European Cyber Security Organisation (ECSO) Elements from ECSO SRIA

Roberto G. Cascella

Senior Policy Officer – ECSO

European Big Data Value Forum

– 23 November *2017* – *Versailles (France)* –

About the European Cybersecurity PPP

A EUROPEAN PPP ON CYBERSECURITY

The European Commission has signed on July 2016 a PPP with the private sector for the development of a common approach and market on cybersecurity.

AIM

1. Foster cooperation between public and private actors at early stages of the research and innovation process
2. Stimulate cybersecurity industry
3. Coordinate digital security industrial resources in Europe

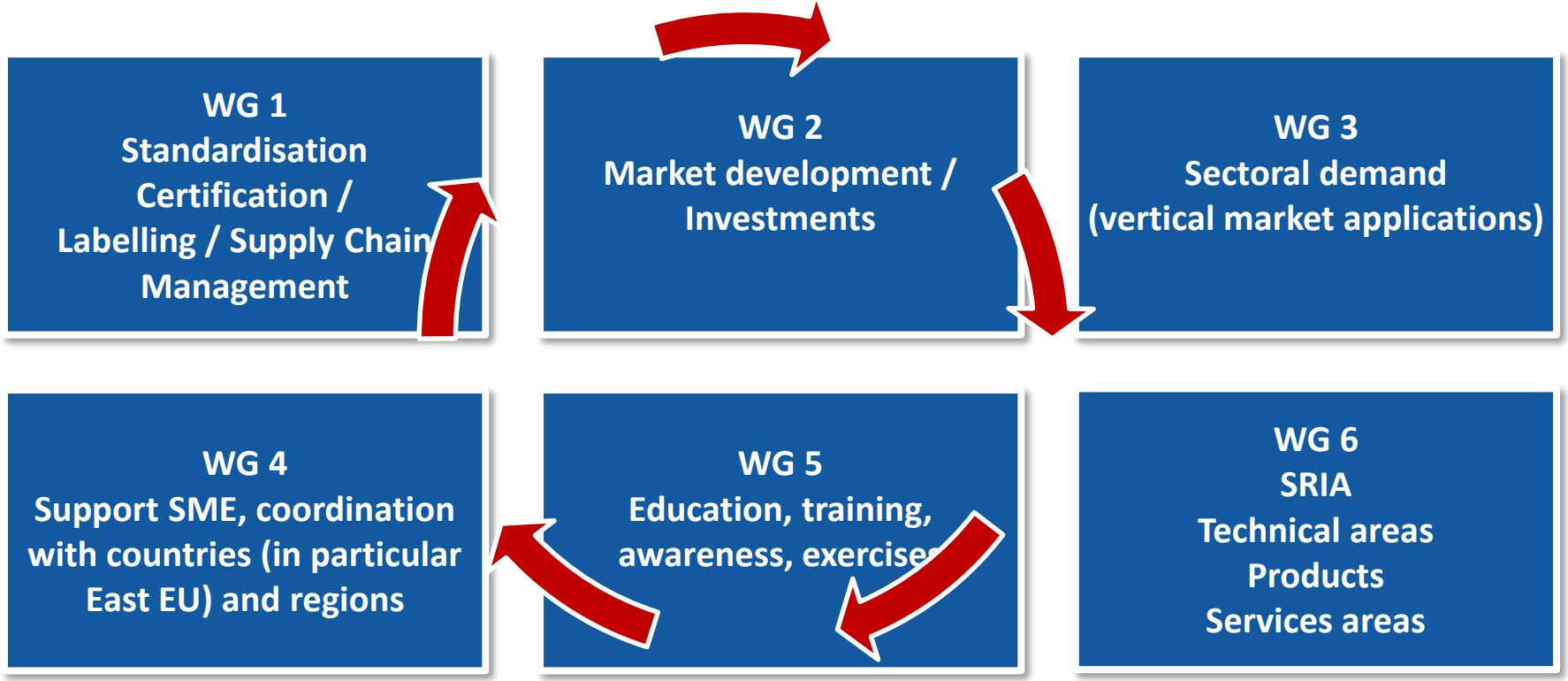
BUDGET

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). Cybersecurity market players are expected to invest three times more (€ 1350 mln: leverage factor = 3) to a total of €1800 mln.

SUPPORT

European Cyber Security Organisation – ECSO Association has been created to engage with the EC in this PPP.
ECSO is open to any stakeholder (public / private; user / supplier) allowed to participated in H2020 projects.

Working Groups



Main achievements / deliverables in the first 15 months of the cPPP and ECSO

WG activities: realizing wider objectives

- WG1 (128 members with 264 experts): Initial positions for an EU certification framework: SOTA, COTI, Meta-Scheme. Initial cooperation (MoU) with CEN/CENELEC – ETSI for standards
- WG2 (72 members with 137 experts): Market analysis: Support Cybersecurity Industry Market Analysis (CIMA project led by EC-PWC-LSEC). Investments: initial discussions with banks & insurances; support to national bodies to understand and develop investments for start-ups. International cooperation: dialogue with US; involvement via members in EC CSA projects (Japan and US); request of dialogue from other countries in stand-by.
- WG3 (115 members with 227 experts): SOTA under finalisation; involvement of DG ENER in the cPPP; initial dialogue with ISACs (finance, energy); more concrete activities under definition.
- WG4 (69 members with 121 experts): SME – Position paper (role of SMEs in the cybersecurity ecosystem); Regions – partner as advisor in proposal for INTERREG (with 7 regions: ECSO members and not). Support to proposal for thematic partnership in Interregional cooperation in cybersec domain (5 regions)
- WG5 (90 members with 181 experts): Initiation of a EHR-4CYBER Network; mapping of educational and professional training courses; started tackling gender issues on education & training
- WG6 (147 members with 320 experts): Defining research priorities: SRIA. One year after: analysis review of technology and needs evolution. Link with other PPPs (BDVA, EFFRA, 5G)

WG6 SRIA:
Technical areas, Products, Services areas

Objectives

- Coordination of results and expectations from EC R&I projects
- Coordination of cybersecurity activities across cPPPs and EIT
- Support cPPP implementation and H2020 cybersecurity projects
- Detailed suggestions for the WorkProgramme 2018 - 2020 using an updated and focussed SRIA

Synthesis of activities

Strategic Research Innovation Agenda (SRIA) delivered to the European Commission as input for the 2018 – 2020 H2020 Work Programme: good acceptance of suggested priorities. Work with other PPPs and similar EU activities to coordinate cyber security objectives (BDVA, EFFRA, 5G IA, ..)

Ongoing activity: focus on cyber security strategy priorities for update of SRIA and identification of priorities beyond 2020

ECSO STRATEGIC RESEARCH & INNOVATION AGENDA v1.2

→cPPP SRIA v1.0 and industry proposal as initial guidelines

→Available on ECSO website: https://www.ecs-org.eu/documents/publications/59e615c9dd8f1.pdf

Detailed structure: 7 main thematic priority areas

- 1 European Ecosystem for the Cybersecurity
  - Cyber Range and simulation
  - Education and training
  - Certification and standardisation
  - Dedicated support to SMEs
- **2 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
- **3 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
- **4 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
- **5 Maintain a secure and trusted infrastructure in the long-term**
  - ICT protection
  - Quantum resistant crypto
- **6 Intelligent approaches to eliminate security vulnerabilities in systems, services and applications**
  - Trusted supply chain for resilient systems
  - Security and privacy by-design
- **7 From security components to security services**

ECS
EUROPEAN CYBER SECURITY ORGANISATION

ECSO inputs to

- LEIT ICT WP 2018-2020 (Cybersecurity and more)
- Secure Societies – Protecting freedom and security of Europe and its citizens

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

A look into the ECSO SRIA: Big Data areas of interest

Application to vertical sectors (SRIA §6)

- Industry 4.0, Energy, Smart Cities, eHealth → Big Data analytics to model and identify cybersecurity threats

DETECT: Information Sharing, Security Analytics, and Cyber-threat Detection (SRIA §7.4)

- Intelligent Big Data security analytics
  - New collaborative (distributed) intelligence threat detection techniques also addressing information sharing, level of abstraction, heterogeneous data from security appliances (machine learning and graph-processing techniques)
  - Need for IDS that will scale-up to Big Data (processing, storage, etc.)
  - Improvement of detection and analysis of cyber-threats at a system, network meta-system and process level based on a combination of existing and new techniques
  - Collaborative security analytics taking into account confidentiality and privacy constraints on usage
  - Anticipation of nascent attacks by detection of suspicious precursor activities (behavioural algorithms)

Remove trust barriers for data-driven applications and services (SRIA § 8.1)

- Data Security and privacy technologies → Techniques to protect data and algorithms operating on them as operations on manipulated or biased data sets can lead to discriminating decision making

ICT Infrastructure Protection (SRIA § 8.2.1)

- Threat Management → Extending security information and event management (SIEM) systems with predictive capabilities, big data analytics for security, association of detection and remediation/mitigation
- ICT system protection and risk management → algorithms resilient to attacks designed to mislead the AI engine

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 Officer
roberto.cascella@ecs-org.eu

Follow us
Twitter: @ecso_eu

ABOUT ECSO

The ECSO approach is going beyond the work of a typical Association supporting a cPPP, as it tackles, on top of Research & Innovation issues, all those topics that are linked to the market development and the protection of the development of the Digital Single Market, in the frame of the European Cybersecurity Strategy.

A peculiarity of ECSO is to include among its members (also at Board of Directors level and within the working groups*) **high representatives and experts from national and regional public administrations**. This approach is fundamental

- in a sector dealing with "security" as application of cybersecurity is and will remain a sovereign issue.
- **to increase the quality of the ECSO recommendations** to the European and national institutions → allowing a faster decision making by public bodies and a viable implementation by the private sector of the decisions taken (regulations, standards etc.).

For this reason **ECSO itself is a public – private body**, creating a **new and dynamic multi-stakeholder dialogue**, preparing for the future evolutions and needs in this sector, as envisaged in the EU cybersecurity strategy.

***ECSO working groups are dealing with the different aspects of what we call "cybersecurity industrial policy"**

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

EUROPEAN COMMISSION

ECS
EUROPEAN CYBER SECURITY ORGANISATION

Governance

ECSO –Board of Directors
(Management of the ECSO Association: policy/market actions)

INDUSTRIAL POLICY

R&I

Coordination / Strategy Committee

WG 1	WG 2	WG 3	WG 4	WG 5	WG 6
Standardisation / certification / labelling / supply chain management	Market deployment / investments / international collaboration	Sectoral Demand (Industry 4.0; Energy; Transport; Finance; eGov; Health; Smart Cities; Telecom/media)	Support to SMEs and REGIONS (in particular East EU)	Education, training, cyber ranges, awareness	Strategic Research & Innovation Agenda Technologies, Products & Services

- 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 Advisory Group (GAG)
- Research Centers (large and medium / small), Academies / Universities and their Associations

ECSO General Assembly

ECSO - Purpose & objectives

- **Short term**
  - R&I priorities for H2020 (2018-2020 work programme);
  - EU Certification & Labelling Framework
  - European HR Network to foster education and training and support job growth in cybersecurity
  - Increase membership (users & operators), stabilise governance
  - Develop dialogue and harmonisation of objectives
  - Suggestions for a new EU Cybersecurity Strategy and future investments (in the 2020 – 2026 MFF)
- **Medium Term**
  - Prepare for post H2020 ("FP9")
  - Standardisation
  - Regional approach (smart specialisation & regional funds)
  - Support to SMEs
  - Develop with concrete actions, education, training, awareness and cyber ranges
  - Development of trusted components, systems, services strategic for Europe
  - Build International dialogue / cooperation
- **Long Term**
  - European industry among cybersecurity market leaders in targeted sectors
  - Support to business development and global competitiveness

ECSO membership

At the time of the signature ceremony of the PPP contract (5th July 2016), ECSO counted 132 founding members. Now we are **218 organisations from 28 countries and counting (already 5 new request since mid September)**

- Associations : 21
- Large companies and users: 70
- Public Administrations: 15
  AT, BE, CY, CZ, DE, EE, ES, FI, FR, IT, SK, FI, NL, NO, PL, UK + observers at NAPAC (BG, DK, HU, IE, LT, LU, LV, PT, RO, SE, SI, MT, …)
- Regional clusters: 3
- RTO/Universities: 55
- SMEs: 54

Looking for increased membership from users / operators

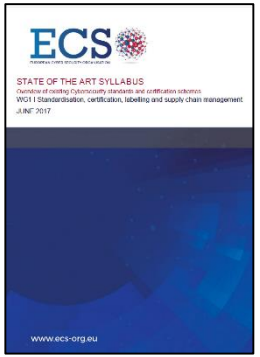
AUSTRIA	6	LATVIA	1
BELGIUM	11	LITHUANIA	1
BE - EU ASSOCIATIONS	10	LUXEMBOURG	4
CYPRUS	4	NORWAY	4
CZECH REP.	2	POLAND	7
DENMARK	3	PORTUGAL	5
ESTONIA	7	ROMANIA	1
FINLAND	8	SLOVAKIA	3
FRANCE	23	SPAIN	28
GERMANY	19	SWEDEN	1
GREECE	4	SWITZERLAND	4
HUNGARY	2	THE NETHERLANDS	14
IRELAND	3	TURKEY	2
ISRAEL	2	UNITED KINGDOM	9
ITALY	30		

Update of WGs activities

➢ WG1 (standards / certification / label / trusted supply chain)

Initial activities focused on the overview of existing cybersecurity standards and certification schemes relevant for the activities of WG1 (SOTA – public document which will regularly), and the identification of the challenges relevant for the industrial sector (COTI – which will remain an internal document). They have been used as basis for ECSO recommendations for EU certification in the Meta – Framework document (soon finalised).
Contact: roberto.cascella@ecs-org.eu

ECSO WG1 STATE OF THE ART SYLLABUS
Overview of existing Cybersecurity standards and certification schemes
→ 202 pages – 97 contributions – 290 standards and certification schemes listed
→ Scheduled revision every 6 months, in order to maintain representativeness of the document
→ Available on ECSO website: https://www.ecs-org.eu/documents/publications/59e61366c048b.pdf



➢ WG2 (market / funds / international cooperation / cPPP monitoring)

Initial internal work on business models (also with insurances and private funds), funding programmes (also beyond R&I) and taxonomy for cyber security solutions. Priorities for international cooperation under definition. Work with EC for the definition of cPPP monitoring KPIs / criteria.
Contact: danilo.delia@ecs-org.eu

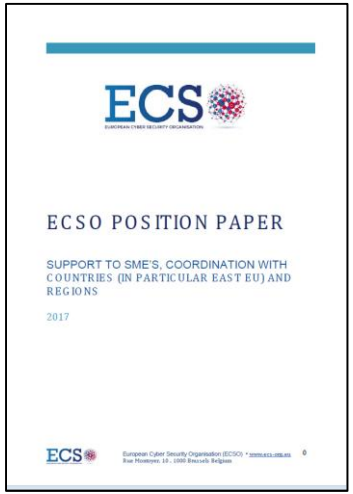
Update of WGs activities

➢ WG3 (verticals: Industry 4.0; Energy; Transport; Finance / Bank; Public Admin / eGov; Health; Smart Cities)

State of the Art deliverable being drafted, engagement with users initiated. SubWG meetings ongoing to define detailed needs / objectives / actions. Initial meetings with different Directorate Generals at the European Commission (ICT, energy, transport, internal security, etc.) to better define technology priorities. User outreach also ongoing.
Contact: nina.olesen@ecs-org.eu

➢ WG4 (SMEs, Regions, East EU)

SMEs: discussions on other forms of support to SMEs other than R&D (e.g. EU regional funds); SME hub; cooperation with large companies; certification issues / labelling; workforce.
Regional aspects: cooperation with "EU Regions"(DG REGIO + DG CNECT + DG JRC, DG GROW, ECSO members and regions not ECSO members): identification of regional and structural funds for cybersecurity; gathering of Regions to better target these resources.
East EU aspects: to be developed soon.
Contact: danilo.delia@ecs-org.eu



ECSO WG4 Position Paper
Support to SMEs, Coordination with Countries (in particular East EU) and Regions
→ Available on ECSO website: https://www.ecs-org.eu/documents/publications/59706a2c224b3.pdf

Update of WGs activities

➢ WG5 (education, training, awareness, cyber ranges…)

SubWG meetings ongoing to define detailed needs / objectives / actions. ERH-4CYBER Network started, to promote and harmonise education and training among ECSO members (and beyond) and support job creation

Contact: nina.olesen@ecs-org.eu

➢ WG6 (SRIA)

Strategic Research Innovation Agenda (SRIA) delivered to the European Commission as input for the 2018 – 2020 H2020 Work Programme: good acceptance of suggested priorities. Work with other PPPs and similar EU activities to coordinate cyber security objectives (BDVA, EFFRA, 5G IA, ..)
Ongoing activity: focus on cyber security strategy priorities for update of SRIA and identification of priorities beyond 2020
Contact: roberto.cascella@ecs-org.eu

ECSO STRATEGIC RESEARCH AND INNOVATION AGENDA v1.2
→cPPP SRIA v1.0 and industry proposal as initial guidelines
→Available on ECSO website: https://www.ecs-org.eu/documents/publications/59e615c9dd8f1.pdf