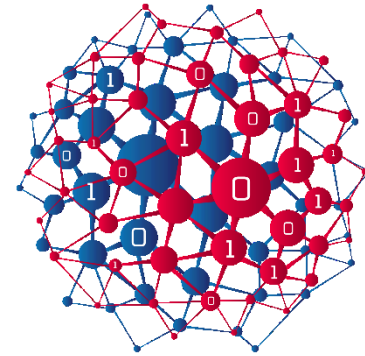


ECS

EUROPEAN CYBER SECURITY ORGANISATION



Working for a cyber resilient digital Europe

Fabio Martinelli

**Consiglio Nazionale delle Ricerche (CNR)
European Cyber Security Organization (ECSO)**

A propaedeutical introduction of cybersecurity in Europe



HISTORY

- 2013: first European Cyber Security Strategy
- 2013: creation of the Network and Information Security (NIS) EU platform
- 2015: first European cyber security research agenda
- 2016: signature of the cPPP between the EC and ECSO, signature of NIS directive and GDPR
- 2017: update of the EU cybersecurity strategy / Cybersecurity Act proposed
- 2018: adoption GDPR and NIS Directive / Competence Centre Regulation proposed
- 2019: adoption of Cybersecurity Act, starting of the 4 Pilots on Competence Centres

About the European Cyber Security 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 in order to allow people in Europe to access innovative and trustworthy European solutions (ICT products, services and software). These solutions take into consideration fundamental rights, such as the right for privacy.
2. Stimulate cybersecurity industry, by helping align the demand and supply sectors to allow industry to elicit future requirements from end-users, as well as sectors that are important customers of cybersecurity solutions (e.g. energy, health, transport, finance).
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.

Cybersecurity challenges in Europe



- **Growing digitalisation** of the Society and of the EU Industry / Economy: challenging understanding of its effective evolution and impact on protection from cyber threats of democratic life, citizens, resilience and reliability of infrastructures and services
- **Cyber threats evolving very quickly:** approaches and organisations should be very flexible, systems should be resilient
- **Challenging data ownership and management** (citizens privacy, national security / public admin, companies' Intellectual Property ...)
- **Market fragmentation:** difficulty for EU companies to compete on the national, EU and global level (many SMEs with limited access to market, lack of European Champions, 28 national sovereign countries)
- **Cybersecurity and ICT market dominated by suppliers from outside Europe.** Innovation led by imported ICT products. Strategic supply chain dependency hampering EU digital autonomy aspiration
- **Missing EC cybersecurity industrial policy** to develop the whole ecosystem →
 - **EU R&I results hardly reaching the market.** Innovation: strong in Europe but lack of a consistent transnational approach and global EU strategy.
 - **Lack of sufficient coordination at local** (smart cities and regions: where the effective implementation happens!), **national and EU level**
 - **Need for a comprehensive EU cybersecurity vision and strategy** (identify / protect / detect / respond / recover)
 - **Need for better understanding of effective market needs at EU policy making level** (looking mainly at implementation of EU policies)
 - **Insufficient public and private investments** (also, lack of synergies). Weak entrepreneurial culture, lack of venture capital.
 - Need for **harmonised Risk Management, Threat Intelligence and Fast Operational response** to crisis
 - **Human factor a growing issue:** education (also, cyber-hygiene), training, awareness (citizens, professionals and decision makers)

ECSO • BOARD OF DIRECTORS

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

ECSO • GOVERNING BODIES

Coordination / Strategy Committee

NAPAC (National Public Authorities Committee)
NAPAC-GAG (Governmental issues NAPAC R&I)

Scientific & Technology
Committee

Financial Committee

WG

Standardisation,
certification and
supply chain
management

WG

Market deployment
Investments and
international
collaboration

WG

Sectoral demand
Industry 4.0, energy,
transport, financial
services, public
services, healthcare,
smart cities Telecom
and media

WG

Support to SMEs,
coordination with
countries
and regions

WG

Education,
training,
awareness,
cyber ranges

WG

SRIA and Cyber
Security
Technologies

ECSO • GENERAL ASSEMBLY

- SMEs solutions and services providers ; Local and regional SME clusters and associations; Start-ups, incubators and accelerators
- Large companies solutions and services providers / users
- National / European organisations or associations
- Regional / local administrations; Regional / local clusters for solutions and services providers or users
- Public or private operators of essential services
- National public administrations
- Research Centres ; Academia; Universities and their associations

ECSO membership growing (status as of 1 November 2019)



132 founding members: now we are **263 organisations** (including last requests - in brackets) from **29 countries** and counting ECISO is also reaching out to all the members of our **28 associations**, i.e. a Community of **more than 2000 bodies** and **almost 2000 experts** directly engaged in our working groups

AUSTRIA	7	LATVIA	1
BELGIUM	15 (+1)	LITHUANIA	1
EU ASSOCIATIONS	13	LUXEMBOURG	4
BULGARIA	2 (+1)	NORWAY	6
CYPRUS	6	POLAND	6
CZECH REP.	3	PORTUGAL	4
DENMARK	5	ROMANIA	2
ESTONIA	8	SLOVAKIA	1
FINLAND	9	SLOVENIA	1
FRANCE	29	SPAIN	34 (+1)
GERMANY	23	SWEDEN	3
GREECE	7	SWITZERLAND	5
HUNGARY	3	THE NETHERLANDS	14
IRELAND	5	TURKEY	4
ITALY	30	UNITED KINGDOM	9

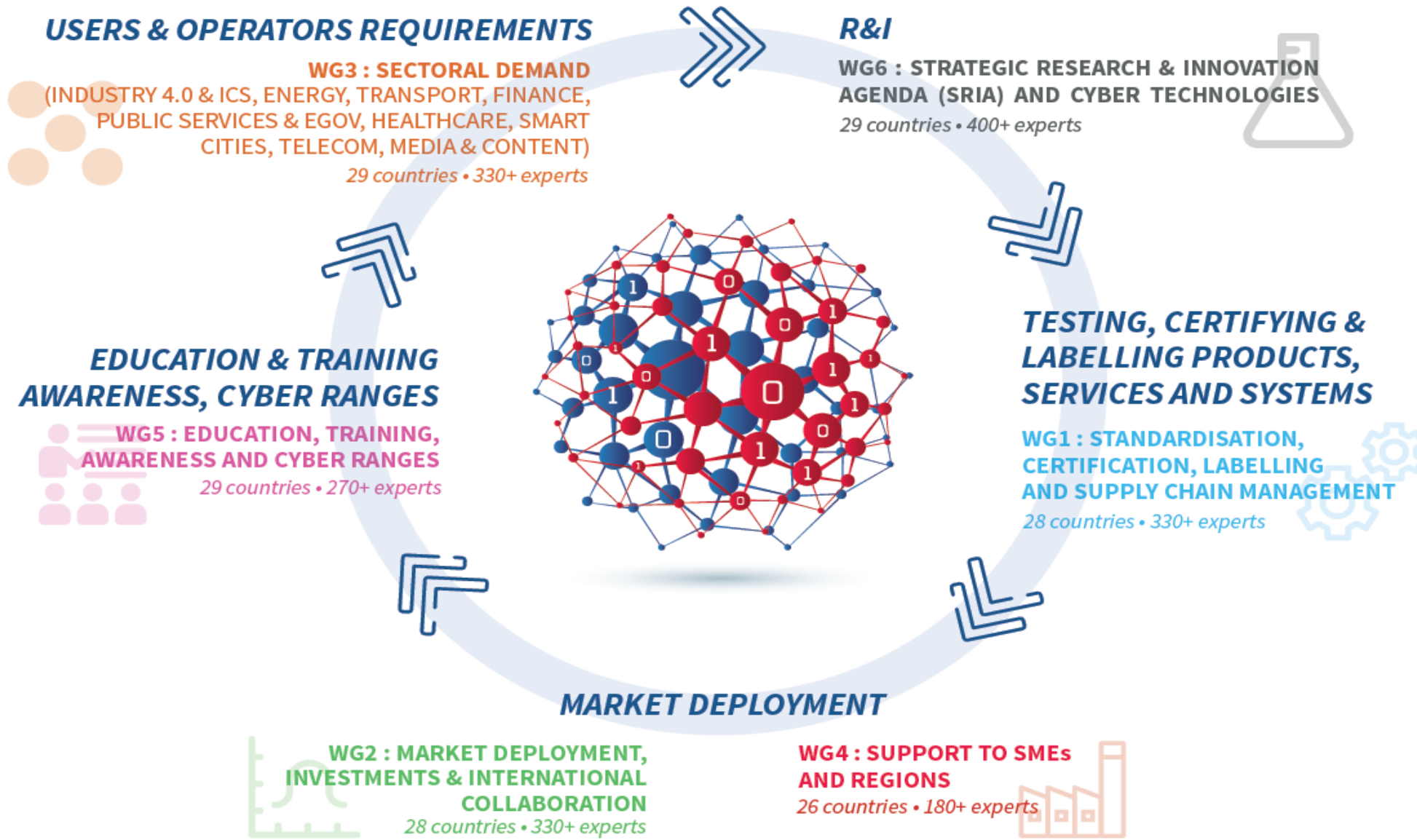
- Associations : 26 (+2)
- Large companies: 55
- Users / Operators: 16
- Public Administrations: 21
AT, BE (2), BG, CY, CZ (2), EE, FI, FR, GE, GR, IT, NL, NO, PL, RO, SE, SK, SP, UK
- Observers at NAPAC (DK, HU, IE, LT, LV, MT, PT, SI, ...)
- Regions / clusters: 9
- RTO/Universities: 72
- SMEs: 61 (+1)

ECISO coordination on cybersecurity activities in Europe (R&I and market issues) with the different main EU actors



- **Dialogue with EU Institutions:** EP (MEPs and Committees), Council of the EU, EC (DG CNECT, DG RTD, DG ENER, DG MOVE, DG JRC, DG DIGIT, ...)
- **Cooperation with EU Agencies:** ENISA, EUROPOL, EDA, ESA, EASA, EIT, EIB ... and EEAS
- **Coordination with other PPPs and JUs:** EURobotics (Robotics), ECSEL (embedded electronics), BDVA (Big Data), AIOTI (IoT), EFFRA (Industry 4.0), 5G IA (5G), EUROHPC (HPC), INATBA (blockchain), A.SPIRE (process)
- **Coordination with the 4 Pilots (40% members of ECISO):** CONCORDIA, CYBERSEC4EUROPE, ECHO, SPARTA
- **Cooperation with European sectoral associations:** Finance, Energy, Transport, Telecom, Health, Defence & Space, Manufacturing
- **Cooperation with National Bodies:** national public admin (NAPAC representatives), national cybersecurity associations, ...
- **Coordination / cooperation with International Bodies:** UN (ITU), WEF, OSCE, signed MoU with CEN/CENELEC and ETSI ...
- **Dialogue with non-EU public administrations and private sector:** Japan (METI, MoI, ...), US (DHS, CISA)

ECSO Working Groups – cybersecurity 360°

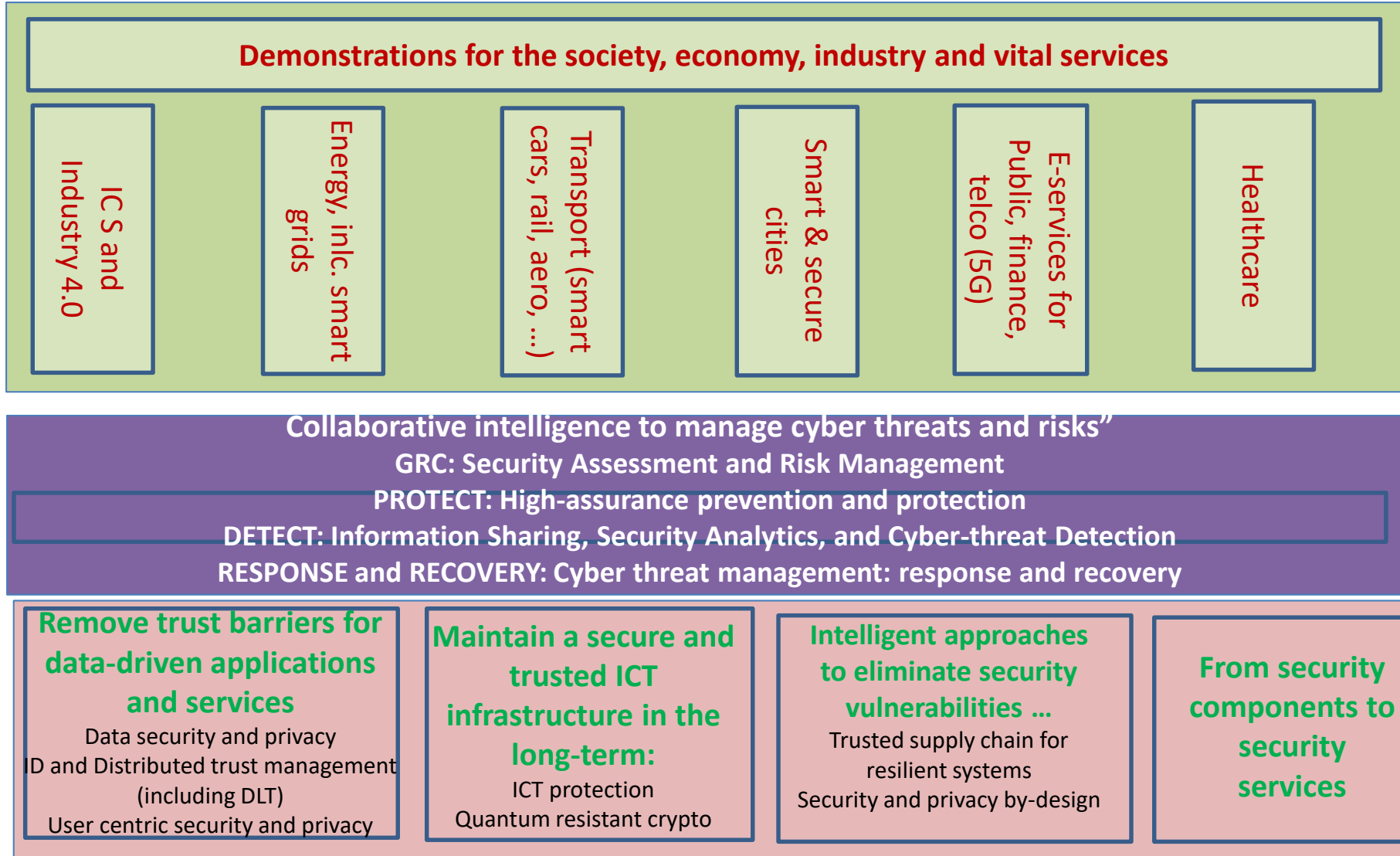


From policy suggestions to concrete achievements

- ✓ **WG1 - Certification & Standardisation:** Input for the EU Certification Framework (meta-scheme methodology) and the Cybersecurity Act legislation; State of the art Syllabus and industry needs for certification and standardisation; Security assessment and priorities for certification
- ✓ **WG2 – Market, Investments and International cooperation:** Cybersecurity market analysis; Taxonomy and Radar (identification of competences / products); Towards a EU Cybersecurity Investment Fund; International cooperation (e.g. Japan)
- ✓ **WG3 – Vertical sectors:** Identification of needs for the different vertical sectors (Industry 4.0, Energy, Financial, Public Services / eGov, Health, Transportation, Smart cities, Telecom – media & content); Trusted exchange of cyber threats among users
- ✓ **WG4 - Support to SMEs and Regions:** ECSO SME Hub – Registry and EU Cybersecurity Label; SMEs / Investors matchmaking; Network of Regions and their competence centres for smart cooperation in cybersecurity - European Cyber Valleys Project and inter-regional acceleration programme (services for SMEs)
- ✓ **WG5 – Education, Training, Awareness and Cyber Ranges:** EHR4CYBER: sharing of best practices for skills development and job creation); Women4Cyber for gender balance; Youth4Cyber (under development) for cyber-hygiene and carrier; Support to Cyber Ranges federation
- ✓ **WG6 - R&I priorities and innovative technologies:** SRIA (Strategic Research and Innovation Agenda) for H2020 priorities; Horizon Europe and DEP priorities; Support to coordination of cybersecurity activities across cPPPs, CCN Pilots and other EU Initiatives; Analysis of cyber security synergies for dual use
- ✓ **cPPP Monitoring:** delivering investment in the SRIA perimeter satisfying cPPP commitments (already above financial objectives)

Main thematic priority areas - WG6

Education and training (Cyber Ranges)



Certification, standardisation, Market, SMEs support, Go To



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

www.ecs-org.eu

E-mail:
Dr. Fabio Martinelli
Fabio.Martinelli@iit.cnr.it

Follow us
Twitter: [@ecso_eu](https://twitter.com/ecso_eu)