SPARTA

D10.4

Sustainability and Exploitation Plan

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

Deliverable type	Report
Deliverable reference number	SU-ICT-03-830892 / D10.4 / V1.0
Work package contributing to the deliverable	WP10
Due date	January 2020 – M12
Actual submission date	31st January, 2020

Responsible organisation	LEO
Editor	Claudio Porretti
Dissemination level	PU
Revision	V1.0

Abstract	This document aims to describe a strategy for further development of SPARTA results identifying key exploitable areas and target stakeholders, as well as targets, indicators and milestones and guidelines for future exploitation
Keywords	Exploitation, Stakeholders, Sustainability, IPR, Market, Cyber Security

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

Editor

Claudio Porretti (LEO)

Contributors (ordered according to beneficiary numbers)

Evaldas Bruze (L3CE)

Philippe Massonet (CETIC)

Vivek Nigam (Fortiss)

Michal Choras (ITTI)

Alessandro Armando (CINI)

Elena Kaiser (SMILE)

Reviewers (ordered according to beneficiary numbers)

Christophe Slim (CEA)

Michal Choras (ITTI)

Executive Summary

An Exploitation Plan (EP) ensures the use and the dissemination of the knowledge achieved during the project, allows to underline the added value of the project, and boosts further scientific developments.

This document aims to describe a strategy for further development of SPARTA results identifying key exploitable areas and target stakeholders, as well as targets, indicators and milestones and guidelines for future exploitation.

Three types of exploitation has been analysed for SPARTA:

- The whole SPARTA Project exploitation, based on the overall concept of SPARTA that is to provide valuable inputs for the future set-up of a Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre.
- The Exploitation of the four SPARTA Research Programs (T-SHARK, CAPE, HAII-T and SAFAIR) and the Cyber Training & Exercise Framework
- The Individual Partner Exploitation

The sustainability of exploitation has been taken into account as well as Intellectual Property Rights (IPR) issues.

Finally, main steps and activities for the final SPARTA Exploitation Plan will be described.

Table of Content

Chapter 1 Introduction 1
Chapter 2 Exploitation 2
2.1 The SPARTA project 2
2.2 Types of Exploitations for SPARTA Project 2
2.2.1 Whole SPARTA Project exploitation 3
2.2.2 Exploitation of SPARTA Research Programs: 8
2.2.3 Cyber training & exercise Framework (Ct&eF) 16
2.2.4 Individual Partner Exploitation 16
Chapter 3 Sustainability and IPR 22
3.1 Sustainability Plan 22
3.2 IPR issues 23
3.2.1 Protect IP 23
3.2.2 Assignments 23
3.2.3 Licensing 23
3.2.4 Joint Ventures 24
3.2.5 Non-Disclosure Agreements (NDAs) 25
3.2.6 Consortium Agreements (CAs) 25
3.2.7 SPARTA Consortium Agreement differences respect to DESCA model 25
Chapter 4 Actions to develop the Exploitation Plan 29
Chapter 5 Summary and Conclusion 31
Chapter 6 List of Abbreviations 32
Chapter 7 Bibliography 34

List of Figures

Figure 1: Rise in the number of highly sophisticated cyber – attacks..... 4
Figure 2: Market Restraint..... 5
Figure 3: Sustainability Plan..... 22
Figure 4: Exploitation Plan activities..... 29

List of Tables

Table 1: Benefits of licensing for both parties..... 24
Table 2: Comparison between Assignments and Licence agreement 24

Chapter 1 Introduction

The aim of this document (D10.4 Exploitation And Sustainability Plan) is to describe a strategy for further development of SPARTA results.

In order to do this, key exploitable areas and target stakeholders will be identified, as well as targets, indicators and milestones and guidelines for future exploitation.

This will allow to create a long-lasting community of Cybersecurity Practitioners, Industry/SMEs, and RTOs/Academia, centered on a set of tools and techniques, which will successfully collaborate to define, develop, share, and evolve solutions that will help practitioners prevent and fight against cybersecurity.

The plan will require the review of local information, the identification of stakeholders that enable the further development of the solutions, the identification of funding sources, and the establishment of common requirements and replication strategies.

This document will report the modalities of project results' exploitation and licensing, including a common IPR framework, taking into account that for a successful exploitation it is necessary to think about concrete objects that are able to survive after the end of the project.

Exploitation and sustainability are strictly connected: the exploitation plan should organize all the exploitation process, drive the consortium to reach all the goals stated at the beginning of the project.

Section 2 is dedicated to the description of SPARTA Exploitation, while in Section 3 sustainability and IPR issues will be addressed.

In section 4, indicators and milestones will be proposed for the SPARTA Exploitation Plan.

Chapter 2 Exploitation

2.1 The SPARTA project

The SPARTA project aims to bring together a unique set of actors at the intersection of scientific excellence, technological innovation, and societal sciences in cybersecurity.

Strongly guided by concrete and risky challenges, it will setup unique collaboration means, leading the way in building transformative capabilities and forming world-leading expertise centers.

Through innovative governance, ambitious demonstration cases, and active community engagement, SPARTA aims at re-thinking the way cybersecurity research is performed in Europe across domains and expertise, from foundations to applications, in academia and industry.

The main objective of the project is to create a networked governance for advanced cybersecurity research in Europe, defining and sustaining an EU-wide roadmap at the cutting-edge of cybersecurity research and innovation.

As part of the SPARTA project, the following four programs will be executed to demonstrate how research and innovation collaborations take place in the network:

1. **T-SHARK** (Establish a Full-Spectrum Cybersecurity Threat Intelligence Framework by developing comprehensive solutions based on novel technology developments and cross-disciplinary breakthroughs)
2. **CAPE** (Continuous Assessment in Polymorphous Environments)
3. **HAII-T** (Developing a foundation for secure-by-design Intelligent Infrastructure built on strong formal approaches)
4. **SAFAIR** (Investigate approaches to make systems using Artificial Intelligence more reliable and resilient)

2.2 Types of Exploitations for SPARTA Project

On the basis of what described in the previous paragraphs, the exploitation of the SPARTA project results can be distinguished as follows:

- Whole SPARTA Project exploitation, based on the overall concept of SPARTA (provide valuable inputs for the future set-up of a Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre)
- Exploitation of SPARTA Research Programs based on specific objectives and result of such programs

In addition to the above programs, another exploitation could derive from the “Cyber training & exercise Framework“, that is the outcome of Work Package 9 (“Cybersecurity training and awareness“).

Furthermore, each partner can individually exploit the knowledge and the experience acquired during the participation in the SPARTA project.

2.2.1 Whole SPARTA Project exploitation

2.2.1.1 Identification of target stakeholders and key exploitable areas

The SPARTA objectives and expected results can be summarized as follows:

- Create a networked governance for advanced cybersecurity research in Europe
- Build sustained collaborations with academic, industrial, governmental, and community stakeholders
- Innovate to address transformative strategic challenges
- Support cybersecurity design, testing, evaluation, and certification capabilities
- Enhance awareness and training capabilities and develop cybersecurity skills

On the basis of what listed above, the following target stakeholder can be interested to SPARTA objectives and results:

- Governmental bodies
- Operator of ciber securitry services
- Service providers (including certificaiton)
- Technology providers
- Cybersecurity proticioners
- Researc and Academia

and the areas that can have major improvement due to SPARTA results are:

- Cyber security research
- Cooperation in cyber incident prevention and managment
- Shared and connected platforms –interoperability
- Education and Training
- Assurance, Audit, and Certification
- Threat Intelligenge
- Assessment and certification

2.2.1.2 Market driven analysis

The growing digitization in different nations is leading to increase in data and security breaches, resulting in cyber-crime. The next major conflict between world powers may not begin at sea or along a disputed border, but in cyberspace. In the past decade, hackers have targeted voting systems in the United States, electrical grids in Ukraine, uranium enrichment facilities in Iran and hospitals, universities and major corporations around the world. In 2010, a cyber-weapon called Stuxnet was accidentally discovered to have migrated from an Iranian nuclear facility to computer networks around the world. In 2012, Iran launches a cyberattack on the Saudi Arabian national oil company with a digital worm called “Flame”.

In 2014, the FBI says North Korea was behind a cyberattack that released confidential data from Sony Pictures. In December 2016, nearly 250,000 people in Ukraine lost electricity as the result of a suspected Russian cyberattack. The recent hack of the Equifax credit-reporting agency that potentially affects 145.5 million U.S. consumers showed a level of sophistication that suggests they were sponsored by a foreign government. In May 2017, 74 countries suffered losses due to the 45,000 WannaCry ransomware attack. In most cases, the breaches are a result of espionage or threats pertaining to national security, which have damaging effects on a nation.

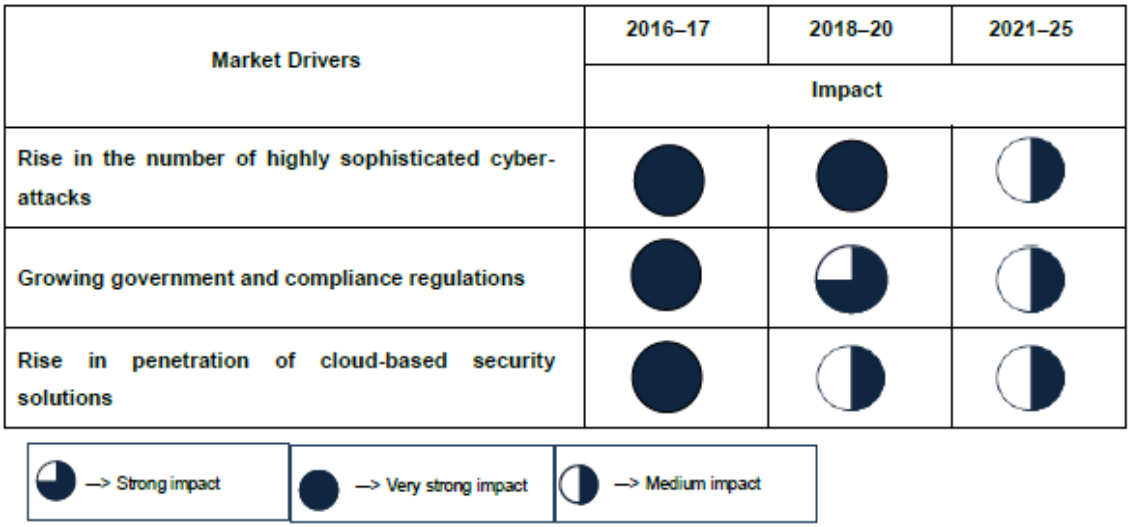


Figure 1: Rise in the number of highly sophisticated cyber – attacks

Growing government and compliance regulations

The increasing number of government regulations regarding data security & privacy and compliance is propelling the growth of cyber warfare solutions, worldwide. In February 2016, the President of the United States announced the implementation of the Cybersecurity National Action Plan (CNAP) to strengthen cybersecurity and issued an executive order to create a commission for enhancing national cybersecurity as a central feature of CNAP.

Rise in the penetration of cloud-based security solutions

The evolution of cloud storage has increased the threat of cybercrimes and data breaches across verticals such as defense, government, and homeland security, among others. These verticals prefer using cloud security, as the costs incurred in the implementation of on premise solutions are high. The adoption of cloud-based security is expected to increase in the near future, owing to the growing adoption of cloud storage systems and deterrence of cyber espionage.

2.2.1.3 Market restrains analysis

Lack of shared real time information

In a digitally connected world, people are increasingly reliant on technology for professional and personal purposes. Organizations are facing cyber risks on a daily basis, owing to growing digitization. Threat analysts are focusing on finding solutions to mitigate the damages caused by constantly evolving threats.

However, the knowledge about emerging cyber threats and their impact is not shared on a real-time basis on a global scale. Thus, lack of real-time information in organizations and government agencies may hamper the management of military forces, lead to economic damage, and cause panic.

Lack of skilled workforce

For several nations around the world, the lack of workforce for tackling cyber threats is a major concern. Organizations are facing a shortage of skilled workers and cyber personnel to respond to cyber-attacks or prevent them. The lack of coordination and planning among network security agencies and insufficient funding from several governments for securing information are the key factors challenging the deterrence of cyber espionage and warfare.

Market Restraint	2016–17	2018–20	2021–25
	Impact		
Lack of shared real-time information on constantly evolving threats			
Lack of skilled workforce to tackle emerging threats			
 —> Strong impact	 —> Medium impact	 —> Low impact	

Figure 2: Market Restraint

2.2.1.4 Market potential

Towards a EU cyber strategy

The European Commission has placed cybersecurity high on the agenda in its proposals for the next long-term European Union's budget for the period 2021-2027. The Commission identified cyber-security as one of the key priorities for the years to come, implementing a number of actions:

- On 13 September 2017, the Commission and the EU High Representative for Foreign Affairs and Security Policy, presented a joint communication "Resilience, deterrence and defence: Building strong cybersecurity for the EU" known as the cybersecurity package.
- A year later, the Commission presented a proposal for the creation of a European cybersecurity competence centre with a related network of national coordination centres. The competence centre is supposed to become the main body that would manage EU financial resources dedicated to cybersecurity research under the two proposed programmes – Digital Europe and Horizon Europe – within the next MFF 2021-2027.
- The NIS Directive (Security of Network and Information Systems) , in force since 9 May 2018, represents the first piece of EU-wide legislation on cybersecurity, with a focus on protecting critical infrastructure. Among other things, it established the NIS cooperation group, to ensure strategic cooperation among Member States, and the network of computer security incident *response teams (CSIRTs*), to ensure both the exchange of information on cybersecurity and cooperation on specific cybersecurity incidents.

Cybercrime is a fast growing threat to the Union, its citizens and its economy. In 2017, 80% of the European companies experienced at least one cyber incident. The Wannacry-attack in May 2017 affected more than 150 countries and 230 000 IT-systems and had significant impacts on critical infrastructures, such as hospitals. This underlines the necessity for the highest cybersecurity standards and holistic cybersecurity solutions, involving people, products, processes and technology in the Union, as well as for the Union's leadership in the matter, and for digital autonomy.

The European Cybersecurity Industrial, Technology and Research Competence Centre (the 'Competence Centre')

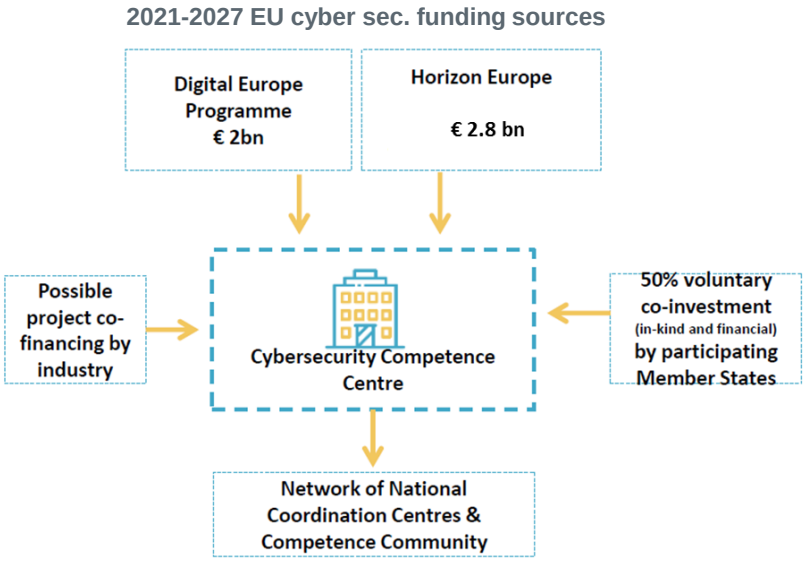
According to the Commission, the cybersecurity industry in Europe developed largely beyond the boundaries of their national markets. As a consequence, while European companies tend to be strong and innovative, they are smaller in size in comparison to their US, Israeli, Chinese, and South Korean counterparts. Only unifying the cyber expertise, the EU could transform it into products and solution and cover the whole cybersecurity value chain in order to compete with other global players. At the moment, the Union depends on non- European cybersecurity providers.
However, it is in the Union's strategic interest to ensure that it retains and develops internal cybersecurity technological capacities.

In March 2019, The European Commission approved the creation of:

- The European Cybersecurity Competence Center, with a coordinating role, will supervise the implementation of relevant parts of the Digital Europe and Horizon Europe programmes by allocating grants and carrying out procurements.
- A Network of 27 National Coordination Centres (NCC), one for Each Member State, that will function as contact point at the national level for the Competence Community and the Competence Centre. They are the "gatekeeper" for the Community in their country support to carry out actions under this Regulation, and they can pass on financial support to national/local ecosystems.
- Cybersecurity Competence Community is a large, open and diverse group of cybersecurity stakeholders from research and the private and public sectors, including both civilian and defence authorities.

in order to invest in stronger and pioneering cybersecurity capacity in the EU.

The European Competence Centre & NCC should help ***to increase the resilience and reliability of critical infrastructure*** for the functioning of society such as transport, health, and banking systems and the Digital Single Market and to provide special ***support for SMEs*** by facilitating their access to knowledge and training.



The EU Competence Centre would also become the main implementation mechanism for activities in support of the cybersecurity industry (including deployment, investment and research) under both *Horizon Europe and Digital Europe* in the next MFF (2021-2027).
The Competence Centre should be the Union's main instrument to pool investment in cybersecurity research, technology and industrial development and to implement relevant projects and initiatives together with the Network. The proposal entitles the Competence Centre to implement relevant parts of the two programmes by allocating grants, enhancing coherence and synergies between them, and carrying out procurements. For this purpose, the Commission proposes to allocate nearly **€2 billion from Digital Europe** for the 2021-2026 period and **€2.8 billion from Horizon Europe** for setting up the Competence Centre, with the possibility of voluntary contributions by member states. It is envisioned that the bulk of the funding will be allocated through **open calls for proposals and calls for tender.**

The Competence Centre will manage and eventually disburse financial support to recipients, which would typically be academic and research entities, industrial companies, or public authorities.

The Competence Centre will also seek to *promote joint procurement of strategic cybersecurity infrastructures and tools* together with one or several other entities – typically public authorities.

Some funding will be made available directly to National Coordination Centres for them to carry out tasks under this Regulation. They will also be able to financially *support their respective national ecosystems* through the use of so-called cascading grants.

The Competence Centre the Network, and the Cybersecurity Competence Community should help advance and disseminate the latest cybersecurity products and processes, including dual use, and should be at the in critical sectors such as transport, energy, health, financial, government, telecom, manufacturing, defence, and space to help them solve their cybersecurity challenges.

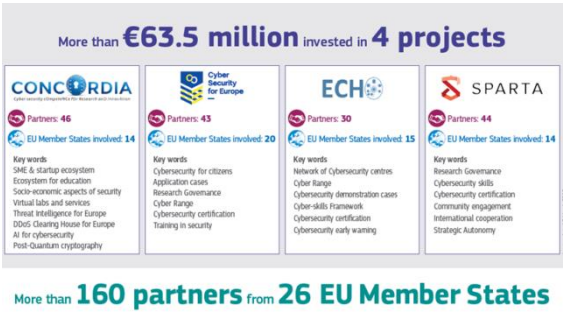
The Competence Centers will also facilitate and accelerate the standardization and certification processes as defined in the previous Cybersecurity Act proposal (supporting ENISA). ENISA will also have a key role in establishment of European Cybersecurity Competence Network & Centre. To make all this plans possible, staff will be increased by 50% and ENISA's total budget will be doubled to €23 million over the next five years.

Horizon Europe will be the sole centrally managed EU programme supporting research and technological development and the main programme for demonstration, piloting, proof-of-concept, testing and innovation including pre-commercial deployment.
Novel digital technologies (such as AI, robotics, HPC and big data) developed by Horizon Europe will progressively be taken up and deployed by Digital Europe.

The Digital Europe Programme (DEP) will focus on large-scale digital capacity and infrastructure building, with the objective of wide uptake and deployment across Europe of critical existing or tested innovative digital solutions, for the fields of high performance computing, big data analytics, cybersecurity, distributed ledger technologies, robotics and artificial intelligence. In the future only the Digital Europe Programme will support the deployment of digital services in areas of public interest.

SPARTA pilot and cyber situational awareness

SPARTA is one of the four Horizon 2020 **pilot projects** (together with CONCORDIA, ECHO, and CyberSec4Europe) to develop a sustainable European cybersecurity **competence network.**
Financed by the EU with 16 million euros through the Horizon 2020 program, Sparta aims to combine scientific and technological to guarantee the prevention of cyber-attacks and the reaction in case of incident in critical sectors, with the most innovative cyberspace monitoring solutions and techniques and incident automated response capability.



The SPARTA project contributes to strengthen the strategic autonomy of the EU in IT security. The project, which is being funded under the EU's H2020 Program, will tackle very concrete issues, in particular in these four areas:

- Health
- Energy, finance and transport

- Information and communication technologies industry
- E-government and public administration.

This type of protection is essential for Europe to benefit from the **415,000 million euro a year** and from the **hundreds of thousands of new jobs** that the Commission estimates will be generated thanks to the new digital tools.

The SPARTA consortium, which is led by CEA (the French Alternative Energies and Atomic Energy Commission), brings together 44 institutions from 14 EU Member States that are active in the field of cybersecurity at the intersection of scientific research, technology development and social sciences. Together, they want to come up with a new way of thinking about research, innovation and training in European cybersecurity – from its scientific foundations right up to its industrial applications.

A roadmap that will be drawn up as part of the project aims to develop an ambitious plan for research and innovations in cybersecurity and to make a significant contribution to developing a globally leading competence network based in the EU. In addition to this, the project will develop *digital applications and platforms* that meet the highest security standards and can be used for training.

It is a decisive capacity for the EU to compete with the world's most advanced economies and become a key player in the global economy of the future.

2.2.2 Exploitation of SPARTA Research Programs:

As mentioned in 2.1 in the SPARTA project four programs will be executed to demonstrate how research and innovation collaborations take place in the network:

1. **T-SHARK** *(Establish a Full-Spectrum Cybersecurity Threat Intelligence Framework by developing comprehensive solutions based on novel technology developments and cross-disciplinary breakthroughs)*
2. **CAPE** *(Continuous Assessment in Polymorphous Environments)*
3. **HAII-T** *(Developing a foundation for secure-by-design Intelligent Infrastructure built on strong formal approaches)*
4. **SAFAIR** *(Investigate approaches to make systems using Artificial Intelligence more reliable and resilient)*

The following paragraphs analyse the possible exploitation that could derive from SPARTA Research Programs results.

2.2.2.1 T-Shark

The T-SHARK Program in SPARTA means to establish a Full-Spectrum Cybersecurity Threat Intelligence Framework by developing comprehensive solutions based on novel technology developments and cross-disciplinary breakthroughs. It will provide decision-making tools, fostering a common cybersecurity culture, raising preparedness for possible disruptions and attacks.

Objectives and expected results of T-SHARK program

Evolving cyber-threats varying in scope, scale, duration, intensity, complexity, sophistication and impact, are getting increasingly common and demand a mobilization of the full range of respective tools and instruments, as well as a joint response. A collective cross-sectorial and wide-ranging approach, providing comprehensive situational threat intelligence, enabling future prediction, and informed and effective decision-making, is indispensable to address a widening and deepening landscape of hazards raging. Much of the current organization of cybersecurity supervision is

organized as a reactive activity, focusing on individual incident handling, driven by technology aspects, resulting in limited abilities to spot on early stage new generation threats.

To reach catch up with evolving cybersecurity threats, these practices should evolve to more comprehensive, wider spectrum, prediction based, cognitive computing capabilities.

The objective of T-Shark research programme is to develop and validate methodological, organizational and technological solutions extending cybersecurity towards comprehensive organization of security functions, that would focus more on threat prediction and full-spectrum cybersecurity awareness by providing high situational awareness, informing decision and policy makers on broad or long-term issues and/or providing a timely warning of threats.

It will expand the reach of threat understanding, from current investigative-level definition, up to strategic considerations on current, future and down to real-time events handling and prevention.

The T-SHARK Program addresses four challenges:

1. How to handle complex of cybersecurity threats?;
2. How to deal with early cyber attacks' kill chain phases?;
3. New methods and solutions for prediction and awareness- and knowledge-based cybersecurity management;
4. Secure threat intelligence information exchange between sharing partners in line with GDPR);

Activities will be performed cross-vertical, cross-domain to assure comprehensiveness aspect of the challenges addressed and demonstrated via use-cases.

Expected results (deliverables):

- Developed cybersecurity threat intelligence common data model. This will be the design and specification for the data model agreed as common standard to be used for cybersecurity threat intelligence, as well practical implementation of ENISA proposed cyber-incidents data model.
- Developed cybersecurity threat analysis model. This deliverable will define the process, structure, criteria, rule-sets used to perform full-spectrum cybersecurity threats analysis
- Developed comprehensive full-spectrum cybersecurity threat intelligence methodology. This deliverable will provide the collection of tools, methods, skills and procedures defining the approach how full-spectrum cybersecurity threat intelligence should be organized and executed in the end-user organizations.
- Developed cybersecurity threat prediction framework. This deliverable will provide the definition of approach, methods to be used and process organization to provide comprehensive prediction of full-spectrum cybersecurity threat.
- Developed cybersecurity threat prediction legal framework. This will be a report on the outcomes of all legal debates, challenges legal aspects analysis and assessment, as well recommendation for further cybersecurity policy and regulation development.
- Developed Visual Analytics System for Cybersecurity threat analysis. This will be a suitable visualization techniques and integrated Visual Analytics components based on available data and analysis models, as well as human computer interaction methods based on the Visual Analytics enabled visual interfaces

Identification of target stakeholders for the T-SHARK program:

- Policy and legislation: Ministries and other national and EU institutions, responsible for cybersecurity and/or related domains regulation development and having the mandate for it (EP, Central EU agencies, EU MSs' MoI, MoD, MoJ).
- Operational cybersecurity: institutions, responsible for cybersecurity and acting at operational level. (EU and national CSERT's, National Defense and Security agencies, LEA networks).

- Operational InfoOps, PsyOps, Stratcom: institutions, responsible for analysis of informational contexts, analysis of publicly accessible online sources monitoring, social media and other sources monitoring and analysis in digital and kinetic environment. (NATO, EU, MSs' Stratcoms, hybrid fusion cells).
- Research & Education Institutions entities and individuals involved in advanced research in the fields of Cybersecurity, Cyber offensive capabilities and tools development, AI, advanced analytics, related social sciencies: social psychology, behavior and similar (CoE, RTO, Universities, Academia).
- Industry: start-ups, SME's, large businesses involved in cybersecurity supply chain
- Thematic Foundations, Associations: National and regional cybersecurity and cyber clusters, associations uniting Industry, international associations and specialized institutions (ECSO, JRC).

Identification of exploitable areas for the T-SHARK program:

As the T-Shark program is focused on the development of predictive and preventive capabilities of complex cybersecurity threats, the following key areas can be candidate for T-Shark program exploitability outline:

- Phenomena knowledge: Top tier cybersecurity threats, rapidly growing phenomena in the market, in scale, intensity, variety of actors involved. Cybersecurity threats, such as multi-staged attacks, full-spectrum attacks, uniquely designed and highly individualized attacks, hybrid offenses organized or sponsored by top companies or governments are new types of challenges evolving. Understanding this phenomena and clearly defining the taxonomy, will lead to more focused and efficient R&I&D activities
- Governance Framework: T-Shark is multinational R&I&D programme with high diversity per geography, disciplines, and competence areas with multiple innovation points addressed simultaneously (mission approach). Execution and governance of the programme activities is also one of the areas of innovation. Lessons learnt and compilation of practices will be one of the areas for future exploitation.
- Complex Threats Concept: Concept of integrated cybersecurity threat intelligence combining classic cyber security with information security, strategic communication and other origination spheres of threats
- T-Shark Methodology: Comprehensive full-spectrum cybersecurity threat intelligence methodology started in ECOPOL project in Lithuanian Stratcom and to be evolved in T-Shark programme will be the main exploitable area in the means of:
    - Complex threats taxonomy
    - Analysis of threats having hybrid nature
    - Intelligence process
    - Prediction techniques
    - Visual analytics application for improved decision-making
- T-Shark Platform: once build, integrated intelligence platform for cyberthreats data exchange, fusion, monitoring, visual analytics and decision making-process support including tooling and data sets, will be basis for future next generation solutions development as well common piloting environment for various outcomes from R&I&D results.
- Regulatory and legal research results. It is highly recognized that efficient cybersecurity organization in the future must be built based on the prediction and focusing on prevention. In order to succeed, technical implementation is not enough. Set of regulatory challenges are defined inside of T-Shark programme and will be examined using Moot Court method. The outcomes (both positive and negative) will serve as an recommendation and further research areas definition for future regulations applicable for cybersecurity domain.
- Standardization and best practices. In order to address complex cybersecurity threats ambiguously it is necessary to build complete situational context picture, that very often goes

beyond one country borders. Naturally it demands for data exchange, integration as well common agreement on formats, methods, interfaces, data structures. All common agreed standardization techniques will be tested among 14 of T-Shark MS representatives and will create a basis for future roll-out into EU level standards

Possible exploitation of T-SHARK program results:

In the following areas:

- **End-user organizations intelligence process**
  - Higher situational awareness and better cybersecurity resource planning and management;
  - Lowered impact of cyber incidents through the early handling of known priority threats;
  - More informed cybersecurity decision-making process;
  - Enhanced personal data processing and sharing practices in line with new data protection standards;
  - Broadened cybersecurity beyond technological solutions, linking advanced tech intelligence to other environments (cyber and kinetic) and providing a comprehensive cybersecurity threat map;
  - More effective collaboration with enforcement and other response institutions and higher success rate response focusing on detection, traceability and prosecution of cyber perpetrators;
  - Good practice uptake from defence doctrine on InfoOps and StratCom resulting in more synchronized and standardized procedures as well technical capabilities. In that way solutions will be able potentially to support dual use, and could be deployed for both - civilian and military missions and operations;

- **Policy and standardization**

Will serve for the implementation of the following regulations:

  - Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union
  - Joint Communication to the EP and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU
  - Directive (EU) 2013/40 on attacks against information systems
  - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
  - A Global Strategy for the EUFSP

Legal challenges examined in the T-Shark will be contributed to SPARTA WP2, as well presented to the ecosystem stakeholders as recommendations for policy developments

All international, collaborative aspects of T-Shark implementation will come-up as candidates for standardization:

  - T-Shark data model
  - International threats information exchange format
  - Threat information structure for analysis

- **Competence development**
  - T-Shark will contribute to the SPARTA cybersecurity skill matrix, the framework structuring up-to-date cybersecurity competences as well future perspectives. It will give for progressive universities possibility to define the curricular for next generation

cybersecurity specialist and develop competitive professionals with minimum innovation adoption delay.
    - The integration of Strategic, Operational and Tactical intelligence into one solution , as well combining technical parameters driven and social theories based complex prediction and analysis approach establishment, that will be automated and executed on unified technical platform will create new competence in cybersecurity assurance competence matrix that will require new set of trainings developed into comprehensive threat cybersecurity intelligence course. The course will be made available for EU cybersecurity practitioners

- **Certification**
    - ENISA have published assessment of cybersecurity threat intelligence processes and related standards development targets. It introduced Threat Intelligence Platforms maturity model that includes technology, processes and people perspectives. It defines four different levels. T-Shark platform establishment in combination with Method for the end-user using it, will enable to certify themselves on the 3rd level.
    - Will contribute to overall SPARTA certification lab that will provide cybersecurity certification for EU based practitioners and end-user organizations.

- **Collaboration**
    - Will create the basis for more concreate end-users and RTO collaborative activities
    - Mission oriented programme organization integrated social science, technical science and end-users into one team, enabling near to 360 perspective on the chosen challenge implementation
    - LEA, intelligence, national security and defence industries collaboration is enabled through T-Shark Arbitrage Group.

2.2.2.2 CAPE

The CAPE Program focuses on providing practical tools to product and service developers, in the following key areas.

- First, it addresses the definition of assessment targets, including in the scope differential assessment.
- Second, it includes in assessment the creation and validation of proper audit trails for intrusion detection, impact assessment and forensics. It also includes in its scope the capability to go beyond assessments of components and products, but also complex services, to take into account a more comprehensive component-based approach.
- Finally, it links with the training program to ensure that certified components and services are properly developed and operated.

The program will face challenges that will be demonstrated over use cases. In particular the use case managed by Task 5.2 and related to "*Converging tools for assessing Connected & Cooperative Car Cybersecurity (CCCC) in the context of Euro NCAP"*, it's the one that is best suited for possible future exploitation.

Moreover, also the output of Task 5.1 (tools that address aspects assessment automation) can be taken into account for exploitation.

Objectives and expected results of CAPE program

The CAPE Task 5.2 key objective is to propose and implement techniques for the integration of the safety and security objectives. This includes techniques for the extraction of security relevant information from safety analyses; techniques for evaluating the trade-offs between safety and

security, such as the impacts of security counter-measures in safety-critical systems; techniques for modelling and implementing which take an holistic perspective to safety and security, i.e., safe and secure by design; techniques for updating a system; and its relation to assessment standards.

The objectives of T5.1 “Assessment procedures and tools” are to address aspects assessment automation, augmenting the assessment toolbox to support pre-assessment by users, as well as incremental assessment and continuous monitoring. It delivers practical tools for developers to support T5.2 and T5.3 activities, as well as to support certification activities of WP11. The current result is an assessment framework composed of 15 tools that cover different phases of the development lifecycle. Some of the tools are technology specific, e.g. Frama-C that verifies security properties of C programs. It is expected that some of the tool outputs car be used as input to the certification process, thus providing some automation support to the auditing process

Identification of target stakeholders for the CAPE program:

In principle, any player concerned with the development of safety critical-systems is a stakeholder of Task 5.2. For example, safety and security engineers can profit from the techniques to be developed in the task. Similarly, requirement engineers can profit with from the understanding of the co-analyses techniques to be developed.

For what concerns Task 5.1, there are two main classes of stakeholders: (1) cybersecurity analysts and developers and (2) cybersecurity certification auditors. The assessment tools are mostly designed for cybersecurity analysts and developers that are responsible for defining, implementing, deploying and operating the security architecture of a software system. Some of the outputs of these tools can be used as input for the certification process. Cybersecurity certification auditors can use the certification-oriented output provided by the SPARTA assessment tools as input to the certification process. This contributes to automating parts of the certification process and thus improving the productivity of the certification process

Identification of exploitable areas for the CAPE program:

Task 5.2 is given a greater emphasis in the Connected Car vertical. Therefore, automotive developers can profit from the deliverables of the task, as they will be applied to an automotive scenario. For example, the security requirements identified can be directly used, as well as the models/tools developed for validation and verification.

More generally, the techniques/tools developed by the Task 5.2 can be exploited in several other domains related to safety-critical systems. This includes:

- Cyber-Physical Systems, such as in the automotive industry or Industry IoT systems;
- Model-Driven Engineering: The techniques are built using principles from Model-Driven Engineering. Therefore, areas that use this methodology can exploit the techniques/tools developed by the Task 5.2.
- Highly Automated Systems. Some of methods and requirements to be developed for the connected car can be exploited for the development of safety-critical systems with a high degree of automation.

For task 5.1 the exploitable areas at this stage is the SPARTA assessment framework and the 15 assessment tools. Some of these are mature tools that will be extended in SPARTA, whereas others are still at the design phase.

Possible exploitation of CAPE program results:

The main scenario considered by the Task 5.2 in the connected car vertical is a platooning scenario. The results of the Task 5.2 can directly be used for the development of such solutions; for example,

the HARA/TARA analyses, trade-off analyses, security requirements, verification and validation tools/methods that will result from the program.

The SPARTA assessment framework provided by Task 5.1 is mostly composed of open source code that can be made available to SPARTA associate partners for validation and feedback.

2.2.2.3 HAII-T

The HAII-T Program in SPARTA leverages and coordinates the collective expertise in the research teams to address multiple facets of cybersecurity with the ambition of developing a foundation for secure-by-design Intelligent Infrastructure built on strong formal approaches. It aims to leapfrog incumbents and position the European industry at the forefront of the upcoming II race.

Objectives and expected results of HAII-T program

The main outcome of the program will be the secure-by-design orchestration framework and the design toolkit. The framework will support the design through secure operating systems, hardening of legacy technologies and components, the secure orchestration of complex II and both resilience and privacy by design.

Identification of target stakeholders for the HAII-T program:

- IoT device manufacturers
- IoT System Integrators
- Academia
    - research results
    - new training curricula
- Certification bodies

The target stakeholders are IoT device manufacturers, system integrators, and in particular academia. The research results of HAII-T should be considered for legacy devices as well as for upcoming or future ones.

Identification of exploitable areas for the HAII-T program:

- provisioning of the security-enhanced open source operating system for IoT devices (SE-RioT)
- Security enhanced IoT app market
- HAII-T Secure-by-Design Orchestration Toolkit for the IoT
- Resilience-by-design of information infrastructure

The term “secure” here encompasses privacy and resilience.

The provided research results can be considered within SE-RioT or other OS-hardening concepts. The hardening concepts will mainly focus on low-level components, including changes to operating systems, or even entire architectures (realised through RISC-V and FPGA extensions).

Possible exploitation of HAII-T program results:

- rollout of SE-RioT to the community
- rollout of the Security enhanced IoT app market
- rollout of the HAII-T Secure-by-Design Orchestration Toolkit for the IoT
- rollout of the training scenarios based on the use cases

- design of secure and resilient control plane architecture for SDN fabrics in the IoT context
- design of byzantine fault and intrusion tolerant protocol for IoT and V2X network ecosystems

The main exploitation is through research results. The open sourcing of the results will depend on the results achieved during the program.

2.2.2.4 SAFAIR

SPARTA's smaller, exploratory SAFAIR Program will investigate approaches to make systems using Artificial Intelligence (AI) more reliable and resilient through enhanced explainability and better threat understanding, providing methods and tools for analysis of security threats for AI systems, and solutions for protection.

Objectives and expected results of SAFAIR program

In a nutshell, the work to be done in SAFAIR addresses the following goals:

- Design and development of threat analysis supporting tools for AI systems, in order to make them more understandable by both developers and users
- Design and development of defensive and reactive security mechanisms that make AI systems more security- and privacy-aware and more resilient against the identified threats
- Design and development methods to increase AI systems reliability and resilience through enhanced explainability of the functioning
- Ensuring the fairness of AI systems by providing mechanisms to reduce bias in the decisions based on AI and ensuring accountability and compliance with privacy and data protection EU regulations
- Demonstration and validation of developed solutions based on the efficiency criteria

Identification of target stakeholders for the SAFAIR program:

- Cyber security practitioners including SMEs and large industry organisations dealing with secure IA
- Technology providers and solution vendors offering services and products applying IA
- Cyber security policy makers and governmental institutions
- Organisations providing cyber security training, including academia/RTO focusing on AI security

Identification of exploitable areas for the SAFAIR program:

- Threat analysis for AI systems
- Cyber protection of systems using AI
- Privacy and data protection in AI

Possible exploitation of SAFAIR program results:

- Improved AI-based systems protection, improved defensive and reactive capabilities against adversarial attacks, improved reliability and resilience of AI systems through addressing explainability and fairness aspects
- Contribution to the European roadmapping, research agendas, policies, regulations dealing with the AI security and corresponding privacy and data protection aspects
- Contribution to the European training, awareness-raising and research/educational efforts in the AI area

2.2.3 Cyber training & exercise Framework (Ct&eF)

Cyber training & exercise Framework (Ct&eF) is the environment where cyber-security students and professionals can practice technical and soft skills and be trained on emulated large-scale complex networks in the way to respond to real-world cyber-attack scenarios under specific (and general) domains.

Cyber Training & Exercise Framework will consist of several components for cyber security training, depending on designed curricula. One of those components will be probably CyberRange.

Objectives and expected results of Ct&eF

Ct&eF is an isolated, fully controlled and monitored virtual training environment designed for cyber-security training; it contains the description of architecture of required infrastructure, the scenarios and the methodology of providing training and exercise; so that trainees can experience and participate in real-world simulated cyber-attack or defense scenarios.

The more realistic the simulated scenario the more prepared the trainees will be to face real-world attacks. It is also used for cyber-warfare training and cyber-technology research and development. It provides tools that help strengthen the stability, security and performance of cyber-infrastructures. The framework includes endpoint prevention, detection and response, operation technology security and attack simulations.

Identification of target stakeholders for Ct&eF

Cyber-security university students and professionals.

Identification of exploitable areas for Ct&eF:

E-learnig and Cyber training.

Possible exploitation of Ct&eF:

Projects related to Cyber Ranges, proposition for an EU Cyber Academy.

2.2.4 Individual Partner Exploitation

Each partner will benefit of SPARTA results in different way depending on the partner group. The exploitation interests described by partners in the SPARTA proposal [2], are reported below.

Some of them have updated the description, having had at this stage of the project (approximately one year from the start) a greater understanding of how to exploit the results for their own benefit.

CEA: Exploitation by CEA will cover networking capabilities, research organization techniques, as well as innovation and technological transfer. CEA will use the results of SPARTA as a basis for extended cybersecurity research and networking projects. SPARTA will contribute to reinforce the centre of competence in cyber security of CEA. Organizationally, CEA will build on a successful SPARTA direction to continue to serve the interests of the French and European research community, in future networking projects and collaborations. Technically, the results coming from the R&D&I activity will be matured to reach higher TRL in order to fill one of CEA main missions. When successful mature technologies emerge, they are transferred from CEA to its partners by means of the following mechanisms: 1) Joint Laboratories, consisting of specific contracts aiming at transferring some well-defined intellectual property from CEA to industry, possibly using a team of

dedicated personnel, 2) patents and intellectual properties sale, and 3) the creation of start-up companies

JR will focus on strengthening their technologies and tools towards cyber resilience and ready for market take-up. Their position as player for the development of individual security models and SPARTA will contribute to the expertise exchange in cyber security across EU bodies and organisations. JR will organise a yearly workshop dedicated to cybersecurity and will contact the Austrian economic chamber to suggest the co-organization of a cyber-security roadshow.

TNK: SPARTA gives TNK the opportunity to extend and diversify the portfolio of research services to a broader scope. We have successfully launched the Security Engineering Services (SES) providing hardware/software entangled security solutions for our industrial customers. The work proposed will allow TNK to expand their portfolio of hardware/software entangled security solutions to the area of cybersecurity applications. It is expected that collaborations with security experts the consortium will be reinforced and that new business opportunities will arise. ambition to land new contracts and win long-term business partners.

CETIC: The results from SPARTA will contribute to enhancing security engineering of IT infrastructures (Cloud, network and IoT) and cybersecurity certification. The CETIC exploitation plan will cover the value proposition canvas and the business proposition canvas to define unique selling points, potential customers and distribution channels etc.

UNamur suggests to multiply the projects results to wide audiences, measures, which would include the list of exploitable results, the main targets for each of the result and main contributors taking into account the profile of the partners, as well as the indicators of the impact. UNamur as a university can target society as a whole (including research com-munity, institutions, students, school children (when it comes to awareness raising results).

CESNET will utilize SPARTA results to improve cyber-situational awareness of its national and research educational network with more than 300 organizations and 400 thousand users. This gives a possibility to evaluate the system in comparison with already existing and deployed tools. The amount of data collected every day is more than 200 GB which they deem sufficient for revealing issues concerning performance. CESNET-CERT and SOC will have access to the results and will identify any functional issues and scope for improvement. They will showcase novel approaches and technologies as pilots in academic network and research community, perform training activities and present applied research results to operators and national authorities. Their main target will be network operators and Czech ISPs and the Government.

BUT exploitation goals are to create (based on existing program) and run a Bachelor's and Master's study program in Information Security that can serve as a best practice for EU universities, deploy and use the cyber range infrastructure to support hands-on training in study programs, design and implement novel cryptographic technologies for privacy protection that will be used for next follow-up projects on privacy and digital identity protection and that will be transferred to commercial products by industry partners.

Other activities that can be undertaken are:

- Use the newly developed study plans in the actual education process at the university
- Extend the existing lab and infrastructure, get the infrastructure interconnected to other partners within the consortium
- Design, implement and test the cryptographic technologies and integrate them into novel systems and products developed at the university

NIC: Through the CSIRT.CZ, the National CSIRT of the Czech Republic that is operated by CZ.NIC on the basis of the Cyber Security Act and the public contract with National Cyber and Information Security Agency, the results from the SPARTA project will be utilized to improve awareness of the cybernetic environment situation. At the same time, it will enable evaluating the system in comparison with already existing and deployed tools with data obtained from a unique network of more than 4000 end devices (TURRIS routers), which also work as network probes.

FTS exploitation goals are: research on security topics that can have real impact on industry practices; knowledge and expertise acquisition; dissemination through publications, tech-day events with industry, and prototype demonstrators.

FGH: Fraunhofer aims to provide its clients from industry, politics and science with recommendations for action and perspectives for key decisions. SPARTA provides a promising opportunity for Fraunhofer to further improve its scientific basis and to provide its customers with a new quality of focussed and well-founded recommendations. The results of SPARTA as well as the contacts established with actors will be exploited in different ways. The exploitation will not be restricted to the involved Fraunhofer institute but results and contacts will also be shared with other relevant institutes of the Fraunhofer Society.

SAP as a leader in business software delivered via the cloud and on-premise, SAP drives the digital transformation of the economy. Security and privacy are critical factors for the success of this transformation, and innovative security solutions are an important part to maintain SAP leading position. In consequence, SAP invests significantly in security research and innovation, by running its own security research group, and by collaborating with leading universities and research institutes. SPARTA and the upcoming Cybersecurity Competence Network are expected to strengthen SAP's links with the scientific community: increase reach and accessibility to early research, and use results form demonstrators addressing important security challenges of SAP and its customers to exploit their potential for improving the security of products and services

TUM exploitation goals are research on interesting topics and provide an environment for Ph.D. candidates and young researchers. Also create lectures and seminars in order to educate students. Also tools will be developed, that may later be extended to marketable security solutions. To encourage open research we intend to publish all our data and tools (both code end experimental steps) in order to allow third parties to reconstruct and re-enact our results.

UBO: The University of Bonn aims to improve prototypes resulting from previous national research projects. The main goals are a) to further develop the knowledge in the areas IT security awareness and Threat Intelligence sharing and b) to evolve the TRL of existing prototypes.

UKON aim to strengthen our reputation and expertise in the cybersecurity domain and anticipate that this will lead to new collaborations, a further increased adoption of UKON research in both academia and industry, and potentially to subsequent projects in the area of cyber security in the long term. The targeted impact of scientific publications is to attract interest of the industry to initiate follow-up research and development projects. Additionally, UKON will use the knowledge gained in SPARTA for further research and within UKON Master and PhD programs.

UTARTU: The SPARTA project gives the University of Tartu enhance collaboration in the field of Cybersecurity, it opens the new potentially research and business opportunities. The main goals include contribute to the fields of the secure system design using novel technologies, contributing to the cyber security awareness and strengthening, establishing channels for developing and sharing recommendations for the best practices and decision-making support.

KEMEA is interested in bringing new solutions and training methodologies to the Hellenic Ministry of Interior. They will validate new solutions and build synergies with LEAs, critical infrastructures and scientific community. They will bring the SPARTA solutions to the attention of the Greek Ministry of Interior. Having strong links, under its constitutional law, with all Ministry supervised entities and to European associations and organisations (e.g., ESCO, EENA, Europol, CEPOL ENLETS).

NCSRD will focus on acquiring and transferring new knowledge on eGovernance and Critical Infrastructures protection services, developing a cyber-physical vulnerability framework. SPARTA will enhance their cyber-physical vulnerability analysis capabilities. They will participate in at least 6 conferences and workshop during the project period, will organise a daily session in the annual Demokritos Summer School and one workshop with national CI operators.

EUT will focus on developing a set of algorithms, technology and solutions to be included in the solution portfolio implemented in the commercial products of collaborating security companies. This

will improve their management and manufacturing digitization processes with security and privacy by design novel tools. They will participate in forums focused on security techniques and methodologies, carrying out demonstrations and technical WS

INDRA: Minsait Cybersecurity Technology branch develops novel products that are commercialised through its different vertical divisions as well as partners and channels all across the globe. For both disciplines (cyber situational awareness and cyber range), Indra has its own lines of product, which are regarded as strategic within the portfolio of cybersecurity products. The former is more in an initial research stage, whereas the latter is much more mature after +7 years of intensive research.

TECNALIA's exploitation strategy for SPARTA will be mainly related to technology transfer and to improve our knowledge in certain technologies to feed our research lines, turning knowledge acquired during the project into tools and mechanisms that will be transferred to the market. The exploitation target are companies interested in the development and deployment of cyber-security technologies, with special emphasis on companies interested in the deployment of advanced cyberattacks detection technologies in the industrial and health sectors. TECNALIA will transfer the knowledge and lessons learned to the companies interested in the development and deployment of cybersecurity technologies, with special emphasis on companies interested in the deployment of advanced cyberattacks detection technologies in the industrial and health sectors. TECNALIA IPR will be managed according to the consortium agreement to be signed in the negotiation phase. This will cover the use of foreground and background to ensure fair and open access to results and required components during the project and for exploitation.

VICOM is interested in developing cyber-secure AI technologies in the European framework and transferring the outcomes to the Basque and Spanish ICT industry. VICOM will maintain and strengthen their position as a reference agent in cybersecurity related R&D, supporting the Spanish cybersecurity network. They will invite external stakeholders to join dissemination activities and will promote the project outcomes in scientific publications, conference proceedings and event participation.

ANSSI expects that SPARTA will contribute to support its missions at the European level for all the domains listed above (R&D orientation and coordination, impact study on the certification capacities and link with the European certification scheme currently still in negotiation, awareness and training by building upon national referential like SecNumEdu).

IMT exploitation goals cover education and training, scientific research and technology transfer. In terms of training, SPARTA contributions will be included in the engineering programs, masters and professional education offerings of IMT. They will be promoted to our students. For professional education it will be marketed by our subsidiary Telecom Evolution.

INRIA: With regard to the exploitation of results, Inria intends to leverage on its capacity to produce high-quality software components that are produced as part of open-source projects, or under commercial license agreements.

TCS will exploit SPARTA results at various corporate levels, from the Advance Studies Lab to the Technical directorate levels. Showcase to supporting and/or interested business lines for potential transfers to corporate portfolio and route to market resulting offer across multiple sectors and critical infrastructures (e.g. defence, aerospace, security markets). Exploitation potential could ultimately reach up to 65 countries worldwide and a wide range of public and private organisations.

YWH: Bridging ethical hacking and EU Cybersecurity Actors

CINI: being a consortium formed by academic institutions, CINI's exploitation evolve around three main goals: i) improve the scientific know-how and the research potential through collaboration activities and knowledge transfer; ii) improve the ability to train, recruit, and prepare a new generation of skilled students capable to address the emerging cybersecurity threats, and iii) foster cyber security technology transfer from academia to enterprises, SMEs and startups. Research results from SPARTA will flow into the academic curricula and teaching programs at all levels (bachelor, master, doctorate) of the universities composing the CINI's consortium. Moreover, MSc and PhD

students will have the opportunity of being involved in the SPARTA activities. Teaching material and cybersecurity laboratory experiments will be updated with latest technological achievements and simulated t scenarios, SPARTA's results will be exploited for attracting industry research contracts and to launch new academic spin-offs.

CNIT: being a consortium formed by academic institutions, CNIT's exploitation evolve around three main goals: i) improve the scientific know-how and the research potential through collaboration activities and knowledge transfer; ii) improve the ability to train, recruit, and prepare a new generation of skilled students capable to address the emerging cybersecurity threats, and iii) foster cyber security technology transfer from academia to enterprises, SMEs and startups. Research results from SPARTA will flow into the academic curricula and teaching programs at all levels (bachelor, master, doctorate) of the universities composing the CNIT's consortium. Moreover, MSc and PhD students will have the opportunity of being involved in the SPARTA activities and thus benefit from the relevant opportunities. Teaching material and cybersecurity laboratory experiments will be updated with latest technological achievements and simulated t scenarios, SPARTA's results will be exploited for attracting industry research contracts and to launch new academic spin-offs.

CNR will focus on increasing their research capabilities, exploiting and improving current cyber security and privacy technologies, in particular the ones related to data usage control, which being deployed in growing domains. CNR will prioritize the need to continue protecting citizen's privacy. They will promote SPARTA over a number of international and journals organised by them, such as IFIP Trust Management conference, International Conference on ICT Systems Security and Privacy Protection or the TELERISE workshops. The outcomes will be also disseminated over the Italian technological platform in security research (SERIT), co-led by CNR.

ISCOM will exploit the project results to develop new methodologies in cyber-security certification.

LEO: Leonardo CyberSecurity and ICT Line of Business Research and Development. continuously develop and enrich its portfolio of cybersecurity products. SPARTA research activities are closely related to this portfolio and Leonardo plan to incorporate main results thus facilitating the innovation to market transition. The Resulting solutions will be delivered nationally, at the EU level and in international target markets (up to 40+ countries) in eGovernment, Critical Infrastructure, Defence, security and Aerospace markets).

KTU: SPARTA gives KTU an opportunity to expand their portfolio of entangled security solutions to the area of cybersecurity applications on the national and international scale. It is expected that international collaborations with security experts of the consortium will be reinforced and that new business opportunities will arise. Main goals are research and development on new cyber threat intelligence technologies and disseminate them through public-public and public-private partnerships and extend the KTU role as a key player's in cybersecurity related activities of the Lithuania and Baltic region. KTU will use the know-how gained in the project within collaborations with existing and new partners. Those partners are national cyber security authorities, telecommunications, industry and financial companies and innovative SMEs in the security domain.

L3CE's main interest is demonstrating the relevance and usability of newly developed solution "Full spectrum cyber security threat intelligence" for the successful operation of different stakeholder groups. The SPARTA outcomes will be transferred to Cybersecurity Practitioners, defence and military agencies. They will address three main target groups, such as external audiences (National, Regional, European Policy Makers); connected groups/audiences (FIDES, LEA networks, ENLETS); internal audiences over dissemination activities with end users positioned to take an advantage of the SPARTA results.

LKA: The results of the project will increase the expertise of the LKA in the field of cyber security and full-spectrum threats analysis. As LKA implements scientific researches for the MOD, which is responsible for formulation of national defence and security policy, as well as the national policy in the area of cyber-security, the results of the project will also contribute to the overall strengthening of national cyber security system: threat identification, perception, resilience, preventive measures

and so on. It is expected that the project will be beneficial for the whole national cyber security system enhancement and creation of useful partnership networks both at national and international levels.

MRU suggests agreeing on Roadmap for exploitation, by which the consortium will seek to multiply the projects results to wide audiences, measures, which would include the list of exploitable results, the main targets for each of the result and main contributors taking into ac-count the profile of the partners, as well as the indicators of the impact. MRU as a university can target society as a whole (including research community, institutions, students, school children (when it comes to awareness raising results).

LIST will focus on further researching on new enabling technologies and disseminating them through public-public and public-private partnerships in the greater region of Luxembourg. SPARTA will help becoming a key player in cybersecurity related activities of Luxembourg.

SMILE: Building on the results from SPARTA, SMILE will create dedicated dissemination and training support content targeted for the private and public sectors and the general public. The support will be tested and validated in partnership with SPARTA's network of excellence and SMILE's complementary ecosystem.

UNILU: As an academic partner, UNILU exploitation will be driven mainly by preparation of scientific publications for journals and conferences, organisation of Training and Courses based on the results of the project, awareness actions near user actors interested in cybersecurity.

LMT goals are to be a test bed for the "T-SHARK – Full spectrum cybersecurity awareness" Program and to provide all required support from mobile network operator side. LMT has been working on couple of research and development projects which are aimed to military in industry. Also, we see the projects "Full spectrum cyber security threat intelligence" as very importance for the industry.

NASK will develop methods and tools for detection and analysis of the threats relevant to a national CSIRT. The outcomes will be used in daily operations at CERT Polish and the information will be shared with a wide network of European CSIRTs using pre-existing and new collaboration channels. They will promote scientific conferences and academic journal submission in open-sourcing with a focus on CSIRT and vendors of cybersecurity solutions

ITTI will exploit the technical results in its work on innovative cyber detection machine learning based algorithms for sectors such as healthcare, law enforcement and network management. ITTI has also experience in developing feasibility studies, roadmaps, security guidelines and actions plans for national and European bodies (e.g. NATO). ITTI is going to exploit the SPARTA project results in order to enhance its consulting skills and services offered in the areas of cyber security sector for existing and new customers.

PPBW exploitation goals are related especially with developing training modules for public and private institutions. Through trainings which are organized by PPBW for public and private institutions in Poland (in 2017 PPBW has trained totally 3000 people from more than 1000 institutions. These were trainings on only dedicated to cybersecurity). They organise dozens of conferences, seminaries, trainings and meetings yearly for different type of public institutions (including LEA) in Poland (in 2017 PPBW has trained totally 3000 people from more than 1000 institutions).

INOV's main interest is increasing the expertise in the field of cybersecurity and to transfer this knowledge to the potential Portuguese end-users via their established partnerships with national CSIRTs, Cybersecurity Practitioners and local authorities. INOV will also exploit the project results by improving existing solutions and products and new research and business opportunities. INOV, as a responsible for INESC CSIRT (Portuguese national CSIRT network), which will be directly target.

IST: The results of the project will be taught in several of the courses of those programs. IST also aims to exploit the results of the project directly in its research after the end of the project. The team will push further the development of the research results obtained in this project. It will also foster the adoption by companies of the technologies it will develop in the project. For that purpose, it will promote these technologies in the context of consultancy activities it does with companies.

Chapter 3 Sustainability and IPR

3.1 Sustainability Plan

For a successful exploitation it is necessary to think about concrete objects that are able to survive after the end of the project.

The following steps need to be assured in order to pursue an efficient sustainability:

- STEP 1: Identify what outcomes does the coalition want to sustain over time and what strategies does the coalition need to sustain to achieve their outcomes
- SPEP 2: Identify what resources are required (cash, talent, technology, space, training) the coalition to sustain the strategies and outcomes overtime
- STEP 3: Create useful use cases. Use cases provide a rationale for fundraising and grant-seeking activities. They communicate the organization's values, purpose, and mission. The SPARTA project includes four different programs and each of them provides some use cases to demonstrate objectives and goals of the project. A useful use case should:
    - Grab attention
    - Build interest
    - Stimulate desire
    - Make a call to action
- STEP 4: Take into account Intellectual Property Right (IPR) issues (see par. 3.2 for details)
- STEP 5: Determine Funding Strategies, describing how the coalition plans to provide or develop needed resources to fund identified strategies.

Figure 3: Sustainability Plan

3.2 IPR issues

Commercialisation is the process of turning products and services into a commercially viable value. Concerning Intellectual Property (IP), this term can be more specifically defined as the process of bringing IP to the market in view of future profits and business growth.

3.2.1 Protect IP

Taking steps to protect intangible assets is not only necessary for companies proper management, but also for getting full benefit from those assets.

When considering IP protection, it must be noted that IP assets can be protected by several types of IPR, and consequently the most appropriate protection strategy must be chosen pertinent to the marketing strategy.

IPR require constant monitoring, which is the responsibility of the owner. Hence, it is best practice to monitor the market and competitors to be sure of identifying any infringing actions.

Applying for customs protection to fight against counterfeiting and piracy is also a cost-effective prevention measure to deter infringing conducts. It allows the fake goods to be seized and destroyed before entering the market.

Alternative Dispute Resolution (ADR) mechanisms may also be utilised as time and cost efficient measures to solve IP related disputes out of court.

3.2.2 Assignments

An IP assignment is a transfer of ownership of an IPR, such as a patent, trade mark or design, from one party (the assignor) to another party (the assignee). Consequently, the assignee becomes the new owner of the IPR.

Assignments are useful tools for commercialisation, when the owner of the IP does not have enough capabilities (financial, HR, marketing, etc.) to market the developed intellectual asset and/or when the owner would like to realise an immediate cash flow from an IP asset, which he does not plan to exploit with its own resources.

By its very nature, an assignment process involves detailed negotiations and requires exclusive information to be shared between the parties, even though the process does not lead to an agreement in the end.

Therefore, Non-Disclosure Agreements (NDAs) are important tools to guarantee that any shared confidential information will not be disclosed or used for purposes other than the negotiation.

3.2.3 Licensing

Licensing has a vital role in companies' commercialisation strategies, since there are significant advantages of licensing IP, creating a win-win situation for both parties as showed in the following table:

For Licensor	For Licensee
Opportunity to reach new markets with existing products/ services.	Opportunity to create new businesses.

For Licensor	For Licensee
Opportunity to enter a market with existing clientele of the licensee, which reduces risks for market failure.	Opportunity to provide licensor's already available/well established products/services to the clients, which reduces risks for market failure.
No need to invest in marketing and distribution.	No need to invest on R&D.
The licensor retains ownership of the IP while receiving royalty income from it.	The licensee does not need to "purchase" the IP and use the opportunity to test market success of the licensed product/service without investing much.

Table 1: Benefits of licensing for both parties

Besides, licence agreements can also be seen as an instrument for the distribution of risks between the licensor and the licensee.

Licensing agreements are usually long term business partnerships. It is therefore common that before entering into such an agreement, carrying out a due diligence audit and signing preparatory agreements, such as Non-Disclosure Agreements (NDAs) or Material Transfer Agreements (MTAs) help both parties mitigate the risks during the negotiations and towards the licensing period.

The difference between Assignments and Licence agreement is reported in the following table:

Assignment	Licensing
The party "selling" the IP: assignor The party "buying" the IP: assignee	The party "renting out" the IP: licensor The party "renting in" the IP: licensee
The owner of IP changes and becomes the assignee.	The owner of IP does not change and remains the licensor.
An assignment is a permanent transfer of rights	A licence is a temporary transfer of certain rights.

Table 2: Comparison between Assignments and Licence agreement

3.2.4 Joint Ventures

Joint Ventures are business alliances of two or more independent organisations (venturers) to undertake a specific project or achieve a certain goal by sharing risks.

IP has an important role in the creation of such collaborations, since venturers bring their own intellectual assets for the success of a JV and they should agree on their initial contributions, responsibilities and obligations within the alliance as set out in JV agreements.

Advantages

- Gives opportunity to exploit and share IP assets with reduced financial investment.
- Allows companies to access new markets by sharing risks.

- Creates possibilities to leverage existing technologies and patents developed by each venturer.
- Provides companies with the chances to develop new IP with less investment.
- Allows utilisation of unused IP assets.

Disadvantages

- There may be an imbalance in expertise, intellectual assets and investment brought into the JV by the venturers.
- Coping with different management cultures in IP management may be difficult.

3.2.5 Non-Disclosure Agreements (NDAs)

NDAs are legally binding contracts establishing the conditions under which one party (the disclosing party) discloses information in confidence to another party (the receiving party).

The common characteristic of these agreements is that the disclosed information is valuable for the disclosing party to the extent that it must be kept away from the public domain.

Therefore, an NDA is a tool to be used to reduce the risks for possible disclosure of information, when there is a need to grant access to confidential information, e.g. when entering into a partnership such as licensing.

3.2.6 Consortium Agreements (CAs)

CAs are contracts, made between “consortium partners”, to set out rights and obligations during a temporary partnership for the purposes of carrying out a specific project.

CAs minimise the probability of later disputes as they provide rules and responsibilities for the parties during the project together with the access rights to be granted to the partners concerning the project results.

The following point have to be considered in CAs:

- Define the project and the project term.
- Describe the management rules of the consortium including the
- IP management scheme.
- Provide the list of background IP provided by each consortium
- partner and define the related access rights and conditions.
- Set out the rules for exploitation and dissemination of results:
    - results ownership regime and provisions,
    - access rights of other partners,
    - responsibilities with regard to IP protection of results,
    - provisions for transfer of ownership,
    - involvement of third parties,
    - other responsibilities for exploitation and dissemination (publications, handling confidential information in promotional activities etc.)

3.2.7 SPARTA Consortium Agreement differences respect to DESCA model

The consortium agreement signed by all SPARTA partners is based on DESCA model [3].

Some adjustments have been made in order to be aligned to the specific context and to the interests of the partners involved in the project.

For what concerns Exploitation, IPR, Licence and Access Rights, the following modifications have been made respect to DESCA model.

Exploitation

In the SPARTA CA the following definition of Exploitation was added to §1.2 (such definition is not present in the DESCA document). This addition regards the use of results in further research activities other than those covered by the action concerned.

"*Exploitation or Exploit means the use of Results in further research activities other than those covered by the Action concerned, or commercial exploitation in developing, creating and or marketing of a product or process, or in creating and providing a service, or in standardization activities*."

Veto rights

The SPARTA C.A. adds the following clause to §6.2.4.2.3: "*a party requesting to leave the consortium which may veto decisions relating to the terms and conditions of its leave being expressly specified that such party shall inform the other Parties of its intent to leave the Consortium at least three (3) months before the date on which its departure will be effective or negotiate to find solutions, in good faith and on a best effort basis, to issues that may result from its leaving for other Parties*".

Members

Regarding the General Assembly Member, the following clause was added (§6.3.1.1.2): "*Each General Assembly Member shall be deemed to be duly authorized to deliberate, negotiate and decide on all matters listed in Section 6.3.1.2. of this Consortium Agreement subject to approval of the legal representatives of each Party, according to each Party's internal regulations and procedures*".

Strategic Direction board

DESCA does not envisage a "Strategic Direction" board, the SPARTA supervisory body for the strategy of the Project and a decision-making body of the Consortium, which reports to and is accountable to the General Assembly. In this regard, the SPARTA C.A. establishes that:

The General Assembly has the prerogative to cancel a decision taken by the Strategic Direction in relation to Content, finances and intellectual property rights

- on the proposal for changes to Annexes 1 and 2 of the Grant Agreement to be agreed by the funding Authority
- on the change in the Consortium Plan,
- on the evolution of the consortium on the identification of a breach by a Party of its obligations under the Consortium Agreement or the Grant Agreement
- on the Declaration of a Party to be a Defaulting Party and the remedies to be performed by a Defaulting Party.

In addition, the Strategic Direction board can also, upon its own initiative, take decisions in relation to content, finances and intellectual property rights on the above points.

Dissemination of own Results

The disseminations of own results envisages some clauses regarding possible objections. Compared to DESCA, SPARTA C.A. adds two more clauses: an objection is justified when the

proposed publication includes a Confidential Information of the objecting Party or is subject to ethical issues (§ 8.4.2.4)

Access Rights General principles

Respect to DESCA, SPARTA C.A. adds a clause regarding Research Organisations which – in specific cases – are allowed to sub-licence to third parties.

Sublicensing

SPARTA CA adds the following: "*Any Access Rights granted expressly exclude any rights to sublicense to third parties other than Affiliated Entities unless expressly stated otherwise or unless a party, such as a Research Organization, is unable to exploit directly the results and accordingly needs to sublicense the Access Right in order to carry out an Exploitation activity being specified that in such a case the possible sublicense shall be made by a traceable agreement specifying the attached terms and conditions and protecting the proprietary rights of the Party or Parties concerned*".

Access Rights For Exploitation

SPARTA CA regarding "Rights to Results if Needed for Exploitation of a Party's own Results", states that they shall be granted on Fair and Reasonable conditions and upon prior written agreement. Access rights to Results for internal research activities and for educational and non- commercial teaching purposes are hereby requested (in accordance with the requirements of the Grant Agreement), and shall be deemed granted on a royalty-free basis, non-exclusive, basis to and by all Parties as of the date of the Grant Agreement entering into force.

Access Rights Non Covered By The GA/CA

SPARTA CA states that Any grant of Access Rights not covered by the Grant Agreement or this Consortium Agreement, shall be at the absolute discretion of the owning Party and subject to such terms and conditions as may be agreed between the owning and receiving Parties.

Party Joining The Project After The Date Of GA

This section differs from the original DESCA and concerns Party joining the Project in accordance with the provisions of the Grant Agreement and this Consortium Agreement after the date of the Grant Agreement entering into force which will be granted Access Rights, as provided for in Sections 9.1-9.6 above, effective as from the date of its signature of the declaration of accession, provided however, as regards Results developed before the accession of the new Party, the new Party will be granted Access Rights on the conditions applying for Access Rights to Background.

Specific Provisions for Access Rights to Software

This section differs from the original DESCA and regards the general provisions for Access Rights which are provided Section 9 are also applicable to Software.

Parties' Access Rights to Software do not include any right to receive source code or object code ported to a certain hardware platform or any right to receive respective Software documentation in any particular form or detail, but only as available from the Party granting the Access Rights.

It is understood that any request for Access Rights shall be made by writing and shall be granted by separate agreement.

Parties' Access Rights To Software

This section differs from the original DESCA. It concerns parties' Access Rights to Software which do not include any right to receive Source Code or Object Code ported to a certain hardware platform or any right to receive Source Code, Object Code or respective Software Documentation in any particular form or detail, but only as available from the Party granting the Access Rights.

Unless otherwise agreed by the owner of the Software, Access Rights to Software apply only to the Object Code (i.e. the compiled, assembled, or machine executable version of the Software).

The intended introduction of Intellectual Property (including, but not limited to Software) under Controlled License Terms in the Project requires the approval of the Strategic Direction to implement such introduction into the Consortium Plan. However, Parties have listed in Attachment 5 the Intellectual Property under Controlled License Terms that will be used in the Project and for which the Parties have upfront permission to use it in the Project.

General Provisions For Access Rights

This section differs from the original DESCA regarding general provisions for Access Rights.

Parties' Access Rights to Software do not include any right to receive Source Code or Object Code ported to a certain hardware platform or any right to receive Source Code, Object Code or respective Software Documentation in any particular form or detail, but only as available from the Party granting the Access Rights.

The intended introduction of Intellectual Property (including, but not limited to Software) under Controlled Licence Terms in the Project requires the approval of the General Assembly to implement such introduction into the Consortium Plan.

Sublicense Access Rights

This section differs from the original DESCA and deals with Access Rights, affirming that each of them and possible sublicense granted according to the provisions of Section 9.8.4 shall be made by a traceable agreement specifying the attached terms and conditions and protecting the proprietary rights of the Party or Parties concerned.

Chapter 4 Actions to develop the Exploitation Plan

On the basis of what described in the previous paragraphs, here we present a plan to identify main steps and activities for the final SPARTA Exploitation Plan. The development of the plan will take place in four steps.

Figure 4: Exploitation Plan activities

a) **Identify Stakeholders And Exploitable Areas**: The result of this activity is represented by the outputs of the present deliverables. The analysis covers the whole SPARTA project as well as the specific SPARTA programs.

b) **Confirm key results areas that will be exploited**: The analysis made in step a) is carried out at the beginning of the SPARTA project, whose duration is three years. An activity that confirm or modify key exploitable areas needs to be carried out toward the end of the project.

c) **Confirm target groups and beneficiaries:** For the same reason as above, toward the end of the project.it is necessary confirm/modify the stakeholders identified in step a), as well as it is necessary to update the market an competition analysis

d) **Finalize the Exploitation Plan**, which includes the following activities

- Define targets, indicators and milestones to ensure the project's results are properly exploited after the completion of the current project
- Check sustainability (see Section 3)
- Specify guidelines for the transfer of project results outside the original project network.
- Timeline to bring proposed solutions to market
- Timeline for dissemination activities

- Business model:
  - *Pricing*
  - *Financial Plan, if relevant*

Preliminary definition of management structures and procedures, including governance, policies, systems, structures and operation processes and risk management

Chapter 5 Summary and Conclusion

In this deliverable we have described how SPARTA project results can be exploited for future developments taking into account Sustainability and IPR issues.

First of all it's necessary to identify the main results of the SPARTA project that could be exploited, that are:

- Results related to the overall concept of SPARTA project that is to provide valuable inputs for the future set-up of a Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre.
- Results derived from SPARTA Research Programs based on specific objectives of such programs

Second step is identify relevant target stakeholders for this type of exploitable areas,

The exploitation needs to be and sustainable, so the exploitation plan must be linked to a sustainability plan that identify resources required to sustain outcomes, consider IPR issues, and determine funding strategies.

Considering the project duration (three years) the exploitation plan must foresee, toward the end of the project, to confirm/modify key results areas that will be exploited (according to sustainability) and confirm/modify target stakeholders.

As last step, a business model needs to be provided. This will be the subject of deliverable 10.6 "Commercial Deployment Plan".

Chapter 6 List of Abbreviations

Abbreviation	Translation
AI	Artificial Intelligence
ADR	Alternative Dispute Resolution
CA	Consortium Agreement
CAPE	Continuous Assessment in Polymorphous Environments
CERT	Computer Emergency Response Team
CNAP	Cybersecurity National Action Plan
CSIRT	Computer Security Incident Response Teams
Ct&eF	Cyber training & exercise Framework
DESCA	Development of a Simplified Consortium Agreement
ECSO	European Cyber Security Organisation
ENISA	European Union Agency for Cybersecurity
ENLETS	European Network of Law Enforcement Technology Services
EU	European Union
EUFPS	European Union's Foreign And Security Policy
GA	Grant Agreement
HARA	Hazard Analysis and Risk Assessment
HAII-T	High-Assurance Intelligent Infrastructure Toolkit
II	Intelligent Infrastructure
IoT	Internet of Things
IP	Intellectual Property
IPR	Intellectual Property Rights
JRC	Joint Research Centre
JV	Joint Ventures
LEA	Law Enforcement Agencies

Abbreviation	Translation
MoD	Ministry of Defence
MoI	Ministry of Interior
MoJ	Ministry of Justice
NCC	National Coordination Centres
NDA	Non-Disclosure Agreement
NIS	Network and Information Security
R&D	Research and Development
RTO	Research and Technology Organisations
SAFAIR	Secure and Fair AI Systems for Citizen
SME	Small Medium Enterprise
SPARTA	Strategic Programs for Advanced Research and Technology in Europe
TARA	Threat Assessment & Remediation Analysis

Chapter 7 Bibliography

[1] European IPR Help Desk (http://www.iprhelpdesk.eu/)
[2]] Strategic Programs for Advanced Research and Technology in Europe (SPARTA) - (Proposal ID: 830892)
[3] DESCA - Horizon 2020 Model Consortium Agreement (www.DESCA-2020.eu) Version 1.2, March 2016