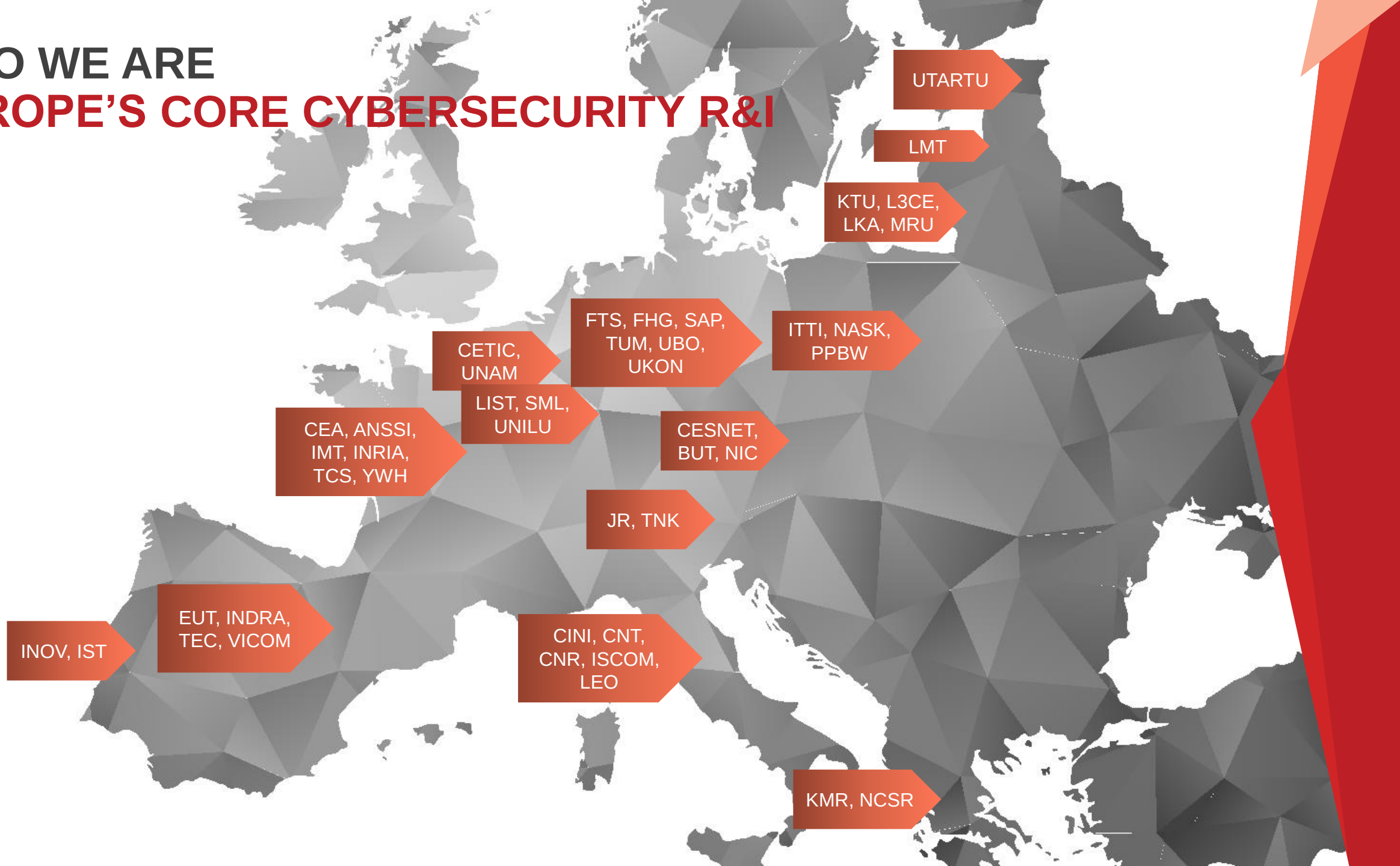
NOW'S THE TIME FOR EUROPEAN CYBERSECURITY

F. KIRCHNER
CyberTech
Rome, Italy

@sparta_eu
sparta.eu
September 24, 2019

WHO WE ARE
EUROPE'S CORE CYBERSECURITY R&I



SPARTAN DISRUPTIONS

STRATEGIC SURPRISE

Risky and complex developments

Concrete and transformative results

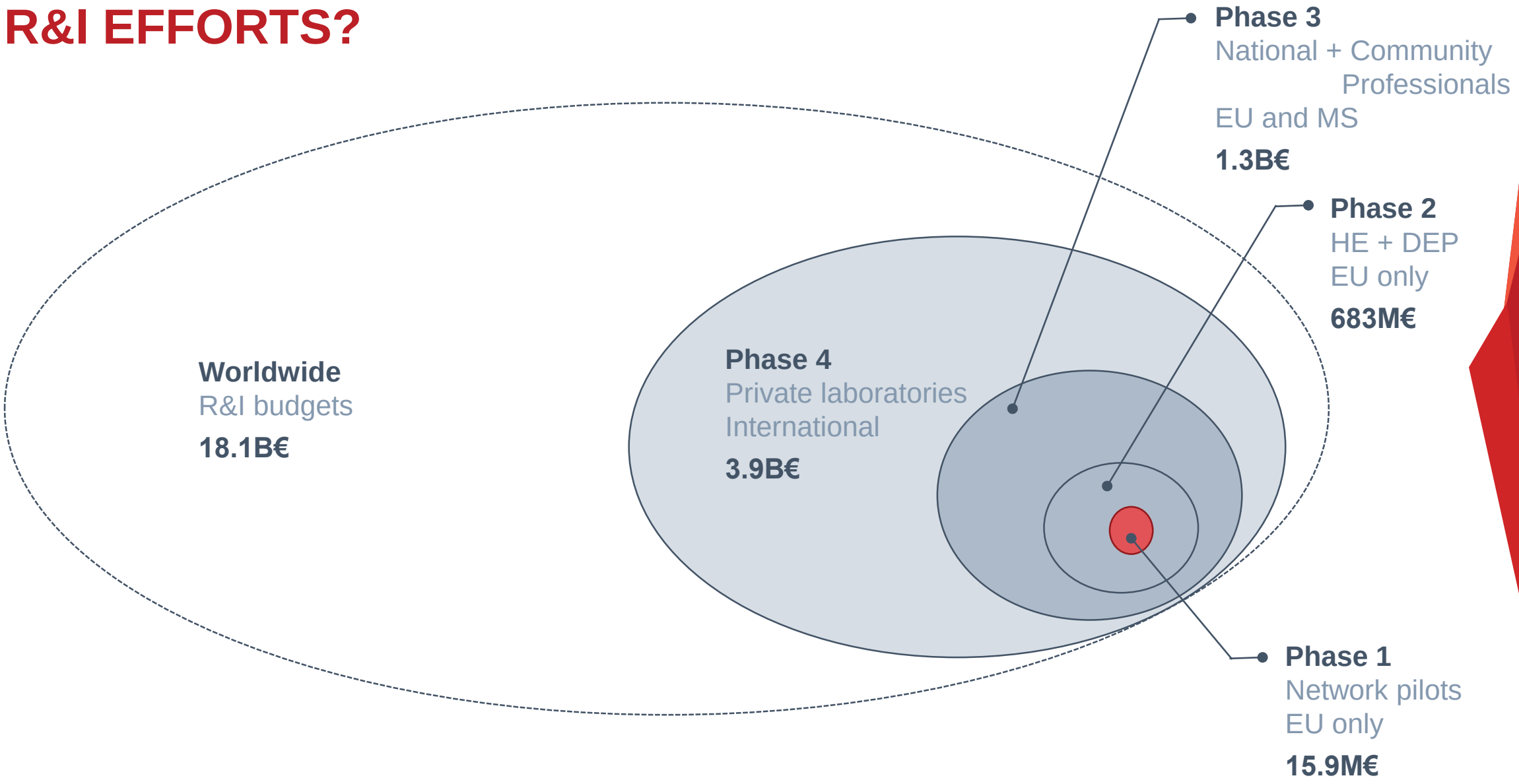
NETWORK OF COMPETENCE CENTERS

- Strong academic performers
- Insufficient critical mass

- Diversity and inclusion
- Open leadership

- Intensified partnerships
- World-leading capacities

HOW BIG ARE CYBERSECURITY R&I EFFORTS?



SOURCES: US FY2019 FEDERAL CYBERSECURITY R&D STRATEGIC PLAN IMPLEMENTATION ROADMAP
ENISA CONSULTATION PAPER - EU ICT INDUSTRIAL POLICY: BREAKING THE CYCLE OF FAILURE
PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 2018/0328

THE COMPETITION
SKILLFUL AND ORGANIZED

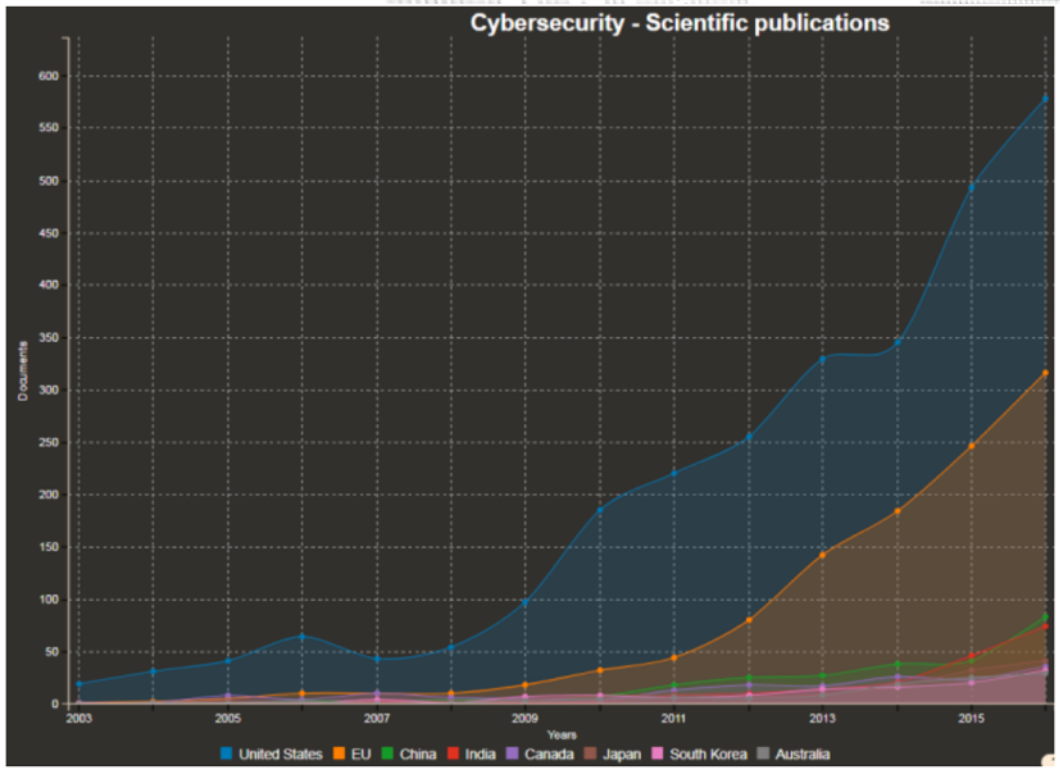


Figure 32. Scientific publications in Cybersecurity per country (Europe = orange).

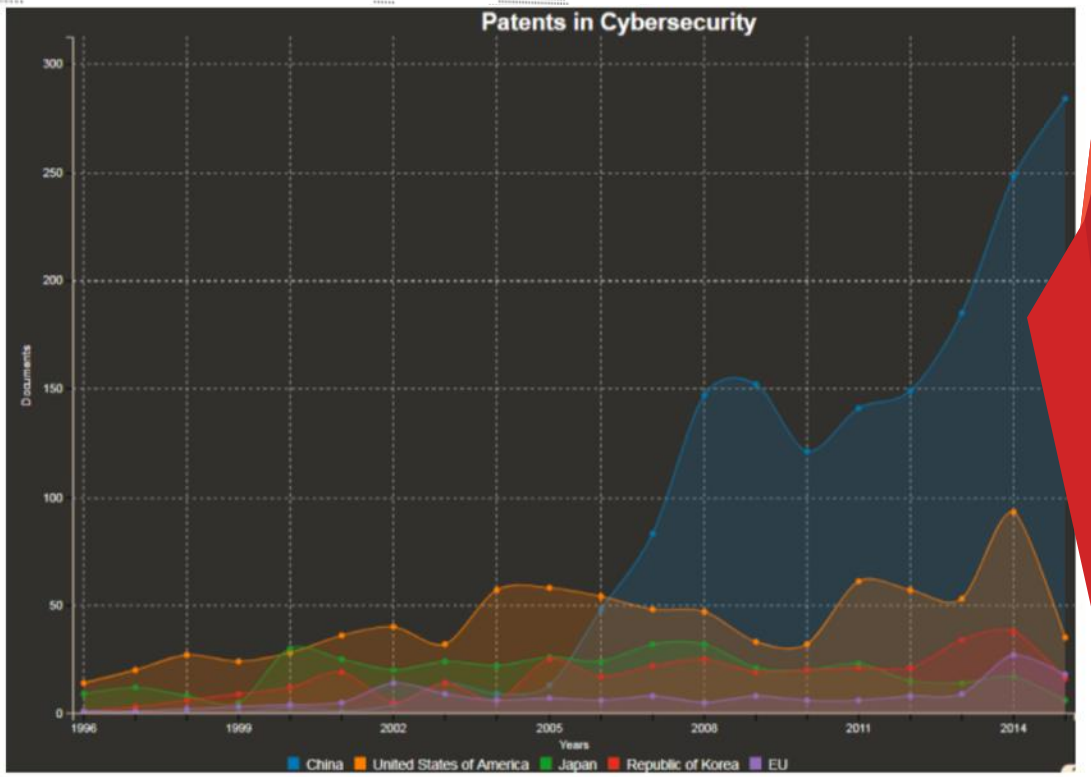


Figure 35. Patents in Cybersecurity per country (Europe = pink)

SOURCE: JRC TECHNICAL REPORTS, EUROPEAN CYBERSECURITY CENTRE OF EXPERTISE, CYBERSECURITY COMPETENCE SURVEY, EUR 29330 EN

SPARTAN ASSETS

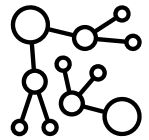
Expertise
135 m.yr

Infrastructure
30+ initial inventory

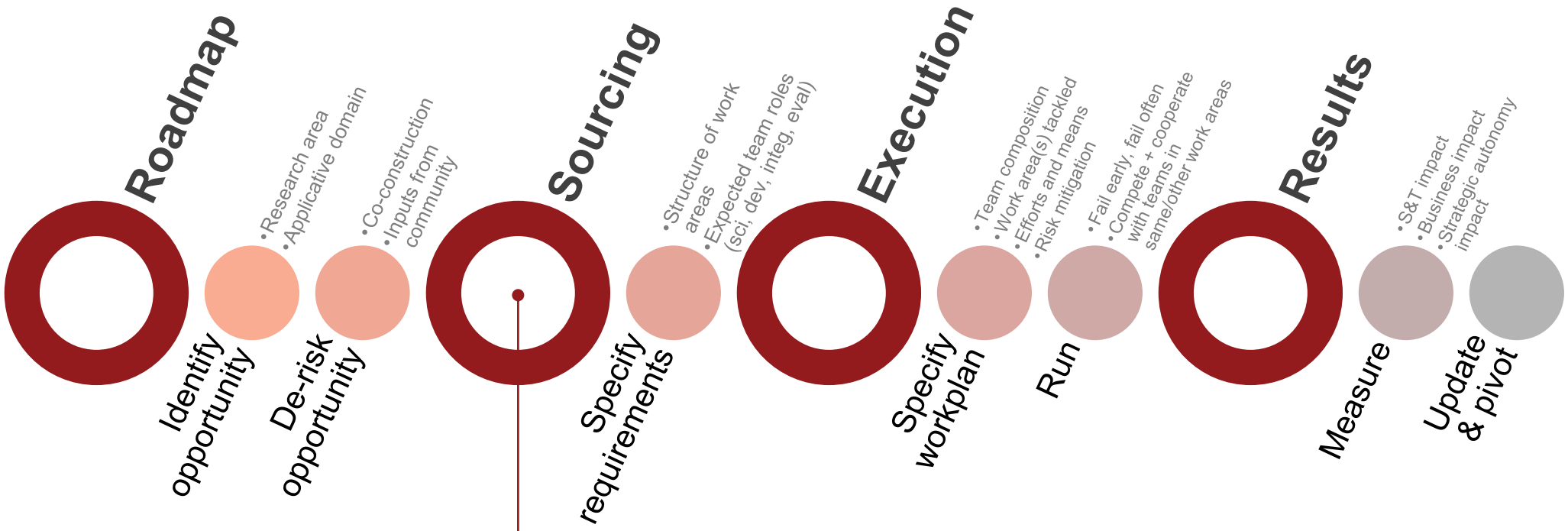
PILOT NETWORK

Ecosystems
60+ initial supporters

Dynamics
Regional x National



THE INNOVATION PUMP
FLOWING IDEAS INTO INNOVATION



- **T-SHARK** Full-spectrum cybersecurity awareness
- **CAPE** Continuous assessment in polymorphous environments
- **HAII-T** High-assurance intelligent infrastructure toolkit
- **SAFAIR** Secure and fair AI systems

THE INNOVATION PUMP
FIRST MOONSHOTS

T-SHARK Full-spectrum cybersecurity awareness

- **objective** : expand the reach of threat understanding, from the current investigation-level definition, up to strategic considerations, and down to real-time events
- **requires** : collection of heterogeneous data, models and predictions for multi-level security, AI and visualization
- **strengths** : regulation encouraging information-sharing (NIS directive, French OIV law, ...), strong culture of data protection (GDPR, cryptography, ...)
- **aims at** : providing decision-making tools, fostering a common cyber security culture, raising preparedness for possible disruptions and attacks
- **capabilities** : thoroughly supervise critical systems including when they are not provided / integrated by EU actors, raise awareness and citizen involvement

CAPE Continuous assessment in polymorphous environments

- **objective** : enhance assessment processes to be able to perform continuously over HW/SW lifecycles, and under changing environments
- **requires** : binary and code verification, scalable monitoring, network reaction, HW/SW roots of trust, dynamic assurance cases
- **strengths** : one of the best evaluation ecosystem in the world (Common Criteria, smart cards, ...)
- **aims at** : building tools for continuous trust in sovereign and foreign-sourced components, systems, and services
- **capabilities** : drastically increase evaluation capabilities in a world where most of the components are developed outside of the EU, prepare future certification

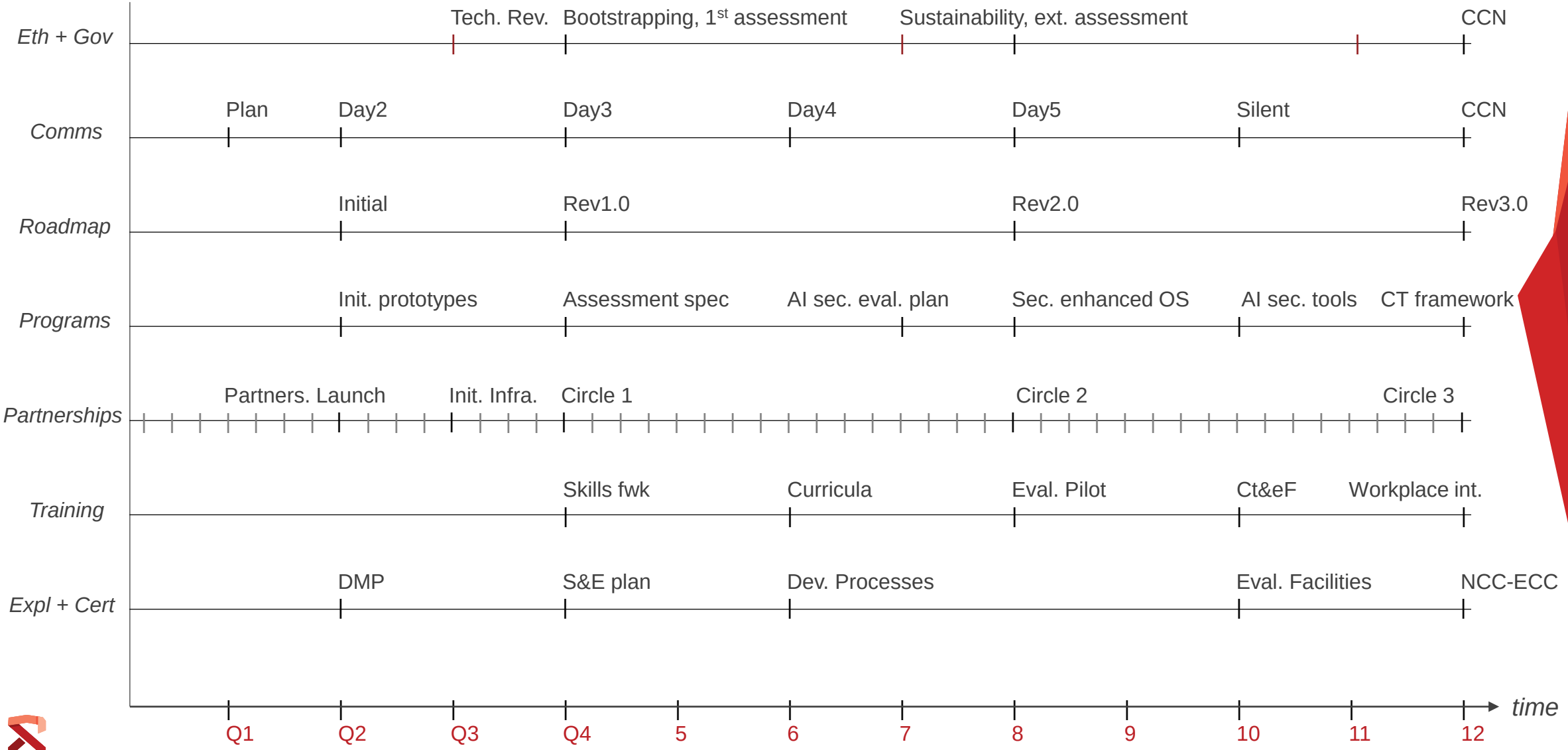
HAII-T High-Assurance Intelligent Infrastructure Toolkit

- **objective** : manage the heterogeneity of the IoT by providing a secure-by-design infrastructure that can offer end-to-end security guarantees
- **requires** : formal security models, application security, verification and validation, verified and scalable cryptography, secure OS
- **strengths** : building on EU's lead position on formal methods for safety and security
- **aims at** : providing a full verified software stack from applications down to the system software and SW/HW interface, which can serve in a variety of IoT devices
- **capabilities** : simplify the the deployment of IoT applications ; facilitate their certification

SAFAIR Secure and fair AI systems

- **objective** : Evaluating security of AI systems, producing approaches to make systems using AI more robust to attackers' manipulation. Furthermore, the goal is to make AI systems more reliable and resilient through enhanced explainability and better understanding of threats
- **requires** : adversarial machine learning, data from different AI application domains
- **strengths** : increasing adoption of AI technology in various information systems within EU, recent strategy of EU member states to collaborate on Artificial Intelligence
- **aims at** : providing methods and tools for analysis and assessment of security threats for AI systems, and solutions for protection
- **capabilities** : exploratory

OVERVIEW
FIRING ON ALL CYLINDERS



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