

# SRI ROADMAP FOR CYBERSECURITY

**Thomas Jensen, INRIA** 

@sparta\_eu sparta.eu

July 2021

## 1 – INTRODUCTION THE SPARTA ROADMAP

#### **Mission-oriented:**

Shape the cybersecurity technologies required to establish and maintain a European Strategic Digital Autonomy

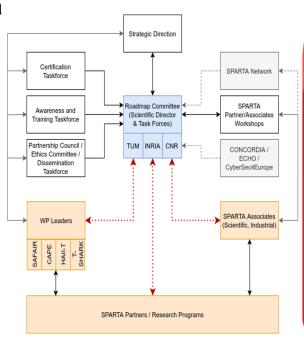
Design process: agile and open

### **Expected outcome:**

- ► Roadmap provides a mid- to long-term vision on cybersecurity challenges
- Roadmap provides guidelines for decision makers to develop strategies
  - to strengthen the EU's cybersecurity capacity,
  - to close cyber skill gaps and,
  - ▶ to address emerging challenges appropriately

#### **Cross-Pilots:**

Harmonize the different roadmapping approaches of the 4 pilots



## **ROADMAP PROCESS**

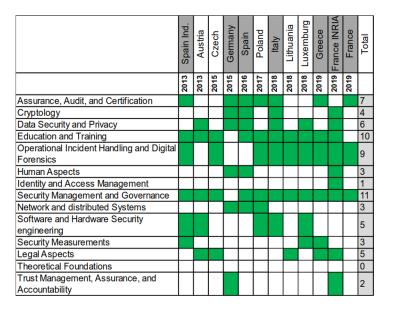
## **Initial Roadmap Design**

- Defined with input from SPARTA's partners:
  - Collected 60 "seed challenges" to establish European Strategic Autonomy
- Roadmap foundations:
  - Analysis of strategic research Agendas (national, EU) and Alignment to JRC Taxonomy.

Research Domains

Technologies

Sectors



|   | Spain Ind. | Austria | Czech | Germany | Spain | Poland | Italy | Lithuania | Luxemburg | Greece | France INRIA | France | Total |
|---|------------|---------|-------|---------|-------|--------|-------|-----------|-----------|--------|--------------|--------|-------|
|   | 2013       | 2013    | 2015  | 2015    | 2016  | 2017   | 2018  | 2018      | 2018      | 2019   | 2019         | 2019   |       |
| Artificial intelligence;                                  |            |         |       |         |       |        |       |           |           |        |              |        | 4     |
| Big Data;   |            |         |       |         |       |        |       |           |           |        |              |        | 4     |
| Blockchain and Distributed Ledger<br>Technology (DLT);    |            |         |       |         |       |        |       |           |           |        |              |        | 2     |
| Cloud and Virtualisation;                                 |            |         |       |         |       |        |       |           |           |        |              |        | 4     |
| Embedded Systems;   |            |         |       |         |       |        |       |           |           |        |              |        | 3     |
| Hardware technology (RFID, chips, sensors, routers, etc.) |            |         |       |         |       |        |       |           |           |        |              |        | 0     |
| Industrial Control Systems (e.g. SCADA);                  |            |         |       |         |       |        |       |           |           |        |              |        | 6     |
| Information Systems;                                      |            |         |       |         |       |        |       |           |           |        |              |        | 1     |
| Internet of Things;                                       |            |         |       |         |       |        |       |           |           |        |              |        | 4     |
| Mobile Devices;   |            |         |       |         |       |        |       |           |           |        |              |        | 1     |
| Operating Systems   |            |         |       |         |       |        |       |           |           |        |              |        | 0     |
| Pervasive systems   |            |         |       |         |       |        |       |           |           |        |              |        | 0     |
| Quantum Technologies;                                     |            |         |       |         |       |        |       |           |           |        |              |        | 2     |
| Robotics;   |            |         |       |         |       |        |       |           |           |        |              |        | 2     |
| Satellite systems and applications;                       |            |         |       |         |       |        |       |           |           |        |              |        | 1     |
| Supply Chain;   |            |         |       |         |       |        |       |           |           |        |              |        | 2     |
| Vehicular systems   |            |         |       |         |       |        |       |           |           |        |              |        | 0     |

|                                   | Spain Ind. |      | Czech |      | Spain | Poland |      |      | Luxempurg | Greece | Fra  | France | Total |
|-----------------------------------|------------|------|-------|------|-------|--------|------|------|-----------|--------|------|--------|-------|
|                                   | 2013       | 2013 | 2015  | 2015 | 2016  | 2017   | 2018 | 2018 | 2018      | 2019   | 2019 | 2019   |       |
| Audiovisual and media             |            |      |       |      |       |        |      |      |           |        |      |        | 0     |
| Defence                           |            |      |       |      |       |        |      |      |           |        |      |        | 1     |
| Digital Infrastructure            |            |      |       |      |       |        |      |      | Г         |        |      |        | 0     |
| Energy                            |            |      |       |      |       | Г      |      |      |           |        |      |        | 4     |
| Financial                         |            |      |       |      |       |        |      |      |           |        |      |        | 3     |
| Government and public authorities |            |      |       |      |       |        |      |      |           |        |      | Г      | 1     |
| Health                            |            |      |       |      |       | Г      |      |      |           |        |      |        | 5     |
| Maritime                          |            |      |       |      |       |        |      |      |           |        |      |        | 0     |
| Nuclear                           | Т          |      |       |      | Г     |        | Г    |      | Г         |        |      | Г      | 0     |
| Public safety                     |            |      |       |      |       |        |      |      | Г         |        |      |        | 0     |
| Tourism                           |            |      | Г     |      |       | Г      |      |      | Г         |        |      |        | 1     |
| Transportation                    |            |      |       |      |       |        |      |      |           |        |      |        | 4     |
| Smart ecosystems                  |            |      |       |      |       |        |      |      |           |        |      | Г      | 1     |
| Space                             |            |      |       |      |       |        | Г    |      |           |        |      | Г      | 1     |
| Supply Chain                      |            |      |       |      |       |        |      |      |           |        |      |        | 0     |

## **ROADMAP V1**

13 MPs defined
Goal
Timeline
Contributions

Original SPARTA research programs marked in red squares

#### SAFAIR Enhanced explainability and better threat understanding in AI context Systems using AI more reliable and resilient More effective methods and tools for analysis of security threats for User-centric Data Al systems Governance Comprehensive cybersecurity threat A set of techniques and solutions The goal of any activity in intelligence for AI systems protection privacy is to give the ability for individuals to control their Early stage cybersecurity Systems in place to ensure threats detection, prediction personal data and decide fairness of AI systems Security and Safety Co-Complex Dynamic and response capability what to reveal, to whom, and Systems of Systems assessment under what condition. To this Defensive and reactive Capability to tackle end, several dimensions mechanisms geared towards novel Development of Develop methods and complex cybersecurity need to be considered: at the cybersecurity threats Cybersecurity Cybertools for the automated threats (Full spectrum, principle and regulation level, physical systems, where assessment of complex Multi-Stage, Unique, longat the PET level, and in Cybersecurity systems being able security and safety are dynamic systems of term, APT's) existing systems of our to detectstegomalware covered. systems. connected world. 2024 2021 2022 2023 2025 2026 2027 2028 2029

## Certification organization and support

Identification of commonalities and differences between national cybersecurity certification initiatives and recommendations for convergence at European level.

#### Education and Training in Cybersecurity

Provide best-practice curricula for both universities and training institutions reflecting skills necessary for a wide spectrum of roles in cybersecurity. Rollout the programs at a substantial number of universities.

#### HAII-T

Secure-by-design development framework and toolkit supporting the design, development and verification of security-critical, large-scale distributed II systems.

#### Trustworthy Software

A comprehensive collection of theories, techniques and tools that can enhance the trust we have in the security of our software.

#### Autonomous Security for Self-protected Systems

Following the idea of autonomous computing, this challenge ultimately aimed to develop a computer system capable of self-managing its own security. The goal is thus to produce an environment that will be able to correct by itself the security defects that attacks would have revealed.

#### Quantum Information Technology

a ability
introl their
lecide
hom, and
in. To this
sions
red: at the
tion level,
d in

Guantum theory is entering
the area of
information technology.
Quantum communication is
emerging as a technology
and it is likely that building a
universal quantum
computer will become
feasible in the next decades.

#### Next-Generation Computing Architectures

It becomes important to research new security technologies and integrate them into Next-generation computing components and systems to ensure European technical sovereignty while leveraging global trends.

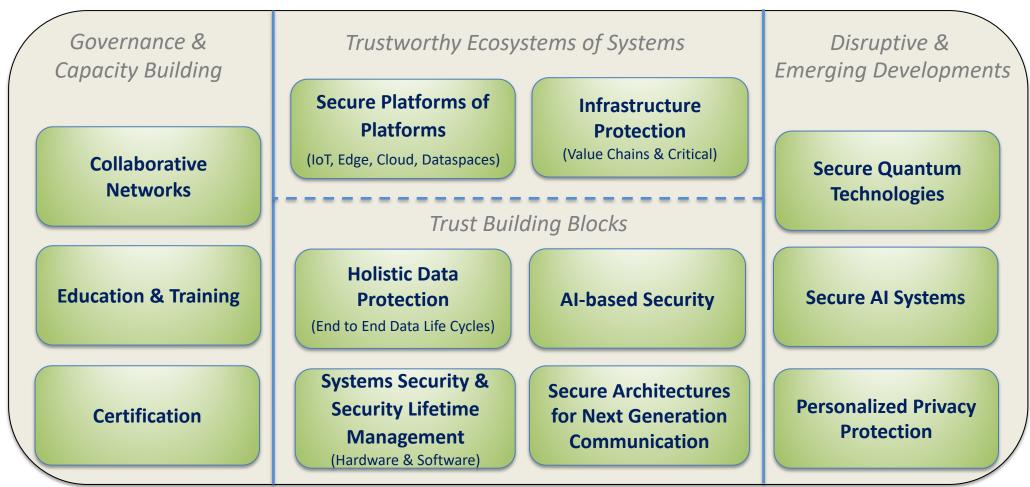
#### 5+NG Security

5G technology does not only provide a new, faster and more reliable communication facilities, it also opens the possibility for transferring a higher amount of (sensitive) data. This data should be protected from abuse and software providers or dishonest network facility providers.



# Cybersecurity Research Focus Areas Priorities The 4 Pilots & ECSO Perspective

As per May 2021



Each of these Cybersecurity Research Focus Areas Priorities are generally intertwined with each other.





## **THANK YOU!**

@sparta\_eu | sparta.eu

roadmap@sparta.eu

April 2021

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

