The European Public Private Partnership and ECSO (European Cyber Security Organisation)

Luigi Rebuffi

Secretary General

ECSO - European Cyber Security Organisation

“How S@fe is Your Business?”

Nicosia - 2 February 2017

ABOUT THE CYBERSECURITY cPPP

cPPP (contractual Public Private Partnership) between the E.Commission and ECSO as representative of the private sector (and more …)

GOALS:

1. Foster cooperation between public and private actors
2. Stimulate cybersecurity 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).
- The other cybersecurity market players are expected to invest three times more (€1350 million : leverage factor = 3) for a total of €1800 million.

ABOUT THE CYBERSECURITY cPPP

LINKING RESEARCH AND CYBERSECURITY INDUSTRIAL POLICY

1. Main Commission cPPP objective: focus on R&I, developing a SRIA (priorities for a Strategic Research and Innovation Agenda)
2. The ECSO Association will tackle other industry policy aspects and the development of the European cybersecurity industry

INITIAL REFERENCE DOCUMENTS (see www.ecs-org.eu)

1. Industry proposal
2. Strategic Research and Innovation Agenda (SRIA) proposal

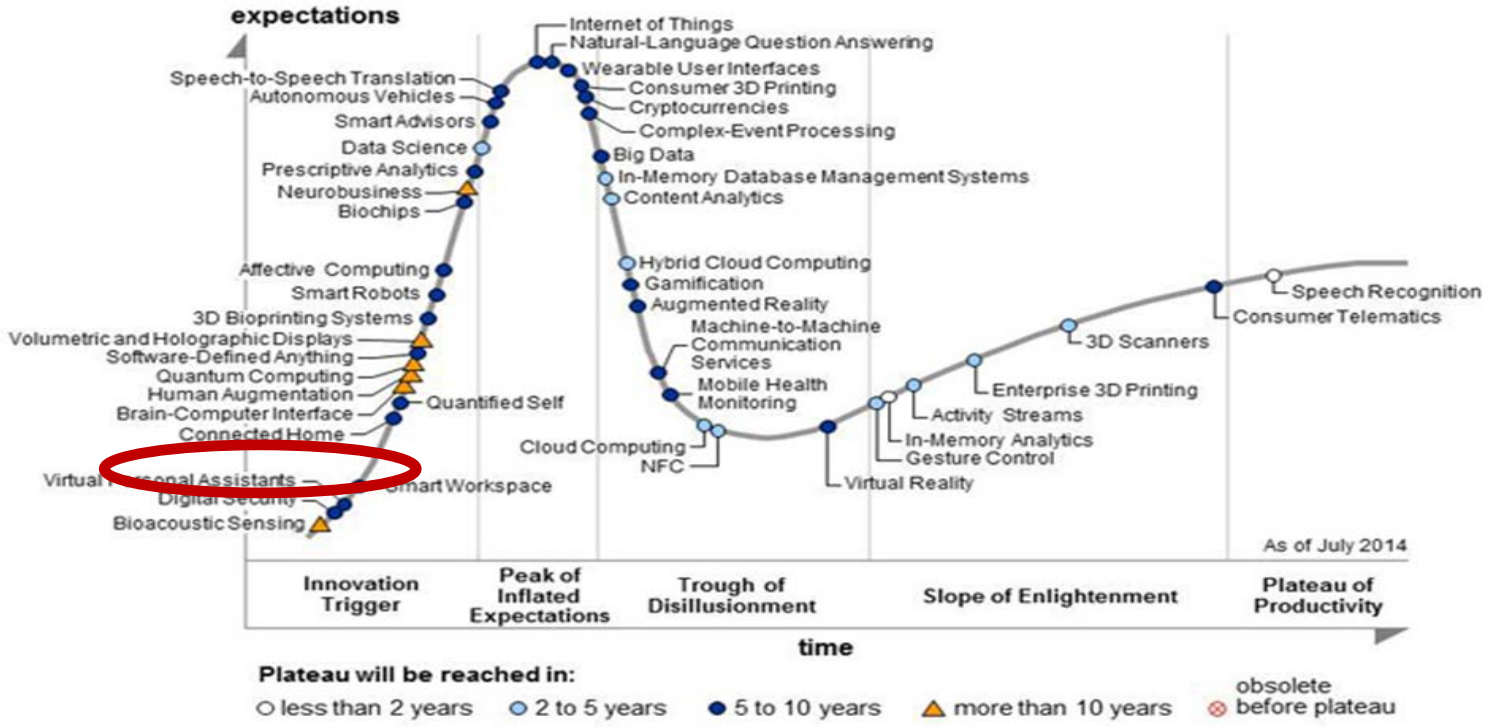
INDUSTRY PROPOSAL

Identifies industrial cybersecurity challenges in Europe

- Global cybersecurity and ICT market dominated by American and Asian companies.
- Strategic supply chain dependency.
- Innovation:
  - Led by imported ICT products.
  - Not properly funded
  - Not reaching market
- Weak entrepreneurial culture and lack of venture capital.

Digital security: a market in its infancy

- Digital security is at the beginning of its maturity cycle, if we refer to the "hype curve" published by Gartner in August 2014, with a plateau reached in 5 to 10 years. http://www.gartner.com/newsroom/id/2819918



Comparison of figures in the cyber world

- ICT market (2015) ~ € 3100bln (source Gartner)
- Impact of Cyber threats: € 600bln (~20% of ICT market! - different sources)
- Global (civilian) Cybersecurity Market (2015; sources: Gartner, Visiongain, EOS): € 70bln (2,3% of ICT market)
- Cyberdefence market (2015): € 14 bln
- US intelligence market (2015): US$ 45.6 bln
- Yearly investment by US Fed Govt ➔ US$ 17bln (providing sustainability of the supplier companies and the technologies developed which could then be partially used for more civilian applications)
- Yearly investment in US for R&I ~ US$ 1,5 bln
- EU cPPP on R&I ➔ € 450mln in 4 years
- Venture Capital investment in US (estimation 2016) ~ US$ 4 bln
- Venture Capital investment in EU € a few tens of million €

Two market reasons to invest:

- Develop presence of EU industry in cybersecurity market
- Protect from cyber threats those markets where Europe is leader (or for strategic reasons)

INDUSTRY PROPOSAL

Identifies industrial operational and strategic objectives

1. Protecting critical infrastructures from cyber threats.
2. Use of massive data collection to increase overall security (intelligence).
3. Increased European digital autonomy.
4. Security and trust of the whole supply chain
5. Investments in economic areas where Europe has a clear leadership.
6. Leveraging upon the potential of SMEs.
7. Increase competitiveness.

cPPP Monitoring:
Key Performance Indicators

3 main kinds of KPIs

1. **Industrial Competitiveness**
   - **Market development – applications, etc.**

2. **Socio-Economic Security**
   - **Employment, legislation, “by design” solutions**

3. **Implementation and operational aspects of the cPPP**

ECSO : A UNIQUE PPP ASSOCIATION

Security is a national prerogative.

➔Stronger participation in ECSO of representatives from the national administrations, also at decision making level.

➔ Interest from National Public Administrations: Representatives to the two EU H2020 Programme Committees + Ministries (Interior, Economy, etc.) + Regulatory Bodies + Public users.

➔ Participation in Working Groups & Task Forces

➔ to bring a governmental perspective and operational needs from the public administrations

NAPAC : National Public Authority Representatives Committee

Compositions: ECSO Public Administrations (including “observers”)

Objective: create a common vision / strategy across ECSO P.A. on policy and R&I issues discussed in ECSO WGs: advisors to WGs, Coordination & Strategy Committee; ECSO Board and E.Commission

Secretariat: ENISA (supported by ECSO secretariat)

Structure: 2 bodies

- Governmental Advisory Group (GAG): representatives from national administrations dealing with industrial policy related to cybersecurity from EU Member States. This group will tackle “cybersecurity industrial policy” issues. On few occasions, that group can be open to invited observers.
- The R&I Group: national representatives from the public sector (typically those in H2020 Programme Committees) for the definition of the respective Work Programmes.

Purpose and objectives of ECSO/cPPP in short/medium/long term

- **Short term:**
  - R&I priorities for H2020 (2018-2020 work programme);
  - EU Certification & Labelling
  - Increase membership (users & operators), stabilise governance
  - Develop P-P dialogue and harmonisation of objectives
  - Create NAPAC network across EU public administrations
  - Create Network of “regions” (including local organisations)
- **Medium Term:**
  - Standardisation
  - Investment funds
  - Regional approach (smart specialisation & regional funds)
  - Support SMEs
  - Develop education, training, awareness and cyber ranges
  - Prepare for post H2020 ("FP9")
  - Development of components, systems, services strategic for Europe
  - International dialogue
- **Long Term:**
  - cPPP evolution maybe into a JU (more articulated EU structure)
  - European industry among cybersecurity market leaders in targeted sectors
  - Support to business development and global competitiveness

ECSO MEMBERS

185 (at January 30th) organisations having formally requested membership … from 27 countries and counting… divided in categories (each represented at the Board of Directors).

- Associations : 18
- Large companies: 55
- Public Administrations: 12 (UK, ES, IT, FR, DE, SK, EE, FI, NO, CY, PL, NL)
- Regional clusters; 2
- RTO/Universities: 50
- SMEs: 40
- Users/Operators (users are also in large supplier companies): 8

(CNTI has been the first organization demanding ECSO membership)

AUSTRIA	5	ITALY	30
BELGIUM	4	LATVIA	1
BE - EU ASS	8	LUXEMBOURG	3
CYPRUS	4	NORWAY	4
CZECH REP.	1	POLAND	6
DENMARK	2	PORTUGAL	5
ESTONIA	4	ROMANIA	2
FINLAND	7	SLOVAKIA	2
FRANCE	21	SPAIN	29
GERMANY	16	SWEDEN	1
GREECE	2	SWITZERLAND	3
HUNGARY	1	THE NETHERLANDS	10
IRELAND	1	TURKEY	2
ISRAEL	2	UNITED KINGDOM	9

Activities and benefits for members

- Participation in governance and working bodies:
  - General Assembly
  - Association Board
  - Partnership Board
  - Strategy Committee
  - Working Groups
  - Task Forces
  - High Level Events / Workshops / Conferences
  - Representing ECSO at national / EU level
- Networking with stakeholders from all sectors and countries
- Easier access to EU Institutions and national Public Administrations (also from other countries)
- Easier access to information (newsletter, web etc.)
- Proposing / advocating own - common priorities and strategy for R&I, investments, standards / certification, legislations, etc.
- Better understanding of EC call for proposals (for R&I) and access to competitive consortia (ECSO as "honest broker")
- …

Governance

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

EUROPEAN COMMISSION

ECS
EUROPEAN CYBER SECURITY ORGANISATION

ECSO - Board of Directors
(management of the ECSO Association:
policy / market actions)

INDUSTRIAL POLICY

Coordination / Strategy Committee

R&I

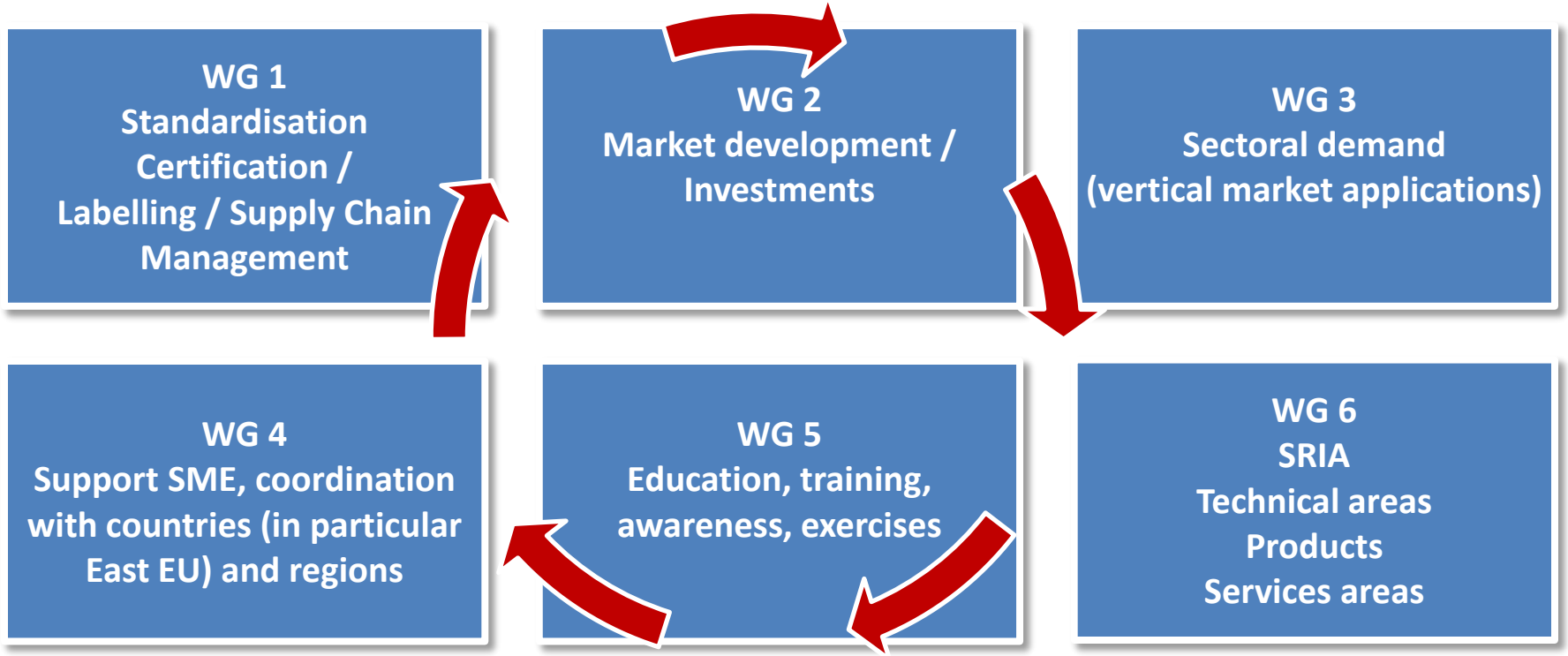
Scientific & Technology Committee

WG 1	WG 2	WG 3	WG 4	WG 5	WG 6
Standardisation Certification / Labelling / Supply Chain Management	Market development / Investments	Sectoral demand (vertical market applications)	Support SME, East EU, Regions ...	Education, training, awareness, exercises	SRIA Technical areas Products Services areas

- SME solutions / services providers; local / regional SME clusters and associations Startups, Incubators / Accelerators
- Others (financing bodies, insurance, etc.)
- Large companies Solutions / Services Providers; National or European Organisation / Associations
- Regional / Local administrations (with economic interests); Regional / Local Clusters of Solution / Services providers or users
- Public or private users / operators: large companies and SMEs
- NATIONAL PUBLIC AUTHORITY REPRESENTATIVES COMMITTEE: R&I Group Policy Group
- Research Centers (large and medium / small), Academies / Universities and their Associations

ECSO
General Assembly

WORKING GROUPS & TASK FORCES



Global overview of WGs activities

- WG1 (standards / certification / label / trusted supply chain): Initial informal suggestions delivered to the European Commission. Next meetings (January) to develop further a common approach and priorities for an EU certification; start discussions on standards in preparation of the CEN/CENELEC workshop and cooperation with ETSI

- WG2 (market/ funds/ cPPP monitoring): WG to be started in February 2017

- WG3 (verticals: Industry 4.0; Energy; Transport; Finance / Bank; Public Admin / eGov; Health; Smart Cities): Priority and objectives under detailed definition with users. Next meeting February 9th. Meetings on specific sectors foreseen (e.g. energy & smart grids with DG ENER and DG CNECT)

- WG4 (SMEs, regions, East EU): Meeting on Regional aspects in February. Discussion on other forms of support to SMEs other than R&D (e.g. EU regional funds)

- WG5 (education, training, awareness, cyber ranges…): One of the main priorities for MT and EE Presidency of the EU in 2017. Next meeting in March.

- WG6 (SRIA): Initial informal suggestions delivered to the European Commission. Further work according to feedback from Commission and H2020 R&D Programme Committee. Contacts with other PPPs and similar EU activities (5G, IoT, Big Data, Smart Cities, Photonics, Robotics, etc.) to be started to coordinate objectives

WG6 / SRIA segmentration into subWGs

- **Ecosystem:** socio-technical projects for the development of an ecosystems favourable to better implement and use innovative solutions and protect applications.

- **Demonstration Projects**: demonstration of available solutions in specific vertical domains to provide national security, protect citizens and economic relevant EU market sectors, allowing economies of scale through engagement with users/demand side industries and bringing together a critical mass of innovation capacities. These projects should eventually deliver results with TRL 6-9.

- **Transversal infrastructures**: projects able to integrate sector-neutral technological building blocks with maximum replication potential, to tackle transversal challenges (common to different application domains). These projects should eventually deliver results with TRL 6-9.

- **Technological components**: mainly devoted to build those sector-neutral technological building blocks with maximum replication potential that can become market references at global level. These projects should eventually deliver results with TRL 3-5.

ECSO WG6 (SRIA): Input to Work Programme 2018-2020 (initial findings, not official ECSO position): Priority areas 1/2

Ecosystem

Ecosystem for Education, training, market growth and SME support

- Cyber Range and simulation
- Education and training
- Certification and standardisation
- Dedicated support to SMEs

Demonstration Projects

Demonstrations for the society, economy, industry and vital services

- Industry 4.0
- Energy
- Smart Buildings & Smart Cities
- Transportation
- Healthcare
- E-services for public sector, finance, and telco

ECSO WG6 (SRIA): Input to Work Programme 2018-2020 (initial findings, not official ECSO position): Priority areas 2/2

Transversal infrastructures

Collaborative intelligence to manage cyber threats and risks

- **GRC**: Security Assessment and Risk Management
- **PROTECT**: High-assurance prevention and protection
- **DETECT**: Information Sharing, Security Analytics, and Cyber-threat Detection
- **RESPONSE and RECOVERY**: Cyber threat management: response and recovery

Technological components

Remove trust barriers for data-driven applications and services

- Data security and privacy
- ID and Distributed trust management (including DLT)
- User centric security and privacy

Maintain a secure and trusted infrastructure in the long-term

- ICT infrastructure protection
- Quantum resistant crypto

Intelligent approaches to eliminate security vulnerabilities in systems, services and applications

- Trusted supply chain for resilient systems
- Security-by-design

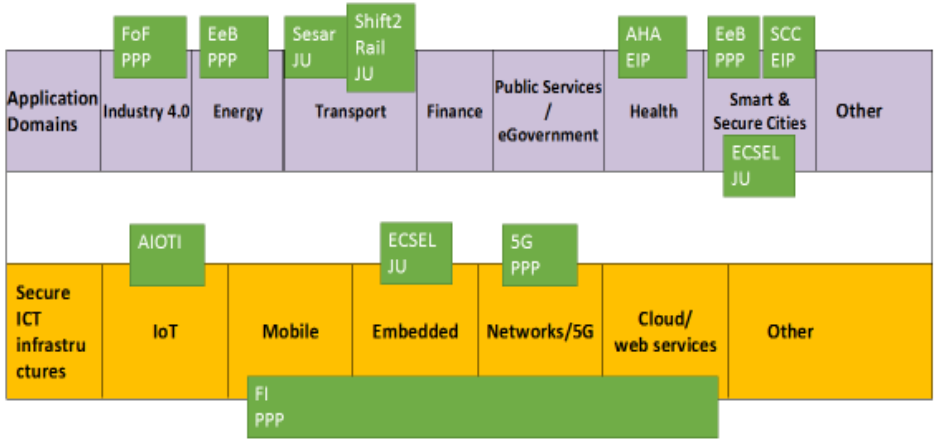
From security components to security services

- Advanced Security Services

Relationships with other cPPPs

Existing PPPs with the European Commission are:

- Factories of the Future (FoF)
- Energy-efficient Buildings (EeB)
- Sustainable Process Industry (SPIRE)
- Big Data Value (BDVA)
- European Green Vehicles Initiative (EGVI)
- Photonics
- Robotics
- High Performance Computing (HPC)
- Advanced 5G networks for the Future Internet (5G)



Other Research Public-Private Partnerships in FP7:

- Future Internet PPP (FI-PPP)
- A 3D printed key to the Factory of the Future
- Nanotech sun block for your home
- Modular, flexible, sustainable: the future of chemical manufacturing

Other important initiatives which could be linked to the ECS cPPP are:

- The AIOTI (Alliance for Internet of Things Innovation)
- The EIP AHA (European Innovation Partnership on Active and Healthy Aging)
- The EIP SCC (Smart Cities and Communities)
- Sesar JU (for a Single European Sky – Air Traffic Management)
- Shift2Rail JU
- ECSEL JU (Electronic Components and Systems for European Leadership)

ECSO WG1 on Certification (initial findings, not official ECSO position): Roadmap for 2017

WG1 segmentration into subWGs:

- **PRODUCTS & COMPONENTS**
- **ICT INFRA OPERATORS:**
- **USERS / INTEGRATORS / OTHER SERVICE PROVIDERS**
- **BASIC LAYER**

Roadmap items

- **Evaluation of all existing testing/certification schemes across Europe and globally** and to various properties such as product domain applicability, security assurance levels, type of vulnerability assessment, time to market, costs and agility.
- **Benchmarking and identifying relevance of each existing scheme** as per the requirements of both public and private sectors
- Mapping and developing opportunities for **harmonization of existing schemes**
- **Developing "best practices" solutions** within the sub-areas, moving toward a "harmonised" approach to cyber security & privacy a consensus based environment
- **Working with public sector partners** to address mutual recognition of "future" schemes
- Accomplishing a **"fast track" process** to achieve actual standards
- **Implementing and piloting these testing and certification solutions** to demonstrate effectiveness and **cost efficiency as well as customer acceptance and trust**

ECSO WG1 on Certification (initial findings, not official ECSO position): Wishes towards the European Commission

- **Cooperation with ECSO WG1** and the **support to achieve the objectives** in order to help other players to join the WG to stream other similar initiatives into this new global public-industrial effort.
- **Dedicated funding for developing the testing/certification systems** (enhancing competitiveness of European industry)
- Support and direct **funding** for major European **pilot** testing/certification demonstration projects
- **Education and dissemination** to the European public sector, the European citizen and the European private sector
- **Assistance in coordination among the different public sector partners** (even within the European Commission Directorates General) and among EU member states
- Eventual **complementary regulatory action to support a harmonized approach** to cyber security & privacy testing/certification and mutual recognition
- **Supporting evaluation and monitoring mechanisms once systems are in place**

More info at: www.ecs-org.eu

CONTACT US

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

Phone:
+32 (0) 27770256

E-mail:
Ms. Eda Aygen
Communication Manager
eda.aygen@ecs-org.eu

Follow us
Twitter: @ecso_eu