TABLE OF CONTENTS

PAGE 3. INTRODUCTORY MESSAGE
What is the cybersecurity Public Private Partnership (cPPP)?
ECSO background and objectives.

PAGE 5. ECSO ACTIVITIES
Events
Collaboration with the European Commission and other bodies.

PAGE 9. AN ASSOCIATION WITH A UNIQUE GOVERNANCE
ECSO Governance
The cPPP Governance
The role of public administrations: a PPP within a PPP

PAGE 12. ECSO MEMBERS
Membership benefits
Membership categories

PAGE 15. HOW TO JOIN ECSO?

PAGE 15. CONTACT US!
INTRODUCTORY MESSAGE

What is the Public-Private Partnership on cybersecurity (cPPP)?

In view of delivering the objectives set in the EU cybersecurity strategy and the Digital Single Market strategy, the European Commission (EC) announced, in its Communication of 5 July 2016, the launch of a public-private partnership on cybersecurity and additional market-oriented policy measures to boost industrial capabilities in Europe.

The aim of the partnership is to foster cooperation between public and private actors at early stages of the research and innovation process to allow people in Europe to access innovative and trustworthy European solutions (ICT products, services and software), taking into consideration fundamental rights, such as the right to privacy.

The partnership also aims to stimulate the cybersecurity industry’s competitiveness and consolidate the market, by helping align the demand and supply and allow industry to elicit future requirements from end-users and different market sectors that are important customers of cybersecurity solutions (e.g. energy, health, transport, finance).

The European Commission invests up to €450 million in this partnership, under its research and innovation programme Horizon 2020. In return the private sector is expected to triple its investment over the next years.

The cPPP is instrumental in structuring and coordinating digital security industrial resources in Europe.
ECSO asbl was established in June 2016 under the Belgian law. It represents the contractual counterpart to the European Commission for the implementation of the cPPP and acts as a pan-European umbrella organisation for a wide variety of sectors and stakeholders (i.e. large companies, SMEs and start-ups, research centres, universities, users, operators, clusters, regions and associations as well as National public administrations. ECSO members originate from EU Member States, countries from the European Economic Area (EEA), the European Free Trade Association (EFTA), and H2020 associated countries.

ECSO’s objectives are to reach the goals set out by the contractual partnership linked to R&I, monitor its implementation in collaboration with the European Commission and support the development of industrial measures/regulations geared towards increasing the competitiveness of the cybersecurity industry in Europe and harmonise the cybersecurity market.
ECSO ACTIVITIES

ECSO is regularly solicited by the European Commission to provide recommendations on specific political and/or technical issues regarding European industrial measures on cybersecurity.

1. Working Groups

To achieve its objectives and structure its work, ECSO has set up several working groups (WG) and respective sub-working groups (SWG) addressing different industrial and R&I aspects.

These working groups are composed and chaired by ECSO members.

STANDARDISATION, CERTIFICATION, LABELLING AND SUPPLY CHAIN MANAGEMENT

Mission and objectives
• EU ICT security certification framework (contribute to the European Commission’s proposed framework)
• Work on certification schemes for specific sectors
• Provide recommendations regarding standards for interoperability
• Propose an EU cybersecurity labelling scheme
• Contribute to testing and validation of the supply / value chain in Europe

Segmentation
• SWG1.1: Products /Components Providers
• SWG1.2: ICT Infrastructure Operators
• SWG1.3: Services Providers/Integrators
• SWG1.4: Basic layer (providing background research and support to the other SWGs)

Collaborations / Partnerships
CEN/CENELEC; ETSI; ENISA; ISO; Multi Stakeholders Platform on Standardisation (DG GROW); national standardisation bodies etc.

MARKET DEPLOYMENT, INVESTMENTS AND INTERNATIONAL COLLABORATION

Mission and objectives
• Develop and maintain a view on the Cybersecurity Industry in Europe as a whole: support ECSO members to improve their market knowledge (products, suppliers, but also cybersecurity insurance solutions):
• Design and facilitate innovative private and public investment capabilities: facilitate to understand the dynamics of the market and create a community of investors, brokers and supporting industries.
• Support international trade: establish dialogue with main trade partners (US, China, Brazil and Japan) and initiating dialogue with developing countries

Segmentation
• SWG 2.1 Market knowledge
• SWG 2.2 Investments and innovative business model activities
• SWG 2.3 International cooperation/ international trade: establish dialogue with main trade partners (US, China, Brazil and Japan) and initiating dialogue with developing countries.
**Mission and objectives**
- Understand users’ needs and suppliers’ available solutions/services/technologies for the different verticals
- Demonstrate use of innovative cybersecurity solutions in the different verticals
- Develop the EU ICT security market and employment
- Improve digital trust and facilitate information exchange
- Improve risk management with better metrics
- Support the use of innovative trusted cybersecurity solutions and services for major societal and economic challenges in Europe
- Support the widest and best market uptake of innovative cybersecurity technologies and services by accelerating the development and wide diffusion of cybersecurity technologies in different industry sectors and creating new business opportunities
- Contribute to a set of industrial policy activities such as defining the needs of sectors for standardisation/certification, research, innovation, education, training and exercises, and local/ regional impact.

**Segmentation**
- SWG3.1: Industry 4.0 and ICS
- SWG3.2: Energy (oil, gas, electricity), and Smart Grids
- SWG3.3: Transportation (road, rail, air, sea, space)
- SWG3.4: Financial Services, ePayments and Insurance
- SWG3.5: Public Services, eGovernment, Digital Citizenship
- SWG3.6: Healthcare
- SWG3.7: Smart Cities and Smart Buildings (convergence of digital services for Citizens) and other Utilities
- SWG3.8: Telecom, Media and Content

**Support to SMEs, coordination with countries (in particular East & Central EU) and regions**

**Mission and objectives**
- Support to the development of SMEs, start-ups and high growth companies
- Develop coordinated activities between clusters (both business oriented and triple helix), Regions and local bodies (for local implementation of solutions/education)
- Development of East EU public and private sectors dealing with cybersecurity

**Segmentation**
- SWG4.1: SMEs, start-ups and high growth companies
  - Venture Capitalists and private investors
  - Public funding opportunities for SMEs
  - Labelling and market analysis
- SWG4.2: Coordination with activities in EU countries and regions
- SWG4.3: Support to East EU Members
EDUCATION, TRAINING, AWARENESS, CYBER RANGES

Mission and objectives
• Increase education and skills on cybersecurity products and safe use of IT tools in Member States for citizens’ individuals and professionals.
• Cybersecurity training and exercise ecosystem leveraging upon cyber range environments
• Awareness-raising and basic-hygiene skills

Segmentation
• SWG5.1: Cyber Range environments and technical exercises
• SWG5.2: Education and professional training
• SWG5.3: Awareness
• Task Force called “EHR4CYBER”: discuss and work on a benchmarking system, foster collaboration through the exchange of best practices, look towards harmonisation of education and training procedures across Europe, develop and harmonise certification for diploma and specialties, as well as foster the recruitment process of cybersecurity specialists.

Collaborations / Partnerships
School of the Future; ENISA; Digital Skills Coalition, etc.

STRATEGIC RESEARCH AND INNOVATION AGENDA (SRIA)

Mission and objectives
• Coordination of results and expectations from European Commission R&I projects
• Coordination of cybersecurity activities across cPPPs and EU initiatives
• Support cPPP implementation and H2020 cybersecurity projects
• Detailed suggestions for the Work Programme 2017 - 2020 using an updated and focused SRIA
• Input to the preparation of the next Framework Programme (FP9) in collaboration with the European Commission

Segmentation
• SWG6.1: Ecosystem
• SWG6.2: Application domains
• SWG6.3: Transversal infrastructures
• SWG6.4: Basic technologies

Collaborations / Partnerships
Other PPPs (Robotics, Factories of the Future, Big Data, 5G, etc); EDA; Programme Committees for LEIT ICT and Secure Societies; IDEAL-IST; SEREN 3; etc.
Working groups do not work in silos. They coordinate their work through meetings, conference calls and at the Coordination & Strategy Committee level.

**ECSO members are invited to contribute to the working groups of their choice and may become chair of a working group or sub-working group.**

2. **Events**

Since its creation, the ECSO Secretariat is regularly solicited to sponsor high-level events throughout Europe and beyond (CYBERSEC, CYBERTECH Israel and Rome, FIC, etc.). ECSO members are often invited to speak at events to present ECSO and engage with new stakeholders. ECSO will organise an annual European Cybersecurity Council gathering the CEOs of ECSO members, high-level EU institution representatives and national public authority representatives.

3. **Collaboration with the European Commission and other bodies**

ECSO has regular operational meetings / workshops with various Directorate Generals and Agencies of the European Commission (DG CNCT, DG ENERGY, DG MOVE, DG REGIO, DG GROWTH, ENISA, EDA etc.), other bodies such as CEN/CENELEC, ETSI, etc. and European Public-Private Partnerships including 5G, Factories of the Future, Big Data, Robotics, etc. to align our frameworks and strategies.
AN ASSOCIATION WITH A UNIQUE GOVERNANCE

European Cybersecurity Council
(High Level Advisory Group: EC, MEP, MS, CEOs, ...)

ECS cPP Partnership Board
(Monitoring of the ECS cPP - R&I priorities)

ECSO - Association Board of Directors
(Management of the ECSO Association - Policy / market actions)

EUROPEAN COMMISSION

INDUSTRIAL POLICY

Coordination / Strategy Committee

Scientific & Technology Committee

RESEARCH & INNOVATION

NAPAC: National Public Authority Representative Committee

ECSO - Working Groups / Task Forces

ECSO - Members

ECSO - General Assembly

(The full list of members of the Board of Directors and Partnership Board is available on the ECSO website)
The management body of the Association is the Board of Directors, elected by the Annual General Assembly according to specific rules described in the ECSO bylaws. The ECSO Board of Directors steers the cybersecurity industrial policy issues and manages ECSO. The Board is supported by the Coordination & Strategy Committee which coordinates the activities of the different Working Groups. The Scientific & Technology Committee, as part of the Coordination & Strategy Committee, coordinates the Working Group activities linked to the SRIA. The Working Groups are composed of ECSO members and tackle priority issues, as defined by the ECSO Board of Directors.

The cPPP governance

The Partnership Board is the formal communication channel between the European Commission and the ECSO Association to discuss the Horizon 2020 Cybersecurity cPPP Work Programme, the implementation of the overall R&I programme related topics and the monitoring of the cPPP commitments (Key Performance Indicators). It allows for an open dialogue between the members to reach the objectives foreseen by the contractual arrangement between the European Commission and ECSO. It provides oversight such as monitoring, advice, community support etc. The Partnership Board is composed of representatives from the European Commission and ECSO Members (with the exclusion of public administration representatives).
National Public Authorities can become full members of ECSO and directly engage with private actors around key strategic and operational issues. The Association has created a specific body called the National Public Authority Representative Committee (NAPAC) which is part of the ECSO governance system and replaces the traditional “mirror groups” that exist in other PPPs. This Committee advises the Board of Directors, the Strategy Committee and each WG when elaborating their mandate and setting their objectives, and provides a position on the final draft of a strategic deliverable.

To better structure its work, the NAPAC is segmented as follows:
• NAPAC Governmental Advisory Group (GAG)
• NAPAC R&I

In ECSO, Public Authorities are strongly encouraged to:
• Participate in the discussions and activities of the ECSO Working Groups to bring a governmental perspective and operational needs from the public administrations;
• Support the definition and implementation of the ECSO Strategic Research and Innovation Agenda and of the ECSO Multiannual Roadmap into the R&I Work Programme;
• Exchange best practices and promote cybersecurity and national / regional research programmes.

Public Authorities’ contributions to the work of ECSO bring considerable advantages in positioning our recommendations to EU Institutions.

Regular Meetings
• 4 working group meetings a year (this can vary from one working group to another). Phone conferences for coordination and exchange of views are also frequent between WG meetings.
• 4 Board of Directors meetings a year
• 2 Partnership Boards meetings a year
• 1 General Assembly meeting a year (usually end June)
ECSO MEMBERS

As of January 2018, ECSO counts 228 Members across 28 countries categorised as followed:

- 22 Associations
- 72 Large companies and users
- 16 Public Administrations 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, …)
- 5 Regional clusters
- 56 RTO/Universities
- 57 SMEs

The list of all ECSO members is available on our website and is regularly updated throughout the year.

Membership benefits

You are
A **USER** of cybersecurity solutions
An **OPERATOR** of Critical Infrastructure
A provider of cybersecurity solution - **SME** or a **LARGE COMPANY**
A University or an **RTO**
A National or European **ASSOCIATION**
A National **PUBLIC ADMINISTRATION**
A **REGION** or national **CLUSTER**

Join a unique pan-European Cyber Security Organisation and …
... have your say on

**CYBER SOLUTIONS AND APPLICATIONS:** Increase the use of trusted cybersecurity solutions in the different applications, implementing Europe-wide strategic projects for specific deployments of existing or near-to-market technologies that demonstrate the potential impact of cybersecurity products across sectors (transport, energy, finance, e-gov, e-health, industry 4.0, etc.).

**RESEARCH AND INNOVATION:** Contribute, at the highest level, to the definition of the next European H2020 calls through the Strategic Research and Innovation Agenda.

**STANDARDS:** Collaborate with other ECSO members, the European Commission, other PPPs and European / national standardisation bodies to improve interoperability of products and systems.

**USE OF FUNDS FOR DEPLOYMENT AND USE OF SOLUTIONS AND SERVICES:** Bring innovative results to market via the systematic use of the full set of available funding tools (at European and national level; public and private).

**EMPLOYMENT:** Develop the cybersecurity job market, Help improve e-skills through trainings, awareness campaigns.

But also...

**LINK TO EU POLICIES:** Coordinate work with the future activities envisaged by the European Commission, as well as the activities of relevant networks (ERNCIP, ISACs, etc.), bodies (ETSI, CEN/CENELEC, etc.), European agencies (ENISA, EDA, etc.), other Public-Private Partnerships (5G, Factories of the Future, Robotics, Big Data, etc.) and European Joint Undertakings.

**BOOST YOUR NETWORK** by engaging with other ECSO Members and public stakeholders from all sectors and countries.

**VOICE YOUR CHALLENGES** and push your ideas forward at a European level.

**ACCESS 1ST HAND INFORMATION** on future legislations, business opportunities and funds.

**ACCESS TO COMPETITIVE H2020 CONSORTIA** and pitch your ideas.

Let’s build together the future of European cybersecurity.
Membership Categories

Large companies - Suppliers and/or users of cybersecurity solutions and services.
National and European Organisations - Associations gathering large companies and SMEs
SMEs or Associations only composed by SMEs, Start-ups, Incubators, Accelerators
Users / Operators
Public Administrations at regional or local levels and clusters
Public Administrations at national level - Official representatives of public administrations
Research Centres, Academia & Universities
Others - Financing bodies, insurance companies, consultancies, etc.

As a member of ECSO and its General Assembly, each organisation / entity will be expected to pay an annual financial contribution – the amount of which will be dependent on its turnover, budget or GDP membership category (see Membership application form available on our website).
HOW TO JOIN ECSO

To be eligible for full membership in ECSO and its General Assembly, the entity should be:

1. Legally established in an “ECSO Country”.*
2. A public body from an “ECSO Country”.

“ Provisional membership” could be provided soon after your membership request has been sent to the ECSO Secretariat. In this case, you’ll be allowed to participate to all ECSO activities (Working Groups, events, etc.) without voting rights and the possibility of being elected, until full membership is formally approved by the ECSO Board of Directors.

ECSO Statutes, ECSO Bylaws and membership application form are available on our website.
* EU Member State, H2020 associated country or an EEA/EFTA country.

CONTACT US!

Follow us on Twitter & visit our website!

@ecso_eu  www.ecs-org.eu