ECSO Status Report

Luigi REBUFFI – ECSO Secretary General

TeleTrusT internal workshop
Berlin - July 5, 2018
www.ecs-org.eu

Evolution of the European political agenda

- **2011**: Initial discussions with the EC for a European **PPP on cybersecurity**
- **2013**: EU Cybersecurity **Strategy**
- **2014**: **Digital Single Market** / Digitalisation EC communication
- **2016**: **cPPP** on Cybersecurity (This is us!)
- **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**

And beyond

- 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)

Main achievements in the first two years: governance & cooperation on policy issues

- ✓ **Membership**: from initial 132 members mid 2016 to about 240 members mid 2018 representatives of all main sectors
- ✓ **Management bodies:** Partnership Board, Board of Directors, 6 WGs, Committees (including NAPAC with national Public Administrations)
- ✓ **Wide communication and dissemination activities**
  - Building a cybersecurity community building across EU from regional to EU level
  - Contribution to more than 150 conferences, about 40 articles
- ✓ **Dialogue / Cooperation with EU Institutions**
  - Regular dialogue with EU Institutions: EP; Council; EC: VP / Commissioners and Cabinets (Gabriel; Ansip; King, Oettinger), CNECT, MOVE, ENER, HOME, JRC, REGIO, GROW; Agencies: ENISA, EUROPOL, EIT, EIB, EASA, euLISA, FRONTEX; EDA; EEAS; Programme Committees; International Organisations (ITU, WEF, …)
    - Recommendations to the E.C. on the cybersecurity package, **MFF and the Network of Competence Centres**
    - Contribution to the EP on **cPPP topics, Cybersecurity Act** and **Industrial Cybersecurity Policy issues**
    - Contribution to Council's **Horizontal Working Party for cybersecurity** on R&I priorities and cybersecurity package
    - Close collaboration with past, present and future **EU Presidencies**

Main achievements in the first two years: from policy suggestions to increasingly more concrete deliverables

ECS
EUROPEAN CYBER SECURITY ORGANISATION

- ✓ **WG1: Input for the EU Certification Framework (Meta-scheme methodology) and the Cybersecurity Act legislation**
- ✓ **WG2: Cybersecurity Market analysis**
- ✓ **WG3: Identification of needs for the different vertical sectors**
- ✓ **WG4: Radar (identification of competences / products); European Cyber Valleys Project (regional aspects)**
- ✓ **WG5: EHR4CYBER (sharing of best practices for skills development and job creation)**
- ✓ **WG6: SRIA (Strategic Research and Innovation Agenda) for H2020 priorities**
- ✓ **cPPP Monitoring: delivering investment in the SRIA perimeter satisfying cPPP committment**

WG1: Our contribution to the EU Cybersecurity Framework

Continuous dialogue with European Institutions and National Public Administrations

Conclusions that can be drawn from our work regarding the EU Cybersecurity Act, used in the "General Approach" agreed by the Council

An adequate EU Certification Framework could solve the present fragmentation challenge

- **Experts from industry** part of decision process **for scheme selection and priority –** A roadmap of intended priorities is needed for the market
- **Minimum common baseline security** needs to be defined **across sectors.** Threat analysis and risk assessment as source for security requirements
- The **scope of certification** should address the entire supply chain: what and how depends on the intended use
  - The level of assurance attained should consider the potential risk and related impact of potential attacks linked with the product/service usage
- **Ethical hacking shall be legally allowed and enforced for high security**; checklists are insufficient!
- Need for a common definition of the proposed assurance levels, i.e., **assessment methodologies (evaluation) associated**
- **Centrally steered harmonization** across CABs, NABs and National Certification Supervisory Authorities (NCSA) is crucial!

The **ECSO meta-scheme approach** can act as a methodological tool (e.g. for ENISA) to structure the landscape and "glue" existing schemes together and specify additional steps

WG1: achieving wider objectives in a wider dialogue for standards and certification

WG1 - standards / certification / label / trusted supply chain (135 members from 27 countries with 289 experts).
Contact: roberto.cascella@ecs-org.eu

STATUS & OBJECTIVES 2018:

- **Mapping of Cybersecurity Act** wrt ECSO Meta-Scheme approach
- **Detailed suggestions for the European Cyber Security Certification Framework** supported by pilot concrete studies (e.g. IoT, smart meters, SCADA / ICS, …);
- Update
  - **Meta-Scheme (v2.0): conformity self assessment and clarification on third party certification**
  - **Meta-scheme in practice with pilots (e.g. SCADA+ICS, IoT, Smart meters)**
  - Update COTI (position vs evolving challenging in cooperation with WG3/ verticals; link to priority certification schemes)
- **Analysis of certification requirements, gaps and priorities for the different sectors / verticals (to the EC and MS) to propose initial EU certification schemes with the support of industry (SME and large)**
- Cooperation with CEN/CENELEC (MoU) & ETSI (MoU) and ENISA

WG2 activities: achieving wider objectives in a wider dialogue for market development and investments

WG2 - market / funds / international cooperation / cPPP monitoring (86 members from 20 countries with 159 experts) Contact: danilo.delia@ecs-org.eu

STATUS& OBJECTIVES 2018

- Market analysis: Support Cybersecurity Industry Market Analysis:
  - Directory and Marketplace for SMEs using common taxonomy in coop with WG4;
  - **Radar of European solutions** (national catalogues for DE, ES, FR, EE, UK) using common taxonomy (draft in September, then deepening the detail level), providing an analytics tool to get the maturity/evolution of EU cybersecurity market both to investors and suppliers.
  - Mapping of events and main stakeholders in cybersecurity (local public & private initiatives supporting business development of innovative companies);
- Investments: Analysis of existing and innovative funding models
  - Proposal of a public-private fund specialized in cybersecurity: Recommendations for **EU investment model** – link with WG4 (envisaging a **European investment fund dedicated to cybersecurity for start-ups & scaleups**) – to be matured further via meetings with investors;
- **cPPP Monitoring** and report on cPPP implementation / investments;
- International cooperation:
  - mapping members' needs; initial dialogue with DG-CNECT and DG-GROW on business Internationalisation beyond the EU (e.g. RSA) ; involvement via members in EC CSA projects (Japan and US).

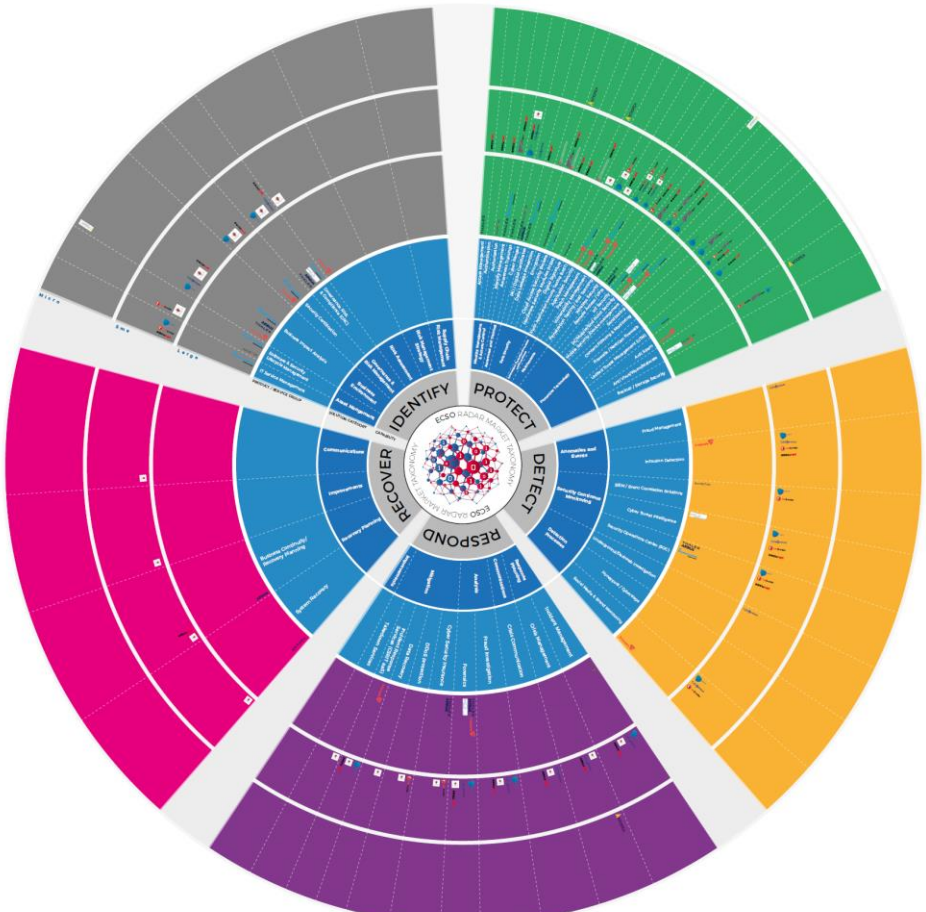
Objectives 2018: Radar of European solutions

ECSO to provide visibility to European solutions

Support ECSO members to **improve their market knowledge** (products, suppliers, but also cyber security insurance solutions)

Create a community of industries and develop the incentives to **share information about the market and its consolidation**

Consolidation Roadmap : how investors and vendors could shape the market and facilitate the development of EU champion

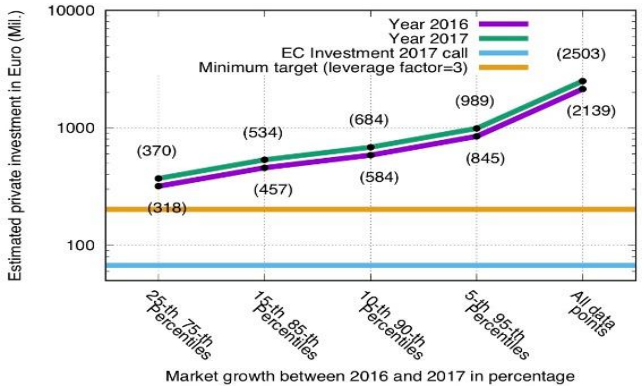


cPPP Monitoring at Glance – 1st Period

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)**

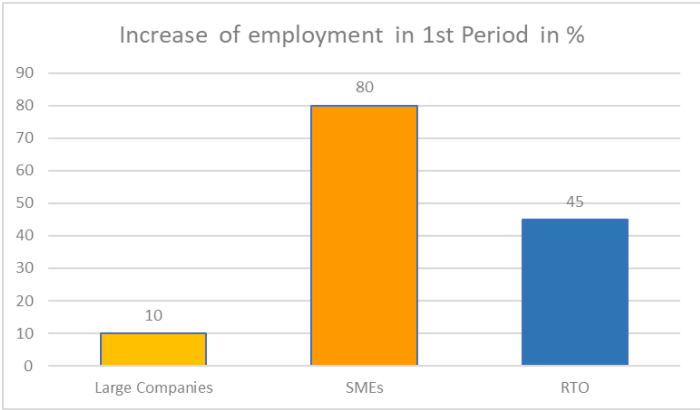


Estimated private investment for 2016 and 207

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%**



WG3 activities: achieving wider objectives in a wider dialogue with users and operators

WG3 - verticals: Industry 4.0; Energy; Transport; Finance / Bank; Public Admin / eGov; Health; Smart Cities; Telecom/Content/Media (128 members from 27 countries with 289 experts): Contact: nina.olesen@ecs-org.eu

STATUS & OBJECTIVES 2018:

- **Sector specific reports on users' needs (SOTA):**
  - Four sector reports finalised and approved (Industry 4.0, Finance, Healthcare, and Smart Cities);
  - One under finalisation (energy): others (eGov, Transport/road; Telecom) to come
- **Mapping (from SOTAs and discussions with users) needs from all the verticals vs WG activities**
- **Operational EU platform for users: harmonisation of incident reporting (**NIS implementation) **towards sectoral operational platforms at EU level also for information sharing and fast reaction to threats** (starting with banks and energy, looking for application sin other sectors for interdependencies);
- **Creation of a Users' Committee for trusted information sharing** (URC – Users Representatives Committee, similar to NAPAC);
- Report on ISAC's needs and their implementation;

WG3 user-driven actions: Users' Operational Platform

Ongoing project:

- Developing **common application for incident reporting and information sharing** (led by banks but applicable other sectors); Governance and functional specifications being defined; Funding needed (CEF, investment from members)
  - **Phase 1: Incident reporting;**
  - **Phase 2: Infosharing;**
  - **Phase 3: Crisis management**

The financial sector and especially banks (Intesa SanPaolo, BBVA, CITIGroup, Rabobank) are leading the way on concrete projects, moving ECSO WG3 towards operational tasks and motivating other user-operators to join ECSO.

NOTE: The energy sector is also interested in the development of a similar platform.

ECSO could provide independent services to its members or some of its members investing in specific resources. E.g. upon request of its members, ECSO could support the development with its members of independent private sectoral European "operational" platforms for secure information sharing and vulnerability / threat intelligence sharing among users in a cross-sector environment that could foster cyber security against supply chain compromise.

ECSO (WG3) could support the creation of platforms and tools to support members in the implementation of the NIS Directive. ECSO could help its OES (Operators of Essential Services) members to use relevant funds to improve their capabilities and create / operationalise platforms and their link with ISACs and CSIRTs for trusted exchange of information and incident reporting.

Creation of an ECSO Users' Committee

- Users / Operators request for a TRUSTED environment at EU level to share information and threats among them (it exists in some countries with different level of efficiency, but not at EU level).
- This approach will better enlighten the Board about sectoral issues and needed actions, increase trust, attract new users as member of ECSO, better define users' needs, etc.
- Creation of a unique Users' Committee for all sectors gathering pure users/operators according agreed rules. Start in September 2018

Take away: Build a TRUSTED environment to foster collaboration among users and share information.

ECSO will concretely help operators to create a trusted environment

to exchange "sensitive" information (beyond ISACs)

WG4 activities: achieving wider objectives in a wider dialogue with SMEs and Regions

WG4 - SMEs, Regions, East EU (76 members from 22 countries with 134 experts): Contact: danilo.delia@ecs-org.eu

STATUS & OBJECTIVES 2018:

- Support to SMEs:
  - Position paper: role of SMEs in the cybersecurity ecosystem;
  - **SME Hub platform and "European (ECSO) Cyber Quadrants**": Marketplace and tool for community building and tools for funding opportunities and projects; Register of EU cybersecurity SMEs; (proposal at Sept Board)
- Investments for start-ups:
  - **Matchmaking events between VCs / Investors and Start-Ups / SMEs:** support to national public and private bodies to understand and develop an EU approach for specific investments in Cybersecurity; (past events: Paris, Tallinn, Brussels; coming events: Milan with integrators & users – 13-14 Sept; Berlin with investors – 29 Nov)
- REGIONS:
  - **Interregional Pilot Action** (5 Regions: Conseil régional de Bretagne (leader), Junta Castilla y Leon/City of Leon (Spain), Regional Council of Central Finland (Finland), Estonia and North Rhine Westphalia): Project to prepare in Jan 2019 an **interregional accelerator programme** with few scale-ups supported by an **EC budget of almost 200M€** for cyber activities in regions (smart commercialisation)
  - **INTERREG "CYBER" project** (7 Regions): Development of **Cyber smart specialisation in EU Cyber Valleys** (cooperation between specialized regions for concrete activities: e.g. supporting local SMEs : Brittany, Castilla y León, Estonia, Tuscany, Wallonia, Slovenia, Slovakia) start-ups' access to market; education / training)
- EAST EU REGION: **Development of a regional cyber ecosystem in East / Central Europe and Balkans** (link with Competence Centres and existing initiative in East EU) - to be proposed at Sept Board. Network of regions interested in partnering to design a regional approach to raise the cybersecurity level in East EU (in particular SMEs, Users/ Operators, RTOs / Universities).

European SME Hub – bring visibility and quality

Creation of a European SME Hub Concept

ECS
EUROPEAN CYBER SECURITY ORGANISATION

Concept : Rating / Ranking of SMEs on the EU Cyber SME register according to:

- Security certifications (security claim)
- AND „ability to execute“ (broadness of coverage)

Creation of “**European Cyber Quadrants**“ for the different value chain elements:
analogue to the Gartner Magic Quadrant, but non commercially biased and with an EU company focus

Basic Functionality

a) **Registration :** Company basic data (Name, Contact data, Legal body, Representatives, etc.).
Information about markets segments covered, according to a predefined three level market segmentation structure

b) **Profile/Dashboard for registered SMEs :** registered SMEs get - after login - to their profile page, where they can edit their company information.

c) **Search functionality :** every company, investor or job applicant can conduct searches on the SME Hub database: searching for market segment(s), quantity and quality criteria and country

Premium Functionality

Registration (extended) requires a verification & approval step: More detailed information to be provided for each market segment:

- Information about size (maximum seats / licenses,…), quality (standards/certifications, years in service, no. of employees servicing that part of market segment, research budget, or similar) and reference.
- Submitted information will be quality checked and approved by a dedicated staff

Profile / Dashboard for registered SMEs

- Dashboard includes the possibility to manage additional information
- As a results the company gets a **special marking and labelling as “Verified European Cyber SME“** which indicates that the provided information has been independently checked

Search functionality

- Premium (verified) companies are prioritised (ranked first) in the search results and marked with the label “Verified European Cyber SME“
- Clicking on them displays more comprehensive company information

Quadrants

- Premium (verified) companies are included in **“Cyber SME Quadrants”** which display for defined market segments (level 2 & 3) the placing of the according SMEs in a neutral and unbiased way
- Non-premium SME are not included in quadrants!

WG5 activities: achieving wider objectives in a wider dialogue for education, training, awareness and cyber ranges

WG5 - Education, training, awareness, cyber ranges (112 members from 28 countries with 225 experts): Contact: nina.olesen@ecs-org.eu

STATUS & OBJECTIVES 2018:

- Cyber Ranges
  - Cyber range report assessing capabilities and motivations.
  - **Organisation of EU/ECSO Cyber Ranges** (Brussels – Oct 2018; Tallinn early 2019)
- Education & Professional Training; Jobs & Skills
  - Position Paper on Gaps in Education & Professional Training (approved).
  - Participation in Digital Opportunity pilot scheme (EC / skills);
  - EHR4CYBER Network (Increase visibility and concrete actions of the ECSO European Human Resources)
    - White Paper (expected December Board)
      - ✓ Sharing best practices
      - ✓ Recommendations / mapping for a European framework for education and competences (matching profiles and skill-sets)
      - ✓ **Cyber Security Professional certification**
    - Online jobs marketplace: **Creation of a Platform for job research at EU level as an internal or external initiative with a self sustainable business model** (proposal at December Board?)
    - **Creation of an ECSO WOMEN IN CYBER initiative:** gender issue on education & training to increase number of cyber experts
- Awareness
  - Awareness for decision makers: Increased **dialogue with CISO** of operators
  - Awareness for citizens:
    - Cooperation with Europol (No More Randsom)
    - Support to the "School of the Future" initiative for cybersecurity education before University level.

WG6 activities: achieving wider objectives in a wider dialogue for R&I and new technologies / services

WG6 - Strategic Research and Innovation Agenda, new Technologies, Cyber Defence (157 members from 28 countries with 351 experts): Contact: roberto.cascella@ecs-org.eu

STATUS & OBJECTIVES 2018:

- Identification of research priorities for EC programmes: SRIA (Strategic Research & Innovation Agenda) priorities already incorporated in the 2018-2020 work programme of H2020. **Update of R&I priorities for the 2020 call**
- Identification (supported also by the new Scientific & Tech. Committee) of the key drivers for the future (beyond 2020) and analysis to review technology and needs evolution, **global trends, and key implications on strategy up to 2027 in a commonly agreed taxonomy: 4 mainstreams:**
  - 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
  - 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
- **Initial priorities for Horizon Europe (SRIA 2.0):** Identification of R&I needs on specific verticals in cooperation with WG3;
- **Study on impact of new technologies (IoT security, AI and Blockchain) on the different WG aspects and verticals** (link with WG3)
- Link with other PPPs to coordinate objectives and strategy for future EU cybersecurity R&I (BDVA, EFFRA, EURobotics, 5G – MoU, AIOTI).
- **Support to Members for the creation of the EU Network of Cybersecurity Competence Centres; Link with the EC for the EU Cybersecurity Competence Centre**
- **Cyberdefence Task Force starting soon activity under WG6**

ECSO Task Force on the future of the European Cybersecurity Definition and Vision

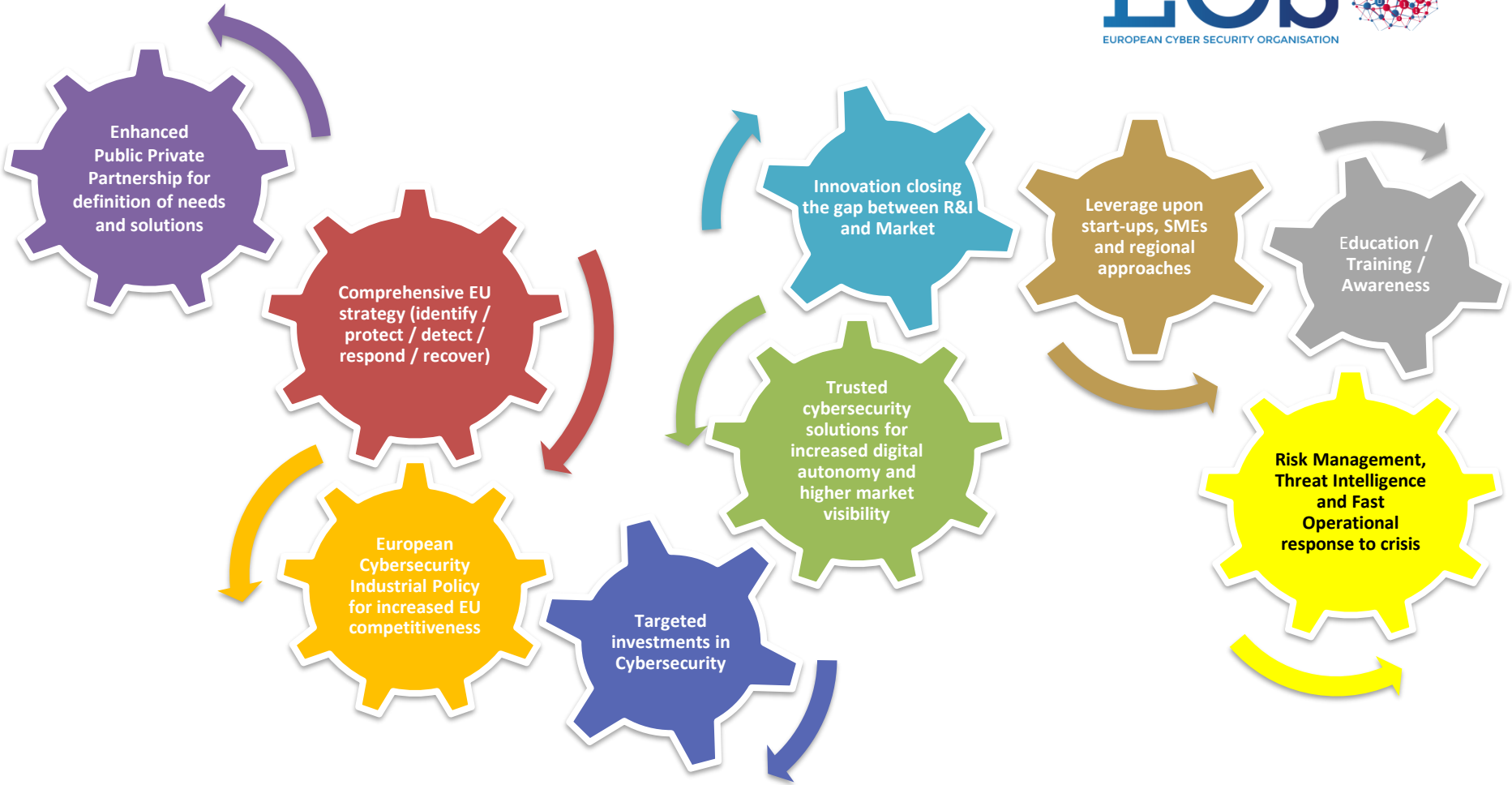
ECSO definition of EU Cybersecurity

European Cybersecurity 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 Cybersecurity in 2027

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

The Cybersecurity Building Blocks recommended by ECSO



What next?
ECSO requested to go operational by its members

- ✓ ECSO is continuing to grow but at the same time it **should evolve**.
- ✓ From the initial support to the cPPP (R&I priorities) we have tackled approaches to develop the full European cybersecurity ecosystem with increasingly **concrete actions**
- ✓ The E.Commission is now envisaging to **invest a larger budget** (under the next MFF) in cybersecurity / cyberdefence, developing local / regional competence and supporting the increase of MS capacities, under a new governance based upon the EU Competence Centre also with the support of a stronger ENISA.
- ✓ ECSO is cooperating with the EC to define such vision and its objectives, under an **enhanced PPP**, going beyond R&I, **representing the whole European Cybersecurity Community**
- ✓ At the same time, ECSO members are identifying **short term operational needs** (job creation; support to info sharing/ incident reporting / fast crisis responses; support to SMEs; etc.) that the envisaged EC measures could not satisfy.
- ✓ **ECSO could support the creation of platforms and operational tools to support its members** (and the EU ecosystem at large) providing independent services and other concrete initiatives demonstrating its added value at European level as a complement to the envisaged EC initiatives.

ECSO membership overview (situation 20 June 2018 – after Board and GA)

132 founding members: now we are **233** organisations from 28 countries and counting (included 6 other membership requests – in brackets – to be confirmed)

AUSTRIA	7	ITALY	26
BELGIUM	13	LATVIA	1
BE - EU ASSOCIATIONS	9	LITHUANIA	1
BULGARIA	2	LUXEMBOURG	4
CYPRUS	5 (+1)	NORWAY	4
CZECH REP.	3	POLAND	5
DENMARK	5	PORTUGAL	2
ESTONIA	7	ROMANIA	1
FINLAND	8	SLOVAKIA	2
		SLOVENIA	1
FRANCE	24 (+1)	SPAIN	32
GERMANY	22 (+2)	SWEDEN	3
GREECE	5	SWITZERLAND	6
HUNGARY	3	THE NETHERLANDS	17
IRELAND	3	TURKEY	3 (+2)
ISRAEL	2	UNITED KINGDOM	8

- Associations : 22
- Large companies and users: 70
- Public Administrations: 20 (+1)

  AT, BE, CY, CZ, DE, EE, ES, FI, FR, IT, SK, FI, NL, NO, PL, UK, BG, SE, GR (+TR)

  observers at NAPAC (DK, HU, IE, LT, LU, LV, PT, RO, SI, MT, …)
- Regional clusters: 6
- RTO/Universities: 65 (+1)
- SMEs: 50 (+4)

Elected ECSO Board Directors at the 2018 GA (June 20th)

Member / External name	Country	Functional status	First Director (3y) or Director (1y)	Permanent Representative
AEI CIBERSEGURIDAD	Spain	Associations	Director	Carlos Prieto-Saiz
EUROSMART	Belgium	Associations	Director	Stéfane Mouille
Finnish Information Security Cluster FISC ry	Finland	Associations	Director	Juha Remes
ACN - Alliance pour la confiance numérique	France	Associations	First Director	Alexis Caurette
EOS	Belgium	Associations	First Director	Paolo Venturoni
ETNO - European Telecommunication Network Operator's Association	Belgium	Associations	First Director	Lise Fuhr
TeleTrusT - IT Security Association Germany	Germany	Associations	First Director	Gerd Müller
SIEMENS	Germany	Large Company	Director	Eva Schulz-Kamm
F-Secure Corporation	Finland	Large Company	Director	Samu Konttinen
Vitrociset	Italy	Large Company	Director	Walter Matta
NXP	The Netherlands	Large Company	Director	Wolfgang Steinbauer
SECOND BALLOT ONGOING (INDRA / ROHDE&SCHWARZ/ SGS)	TBD	Large Company	Director	TBD
AIRBUS Defence & Space - CyberSecurity (Airbus DS CyberSecurity)	France	Large Company	First Director	François Lavaste
ATOS Spain S.A.	Spain	Large Company	First Director	Philippe Vannier
Infineon Technologies AG	Germany	Large Company	First Director	Thomas Fitzek
Leonardo S.p.a. - Leonardo-Finmeccanica-Società per azioni	Italy	Large Company	First Director	Andrea Campora
THALES Communications & Security SAS	France	Large Company	First Director	Yves Lagoude
BKA - Federal Chancellery of Austria	Austria	Public Administration	Director	Katharina-Irene Bointner
Ministry of Digital Affairs, Poland	Poland	Public Administration	Director	Karol Okonski
MiSE - Ministry of Economic Development, Italy	Italy	Public Administration	Director	Rita Forsi
ANSSI - Agence Nationale de la Securité des Systèmes d'Information	France	Public Administration	First Director	Guillaume Poupard
Ministry of Defence of the Republic of Estonia	Estonia	Public Administration	First Director	Kusti Salm
SETSI - INCIBE - CDTI	Spain	Public Administration	First Director	Felix Barrio
Conseil Régional de Bretagne	France	Regions / Cluster	Director	Annie Audic
Goethe University	Germany	RTO / University	Director	Kai Rannenberg
CEA	France	RTO / University	Director	Géraud Canet
CNR - Consiglio Nazionale delle Ricerche	Italy	RTO / University	First Director	Fabio Martinelli
TECNALIA - Fundación Tecnalia Research & Innovation	Spain	RTO / University	First Director	Ana Ayerbe Fernandez-Cuesta
S2GRUPO	Spain	SME	Director	Miguel Angel Juan
CONCEPTIVITY sàrl	Switzerland	SME	Director	Mark Miller
DIGITAL SME - European DIGITAL SME Alliance	Belgium	SME	First Director	Sebastiano Toffaletti
GUARDTIME	Estonia	SME	First Director	Martin Ruubel
EDF - Electricité de France	France	User / Operator	Director	Olivier Ligneul
RIA - Information System Authority , Republic of Estonia	Estonia	User / Operator	First Director	Silja-Madli Ossip
INCERT GIE	Luxembourg	User / Operator	Director	Benoit Poletti
INTESA SAN PAOLO	Italy	User / Operator	Director	Giorgio Cusmà Lorenzo

BECOME MEMBER!
CONTACT US

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

www.ecs-org.eu

Phone:
+32 (0) 27770256

E-mail:
Ms. Eda Aygen
Head of Communications &
Advisor to the SecGen
eda.aygen@ecs-org.eu

Follow us
Twitter: @ecso_eu