EUROPEAN CYBER SECURITY ORGANISATION

Cybersecurity PPP & ECSO Strategic Research Innovation Agenda

Roberto G. Cascella
Senior Policy Manager (ECSO Secretariat)

European Industry Partnerships Collaborative Event
– 17 April *2019* – *Amsterdam (The Netherlands)* –

Evolution of the European political agenda

2013: EU Cybersecurity **Strategy**

2014: **Digital Single Market** / Digitalisation EC communication

2016: **cPPP** on Cybersecurity

2017: Joint Communication on **EU strategy** (establishment of A Network of Competence Centre (calls for pilot projects ended); EU Cybersecurity Research and Competence Centre) Review and **Cybersecurity Act** ("New" EU Cyber Security Agency: ENISA + EU Certification Framework)

2018: Transposition of the **NIS Directive** & application of the **GDPR**

2018: Proposal for a **Regulation** establishing the **European Cybersecurity Industrial, Technology and Research Competence Centre** and the **Network of National Coordination Centres**

And beyond 2018

- European Commission proposal for the **next MFF** (2021 – 2027): May 2018 ➔ expected approval in May 2019
- **Digital Europe Programme** (capacity building projects from 2021) ➔ approval end 2018 / 2019
- **HorizonEurope** (R&D from 2021)
- Expected **evolution of the cPPP** (after 2020) towards a more ambitious governance (EU Competence Centre) and wider objectives, beyond R&D (including capacity building)

Cyber security has become a major global issue

- **Cyber security is a growing issue** at political (elections), societal (social media / privacy) and economic (digitalisation of the industry – Industry 4.0) level
- **Cyber security is a global issue:** cyber threats hit at local / regional / local / international level
- **Digitalisation** (including the massive introduction of IoT and IIoT, and autonomous decisions) **is still a phenomenon not well understood** by the industrial sector (and in particular by SMEs): **security of a digitalised society will be a challenge!**
- **IT** (Information Technology) **and OT** (Operational Technology) **are increasingly closer and interacting (cyber-physical systems) → higher cyber resilience should be provided**: optimisation needed, both to avoid vulnerabilities (lack of security of data for control of manufacturing operation can have disruptive impacts) and for reducing costs
- Current situation sees the use (when possible) of solutions / patches validated / certified wrt the present understanding of threats, **but threats are continuously evolving → we need flexibility and scalability of systems**
- **Risk management is still a challenge** to be correctly implemented in an industrial cycle, while considering potential disruptions and impact of cyber attacks
- **Awareness is still limited** in all kind of stakeholders
- The figure of **CISOs** (Chief Information Security Officers) is increasing in companies, but CISOs still don't get sufficient attention from companies' Management Board and get adequate risk management measures implemented

About the European Cyber Security cPPP

The European Commission has signed on July 2016 a cPPP with the private sector represented by ECSO for the development of a common approach and market on cyber security.

AIM

1. Foster cooperation between public and private actors
2. Stimulate cyber security industry
3. Coordinate digital security industrial resources in Europe

BUDGET

The EC will invest up to €450 million in this partnership, under its research and innovation programme Horizon 2020 for the 2017-2020 calls (4 years). Cyber security market players are expected to invest three times more (€ 1350 mln: leverage factor = 3) to a total up to €1800 mln.

UPDATE: EC will invest more than €500 mln. Private sector investments for the 1st year had a leverage factor 5

ECS
EUROPEAN CYBER SECURITY ORGANISATION

A Public Private Partnership

to strengthen cybersecurity industry in Europe

- mobilising public & private resources under Horizon2020
- helping turn Europe's world-class cybersecurity research into products & services
- building trust among users, businesses, public administrations
- defining minimum common digital security & privacy requirements across different sectors

Technical priorities


Assurance & security


Identity, access & trust management


Data security


Protection of ICT Infrastructure


Cybersecurity services

Non-technical Priorities


Education, training & skills


Development of cybersecurity ecosystem


Boosting SMEs

ECSO membership overview (status 2 April 2019)

132 founding members: now we are **250 organisations (including new requests) from 29 countries and counting**

ECSO is also reaching out to all the members of our 23 associations, i.e. a Community of more than 2000 bodies

AUSTRIA	7	LATVIA	1
BELGIUM	15	LITHUANIA	1
BE - EU ASSOCIATIONS	11	LUXEMBOURG	4
BULGARIA	2	NORWAY	5
CYPRUS	6	POLAND	6
CZECH REP.	3	PORTUGAL	4
DENMARK	5	ROMANIA	2
ESTONIA	8	SLOVAKIA	1
FINLAND	9	SLOVENIA	1
FRANCE	26 +(1)	SPAIN	32 (+1)
GERMANY	22	SWEDEN	3
GREECE	6	SWITZERLAND	5
HUNGARY	3	THE NETHERLANDS	14
IRELAND	4 (+1)	TURKEY	4
ITALY	28	UNITED KINGDOM	9

- Associations **23**
- Large companies **54 (+2)**
- Users / Operators **16**
- Public Administrations **21**

  AT, BE (2), BG, CY, CZ (2), EE, FI, FR, GE, GR, IT, NL, NO, PL, RO, SE, SK, SP, UK

  Observers at NAPAC (DK, HU, IE, LT, LV, MT, PT, SI, …)
- Regions / clusters **9**
- RTO/Universities **69 (+1)**
- SMEs **55**

Our Working Groups

WG1 - Standardisation, certification, labelling and supply chain management

WG2 - Market deployment, investments and international collaboration

WG3 - Sectoral demand

WG4 - Support to SMEs and Regions

WG5 - Education, training, awareness and cyber ranges

WG6 - Strategic research & innovation agenda (SRIA) and cyber technologies

WG6 - Strategic research & innovation agenda (SRIA) and cyber technologies

STRATEGY AND MISSION

Define the cyber security R&I roadmap to strengthen and build a resilient EU ecosystem by designing and developing trusted technologies that address the challenges of digitalisation of the society and industrial sectors to foster EU digital autonomy

WG6: SRIA and Cyber Technologies

ECSO SRIA to identify research priorities for 2018-2020

- ➔ A strategic vision is needed to demonstrate how industrial priorities contribute to the implementation of the strategy
- ➔ 7 thrusts organised in 4 different areas have been identified

1 European Ecosystem for cyber security
2 Demonstrations for the society, economy, industry and vital services
3 Collaborative intelligence to manage cyber threats and risks
4 Remove trust barriers for data-driven applications and services
5 Maintain a secure and trusted infrastructure in the long-term
6 Intelligent approaches to eliminate security vulnerabilities in systems, services and applications
7 From security components to security services

Analysis of the Work Programme 2018-2020 and continuous advocacy of priorities

➔ good match and public & private priorities well aligned

Other activities include:

- **Identification of R&I needs on specific verticals to address new disruptive technologies** – Working papers on new technology drivers Artificial Intelligence, Internet of Things and Blockchain (impact on the different WG aspects and verticals to sustain the industrial policy)
- **Identification of global trends, and key implications on strategy through 2027 (SRIA 2.0)**
- **Collaboration with other cPPPs** ➔ to federate the discussions on cybersecurity challenges with other PPPs under ECSO. Cybersecurity as a glue and horizontal technology
- Collaboration with agencies ENISA and EDA (cybersecurity for dual use technology)

Continuous monitor of the European cybersecure ecosystem, including technology and needs evolution to build, maintain, and provide innovative trustworthy solutions to protect European citizens and industry

WG6: SRIA priorities for R&I

STRATEGIC PRIORITIES

- Cybersecurity Technologies & Services
- Infrastructure & Applications
- Cyber ecosystem

ECS
EUROPEAN CYBER SECURITY ORGANISATION

CYBERSEC TECHNOLOGIES & SERVICES to protect Infrastructure / Applications and citizens' privacy

- Encryption (key management, homomorphic, post quantum, …)
- ID and DLT (blockchain, …) security
- AAA: Authentication; Authorisation; Accounting
- Security / Resilience & Privacy by Design (GDPR, …)
- PET: Privacy Enhancing Technologies
- Information Sharing, Threat Detection and Intelligence (incl. sensors / probes for ICS, SIEMs and SOCs), Artificial Intelligence and Analytics
- Protection of innovative ICT infrastructure
- Risk Management, Response and Recovery
- Tamperproof communication protocols

Pilots and validation of solutions in INFRASTRUCTURE (for use in all sectors) & APPLICATIONS (specific verticals)

- Industry 4.0 (FoF, Robotics, SPIRE, AIOTI, ECSEL)
- Energy (EdB; AIOTI)
- Transport (AIOTI, ECSEL)
- Finance (EU FI-ISAC)
- Public Administration (EU Cloud Initiative; FIWARE, HPC, BDV)
- Health (EIP AHA, AIOTI, ECSEL)
- Smart cities (Smart Cities and Communities; EIT Digital, EdB, AIOTI, ECSEL)
- Telecom (5G; AIOTI)

CYBER ECOSYSTEM: preparing the market to introduce and use innovations

- Standardisation
- Validation / Labelling / Certification (end user awareness for implementation; different needs and different levels, flexibility for evolution)
- Trusted management of the supply chain: Assurance
- Education (cyber-Erasmus)
- Training/ simulation (certification of experts to help employment needs)
- Awareness of citizens, users (Cyber Hygiene) and decision makers (procurement, implementation and use);
- Legislation & Liability
- Investments – Funds / Economics - Business models / Insurances
- Support to SMEs
- Regional / local aspects

ECSO future of the European Cyber Security Definition and Vision

ECSO definition of EU Cyber Security

"European Cyber Security is our common science, knowledge, trustworthy processes, products, services and infrastructures to protect (in a sustainable way) our nations, industries / economies, citizens and institutions against damaging cyber-attacks while respecting our European Values."

ECSO Vision for EU Cyber Security in 2027

- **Europe as global leader in cyber security**, having developed a **comprehensive EU cyber security strategy** built upon a "predict-prevention, protection, detection, respond" approach
- Strong, **resilient and competitive European industrial** (SMEs and European champions) and academic ecosystem
- **Cyber security recognised as an industrial sector, sustained by an industrial policy for Europe, supported by adequate investments** for increased EU competitiveness and digital autonomy
- **Cyber security solutions effectively deployed at national, regional** / local (city) level (driven by smart specialisation)
- Well **informed European citizens and decision makers** and **highly trained cyber security professional workforce**

BECOME MEMBER!
CONTACT US

European Cyber Security Organisation 10, Rue Montoyer
1000 – Brussels – BELGIUM

www.ecs-org.eu

Phone:
+32 (0) 27770252

E-mail:
Dr. Roberto G. Cascella
Senior Policy Manager
roberto.cascella@ecs-org.eu

Follow us
Twitter: @ecso_eu