

ECSO

EUROPEAN CYBER SECURITY ORGANISATION



Cybersecurity PPP & ECSO Strategic Research Innovation Agenda

Roberto G. Cascella

Senior Policy Manager (ECSO Secretariat)

ECSO – EUNITY Workshop
– 24 January 2019 – *Brussels (Belgium)* –

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

cPPP Monitoring at Glance – 1st Period

Investment on R&D

- Nearly 455 million € estimated in 2016 by the European Cyber Security community and 534 million € in 2017
- Nearly 68 million € invested by the EC in the PPP, 4 projects started so far under the frame of H2020 (DS-06-2017), other 13 projects of the 2017 call to be started soon.

➔ **Leverage factor for cPPP investments higher than 3 (target)**

Cyber security employment

- Following our survey, employment has growth between 2016 to 2017 by 10% in large companies, 80% in SMEs and 45% in RTOs.

➔ **cPPP target job growth = at least 10%**

Survey for 2018 investment expected to be launched on 1st February

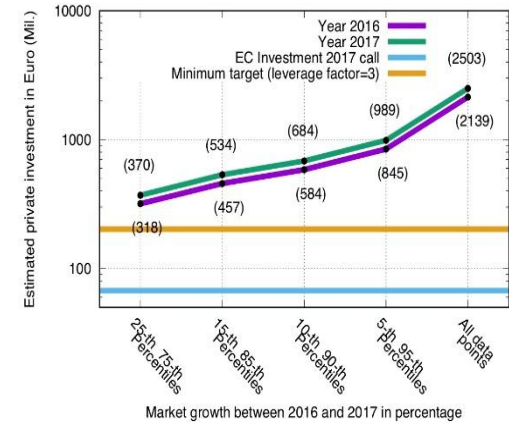


FIG 1 Estimated private investment for 2016 and 2017

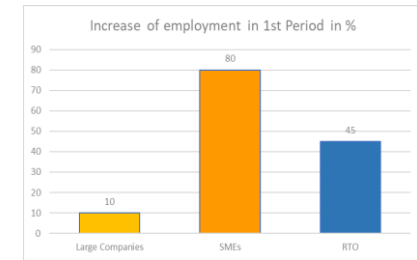


FIG 2 Employment in 1st Period

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

We are representative of all kinds of stakeholders (situation on 8 January 2019)

WG1

Standardisation, certification, labelling and supply chain management



152 members
28 countries
333 experts

WG2

Market deployment, investments and international collaboration



98 members
22 countries
200 experts

WG3

Sectoral applications

Industry 4.0; Energy; Transport; Finance; Public Admin/eGov; Health; Smart Cities; Telecom/Content/Media



139 members
29 countries
330 experts

**233
Members
29
countries**

WG4

Support to SMEs and collaboration with Regions including East & Central Europe



101 members
26 countries
186 experts

WG5

Education, training, raising awareness and cyber ranges



132 members
29 countries
270 experts

WG6

Strategic research & innovation agenda (SRIA) and cyber technologies



178 members
29 countries
414 experts

ECS - cPPP Partnership Board
(monitoring of the ECS cPPP - R&I priorities)

EUROPEAN
COMMISSION



Governance

ECSCO –Board of Directors

(Management of the ECSCO Association: policy/market actions)

INDUSTRIAL POLICY

R&I

Coordination / Strategy Committee

WG 1

Standardisation /
certification /
labelling / supply
chain management

WG 2

Market deployment
/ investments /
international
collaboration

WG 3

Sectoral Demand
(Industry 4.0; Energy;
Transport; Finance;
eGov; Health; Smart
Cities; Telecom/media)

WG 4

Support to SMEs
and REGIONS
(in particular
East EU)

WG 5

Education,
training, cyber
ranges, awareness

WG 6

Strategic Research &
Innovation Agenda
New Technologies,
Products & Services;
Cyber Defence

SMEs and Start-ups,
Incubators /
Accelerators

Associations
(national /
European)

Large Companies:
Supplier or User of
cyber security
solutions

Regions / Clusters

Users /
Operators

Public
Administrations (at
national level)

Research Centres,
Academia /
Universities and
their Associations

ECSCO General Assembly

WG6: Strategic Research and Innovation Agenda

ECSCO 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

Lesson learnt

- Coordination with cPPPs (on specific transversal technologies & verticals) is important to ensure the SRIA presenting coordinated cyber security strategy in EU
- Coordination with the EC Programme Committee and NAPAC R&I Group wrt internal deadlines is key to guarantee high quality delivered when expected
- Development of innovative cybersecurity technologies and validation of the solutions in key infrastructures and applications

WG6: SRIA priorities for R&I

STRATEGIC PRIORITIES

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



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

Coordination of R&I cybersecurity activities in Europe



BDVA:
updated list
of shared
topics and
areas of
collaboration
on AI

EFFRA:
Analysis of
requirements
and cyber
security
challenges for
digitisation of
industry

5G IA:
Common
interest to
work on
cybersecurity
aspects for 5G

EURobotics:
cybersecurity
for
Digitisation of
the Industry
(e.g., eHealth)

Other initiatives
(A.Spire,
ShiftToRail,
ECSEL)
contacted. ...

Federating discussions on cybersecurity challenges with other PPPs under ECSO

Other external collaborations

- **EDA:** Understand EDA research priorities. EDA has joined the ECSO Strategic Technical Committee. ECSO SWG6.5 on cyber defence
- **ENISA:** Contribute to the research priorities identified (crystal ball) and recommendation report. Continuous interaction
- **JRC:** Work on the cybersecurity taxonomy
- **DG-ENER:** Contribute with specific cybersecurity challenges and priorities for the energy sector (with WG3)
- **IoTForum** and **AIOTI:** Focus on cybersecurity for IoT technology to update the research priorities and impact for vertical sectors

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

ECSO SRIA: Where we are heading



Identification of global trends & key implications on strategy → 2027

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 different WG aspects to sustain the industrial policy)

- Technical cyber security challenges: relevance, current status and future directions (roadmap)
- The impact on vertical sectors and their needs (cross-sectorial challenges and specificities of each vertical sector)
- The relevant standardisation activities and the implications for cyber security certification and supply chain management.
- Relevant regulations and legislations and their implications

Initial priorities and challenges for HorizonEurope (2021)

- Society and Citizens (Social Good) → Bring trust into the technology and in the Machine Economy
- Data and Economy → Data as main ICT value and/or target and main driver for decision making
- Basic and Disruptive Technologies (e.g. Artificial Intelligence, Blockchain, Quantum-resistant crypto) → Ensure a sustainable and trustworthy ecosystem, including integrating M2M and M2H interaction and autonomous systems as technical, ethical, safety issues
- Digital Transformation in Verticals → Continuous evolving systems and integration of legacy systems with new technology, threat intelligence and information sharing, and ICT infrastructure protection

➤ Define **Strategic Research and Innovation Agenda (v2.0)**

Link with relevant cPPPs and new initiatives (DEP) to coordinate strategy for future EU cybersecurity R&I

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](https://twitter.com/ecso_eu)

