



# Cyber security challenges

Fabio Martinelli  
National Research Council of Italy (CNR)  
European Cyber Security Organization (ECSO)

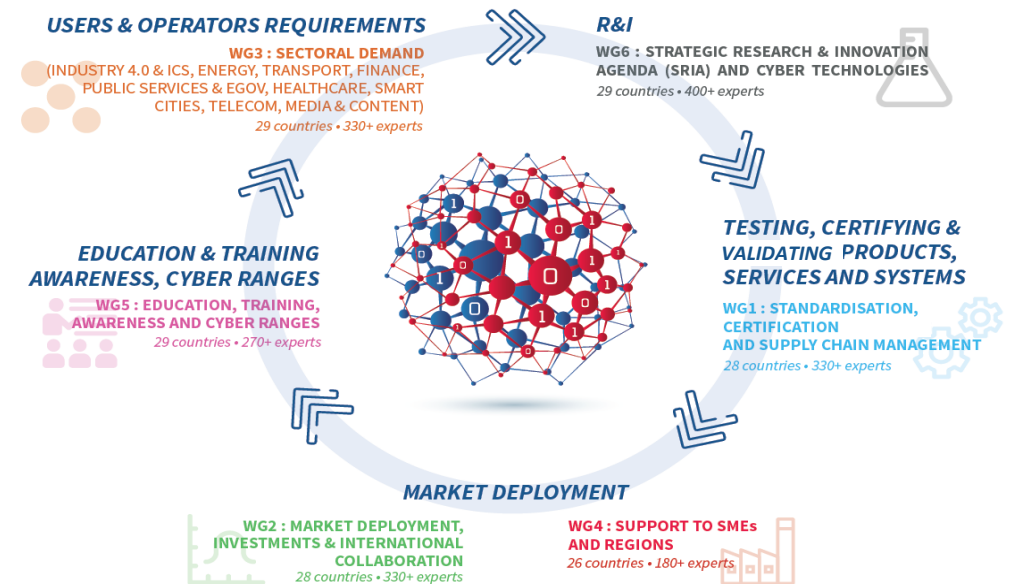
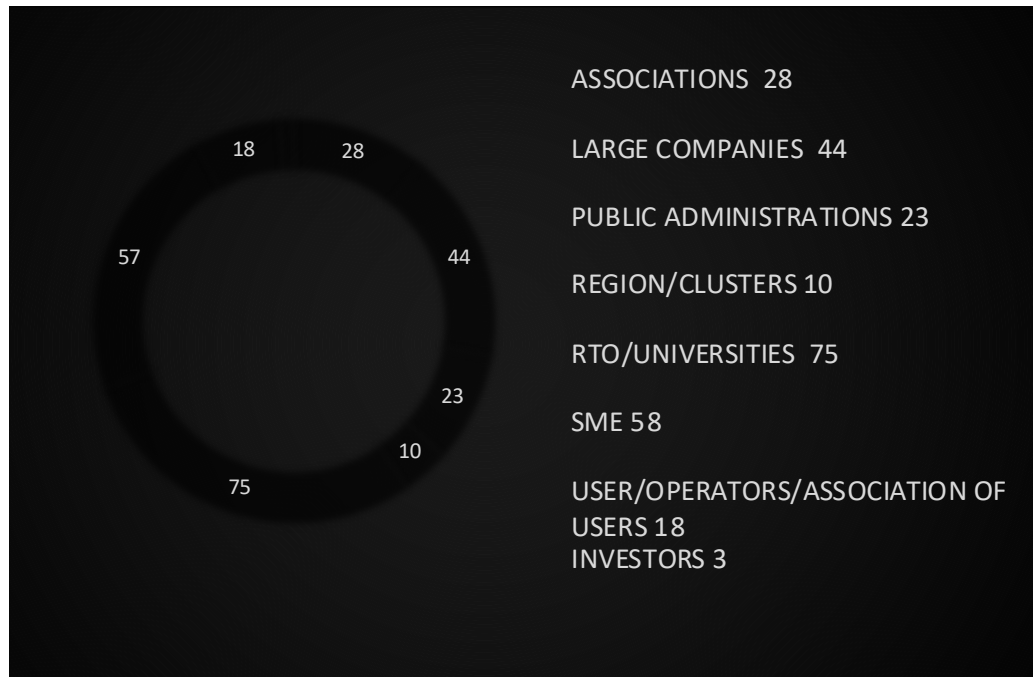
SUPPORTED BY

**GUARD**



# European Cyber Security Organisation

Established in 2016 for the implementation of the contractual Public-Private Partnership (cPPP) on cyber security with the European Commission



Our membership has grown **from 132 members** in 2016 **to 250 members across 29 countries** in February 2021, connecting more than 2000 organisations in Europe

ECSO Working Groups (WG) collaborating with each other: Cybersecurity 360°

Define the cyber security EU R&I roadmap and vision to strengthen and build a resilient EU ecosystem.

Analyse the challenges of digitalisation of the society and industrial sectors to sustain EU digital autonomy by developing and fostering trusted technologies.

SWG 6.1 Ecosystem

SWG 6.2 Digital Transformation in Verticals

SWG 6.3 Data and Economy

SWG 6.4 Basic and Disruptive Technologies

SWG 6.5 Dual use technologies



**European R&I priorities**

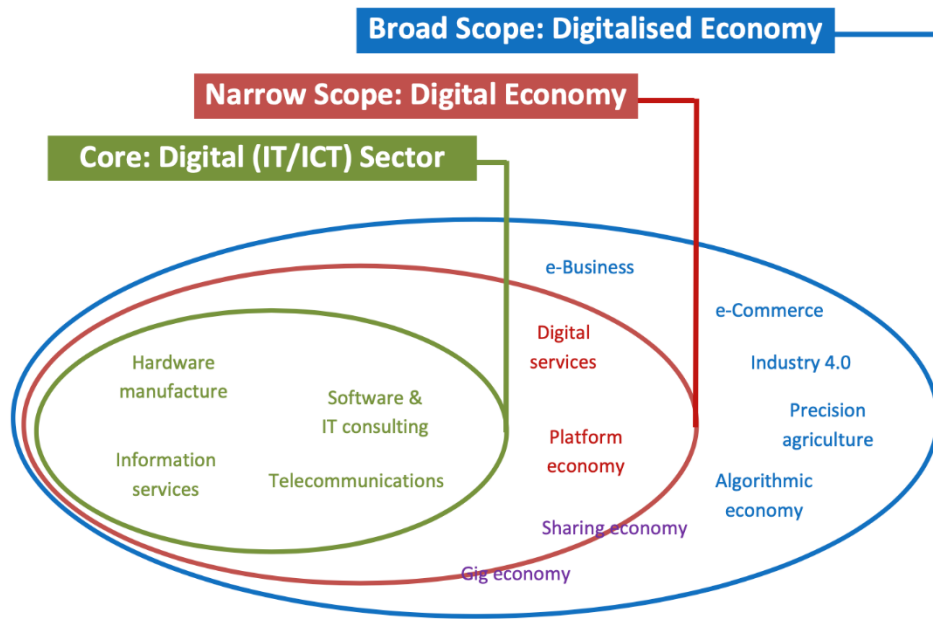


**Transcontinuum (link across techno sectors with other PPPs)**



**Collaborations**

# Digital Economy and Digital transformation



Source: Rumana Bukht & Richard Heeks. "Defining, Conceptualising and Measuring the Digital Economy"

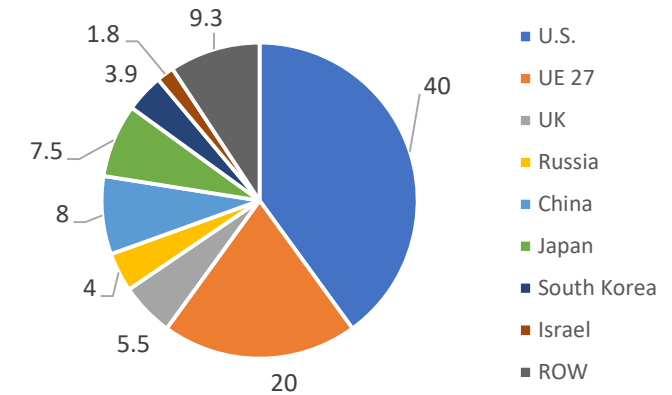
- Growing digitalisation of the Society and of the EU Industry / Economy
- Digital transformation and increase reliance on new technologies
- Cyber threats evolving very quickly: approaches and organisations should be very flexible, systems should be resilient
- Trusted supply chain to ensure business and service resilience



# Market and geopolitical environment

- **Global cybersecurity market** (estimation: ECSO 2018 market analysis): 115 bln € / Market growth rate + 13% by 2022.
- Market dominated by **global suppliers** from North America and Asia: most of the IT hardware and software products are manufactured outside the European Union
- **EU market** about 25 bln € composed by about 12K supplier companies (74% of them are Micro and SMEs).
- **EU public procurement** still leveraging upon non-EU solutions, even for sensitive issues.
- Growing “**sovereignty**” issue (in particular after the COVID with digital transformation)

2018 Cybersecurity market by Country--Market %



Sources: Momentum Partners, Visiogain 2018-2028 Market Report

There is innovation in Europe,  
but still fragmented markets


# ECSO suggestions for priorities

## HORIZON EUROPE PROGRAMME


Priorities for the definition of a SRIA in Cybersecurity by ECSO

### ECOSYSTEM, SOCIAL GOOD & CITIZENS

- Approaches, methods, processes to support cybersecurity assessment, evaluation and certification
- Building and Operating Resilient Systems: Adaptive Software Hardening, Self-Healing systems and RASP
- Development of digital forensics mechanisms and analytical support
- Cyber ranges and simulation environments
- Cyber-physical systems security and cyber secure pervasive technology




### APPLICATION DOMAINS & INFRASTRUCTURE



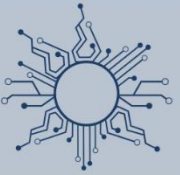
- Cyber resilient digitised infrastructures
- Secure Quantum Infrastructures
- Cyber secure future communication systems and networks
- Vertical sectors cyber challenges (Industry 4.0 and ICS, Energy, and smart grids, Transportation, Financial Services, e-payments and insurance, Public services, e-government, digital citizenship, Healthcare, Smart cities and smart buildings, Robotics, Agrifood)

### DATA & ECONOMY



- Data security and malicious use of data
- End-to-end privacy
- Economic aspects of cybersecurity

### BASIC & DISRUPTIVE TECHNOLOGIES



- Secure and Trustworthy AIs
- Software and Hardware cybersecurity engineering and assurance
- Cryptography
- Blockchains and DLTs
- IoT Security
- AI techniques for better security & malicious use of AI

**ECSO**  
FOR A CYBER RESILIENT DIGITAL EUROPE

Read more at [www.ecs-org.eu](http://www.ecs-org.eu)

## DIGITAL EUROPE PROGRAMME

Strategic areas of investment to develop a Capability Development Plan, increase autonomy and respond to the needs of our industrial sectors

### SUPPORT TO POLICY IMPLEMENTATION



- Develop tools to support the implementation of EU Cybersecurity Act
- Threat management and cross-vertical platforms
- Governance, policy and legal aspects

### SUPPORT TO TECHNOLOGY IMPLEMENTATION



- Deploying resilient digital infrastructures in the field
- Platform for privacy management
- Platform for identity management
- Establishing an engineering platform for trustworthy hardware, software, and systems

### SUPPORT TO COMPETITIVENESS & MARKET DEVELOPMENT



- Investments in Europe and development of regional ecosystem
- Platforms for market support to SMEs
- International cooperation and investments

### SUPPORT TO COMPETENCE BUILDING



- Operational, interoperable and cognitive cyber ranges
- Citizens and social good
- Jobs and professional skills

**ECSO**  
FOR A CYBER RESILIENT DIGITAL EUROPE

Read more at [www.ecs-org.eu](http://www.ecs-org.eu)

# ECSO main (R&D) priorities for a European Cybersecurity (2021 – 2027) wrt main issues

**INFRASTRUCTURE  
RESILIENCE**

**SKILLS**

**DATA & AI**

**CYBER SECURE HW &  
SW SUPPLY CHAINS**

**RISKS / THREATS  
MANAGEMENT**

**EUROPEAN COMPETITIVENESS**

**ECOSYSTEM, SOCIAL GOOD  
AND CITIZENS**

**APPLICATION DOMAINS  
AND INFRASTRUCTURE**

**DATA AND ECONOMY**

**BASIC AND DISRUPTIVE  
TECHNOLOGIES**

# ECSO cybersecurity priorities for Horizon Europe and Digital Europe Programme (expected total EC funding ~2,5 b€ in 2021-2027): suggestion to EC and MS

MAIN PRIORITIES	HORIZON EUROPE PRIORITIES	DIGITAL EUROPE PROGRAMME and other EU funds
<b>Risks / Threat management</b>	<ul style="list-style-type: none"> <li>Emerging threats, risk management, resilient systems, security by design</li> <li>Development of digital forensics mechanisms and analytical support</li> </ul>	<ul style="list-style-type: none"> <li>Threat management and cross-vertical platforms</li> </ul>
<b>Data &amp; AI (including privacy)</b>	<ul style="list-style-type: none"> <li>Data security and malicious use of data</li> <li>End-to-end Privacy</li> <li>Economic aspects of cybersecurity</li> <li>Securing and Trustworthy Artificial Intelligences</li> <li>Artificial Intelligence techniques for better security and malicious use of AI</li> </ul>	<ul style="list-style-type: none"> <li>Platform for identity and privacy management</li> </ul>
<b>Cyber secure HW &amp; SW (including crypto) supply chains</b>	<ul style="list-style-type: none"> <li>Approaches, methods, processes to support cybersecurity assessment, evaluation &amp; certification</li> <li>Software and hardware cybersecure engineering and assurance</li> <li>Cryptography</li> <li>Blockchains and Distributed Ledger Technologies</li> <li>IoT security</li> <li>Cyber-physical systems security and cyber secure pervasive technology</li> </ul>	<ul style="list-style-type: none"> <li>Develop tools to support the implementation of EU Cybersecurity Act</li> <li>Establishing an engineering platform for trustworthy hardware, software. and systems</li> </ul>
<b>Infrastructure resilience</b>	<ul style="list-style-type: none"> <li>Cyber resilient digital infrastructures</li> <li>Secure Quantum Computing Infrastructure</li> <li>Cyber secure future communication systems and networks</li> <li>Vertical sectors cyber challenges: Industry 4.0 and ICS; Energy (oil, gas, electricity) and smart grids; Transportation (road, rail, air; sea, space); Financial Services, e-payments and insurance; Public services, e-government, digital citizenship; Healthcare; Smart cities and smart buildings (convergence of digital services for citizens) and other utilities; Agrifood</li> </ul>	<ul style="list-style-type: none"> <li>Deploying resilient digital infrastructures in the field</li> </ul>
<b>Skills</b>	<ul style="list-style-type: none"> <li>Cyber ranges and simulation environments</li> </ul>	<ul style="list-style-type: none"> <li>Operational, interoperable and cognitive cyber ranges</li> <li>Citizens and social good</li> <li>Jobs and professional skills</li> </ul>
<b>Support to European competitiveness</b>		<ul style="list-style-type: none"> <li>Governance, policy and legal aspects</li> <li>Investments in Europe and development of regional ecosystem</li> <li>Platforms for market support to SMEs</li> <li>International cooperation and investments</li> </ul>



# Areas for possible investments to develop capabilities under the RRF: summary of the initial analysis

- **Cybersecurity for the digital transformation of strategic sectors: cyber resilient critical infrastructures and essential services (c.f. EU CS strategy, NIS2)**
  - Threat intelligence (incl. A.I. supported SOC's) and risk management for the protection of critical infrastructures
  - Resilient cross-vertical platforms for interconnected infrastructures
  - Securing integrity and availability of the global DNS root system
- **Cyber secure communication systems / networks and secure connectivity of products and associated services including secure digital services for B2C (c.f. EU CS)**
  - 5G infrastructure and end point security
  - Secure end-to-end connectivity for digital services (including essential services – e.g. Health)
  - Protection of sellers in eCommerce and retail from cyber threats as well as of users of selling platforms (citizens) from fraud
- **Secure data (c.f. EU Data Strategy, EU CS strategy; State of the Union)**
  - End-to-end data protection and secure data management
  - Protection from data manipulation and fake news
- **Secure and trusted digital identity management (eIDAS Regulation evolution; GDPR)**
  - Self Sovereign Identity based upon advanced PKI infrastructure and blockchain to guarantee easier adoption of digital services while satisfying European / democratic values
- **Cyber security aware citizens / decision makers and highly skilled workforce (c.f. EU CS strategy)**
  - Human aspects: education, professional training and skills development, as well as actions on awareness-raising and gender inclusiveness



# THANK YOU FOR LISTENING!

Fabio.Martinelli@cnr.it

**SUPPORTED BY**

**GUARD**

