Towards a trustworthy and resilient digital Europe

Roberto Cascella

ECSO Secretariat

Cyberwatching Webinar: Effective protection of Critical Infrastructures against cyber threats
– Online, 29 October 2020 –
Market and geopolitical environment


- Market dominated by **global suppliers** from North America and Asia: most of the IT hardware and software products are built outside the European Union (often by EU companies).

- **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)
What is at stake?

• Citizens privacy
• Society
• European values
• Democracy
• Awareness
• National security and sovereignty
• Economic recovery
• Digital autonomy
• Competitiveness
• Increasing Crime
• Increasing market
Timeline of the European approach to cybersecurity

• 2009: EU stakeholders started to advocate for a specific “ICT security” approach on EU R&D
• 2011: Started the discussion with the EC about a possible Public Private cooperation
• 2013: First EU cybersecurity strategy (“building blocks”)
• **2016**: Signature of the cPPP between the EC and ECSO
• 2017: Update of the EU cybersecurity strategy
• 2018: Adoption GDPR and NIS Directive
• 2019: Adoption of Cybersecurity Act (new ENISA mandate, EU certification)
• 2021: European Cybersecurity Centre / Creation of national Cybersecurity Centres; Horizon Europe – Digital Europe Programme; Starting discussions on Digital Service Act and European secure ID; ...
• **2021**: ECSO continues to support the growth of the European Cybersecurity ecosystem & Community
Introducing ECSO: European Cyber Security Orgar

We are the European Commission’s partner in implementing the contractual Public-Private Partnership (cPPP) on cyber security, established in 2016

Our membership has grown from 132 members in June 2016 to 266 members across 29 countries in October 2020, connecting more than 2000 organisations in Europe
ECSO Working Groups (WG) collaborating with each other: Cybersecurity 360°

**R&I**

WG6: Strategic Research & Innovation Agenda (SRIA) and Cyber Technologies
- 29 countries • 400+ experts

**Users & Operators Requirements**

WG3: Sectoral Demand
- Industry 4.0 & ICS, Energy, Transport, Finance, Public Services & eGOV, Healthcare, Smart Cities, Telecom, Media & Content
- 29 countries • 330+ experts

**Testing, Certifying & Validating Products, Services and Systems**

WG1: Standardisation, Certification and Supply Chain Management
- 28 countries • 330+ experts

**Market Deployment**

WG2: Market Deployment, Investments & International Collaboration
- 28 countries • 330+ experts

**Education & Training Awareness, Cyber Ranges**

WG5: Education, Training, Awareness and Cyber Ranges
- 29 countries • 270+ experts

**WG4: Support to SMEs and Regions**
- 26 countries • 180+ experts

29 October 2020
Cyberwatching.eu webinar: Effective protection of Critical Infrastructures against cyber threats
End of 2019 the main issues in Europe were the Digital Transformation and the Green Deal.
Commission priorities for “A Europe fit for the digital age”

and then the COVID-19 come, and the digital transformation accelerated
New Challenges and Objectives for Europe (2020)

Digital Transformation

Next Generation EU

29 October 2020

Cyberwatching.eu webinar: Effective protection of Critical Infrastructures against cyber threats
Main ECSO recommendations to the EC and EP for a Cyber Resilient Europe

**SUPPORT & PROTECTION OF THE EU DIGITAL TRANSFORMATION**

**EU VISION FOR A EUROPEAN CYBERSECURITY ECOSYSTEM BASED ON EU VALUES**

Comprehensive EU Cybersecurity Strategy and Approach
EU Cybersecurity Industrial Policy
Education, Training / Skills and Awareness

**SOVEREIGNTY RECOVERY**

**SOCIODEMIGCOMM DEVELOPMENT**

**INCREASED DIGITAL AUTONOMY**

EU Legislations & Regulations
Public and Private Investments in Research, Capability Development and Capacity Building
Strategic Alliance & Partnership for Trusted Supply Chains

**NEXT GENERATION PUBLIC PRIVATE COOPERATION**

29 October 2020
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.

Scenarios and priorities for Horizon Europe and Digital Europe Programme (ECSO 2021-2027 technology vision of the future shaping the society and the industry)

Initiative with other cPPPs (ETP4HPC, 5G IA, BDVA, etc...) to identify global challenges and need to address them in a transversal and coordinated way

- Coordination with other PPPs, JUs, Pilots on Competence Centres, EC projects and other initiatives to monitor the evolution of the cybersecurity ecosystem and understand the gaps
- Cooperation with EDA on cybersecurity for dual use technologies
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**
- **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

<table>
<thead>
<tr>
<th>MAIN PRIORITIES</th>
<th>HORIZON EUROPE PRIORITIES</th>
<th>DIGITAL EUROPE PROGRAMME and other EU funds</th>
</tr>
</thead>
</table>
| Risks / Threat management              | • Emerging threats, risk management, resilient systems, security by design  
• Development of digital forensics mechanisms and analytical support                                                                                                                                                                                  | • Threat management and cross-vertical platforms                                                                                           |
| Data & AI (including privacy)          | • Data security and malicious use of data  
• End-to-end Privacy  
• Economic aspects of cybersecurity  
• Securing and Trustworthy Artificial Intelligences  
• Artificial Intelligence techniques for better security and malicious use of AI                                                                                                                                 | • Platform for identity and privacy management                                                                                           |
| Cyber secure HW & SW (including crypto) supply chains | • Approaches, methods, processes to support cybersecurity assessment, evaluation & certification  
• Software and hardware cybersecurity engineering and assurance  
• Cryptography  
• Blockchains and Distributed Ledger Technologies  
• IoT security  
• Cyber-physical systems security and cyber secure pervasive technology                                                                                                                                                                   | • Develop tools to support the implementation of EU Cybersecurity Act  
• Establishing an engineering platform for trustworthy hardware, software, and systems                                                                                                           |
| Infrastructure resilience              | • Cyber resilient digital infrastructures  
• Secure Quantum Computing Infrastructure  
• Cyber secure future communication systems and networks  
• 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 | • Deploying resilient digital infrastructures in the field                                                                                                          |
| Skills                                 | • Cyber ranges and simulation environments                                                                                                                                                                                  | • Operational, interoperable and cognitive cyber ranges  
• Citizens and social good  
• Jobs and professional skills                                                                                                                                          |
| Support to European competitiveness    |                                                                                                                                                                                                                         | • Governance, policy and legal aspects  
• Investments in Europe and development of regional ecosystem  
• Platforms for market support to SMEs  
• International cooperation and investments                                                                                                                                                                                      |
Cyber resilient digital infrastructures

A complex scenario

- High-availability and controlled performances in highly complex / heterogeneous technologies (HW/SW, real/virtual)
- Presence of legacy systems / components and need to ensure security and privacy over mixed legacy and innovative technologies
- Complex digital infrastructures lifecycle management process across all stakeholders (supply chain w/o central authority)
- Heterogeneous regulatory scenario

Some challenges ahead

- Real-time & situational awareness, automating mitigation / detection / response / recover
- Securing the whole digital infrastructure lifecycle, including training, education and safety aspects
- Innovation based on the integration of existing security/privacy components in legacy systems
- Distributed decision making and collaboration solutions, e.g., orchestration services.
- Secure virtualization technologies that are transversal to verticals
Deploying resilient digital infrastructures in the field

A complex scenario

- Complex and cross-platform cyber attacks / Threat management
- Integrity and trustworthiness of communications and services
- Virtualization and softwarisation of networks and network functions and the interconnection of different technologies
- Complex trust models to address M2M interaction and to manage complex 5G infrastructures
- Impact of current cryptographic schemes and migration to quantum safe ones

Some challenges ahead

- Increase trust in information sharing mechanisms through control and formal analysis of data and sensors
- Design and implementation of new security mechanisms and automation of attack response mechanisms
- Realistic, open-source and configurable tools and simulators to evaluate new security solutions

29 October 2020
Cyberwatching.eu webinar: Effective protection of Critical Infrastructures against cyber threats
Transversal vertical sectors cyber challenges

Open Source Secure and Resilient Hardware and Software

Cybersecurity / ECSO

Cyberwatching.eu webinar: Effective protection of Critical Infrastructures against cyber threats
Join us! Being and ECSO member allows you to:

**INTERACT** with legislators and decision makers at EU and national level

**BE PART OF** the organisation federating the European cybersecurity community

**GROW** your business network with other members of the Community

**BOOST** your market visibility

**GAIN ACCESS** to investments and funding opportunities at EU and national levels

**SHARE** information and best practices with your counterparts

**TAKE THE LEAD** in proposing new initiatives and services to build the European cybersecurity Market
CONTACT US!

European Cyber Security Organisation
29, Rue Ducale
1000 – Brussels – BELGIUM

E-mail:
secretariat@ecs-org.eu

Follow us:

www.ecs-org.eu

LinkedIn: https://www.linkedin.com/company/ecso-cyber-security/

Twitter: @ecso_eu