberSec4Europe results i
Geography: Denmark
WP: WP3/T3.3

4.1.7.9.2 Educational course

Description: Integraration of CyberSec4Europe results in MSc and BSc courses on security
Audience: Typically 100 students per course
Geography: Denmark
Context: Update of pre-existing course, to be used after the project
WP: All

4.1.7.9.3 Research proposal

Description: Usage of CyberSec4Europe results, capabilities, and networking assets for further European and national public and industry projects
Geography: Denmark; Europe
Context: To be used during the project and afterwards
WP: All

4.1.7.10 University College Dublin & LERO (UCD)

University, Ireland

Role in Project: UCD leads task 3.5 on adaptive security and contributes to task 3.6 on usable security and privacy. These activities are in line with some of the areas of expertise of the Lero research centre program of which UCD is a university member.

The expertise of Lero in the field of adaptive security is fundamental in supporting the activities of task 3.5, particularly in relation to the design and implementation of adaptive security systems from requirements elicitation to security control enforcement. Moreover Lero research has also proposed an asset-centric approach to elicit and model security requirement of software systems. This research is particularly relevant to support the activities of task 3.6 related to modelling and visualization of assets, security requirements and controls, user tasks, threats and attacks, and vulnerabilities and security risks.

Expected Benefits: Participation in the project will allow Lero to strengthen its scientific contribution in the field of adaptive security. It will allow developing security solutions that are proactive and that can satisfy new security goals or counteract security threats that were unknown at design time.

Lero will expand its research collaborations and will explore commercialization of the technological solutions delivered in the project with industrial partners.

4.1.7.10.1 Research proposal

Description: Benefit from the project's results for further research proposal to propose techniques to elicit and represent the adaptation factors that support engineering adaptive authentication. UCD has applied for a Science Foundation Ireland spoke project and are also planning to apply to the ‘Frontiers for the Future’ research programme.
Geography: Ireland
Context: Update of pre-existing proposal, used within the project
WP: T3.5

4.1.7.10.2 Research proposal

Description: Benefitting from the project's results and collaboration to apply to other EU-funded research proposals in the domain of adaptive security.
Geography: Ireland; Europe
Context: Update of pre-existing asset, to be used after the project
WP: T3.5

4.1.7.11 University of Cyprus (UCY)

University, Cyprus

Role in Project: UCY, through its SREC Group, contributes to several tasks of the WP3, WP4, and WP5 core technical WPs.

Expected Benefits: Innovative research in the area of systems security

4.1.7.11.1 Educational course

Description: Use project's cyberanges for the improvement of courses in the area of experimental security
Audience: Depending on the enrolment, 80-100 students
Geography: Cyprus
Context: Update of pre-existing course, to continue to be used after the project

4.1.7.12 University of Luxembourg (UNILU)

University, Luxembourg

Role in Project: UNILU's expertise contributes to the development of research advancements in the area of biomedical data protection, some of which is demonstrated in the medical data exchange use case. Focusing on biomedical data and relevant processing systems, UNILU is investigating mechanisms and techniques to reconcile sharing with privacy and integrity of high-risk data (e.g. genomics; highly sensitive EHRs, as well as other sectors), and study their integration, as incremental security and dependability measures for the high end of risk, to complement other measures considered in the project.

Expected Benefits: These techniques will empower the several stakeholders to perform sophisticated analyses not previously possible, due to the unbalanced risk tradeoffs between highly secure but extremely slow (crypto intensive) options, or high-performance but correspondingly very insecure counterparts.

These techniques will allow overcoming the risks of remote access and/or of processing in unprotected environments, such as public clouds, for critical data and operations in vertical sectors like e-health or e-finance. By putting these technologies in perspective with legal regulations, compliance with the latest frameworks, such as GDPR and NIS, is ensured. By ensuring differentiated IP protection silos according to criticality and/or provenance, coalitions of rational and non-mutually trusted parties may promote ambitious research projects otherwise impossible.

4.1.7.12.1 Educational course

Description: UNILU will integrate the project findings on genomic privacy and privacy-preserving data processing infrastructure in our master and PhD-level courses (e.g., on resilient computing)
Audience: Depending on the level of course between 10 and 350 students per course
Context: Update of pre-existing course, used during the project
WP: WP3

4.1.7.12.2 Research proposal

Description: UNILU aims to submit further research proposals related to the protection of critical information

Geography: Luxembourg; Europe
Context: Update of pre-existing asset, to be used after the project
WP: All

4.1.7.13 University of Malaga (UMA)

University, Spain

Role in project: UMA participates in most of CyberSec4Europe's work activities (WPs 3,4, 5, 8, 9 and 10). In particular, it contributes actively in the secure design of the common research framework and the road-mapping, especially in the aspects related to industrial environments.

Expected benefits: UMA will benefit from the participation in the project by increasing their capacity for enlarging the research group with new researchers. Also, UMA expect to increase their connection with the research community in cybersecurity as well as with the industry.

4.1.7.13.1 Service

Description: Privacy Manager for IoT: this asset is expected to help individuals retain control of their data by their geographically distributed IoT devices by taking advantage of the development of Edge Computing
Geography: Global, given the adoption of IoT and the rapid development of Edge Computing
Context: A new asset, to continue to be exploited after the project
WP: T3.2

4.1.7.13.2 Research proposal

Description: Use of CyberSec4Europe results, capabilities and networking for further national and European projects and project proposals
Geography: Spain; Europe
Context: Update of pre-existing proposal, used during and after the project
WP: All

4.1.7.14 University of Maribor (UM)

University, Slovenia

Role in project: The Faculty of Electrical Engineering and Computer Science (FERI) is actively involved as a contributor in several project tasks (WPs 3, 5, 6 and 9) and as a task leader (T3.7), based on its expertise in the fields of data protection, cybersecurity education and digital forensics. The data protection know-how FERI brings is in the areas of identification and privacy, as well as experience with blockchain technology.

- UM contributes to tasks 3.1 and 3.2 by investigating the blockchain technology as a technology and enabler for Trusted Execution Environments and investigating encryption schemes and other related cryptographic schemes tailored to IoT.
- UM further contributes in task 3.5 by investigating key research challenges for adaptive security compliance in dynamic environments and in task 3.6 by investigating current recommendations and/or guidelines for compliance of usable security and in the design of behavioural-based user authentication mechanisms.

- UM leads and contributes to task 3.7 and contributes to developing novel security awareness monitoring in task 3.10.
- Additionally, UM participates in tasks 4.2, 4.3, 4.4, 4.5, 4.6, 4.9 and 4.10 in which it contributes to the design of a research roadmap for different industrial challenges.
- UM contributes to tasks 6.1 and 6.2 by investigating curricula and reference need for the newer countries in the EU (SI, HU, HR, CZ, SK) and assessing mechanisms for a non-ICT workforce (lawyers, etc.). Finally, UM participates in task 9.4 by conducting an analysis of several SMEs and their compliance to GDPR, eIDAS and other regulations, whereby contributing with a local overview of such practices.

Expected benefits: UM anticipates further facilitating excellent state-of-the-art research and innovation and tightening its links to international participants from all sectors. The outcomes of the project will be also implemented in its curriculum and training for industry. During the project, UM anticipates tgrowing in technological knowledge with the exchange of know-how and experience that will enable the development and deployment of solutions with advanced security capabilities.

4.1.7.14.1 Educational course

Description: Use project's cyberanges for the improvement of courses in the area of experimental security
Audience: On average around 130 students per year (including foreign students) in the University of Maribor, and additional guest lectures (e.g. Ljubljana, Slovenia; Varaždin, Croatia) with around 80 students per year.
Geography: Slovenia; Croatia
Context: Update of pre-existing course, used during the project and to continue to be used after the project
WP: All (primarily WP3, WP4, and WP6)

4.1.7.14.2 Research proposal

Description: Usage of CyberSec4Europe results, capabilities, and networking assets for further European and national public and industry projects
Geography: Slovenia; Europe; possibly beyond Europe
Context: Update of pre-existing proposal, used during the project
WP: All

4.1.7.15 University of Murcia (UMU)

University, Spain

Role in project: UMU works on the validation of the governance model focusing on the research agenda and its testing.

- UMU is responsible for security and privacy enablers to be developed with a focus on authentication and authorization and the tasks related to privacy-preserving data sharing mechanism in task 3.2 and task 3.4 related to the privacy-preserving mechanism linked to user identity.
- UMU is also involved on the scouting activity, the impact of IdM aspects related to regulation especially eIDAS and the methodology for testing and validation for IoT. UMU is involved in gathering requirements from stakeholders and in mapping the research objectives of software on the roadmap.

- UMU contributes to the experimentation and validation of the demonstration case related to smart cities based on the collaboration with Murcia Municipality who have expressed interest in the project integrating the enabler with prototype components in order to solve privacy preservation aspects, and in e-Health based on the group's work on IoT security.
- Additionally, UMU participates in evaluating the educational situation on cybersecurity in Western Europe and in proposing educational content, targeting the academic sector. UMU contributes with the PEANA testbed for supporting testing and validation and also to the methodology for testing and certification.
- UMU is also active in the dissemination of publications.

Expected Benefits: UMU will benefit from the dissemination of the results due to its strong track on high impact journal and conference publication and also in the standardisation activities and the linkage with other regions

4.1.7.15.1 Technical component

Name: Mobile p-ABC
Description: Mobile p-ABC system, leveraged from FP7 ARIES project, uses Idemix ABC system. It is being used in first stage of T5.3 pilot.
Partners: AIT, CTI
Context: An existing asset, being used within the project
WP: WP3/T3.2 and WP5/T5.3

4.1.7.15.2 Technical component

Description: Self-sovereign distributed privacy-preserving p-ABC system leveraged and adapted to blockchain. Envisioned to be used in second-third stage of T5.3 pilot and in pilot T5.7.
Audience: Global
Benefits: Fully distributed approach, split up the role of the Identity Provider (IdP) into several authorities so that a single entity is not able to impersonate or track its user. Signed tokens and the ABC credentials are managed in a distributed way by several IdPs
Partners: AIT, CNR, CTI and Engineering
Context: Updated pre-existing asset developed in H2020 OLYMPUS project, being used within the project
WP: WP3/T3.2, WP5/T5.3 and WP5/T5.7

4.1.7.15.3 Research proposal

Description: Self-sovereign distributed privacy-preserving p-ABC system leveraged and adapted to blockchain, integration with eIDAS. Envisioned to be used in future research proposals and to be integrated in the EBSI (European Blockchain Services Infrastructure).
Audience: Global
Benefits: Fully distributed approach, split up the role of the Identity Provider (IdP) into several authorities so that a single entity is not able to impersonate or track its user. Signed tokens and the ABC credentials are managed in a distributed way by several IdPs
Partners: AIT, CNR, CTI and ENG

Context: Updated pre-existing asset developed in H2020 OLYMPUS project, to be exploited after the end of the project
WP: WP3/T3.2

4.1.7.16 University of Piraeus Research Center (UPRC)

University, Greece

Role in project: UPRC leads the demonstration use case related to the maritime transport sector. UPRC is also actively involved, mainly as a research participant, in research on cybersecurity enabling technologies (WP3), in research roadmapping for industrial challenges (WP4), in university education and training WP6), as well as dissemination activities (WP9) and in community building (WP10).

Expected benefits: UPRC expects to benefit from its participation to CyberSec4Europe in various ways, including, research, education, and community building. Concerning research, UPRC is expecting to actively participate in scientific research and to produce high quality scientific research publications in novel areas of cybersecurity. Concerning education, PRC expects to improve the educational material of both bachelor and master courses in the area of cybersecurity and privacy (SecLab is supporting an MSc course specifically targeted to information security). Finally, concerning community building, UPRC expects to strengthen its relations with other universities, research centres and industrial participants and to improve its coordination with the other participants in novel research, innovation and development activities in cybersecurity.

4.1.7.16.1 Educational course

Description: Utilisation of CyberSec4Europe progress and results in Master and Bachelor courses, such as information security governance, security architecture design, network security, information system security and penetration testing. The aim is to deliver to students and trainees the combined knowledge that is successively obtained during the project from the fruitful collaborative work of industry and cybersecurity research sectors and thus to enhance their security awareness in line with up-to-date sectorial methods and emerging technologies, such as methods for quick identification and adaptation to security threats, novel cyber-attack path discovery algorithms, evidence-based and scenario-based risk assessment approaches, innovative tools for software hardening and PKI services for secure maritime communications.
Audience: Depending on the course; typically between 30-80 students per Bachelor degree course and ranging from 10 to 30 per Master degree course (including guest students, i.e. Erasmus students)
Context: Update of pre-existing course, used during the project and to continue to be used after the project
WP: WP4, WP5 and WP9

4.1.7.16.2 Research proposal

Description: Usage of CyberSec4Europe results, capabilities, and networking assets for further European and national public and industry projects
Geography: Greece; Europe
Context: Update of pre-existing proposal, used during the project and to be continued afterwards
WP: All

4.1.7.16.3 Research proposal

Description: Utilisation of the project's results in developing new research proposals in the area of cybersecurity and maritime transport security
Geography: Greece; Europe
Context: Update of pre-existing proposal, used during the project and to be continued afterwards
WP: WP5 / T5.5

4.1.7.16.4 Technical component

Description: Enhancement of risk assessment platform with targeted security controls for software hardening - updated from pre-existing asset from H2020 MITIGATE
Geography: Europe
Context: Update of pre-existing proposal, used within the project
WP: WP5 / T5.5

4.1.7.17 University of Porto (C3P)

University, Portugal

Role in project: C3P participates in T3.2, T3.3 and T3.4, the smart cities demonstration case in T5.7, as well as the roadmap for industrial challenges for this demonstration case in T4.10.

Expected benefits: Scientific publications, patents and tech transfer for university startups/spinoffs

4.1.7.17.1 Technical component

Description: **ARGUS:** aims to provide a modular approach that uses the cloud-of-clouds to store persistent data and reduce upfront costs while allowing information to remain private and under users' control. We enhance usability by allowing users to share information among themselves by enabling computation, such as machine learning algorithms, without needing to reveal the raw data. In order to achieve this, we make use of semi-anonymization or anonymization methods for detecting potentially identifying data that would need protection from being leaked if it ends up being shared, either purposefully or accidentally!
Benefits: Global reach; a distributed approach
Ownership: Open source
Context: Developed further during the course of the project
WP: WP3/T3.3 and WP5/T5.7

4.1.7.18 Université Toulouse III Paul Sabatier (UPS) – Institut de Recherche en Informatique de Toulouse (IRIT)

University, France

Role in project: IRIT contributes to several workpackages, from developing technical solutions for the demonstration use cases, to community building and road-mapping. IRIT co-leads work on adaptive security and leads on vertical stakeholders engagement and consultation, and participates in clustering and collaboration activities with other cybersecurity projects.

Expected benefits: IRIT will benefit from its participation in CyberSec4Europe by enhancing its security knowledge and expertise, leveraging the acquired knowledge and technologies to improve its research, techonology transfer, and educational capabilities.

4.1.7.18.1 Technical component

Description: Self-sovereign identity management system over W3C web authentication and W3C verifiable credentials. Updated from **VCUCIM** that employs FIDO 1
Benefits: Global
Context: Update of pre-existing asset, developed further during the course of the project
WP: WP3/T3.5 and WP5/T5.1

4.1.7.18.2 Service

Description: Implementation of a CHECK-T in Toulouse
Benefits: Global
Partners: WP2 partners provide useful knowledge and insights
Context: Asset is expected to start during the project and to continue after the project's end
WP: WP2

4.1.7.19 University of Trento (UNITN)

University, Italy

Role in project: UNITN leads WP6 and will contribute to task 6.1, 6.3 and 6.4. Furthermore, UNITN is also actively involved in several WPs: in WP2, WP3, WP4, WP7 and WP9.

Expected benefits: UNITN expects to benefit from its participation in CyberSec4Europe in various ways, including extending and consolidating some of its research competences and extending its education offering. UNITN is expecting to actively participate in scientific research and to produce high quality scientific research publications in areas of cybersecurity. Concerning education, UNITN expects to improve the educational courses in the area of cybersecurity.

4.1.7.19.1 Educational course

Description: Usage of JAMK cyberrange in Master Course: Offensive Technology
Audience: Depending on course between 20 and 40 students per course
Geography: Trento (including short and long term guest students from all over the world)
Context: Update of pre-existing course, used within the project
Partners: JAMK
WP: All

4.1.7.19.2 Educational course

Description: Usage of JAMK Cyberrange in Cyber Challenge IT preparation course
Audience: Depending on course between 20 and 40 students per course
Geography: Trento
Context: Update of pre-existing course, used during the project and to be continued afterwards
Partners: JAMK
WP: All

4.1.7.19.3 Research proposal

Description: Usage of CyberSec4Europe results, capabilities, and networking assets for further European and national public and industry projects
Geography: Italy; Europe; sometimes global
Context: Update of pre-existing proposal, used during the project and to be continued afterwards
WP: All

4.2 Exploitation and Business Plan Summary

The following seven tables summarise the responses from all project partners itemised in the previous sub-sections:

Associations

Both associations or networks are focussed on expanding their reach and essentially leveraging and/or disseminating the results of the project to expand their activities to a wider community after the end of the project.

Associations		Technical component	Product or solution	Service	Education course	Research proposal	Marketing	Internal processes	Within	During	After
OASC	BE						1				1
TDL	BE					2	1	1		4	3
		0	0	0	0	2	2	1	0	4	4

Table 1: Associations

Businesses (Banks)

Businesses		Technical component	Product or solution	Service	Education course	Research proposal	Marketing	Internal processes	Within	During	After
BBVA	ES		1								1
I-BP	FR			1						1	1
ISGS	IT		1					1			1
		0	2	1	0	0	0	1	0	1	3

Table 2: Businesses (Banks)

Legal and Consultancy Firms

None of our SMEs, micro-SMEs or legal firms indicated any plans to exploit project results at present, although it is to be expected that this will change in future reports.

Legal and Consultancy Firms	Technical component	Product or solution	Service	Education course	Research proposal	Marketing	Internal processes	Within	During	After

ARCH	BE				1	2						3
CONCEPT	CH			2		1	1				4	4
ICITA	BL					1						
TLEX	BE			1		8					9	3
VAF	SK			1							1	1
		0	0	4	1	12	1	0		0	15	12

Table 3: Legal and consultancy firms

Local Government

Our one local public administration will continue to collaborate with its WP partner.

Local Government		Technical component	Product or solution	Service	Education course	Research proposal	Marketing	Internal processes		Within	During	After
GEN	IT											
		0	0	0	0	0	1	1		0	2	2

Table 4: Local government

Research Institutes

The primary interest of these institutions is in developing future research proposals based on their experience in the project, as well as further developing the technical components they introduced into WP3/WP5.

Research Institutes		Technical component	Product or solution	Service	Education course	Research proposal	Marketing	Internal processes		Within	During	After
ABI	IT					1					1	1
AIT	AT	1				2					1	2
CTI	GR	2		1	2	2		1			4	7
CNR	IT	1				2					2	
FBK	IT					2					1	2
FORTH	GR			1	1	1						3
SINTEF	NO	2				1	1				4	
VTT	FI	2				1					2	3
		8	0	2	3	11	1	1		0	15	18

Table 5: Research institutes

Software vendors

Not surprisingly, the interest of the large corporates is in developing further the products / technical components they introduced into the project via WP3 and WP5. The licences involved are mostly open source (or acacademic) with some proprietary IP introduced or developed during the project (see below).

Software Vendors		Technical component	Product or solution	Service	Education course	Research proposal	Marketing	Internal processes	Within	During	After
ATOS	ES		4							4	
CYBER	EE		2	1					2	1	
DAWEX	FR		1	1						2	2
ENG	IT			1		1	1			2	2
NEC	DE	1	1						2		2
SIE	DE		2					(1)		1	1
		1	10	3	0	1	1	0	4	10	7

Table 6: Software vendors

Universities

Not surprisingly, the interest of the large corporates is in developing further the products / technical components they introduced into the project via WP3 and WP5. The licences involved are mostly open source (or acacademic) with some proprietary IP introduced or developed during the project (see below).

Universities		Technical component	Product or solution	Service	Education course	Research proposal	Marketing	Internal processes	Within	During	After
GUF	DE				1	1				2	2
JAMK	FI	1	1		2		1		2	3	
KAU	SE	1			2					3	2
KUL	BE	1				1			1		1
BRNO	CZ					1					1
NTNU	NO			1	2	1				4	1
POLITO	IT					1					1
TUD	NL				1					1	
DTU	DK				1	2				2	3
UCD	IE					2			1		1
UCY	CY				1						1
UNILU	LU				1	1				1	1
UMA	ES			1		1				1	2
UM	SI				1	1				2	1
UMU	ES	2				1			2		1
UPRC	GR	1			1	2			1	3	3
C3P	PT	1								1	
IRIT	FR	1		1						2	1
UNITN	IT				2	1			1	2	2
		8	1	3	15	16	1	0	8	27	24

Table 7: Universities

All Categories	Technical component	Product or solution	Service	Education course	Research proposal	Marketing	Internal processes		Within	During	After
	17	13	13	19	42	7	4		12	74	70

Table 8: All categories

Although some of the.outcomes of the partner exploitation plans may at first be considered somewhat counterintuitive in terms of what might typically be expected of, say, a university, it is also not entirely surprising as it reflects the activities of the different types of organisations in the project itself. For example, the main software and technical component research activity, WP3, is led by a university (UMU) and all together comprises 17 universities and three research institutes.

It is also apparent that many organisations have not yet fully considered how or in what way they may leverage their participation in CyberSec4Europe. It is realistic to expect many if not all of this group of organisations to be more focused at the time of the next and the final reports [M36] and [M42].

5 Joint Exploitation

The overall exploitation objectives of CyberSec4Europe are described in the DoA[7] as being to:

- *provide strategic input to the Commission for the future set-up of a Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre, based on the governance model developed and tested in the project through the selected industrial challenges, harmonised through a set of concertation events with the other SU-ICT-03 projects;*
- *leverage individual organisational business plans as well as joint exploitation strategies using the outcomes of the project for future products and activities as well as patents and the generation of IPRs*

Typically we would expect to review the opportunities and plans for exploitation by the consortium as a whole, rather than by individual organisations. However, given the very nature of the project – a pilot or small scale simulacrum of the Network proposed in the legislation and outlined in the original call – CyberSec4Europe, like its sister pilot projects CONCORDIA, ECHO and SPARTA, is an amalgam of smaller projects and initiatives, some of which are interdependent as reflected to a large extent in the individual exploitation plans.

In addition to the above, there are two further considerations we would like to make that have become more apparent since the project started:

- Along with the other pilots, CyberSec4Europe has been encouraged to attract more partners as Associates to participate in the work of the project. Although CyberSec4Europe is only making travel funding available to Associates (a pre-pandemic decision!), these additional partners are invited, as appropriate, to attend meetings or to participate in project work

[7] DoA Annex 1 (part B) p.33

including making contributions to project deliverables. The CyberSec4Europe website provides an Associates page together with its own logotype.

- In the context of the Commission's initiative to build the European Cybersecurity Network starting with the four pilots and ECSO but with the intention to grow the Network to embrace a much wider stakeholder community, it is worth asking whether joint exploitation as familiar from most other H2020 projects should be re-evaluated. Although that is not the intention here, it is anticipated that a consolidated view of the legacy of the four pilots be the subject of inter-pilot discussions over the coming 12 months.

5.1 Exploitation and Business Plans

In order to understand better the realistic opportunities for joint exploitation, the structure of the project can be roughly broken down into four distinct segments:

- Governance, design and pilot (WP2)
- From research and innovation to industry (WP3-WP4-WP5)
- Education, training and standardisation (WP6-WP7-WP8)
- Communication and community building (WP9-WP10)

In terms of joint exploitation, these segments are reflected in the proposed exploitation strategy outlined in the project's DoA[8]:

Segment	Scope	Objective
WP2	Governance, design and pilot	To influence policymakers in both government and industry at the national and European level on continued cross-sector public-private collaboration in all aspects of cybersecurity
WP3-WP4-WP5	From research and innovation to industry	To persist the strong ties developed between industry and research organisations during the course of the project to further stimulate collaboration in cybersecurity research, in the context of a cybersecurity competence network with a central competence hub
WP6-WP7-WP8	Education, training	To strengthen cybersecurity capabilities across the EU through the establishment of templates for ongoing educational programs to improve cyber skills
	Standardisation	To improve standardisation in cybersecurity and in particular support for the European certification framework as specified in the Cybersecurity Act
WP9-WP10	Communication and community building	To continue awareness raising activities beyond the end of the project to reach out to vendors, service providers, businesses and citizens

Table 9: Joint exploitation objectives by WP

[8] DoA Annex 1 (part B) p.33

5.1.1 Governance

> *To influence policymakers in both government and industry at the national and European level on continued cross-sector public-private collaboration in all aspects of cybersecurity*

CyberSec4Europe has been very active in promoting and piloting its vision for a community-led governance model for the Centre and Network, through the concept of CHECKs (Community Hubs of Expertise in Cybersecurity Knowledge) as proposed in WP2 reports and news posts. We have already seen the piloting of embryonic CHECKs in the Occitanie region and in Spain. It was confirmed during the evening panel on 9 July 2020 that the concept of CHECKs is broadly supported.

From the beginning of the project, CyberSec4Europe has also sought to publicly engage in discussion relating to the progress of the legislation and to provide strategic input to post-legislation planning. Five evening panel involving senior representatives from the three European institutions (Parliament, Council and Commission) and other European institutions and agencies, notably the EDPS, ENISA and ECSO, to publicly discuss updates and future plans on the progress of the legislation and aspects of the how the network will interact with the centre in terms of governance models, as worked through WP2.

In addition to governance, CyberSec4Europe is also collecting policy recommendations based on the project's activities in a series of annual reports in task 9.6.

5.1.2 Research to Innovation

> *To persist the strong ties developed between industry and research organisations during the course of the project to further stimulate collaboration in cybersecurity research, in the context of a cybersecurity competence network with a central competence hub*

Each of these three areas of work have their own distinctive agendas but are also able to coalesce to create the innovative crossover from research to practical implementation, using software assets developed in one domain [WP3] and exploited in another [WP5]. The crossover in meeting specific requirements of the use case demonstrators started to take place during the second year of the project with dedicated meetings between the WP3 and WP5. For the partners associated with each task in WP3 and WP5, see Annex A and Annex B respectively.

5.1.3 Education and Training

> *To strengthen cybersecurity capabilities across the EU through the establishment of templates for ongoing educational programs to improve cyber skills*

Irrespective of whether they were directly involved in WP6/WP7, many if not most of the project partners from universiteis and research institutes have been active in participating and organising summer schools and MOOCs as well as improving educational courses through their participation in CyberSec4Europe, all of which can be expected to continue after the end of the project. These activities are reported in deliverables D9.5 and D9.10.

5.1.4 Standardisation

To improve standardisation in cybersecurity and in particular support for the European certification framework as specified in the Cybersecurity Act

A number of key partners, not only those involved in WP8, have participated in a wide range standardisation activities as reported in deliverables D8.1, D8.2, D10.1 and D10.2 which will continue after the end of the project. In particular, as reported in a news post, in 2019 CyberSec4Europe decided to apply for a liaison relationship with two SC27 Working Groups:

- WG 2 Cryptography and security mechanisms; and
- WG 5 Identity management and privacy technologies

This initiated an intensive process including an analysis of CyberSec4Europe's constitution by the ISO Central Secretariat, an assessment of CyberSec4Europe's competencies by both WG 2 and WG 5 as represented by Stephan Krenn (AIT) to WG 2 and Liina Kamm (Cybernetica) to WG 5 and, based on this, letter ballots by both SC 27 and JTC 1.

Just in time for the September meetings of the SC27 WGs, this process was concluded successfully and CyberSec4Europe was approved as a liaison partner, meaning that now CyberSec4Europe members can engage with both WGs. Liina Kamm and Stephan Krenn were accepted as CyberSec4Europe Liaison Officers with Liina chiefly responsible for managing the process.

At the end of 2020, the project launched Insights, a series of monthly webinars initially focused on standards-related topics led by WP8.

5.1.5 Communication and Community Building

To continue awareness raising activities beyond the end of the project to reach out to vendors, service providers, businesses and citizens

The intention and ambition of the two concertation events, in Toulouse in November 2019 and online in December 2020 (CONVERGENCE), was to bring together the cybersecurity stakeholder community and to demonstrate further ways in which industry and knowledge institutes can collaborate across Europe. CONVERGENCE was particularly successful in actively bring together all four pilots and ECSO in three days' worth of collaborative activity, preceded by a panel discussion involving senior representatives from the three Institutions involved in progressing the legislation and planning the future; as well as a closing panel discussion between the four pilot coordiantors, moderated by the Secrety General of ECSO.

TDL, as leader of the dissemination and communication workpackage, is committed to maintaining the CyberSec4Europe website and promoting the continuing activities, both joint and individual, of the project after its end. This will be carried out in concert with the Bucharest Competence Centre.

Over half of CyberSec4Europe partners are members of ECSO and a number have leading roles on the Board of Directors (GUF, ISGS and CONCEPT) and in individual workpackages. This participation in ECSO, and other internatonal bodies, will continue beyond the end of the project.

5.2 Exploitation agreement

As is the custom in H2020 projects, the CyberSec4Europe exploitation agreement will be concluded towards the end of project and will supplement the consortium agreement concluded before the grant was agreed with the Commission.

6 Sustainability Strategy

From the description provided in the DoA[9], this task will:

> *… identify the sustainability strategy of the CyberSec4Europe framework in the context of building a network of competence centres in Europe beyond the completion of the project.*

It could be said that each of the pilot projects comprise three distinct sets of activities:

- Governance
- Technical Activities
- Communications

Consequently, we propose to split the project's sustainability strategy along these lines into three types of output, each of which are instruments to be used during the course of the project in order to achieve the sustainability of the project beyond its completion:

- Strategic input
- Technical collaboration
- Communications and Networking

6.1 Strategic Input

The events and activities associated with the project are intended to make progress towards the EU's ambition to establish a European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

The primary purpose of establishing the four projects was to propose and then pilot governance structures for the planned Centre and Network; additionally, it was considered practicable to demonstrate the types of collaborative activities the future Network would facilitate.

The strategic input that CyberSec4Europe has contributed to includes:

- **Management:** monthly and now bi-monthly coordinators' meetings with DG CONNECT, that, in addition to high-level reporting, have contributed to joint efforts on a common approach to taxonomy, eventually involving all pilot partners, and realised in the Cybersecurity Atlas
- **Governance:** as described above, CyberSec4Europe's WP2 has made significant and well-regarded contributions to the ongoing debate in the European Institutions concerning the future governance structure of the Centre and Network. During 2020, CyberSec4Europe,

[9] DoA Annex 1 (part A) p.50

through TUD, took the initiative to set up and lead a Governance Focus Group, involving all four projects.

Now that each of the pilots are two years old, the strategic landscape appears quite different than it did at the outset, particularly since the planned legislation is close to approval and the location of the Centre was chosen on 9 December 2020. Over the course of 2021 and 2022, as Bucharest ramps up to be fully operational, CyberSec4Europe together with the other pilots and ECSO will have an evolving and significantly different role to play in fulfilling the objectives articulated in the legislation.

6.2 Technical Collaboration

It is clear that CyberSec4Europe alone is not responsible for the sustainability of its pilot activities. By the very nature of the endeavour, the future of the Competence Network is, initially at least, going to be driven by the four pilots, together with ECSO, working together in close collaboration with DG CONNECT. Collaborative activities have been underway from the outset of the pilots and will continue to inform and support the establishment of the Centre and Network

For the first 12-18 months, the four pilots considered the synergies amongst their work activities but made no concerted collaboration. However, during 2020, a number of focus groups were formed by representatives from two or more of the pilots starting to have conversations about potential collaborative endeavours. By the time of the CONVERGENCE event, six focus groups had emerged covering both functional and technical aspects of cybersecurity. The technical groups are:

- Education (led by CONCORDIA)
- Roadmapping (led by SPARTA)
- Threat Intelligence (in the financial sector) (led by CONCORDIA)
- Cyber ranges (led by ECHO)

CyberSec4Europe is involved in all six groups. Since the presentation of these groups at CONVERGENCE, DG CONNECT has requested that each of the focus groups should report into the bi-monthly coordinators' meetings; and, in addition, that new focus groups should be considered for adoption by the four pilots in consultation with the Commission.

6.3 Communications and Networking

The core function of the planned Network is primarily marketing: creating awareness and establishing links within the European cybersecurity community. There are two sets of complementary activities in this area:

- **Communications:** A common Communications Group (rotating lead) was established with the support of DG CONNECT involving representatives from each of the four pilots with the aim of, when appropriate, speaking with 'one voice'.

  Although there was a push for the pilots to abandon their individual dissemination and communication strategies for a common approach, this was resisted at the time – not least because each one was exploring its own contractual obligations.

CyberSec4Europe held the six-monthly rotating chair of the Communications Group between August 2020 and January 2021. CyberSec4Europe took responsibility for creating a distinctive common branding for the initiative which is used on the common website, Twitter account and presentation materials.

- **Cybersecurity Atlas:** The Atlas initiative, undertaken by the JRC and DG CONNECT to create a visual network of cybersecurity expertise in Europe, is currently in its pilot phase and is expected to go public (i.e., made accessible by the general public) at the beginning of March 2021. The four pilots, led by the Communications Group, are being strongly encouraged by DG CONNECT to find synergies with the Atlas, and to create as much of a 'fusion' as possible, particularly in the interim period prior to the Bucharest Competence Centre being in a position to absorb all management and operational responsibilities into its own orbit.

What this will mean in the interim in practice is a matter of further exploration and evolution over the course of 2021 into the ways in which we can embed elements of the results of the pilots in the Atlas which will establish the role of the pilots when the Centre is up and running. So in the short and medium term – the lifetime of the pilots – the four pilots and the Centre will effectively be mutually sustaining.

7 Innovation Management

There are several examples of innovation, whether they be innovative products, solutions or services being developed during the course of the project, either from pre-existing assets introduced by consortium partners or developed from scratch. It is to be expected, and already at this stage evidenced, that the demonstration use cases are the most likely candidates for generating innovation assets that can be successfully exploited, commercially or otherwise, after the end of the project.

7.1 CyberSec4Europe Innovation

For the purposes of this report, we are highlighting three examples of innovation in the project so far.

7.1.1 Flagship 1

From 12-13 January 2021, as part of CyberSec4Europe, JAMK University of Applied Sciences conducted Flagship 1, a two-day cybersecurity exercise that required no previous experience and (uniquely) only accessible online. The event, the first of its kind, was open to representatives from CyberSec4Europe partners although future events may be made available to others. Part of the exercise has been published as an open online course. It is a real world simulation which demonstrates new concepts.

7.1.1.1 Description

During the exercise, participants were provided with guidelines concerning a fictional organisation they were working for. With the available documentation, participants were able to examine and analyse a cyber attack and seek to mitigate the damages. The short duration of the exercise provided an interesting challenge: one of the key questions was what to expect participants to learn in a complex learning situation in such a short time. It was a technical cyber exercise, but was also fun, educational and inspiring as well as offering purposeful roles for attendees with varying technical and non-technical backgrounds.

In the exercise, the fictional organisation's internal and external communication representatives are alerted. A video setting the scene for Flagship 1 is available at JAMK's video sharing service.

- **The exercise in general:** The background story for the exercise was opened for the participants before the exercise. At a generic level, the exercise modeled a situation "at the office" where the exercise organisation did not know what kind of incident it might face, from whom, what the motivation behind it was, and how the incident started.
- **Role of the participants:** A separate survey was sent to enquire about individuals' preferred role in the exercise which varied from hands-on technical roles to more managerial or leadership roles, or an observer role with no hands-on activities. Most of the participants were assigned to an employee, a consultant, or service provider role in the fictional organisation. There could be several fictional organisations in the exercise.
- **The exercise environment** realistically modeled the Internet and its services. For example, there were ISPs (Internet Service Providers) who provided connectivity and services for the exercise organisations. The organisations had environments realistically modelled, both technically and operationally.

The technology behind Flagship 1 is based on Realistic Global Cyber Environment (RGCE), a cyber arena developed in JAMK's cybersecurity research, development and training centre, JYVSECTEC. The platform development started in 2011 and the first national cyber exercises were held in 2013. Since then, RGCE has been used in various realistic cybersecurity exercises and in cybersecurity masters' level cybersecurity education at JAMK. In Flagship 1 an open-source SD-WAN interconnection requirement specification is proven. It is used for interconnecting various cyber range internal and external services and endpoints.

7.1.1.2 Opportunities

The recent cybersecurity attacks in Finland and abroad have shown that communication is an essential part when coping with a cyber attack. A detected successful cyber attack concerns not only the targeted organisation, but also an organisation's ecosystem and its stakeholders. They need to receive timely updates and it helps when people speak the same language, so that internal and external communication can be clear and effective. Therefore, the exercise is targeted to people in charge of communications as well.

7.1.1.3 Benefits

From the feedback after the event from the participants, the expectation that exercise attendees would get a good or improved understanding of how a team could collaborate and communicate during an incident response was met.

JAMK had already created online courses for the technically-oriented attendees of the exercise, but with Flagship it was open for anyone interested.

They saw an opportunity to share the course in public, on the assumption that there might be people interested in the subject who wouldn't know where to start. Taking the course gives first-hand information from a detected successful cyber attack and the chance to perform basic digital forensic investigation. This kind of course is doable within a weekend and from Flagship JAMK were able to learn the need for this kind of course.

7.1.2 Incident Reporting Platform

The Incident Reporting Platform is being developed in CyberSec4Europe in WP5 / T5.4 between Atos, BBVA and Intesa Sanpaolo.

7.1.2.1 Description

The data about the security incidents to be reported is gathered through a graphical interface which integrates the GUI provided by the asset AIRE (Incident Reporting Engine) asset with the GUI provided by the open source tool TheHive.

AIRE allows the collection of general information about the financial entities, users and regulations (such as templates required, recipients of the reports and communication channels) that will be used by different incidents reported by the same organisation or under the same regulatory framework.

TheHive offers by itself a security incident response platform where information about security incidents can be managed. It supports the registration of new incidents and, with this purpose in mind, the administrator can define templates with the information necessary to report the incident to competent authorities.

Currently, there is a lack of solutions in the market focused on the management and generation of mandatory incident reporting according to different regulatory frameworks, in spite of a "report incidents" feature included in many of them. Most SIEM (Security Information and Event Management) solutions available in the market, such as IBM QRadar, Alienvault USM or Splunk, provide the generation of reports about the security incidents detected. However, these reports do not follow any common template and the information included in them does not cover what is required for mandatory incident reporting to the different Supervisory Authorities.

The objective of the Incident Reporting Platform is to enable financial institutions to fulfil the mandatory incident reporting requirements according to the different procedures and methods specified by the applicable regulation or regulatory bodies (such as PSD2 and ECB Cyber Incident Reporting Framework).

The platform covers reporting from the collection of the data related to a detected security incident until the generation of the mandatory reports that have to be sent to the competent authorities.

7.1.2.2 Opportunities

The Incident Reporting Platform will address the common need for standardised and coordinated cybersecurity communication cooperation and could also pave the way for a public and private cooperation that could achieve the common goal of enhanced cyber resilience across Europe and beyond.

Currently, there are no standards defined for mandatory incident reporting and each Supervisory Authority, both at EU and national level, defines the relevant impact assessment criteria, thresholds, timing, dataset, procedures and communication means that must be followed. All these different criteria and patterns cause fragmentation into the overall incident reporting operation for the affected financial entities and are to be managed along the critical path of managing the incident itself. This implies time-consuming reporting processes for the incident management and reporting teams and can even lead to potential faster propagation of threats.

Additionally, in the overall context of incident reporting, there is an increasing importance given to cooperation and threat intelligence data sharing among all the different stakeholders to improve the capacity and resilience of the European cyber environment and give a more efficient and quick answer to the new cyber security threats.

7.1.2.3 Benefits

The main benefits of the Incident Reporting Platform are to:

- Facilitate the collection of information related to the security incident and/or data leak, establishing a data model and tools to gather all the information required to report the incident.
- Facilitate the reporting of the security incident and/or data leak to the competent authorities.
- Facilitate compliance with multiple regulations and supervisory authorities at different levels (local, national, European, industry).
- Facilitate collaboration between the areas or departments of the organisation that are involved in the management and reporting of a cybersecurity incident and/or data leak, providing a tool that will centralise all the information related to the security incident and/or data leak.
- Provide a tool where all the information related to the cybersecurity incidents and/or data leaks can be stored and immediately available for all the areas of the organisation involved in the incident management process.
- Possibility to analyze all the data stored in the incident reporting tool to detect trends and determine the management and mitigation measures that have to be adopted after an incident has occurred, considering measures taken in previous similar incidents.
- Promote a collaborative approach for incident information sharing.
- Foster cooperation among public and private entities to fight against cyber attacks and enhance cyber resilience.

7.1.3 OBSDIAN

OBSIDIAN (Open Banking Sensitive Data Sharing Network for Europe) is being developed in WP5 / Task 5.1 by Informatique Banque Populaire with the support of ABI Lab, CaixaBank, Poste Italiane and Trust in Digital Life.

OBSIDIAN (Open Banking Sensitive Data Sharing Network for Europe) is a financial fraud data sharing network to counteract the high incidence of repeated frauds. State of the art tehcnologies allow participating financial institutions to keep control of their data and only share data that is fraud relevant. All of this takes place in total compliance with regulations pertaining to both banking secrecy and data protection.

7.1.3.1 Description

The objective of this use case is to address the increase in banking fraud and digital banking cybersecurity challenges by creating a European network for sharing fraud information between

open banking players. The role of the proposed network is to enable national and cross-border cooperation between banks to prevent fraud by immediately sharing fraud information (like, for example, an IBAN implied in a transfer fraud) within a secure, trusted network once a fraudulent attack occurs whilst protecting the data in transit. The role of the network is to share fraud information within the network and establish user experience trust levels; and, in so doing, provide network access to data and money laundering information and share terrorist financing information in the network. The core requirements of the OBSIDIAN demonstrator are :

- Bank anonymity
- Regulatory compliance
- Sharing information without transferring underlying data ownership
- Real-time sharing
- Privacy by design

There are four key stages to the demonstrator use case:

(1) Each bank owns a list of fraudulent IBANs associated with frauds and fraud attempts, stored in a local database. In France, at least, each major bank has already built such a list.

(2) Each IBAN is pseudonymised (through hashing and encryption techniques) before being commited into a dedicated OBSIDIAN database

(3) The OBSIDIAN server broadcasts IBAN check requests and federates responses: it doesn't store any business data

(4) The OBSIDIAN client is responsible for guaranteeing the local pseudonymised IBAN database is connected to the network

By centralising information exchange flows, the OBSIDIAN server makes it possible for banks to exchange information anonymously. Additional technologies have been studied to improve the anonymity of the data and the banks; for example, by fragmenting TCP packets on the network and making them transit through several intermediate servers.

When a fraud manager (or a system) of a participating bank detects a suspicious transaction and wants to check the beneficiary's IBAN, she will use the OBSIDIAN client to protect it (through pseudonymisation and encryption) and then send a check request to the OBSIDIAN network.

The underlying principle of the trust network is that it is based on secure multi-party computation (MPC) and consists of:

- centralised architecture for exchange flows
- decentralised data storage
- data protection based on hash and encryption mechanism

This is achieved through a central network server that communicates securely to numerous network clients deployed at each node in the network – the participating financial institutions. Key to the trustworthiness of the network is that no sensitive data is stored on the central network server – all fraud-related data is stored locally at each network node, independent of the network server and all the other nodes in the network.

Fraud data – in this use case, IBANs – is encrypted with Elliptic Curve Diffie Hellman (ECDH) used to generate a shared key each time data is transferred between the network clients and the

server. The implementation deployed uses Elliptic Curve Cryptography (ECC) implemented in JavaScript to offer a very simple OBSIDIAN client consisting of a web app usable for any fraud manager/banking expert without requiring her to install any software on her workstation.

7.1.3.2 Benefits

Today financial fraud is global. As bank strategies are focused on digitalising critical processes like opening a bank account or adding a transfer beneficiary to a bank account, it has become very easy for hackers to carry out fraudulent transactions from their living rooms within a short period of time and without their physical identity being fully exposed. Moreover, they can attack several banks without having to change their mode of operation, given that today banks don't share information on frauds that have been effective and any associated data. Finally, with new applications of technologies like Instant Payment which provide bank users with real time money transfer services, it will be even more difficult to fight fraud, as banks won't have any time delay in which to carry out recalls in case of fraudulent transactions.

OBSIDIAN is the implementation of a trust network aimed at providing banks with a channel to share and exchange critical information about effective frauds, leveraging the latest online open banking services First, by making such sharing possible, banks should be able to improve their ability to detect and react in real time to cases of fraud. For example, if a bank which had detected a transfer fraud were able to share with other banks the information about the IBAN implied in the transfer, these banks could take this information into account in a timely manner to prevent the fraudster from using this IBAN to carry out other fraudulent transactions at other branches of the same bank or other financial institutions nationally or elsewhere in Europe.

A consequence of the lack of cooperation between banks is the rising leadership in Europe of non-European ICT providers in the field of risk scoring, leveraging globalised fraud information centralisation. Several of these ICT providers offer risk management services aimed at scoring transactions in a bank information system to detect which ones are fraudulent. But few or none of them offer services featuring all fraud typologies (transfer fraud, cash machine fraud, cheque fraud, payment fraud etc.); and their solutions are based on black box architectures to protect their competitive advantage.

There's a sovereignty issue, given that this lack of cooperation is an opportunity for these providers to become leaders in the field of centralisation and correlation of fraud information by contracting one-on-one with each bank; as well as to increase their market leadership by fuelling their product roadmaps with sharp knowledge of globalised fraud use cases, and then becoming essential actors by creating evidenced-based addictions to their services.

Hence, the implementation of an OBSIDIAN network would benefit Europe's financial sector by reclaiming key elements of digital sovereignty.

7.2 Patents and IPR

At this stage, there are no patents pending as a result of CyberSec4Europe activities, although it is clear that discussions are ongoing between several partners about commercialisation rights on assets developed during the project. We would expect to report more in this regard in future iterations of this report.

7.3 Licence Types

The licence types associated with the technical components and product / solutions, either introduced into the project from the outset or developed during the course of the project are either proprietary or some form of open source.

7.3.1 Proprietary

Agreements concerning proprietary assets that could be employed in the project were generally ironed out already in the Consortium Agreement, concluded before the project started. Several of the industrial partners introduced software assets, primarily into WP3, containing pre-existing proprietary code:

7.3.1.1 Atos

Atos introduced four assets, two of which (TIE and AIRE) contained proprietary code, although AIRE also contains open source material as a result of project work with other partners.

7.3.1.2 JAMK

JAMK created a new asset, the Flagship cybersecurity exercise, based on its own cyber range assets which it is using to promote their commercial business opportunities, also through a MOOC and various marketing channels. JAMK is also considering white-labelling the Flagship concept.

7.3.1.3 NEC

NEC introduced its Hyperledger-based distributed ledger technology to the project and developed another technical component through its involvement in task 5.2.

7.3.1.4 Siemens

Siemens are developing two sets of products and solutions, both based on open source with some proprietary code, which it envisages to be used internally.

7.3.1 Open source

7.3.1.1 Atos

Atos introduced two assets (DANS and SPEIDI) which are both based on open source.

7.3.1.2 Cybernetica

Cybernetica introduced its open source privacy-enhanced business process models for use cases in tasks 5.5 and 5.6

7.3.1.3 Engineering

Engineering is looking to exploit a service, developed in the project but using assets it introduced assets, through a subsidiary company that is based on an Apache 2.0 licence.

7.3.1.4 Siemens (see above)

7.3.1.5 University of Porto

The University of Porto further developed its open source ARGUS asset in tasks 3.3 and 5.7.

7.3.2 Academic licence

Cybernetica brought its Sharemind MPC Application Server to test the feasibility of privacy-preserving machine learning and other use cases into WP3 (tasks 3.2 and 3.3) as well as WP5 (tasks 5.6 and 5.7). Generally Sharemind is available undr three types of licence:

Sharemind MPC	Licensing	Pricing
SDK & Emulator	Open source (GPLv3)	Free
Academic Server	License from Cybernetica	Free for research use
Application Server	License from Cybernetica	Server-based pricing

Table 10: Cybernetica Sharemind licensing

For the purposes of Cybernetica's participation in CyberSec4Europe, it has been freely available under academic licence

7.4 Advisory Board

The DoA proposes the following:

> *The exploitation plan will be reviewed and updated on an on-going basis and progress towards implementation will be assessed every six months, supported by the Advisory Board to advise the consortium on the more strategic aspects of exploitation, and to drive the commercialisation of project results. The committee is responsible for the uptake of consortium decisions relating to exploitation and the exploitation plan, including the management of associated intellectual property.*[10]

Given the very disparate nature of the project, the CyberSec4Europe Management Board considered it unwieldy to appoint an external advisory board that could effectively advise on all aspects of the project. In fact, for the purposes of advancing innovation and maximising the resultant exploitation opportunities, we consider it to be more effective to set up an Exploitation Board from within the project that can directly interact with all partners as and when appropriate over the remaining lifetime of the project.

8 Conclusion and Next Steps

8.1 A Living Document

As already observed, what has been presented here is the beginning of a process of exploration for individual partners and the consortium as a whole. We will be asking partners to update the exploitation tab on their activity files on a six-monthly basis and to track the development of any proprietary asset discussions between partners.

[10] DoA Annex 1 (part B) p.34

8.2 Exploitation Board

As has been apparent, many CyberSec4Europe partner organisations have not yet fully focused on how they might exploit the results of the project beyond its end. Consequently, as we move into the second half of the project, it is proposed to set up an Exploitation Board in order to raise greater awareness of exploitation potential among all partners, potentially managed through the project's regular General Meetings or formal General Assemblies.

8.3 Furthering Exploitable Assets

Furthermore, we propose seeking out key exploitable results in order to boost visibility and to provide more marketing and other forms of support to assist partners taking exploitable assets through different technology readiness levels (TRLs) and product management gates. In order to create a sense of occasion, it is proposed to hold a competitive final for a select number of the best exploitation candidates either at one of the project's General Meetings or at the next CONVERGENCE event in Brussels, which may be held during the early part of 2022. We will consider inviting an external set of innovation experts to adjudicate at the event.

The next phase of this task will prepare for this activity, including evaluating the criteria for selection, based on mapping to market pull and the integration of research results into commercial offers. In this report, we already highlighted three examples of innovation in the project so far, all of which have the potential to be considered as key exploitable results. Among the criteria for making these choices were these assets' maturity and potential real world impact, and provide examples of what we will be looking for in the pitch session at the next CONVERGENCE event.

8.4 Meeting Expectations

In a later report in this series, we will ask all partners to compare their organisation's intitial expectations of how they would eventually benefit from participation in CyberSec4Europe with how their very advanced exploitation plans have (or have not) met those expectations. The insights gained from this exercise could inform how future collaborative activities are constructed.

Annex A: WP3 Partners by Task

	Common Framework Design	Cybersecurity Enablers and Underlying Technologies	SDL – Software Development Lifecycle	Security Intelligence	Adaptive Security	Usable Security (Human-centred Cybersecurity)	Regulatory Sources for Citizen-friendly Goals	Conformity, Validation and Certification	Continuous Scouting	Impact on Society
	T3.1	T3.2	T3.3	T3.4	T3.5	T3.6	T3.7	T3.8	T3.9	T3.10
ABI										
AIT		AIT					AIT			
ARCH							ARCH			
ATOS		ATOS		ATOS	ATOS		ATOS			
BBVA										
BRNO										
C3P		C3P	C3P	C3P						
CNR		CNR	CNR	CNR	CNR	CNR	CNR			
CONCEPT								CONCEPT		
CTI										
CYBER	CYBER	CYBER	CYBER					**CYBER**		
DAWEX										
DTU	DTU	DTU	DTU	DTU						
ENG										
FBK										
FORTH										
GEN										
GUF		GUF				GUF	GUF		GUF	GUF
I-BP		UPRC								
ICITA										
IRIT										
ISGS										
JAMK										
KAU			KAU			KAU				
KUL	KUL			**KUL**	KUL	KUL				
NEC		NEC	NEC							
NTNU										**NTNU**
OASC										
POLITO	POLITO	POLITO		POLITO		POLITO			**POLITO**	
SIE										
SINTEF			SINTEF							
TDL										
TLEX										
TUD										
UCD					**UCD**	UCD				
UCY		UCY	UCY							

UM	UM	UM			UM	UM	**UM**			UM
UMA		UMA		UMA						
UMU	**UMU**	**UMU**		UMU		UMU	UMU	UMU	UMU	
UNILU		UNILU		UNILU						
UNITN		UNITN		UNITN		UNITN				
UPRC		UPRC			UPRC				UPRC	
UPS-IRIT			UPS-IRIT		UPS-IRIT	UPS-IRIT		UPS-IRIT		
VAF										
VTT	VTT	VTT			VTT	VTT				

Table 11: Partners involvement in WP3 tasks

NB: Task leaders are marked **like this**

Annex B: WP5 Partners by Task

	Open Banking	Supply Chain Security Assurance	Privacy-preserving Identity Management	Incident Reporting	Maritime Transport	Medical Data Exchange	Smart Cities
	T5.1	T5.2	T5.3	T5.4	T5.5	T5.6	T5.7
ABI	ABI						
AIT			**AIT**				
ARCH							
ATOS				**ATOS**		**ATOS**	
BBVA				BBVA			
BRNO							
C3P							C3P
CNR							CNR
CONCEPT							
CTI			CTI				
CYBER					CYBER	CYBER	
DAWEX						DAWEX	
DTU						DTU	
ENG							**ENG**
FBK							
FORTH							
GEN							GEN
GUF							
I-BP	I-BP						
ICITA							
IRIT							
ISGS				ISGS			
JAMK	JAMK						
KAU							
KUL							
NEC	NEC	NEC					
NTNU							
OASC							OASC
POLITO							
SIE		**SIE**					
SINTEF					SINTEF		
TDL	**TDL**						
TLEX							
TUD						TUD	
UCD							
UCY			UCY		UCY		

UM							
UMA		UMA					
UMU			UMU				UMU
UNILU							
UNITN							
UPRC			UPRC		**UPRC**		
UPS-IRIT	UPS-IRIT						
VAF	VAF						
VTT							

Table 12: Partners involvement in WP5 tasks

NB: Task leaders are marked **like this**