EUROPEAN CYBER SECURITY ORGANISATION

# CYBERSECURITY CONTRACTUAL PUBLIC-PRIVATE PARTNERSHIP

*Nina Olesen*
*Policy Manager*
*ECSO*

# CONTENT



- **Cybersecurity contractual Public-Private Partnership**
  - About the cPPP
  - Industry Proposal
  - KPIs
  - Strategic Research & Innovation Agenda

- **European Cyber Security Organisation (ECSO)**
  - ECSO Membership
  - ECSO Members
  - A unique PPP Association
  - Governance
  - Working Groups and Task Forces

# ABOUT THE CYBER cPPP



**BACKGROUND**

In order to deliver the EU cybersecurity strategy (2013) and the Digital Single Market strategy (2015), in its Communication of 5 July 2016 the European Commission announced the creation of a contractual public-private partnership (cPPP) on cybersecurity and the launch of additional market-oriented policy measures to boost industrial capabilities in Europe.

As part of the EU cybersecurity strategy, the European Commission and the European Cyber Security Organisation (ECSO) signed a cPPP on 5 July 2016.

**AIM**

1. Foster cooperation between public and private actors
2. Stimulate cybersecurity industry,
3. Coordinate digital security industrial resources in Europe.

# ABOUT THE CYBER cPPP



**BUDGET**

The EC will invest up to €450 million in this partnership, under its R&I programme H2020 for the 2017-2020 calls. Cybersecurity market players are expected to invest 3 times more (€ 1350 mln) in the next 10 years.

**A DIFFERENT PPP LINKING RESEARCH AND INDUSTRIAL POLICY**

The cPPP will focus on R&I, developing a SRIA and supporting its implementation in the H2020 Work Programme

The ECSO Association will tackle other industry policy aspects for the market and the industrial / economic development
ECSO will support the development of the European cybersecurity industry and EU trusted solutions, including cooperation with Third Countries.

**REFERENCE DOCUMENTS**

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

# INDUSTRY PROPOSAL



## Identifies industrial long term vision and objectives

Main strategic objectives for an industry-led European Cybersecurity cPPP

- The protection from cyber threats of the growth of the European Digital Single Market
- The creation of a strong European-based offering and an equal level playing field to meet the needs of the emerging digital market with trustworthy and privacy aware solutions
- The growth and the presence of European cybersecurity industry in the global market

# KEY PERFORMANCE INDICATORS (KPIs)



1. **Industrial Competitiveness**

2. **Socio-Economic Security**

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

# KPIs

## Industrial Competitiveness



### KPI 1: MARKET DEVELOPMENT

Evolution of cybersecurity revenues in the European and global market, including positioning and market share of the EU industry

### KPI 2: STANDARDS, TESTING, CERTIFICATION AND TRUST LABELLING

Contribution to standards, use of testing, validation, certification infrastructures as well as EU trust labelling procedures, best practices and pilots for innovative elements of the supply chain

### KPI 3: USERS AND APPLICATIONS

Increased use of cybersecurity solutions in the different markets / applications

### KPI 4: PRODUCTS and SERVICES SUPPLY CHAIN

Development of the EU cybersecurity industry and of the European digital autonomy.

### KPI 5: SMEs

Support the creation and development of start-ups having products / services that effectively reach the market.

## Socio-Economic Security



### KPI 6: EMPLOYMENT

Develop employment in cybersecurity sectors (supply and users / operators)

### KPI 7: ECOSYSTEM: EDUCATION, TRAINING, EXERCISES

Development of education, training and skills on cybersecurity products and safe use of IT tools in European countries for citizens and professionals

### KPI 8: PRIVACY & SECURITY BY DESIGN

Development and implementation of European approaches for cybersecurity, trust and privacy by design

### KPI 9: DATA / INFORMATION EXCHANGE & RISK MANAGEMENT

Facilitate process for information sharing between MS, CERTs and Users to increase monitoring and advising on threats; better understanding risk management and metrics

### KPI 10: IMPLEMENTATION OF LEGISLATIONS

Implementation of the NIS Directive and market driving Regulations / Guidelines

# KPIs

## Implementation and operational aspects of the cPPP



**KPI 11: INVESTMENTS**

Investments (R&I, capability, competence and capacity building) in the cybersecurity sectors defined by the cPPP objectives and strategy

**KPI 12: cPPP MONITORING**

Efficiency, openness and transparency of the PPP Consultation Process

**KPI 13: COORDINATION WITH THE EU and THIRD COUNTRIES**

Coordination of the cPPP implementation with EU Member States, Regions and Third Countries

**KPI 14: DISSEMINATION & AWARENESS**

Dissemination and Awareness making the cPPP action and results visible in Europe and internationally, to a broad range of public and private stakeholders

# STRATEGIC R&I AGENDA – SRIA



The SRIA defines the priorities for research, and innovation for European cybersecurity industry in upcoming years.

EMPHASIS IS ON

1. **Transform innovation and applications into new business opportunities** that help to solve the challenges that Europe (and others) are facing.

2. **Bring growth to cybersecurity industry** by creating new technical solutions and services and support their deployment to both European internal market as well as others.

# STRATEGIC R&I AGENDA – SRIA



## Proposed mechanism for SRIA implementation

1. **Ecosystem:** socio-technical projects for the development of an ecosystems favourable to better implement and use innovative solutions and protect applications
2. **Vertical Application Domains**: 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
3. **Transversal Infrastructures**: projects able to integrate sector-neutral technological building blocks with maximum replication potential, to tackle transversal challenges (common to different applications)
4. **Basic Technologies**: mainly devoted to build those sector-neutral technological building blocks with maximum replication potential that can become market references at global level

# ECSO MEMBERSHIP



## Membership criteria

1. Legal Entity established at least in an EU Member State, H2020 associated country or an EEA / EFTA country
2. A public body from an ECSO Country.

## Categories of members

1. **Large companies** : cybersecurity solutions / services providers;
2. **National and European Organisation / Associations** (gathering large companies and SMEs) representing interests at national or European / International level.
3. **SMEs** solutions / services providers directly represented; Associations composed only by SME, Startups, Incubators, Accelerators.
4. **Users / Operators** (where cybersecurity technology / solutions / services provision is not one their business activities): National public administrations or private companies (large or SMEs) directly represented.
5. **Regional / Local public administrations** (with economic interests); Regional / Local Clusters of public / private Legal Entities with local economic / ecosystem development interests.
6. **Public Administrations at national level** (national strategy / regulatory / policy issues, incl. R&I coordination).
7. **Research Centres, Academies / Universities**; Associations composed only by Research Centers, Academies or Universities.
8. **Others** (financing bodies, insurances, consultants, etc.).

# ECSO MEMBERS



167 organisations from 27 countries and counting

- Associations : 19
- Large companies: 52
- Public Administrations: 11
- Regional clusters; 2
- RTO/Universities: 43
- SMEs: 34
- Users/Operators (non telecom): 6

11 public authorities:
UK, ES, IT, FR, DE, SK, EE, FI, NO, CY, PL
More to come soon (BG, NL)

| | | | |
|---|---|---|---|
| AUSTRIA | 5 | ITALY | 28 |
| BELGIUM | 4 | LATVIA | 1 |
| BE - EU ASS | 7 | LUXEMBOURG | 2 |
| CYPRUS | 4 | NORWAY | 4 |
| CZECH REP. | 1 | POLAND | 5 |
| DENMARK | 2 | PORTUGAL | 5 |
| ESTONIA | 4 | ROMANIA | 2 |
| FINLAND | 7 | SLOVAKIA | 2 |
| FRANCE | 19 | SPAIN | 26 |
| GERMANY | 14 | SWEDEN | 1 |
| GREECE | 2 | SWITZERLAND | 2 |
| HUNGARY | 1 | THE NETHERLANDS | 7 |
| IRELAND | 1 | TURKEY | 2 |
| ISRAEL | 1 | UNITED KINGDOM | 7 |

# ECSO : A UNIQUE PPP ASSOCIATION

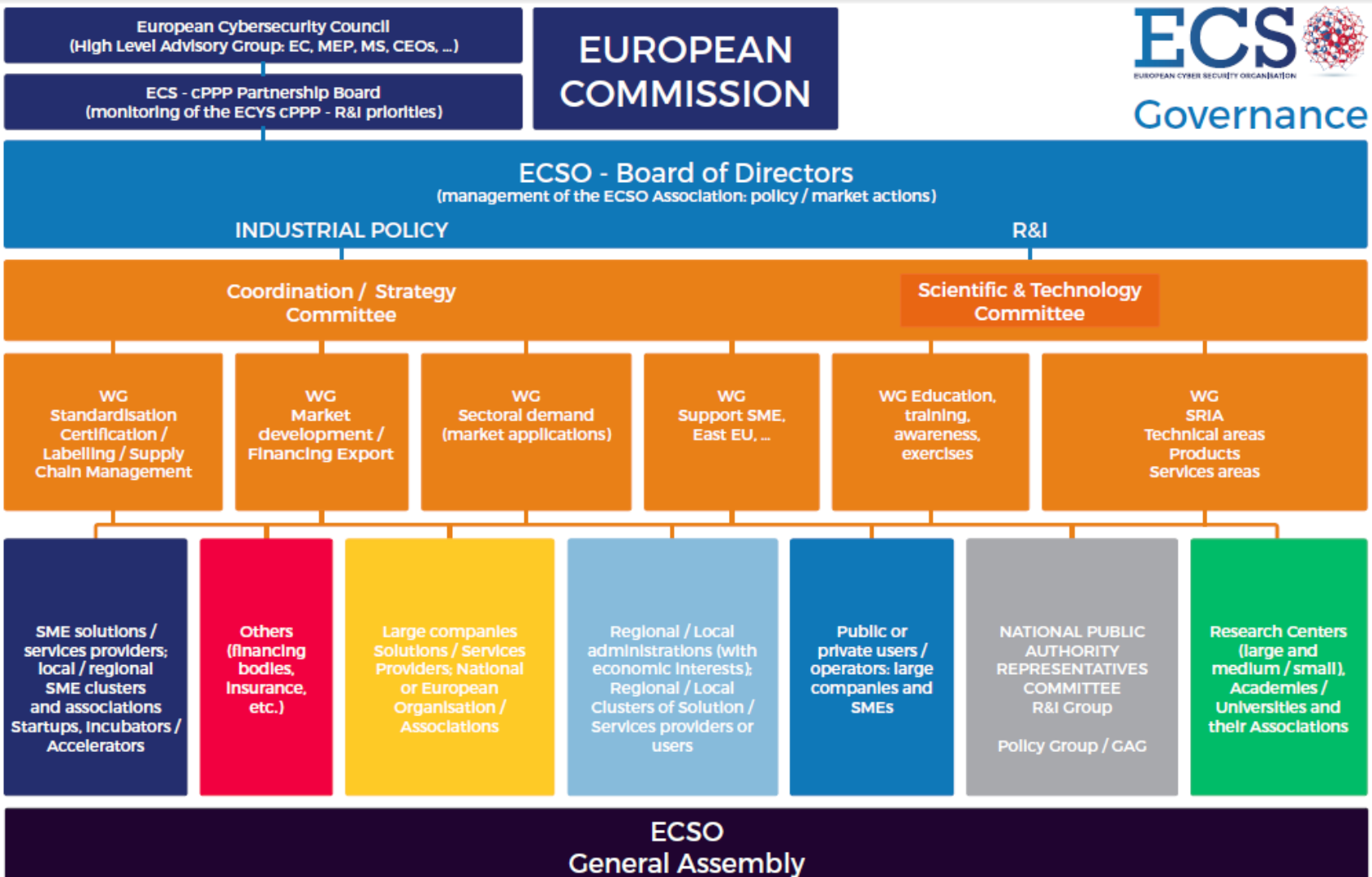


**Security is a national prerogative.**

**NAPAC** : A National Public Authority representatives Committee (NAPAC), instead of traditional “mirror groups”.
This Committee allows Public Administrations to have their own fora of dialogue with their own rules, while remaining in close contact and participating to ECSO activities, including the Board of Directors.

**AIM**

- Participate in Working Groups & Task Forces to bring a governmental perspective and operational needs from the public administrations
- Support the definition and implementation of the SRIA and of the ECSO Multiannual Roadmap into the R&I Work Programme
- Exchange best practice and promote cybersecurity and national / regional research programmes.


European Cybersecurity Council
(High Level Advisory Group: EC, MEP, MS, CEOs, ...)
ECS - cPPP Partnership Board
(monitoring of the ECYS 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
Scientific & Technology Committee
WG Standardisation Certification / Labelling / Supply Chain Management
WG Market development / Financing Export
WG Sectoral demand (market applications)
WG Support SME, East EU, ...
WG Education, training, awareness, exercises
WG 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 / GAG
Research Centers (large and medium / small), Academies / Universities and their Associations
ECSO
General Assembly

# WORKING GROUPS & TASK FORCES



**WG 1**
**Standardisation**
**Certification / Labelling / Supply Chain Management**

**WG 2**
**Market development / Investments**

**WG 3**
**Sectoral demand (vertical market applications)**

**WG 4**
**Support SME, coordination with countries (in particular East EU) and regions**

**WG 5**
**Education, training, awareness, exercises**

**WG 6**
**SRIA**
**Technical areas**
**Products**
**Services areas**

# BENEFITS



1. **You get what you put in**
2. **Networking among ECSO members and across cyber community from local to EU**
3. **Business opportunities / ECSO honest broker**
4. **Direct contribution to the R&I Work Programme**
5. **ECSO: instrument shaped by its members**

# 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
Communication Manager
eda.aygen@ecs-org.eu

Follow us
Twitter: @ecso_eu