ECSO
EUROPEAN CYBER SECURITY ORGANISATION

EU CYBERSECURITY PUBLIC-PRIVATE PARTNERSHIP and ECSO (European Cyber Security Organisation)

ENISA-CEN-CSCG Workshop

19 September 2017

ABOUT THE EUROPEAN CYBERSECURITY PPP

ECS EUROPEAN CYBER SECURITY ORGANISATION

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.

ABOUT ECSO

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

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.

ECSO working groups are dealing with the different aspects of what we call "cybersecurity industrial policy": standardisation and certification; investments (link across public and private funds);international cooperation; needs of the different vertical market sectors; support to SMEs; regional / local aspects; education, training, awareness and cyber ranges; R&I / capability development priorities.

A peculiarity of ECSO is to **include among its members (also at Board of Directors level) 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.

The presence at decision level (Board) and at working level (working groups) of **representatives from public administrations increases the quality of the ECSO recommendations** to the European and national institutions, thanks to a "pre-digested" dialogue and consensus between public and private experts. This will allow 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 - Purpose & objectives

EUROPEAN CYBER SECURITY ORGANISATION

- **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") and a possible "JU-like" structure
  - 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**
  - cPPP evolution into a "Joint Undertaking – like" instrument?
  - European industry among cybersecurity market leaders in targeted sectors
  - Support to business development and global competitiveness

Where we started: « Industry Proposal »

ECS
EUROPEAN CYBER SECURITY ORGANISATION

Identifies industrial cybersecurity challenges in Europe

- Global cybersecurity and ICT market dominated by global suppliers from outside Europe.
- Innovation led by imported ICT products.
- Strategic supply chain dependency.
- Mature commodity market; professional applications under development / evolution (e.g. Digitizing European Industry)
- Market fragmentation.
- Innovation: strong in Europe but not always properly funded due to a lack of a consistent transnational approach and global EU strategy. Results of Research and Innovation are hardly reaching the market.
- Weak entrepreneurial culture, lack of venture capital.
- European industrial policies not yet addressing specific cybersecurity issues.
- Human factor.
- Sovereignty.

Where we started: Objectives

Identifies industrial operational and strategic objectives

1. Protecting infrastructures from cyber threats.
2. Use of massive data collection to increase overall security.
3. Increased European digital autonomy.
4. Security and trust of the whole supply chain.
5. Investments in areas where Europe has a clear leadership.
6. Leveraging upon the potential of SMEs.
7. Support local competence and development.
8. Increase competitiveness.

One year after: Update of the analysis of the situation

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

One year after the preparation of the Industry Proposal for the cPPP: Evolutions in the latest months

- Evolution of the awareness on cybersecurity at national and EU level
- Evolution of threats (e.g. Mirai/ IoT; WannaCry, …) and priorities (also political …)
- Evolution in the dialogue between public and private stakeholders thanks to the cPPP / ECSO
- New EU cybersecurity strategy (to come by end 2017), possibly including large UE projects and higher funding (not only for R&I)

Digitalisation of the industry, of infrastructures and of the society: need for increased cybersecurity

- Impact on all levels: societal and economic
- Need for improved control / ownership / security of data in Europe
- Growth of pervasive and distributed IT infrastructure (IoT, 5G, Cloud) needing local and fast reaction capability
- IT Infrastructure for centralised information (e.g. SOC as platform for security services managed by MSSP and CERTs) to increase wider (/global) security and detection / remediation aspects: Big Data Analytics / Artificial Intelligence
- Virtualisation of networks and software defined services (including security)

Update of the vision & strategy of the “Industry Proposal” for the EU Cybersecurity cPPP: PEST ANALYSIS FOR CYBERSECURITY IN EUROPE

EUROPEAN CYBER SECURITY ORGANISATION

- **Political**:
  - **Interferences in democratic processes;**
  - **New EU regulations;**
  - Sovereignty issues at MS level (limited exchange of information and sensitive technologies)
- **Economic**:
  - Low investments wrt US;
  - Market fragmentation;
  - Large presence of SMEs;
  - Difficult market deployment of R&I results
- **Social**:
  - European concepts of Privacy;
  - **Need for education / training / awareness**
- **Technological**:
  - Data kept in Europe / Cloud;
  - Enhanced encryption for increasing privacy and data security;
  - **IoT security;**
  - **Impact of 5G;**
  - **Analytics / AI;**
  - **DLT and use of blockchain in different applications**

ECSO MEMBERSHIP

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

Membership criteria

1. Legal Entity established at least in an "ECSO Country" (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 Centers, Academies / Universities**; Associations composed only by Research Centers, Academies or Universities.
8. **Others** (financing bodies, insurances, consultants, etc.).

BENEFITS for members

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

1. Your input into strategic political and operational documents: proposing / advocating for your own priorities and strategy for R&I, investment, standards / certification, legislations, etc.
2. Close collaboration with EU institutions at all level and national Public authorities
3. Participation in decision making bodies (General Assembly, Association Board, partnership Board, Strategy Committee, Working Groups, Task Forces, etc.)
4. Participation into high-level events / workshops / conferences and representing ECSO at national / EU level
5. Networking with stakeholders from all sectors and countries
6. Direct access to 1st hand information (newsletter, collaboration platform, etc.)
7. Access to competitive R&I consortia via ECSO
8. Better understanding of business opportunities at EU and national level, in particular when linked to EU regulations, directives, norms etc.
9. Better understanding of job needs and availability in this sector: participation in the foreseen EU Network for cybersecurity job creation and education
10. Coordinated support to SMEs to develop their skills and presence in Europe

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 one new request)**

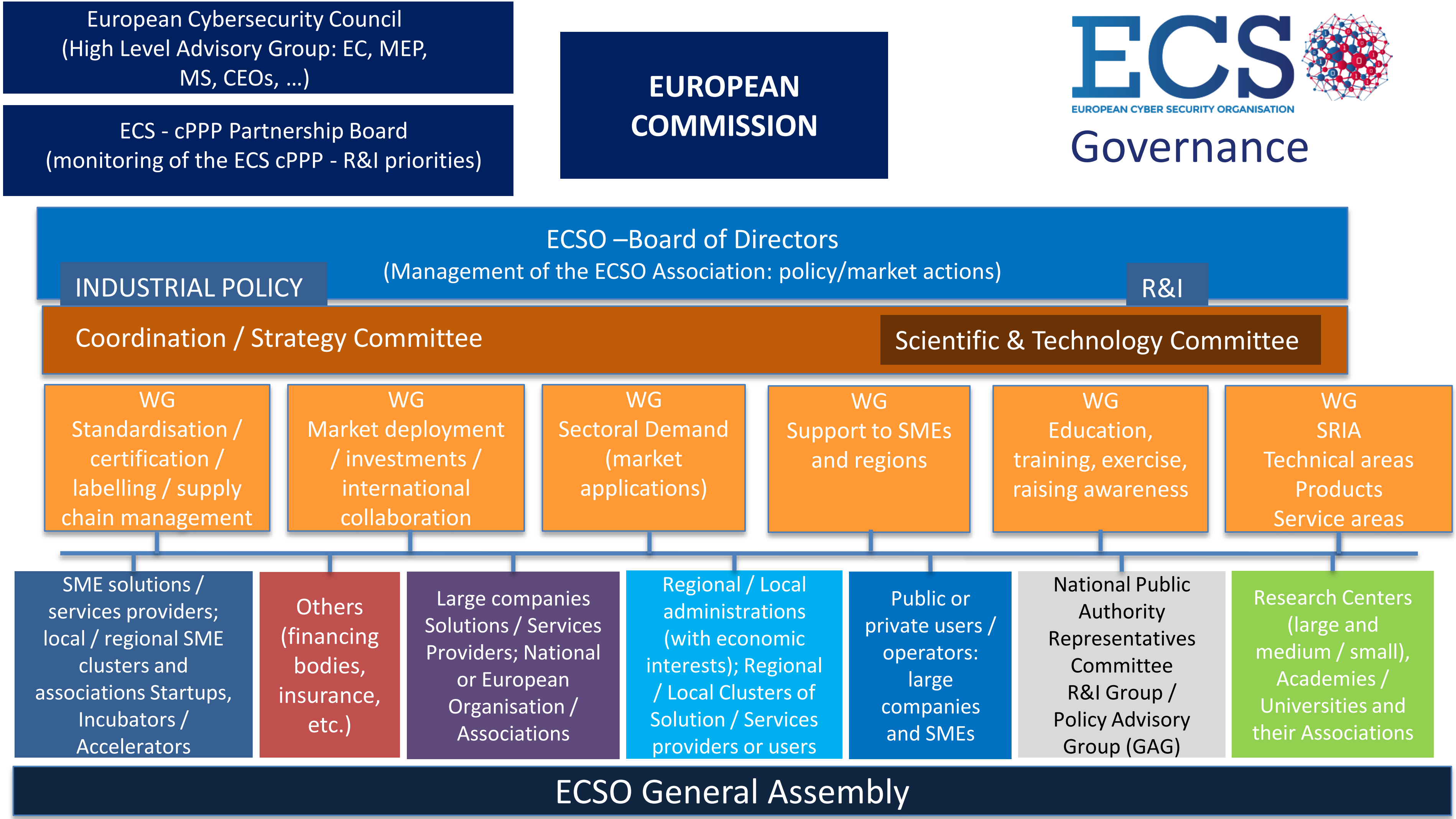
- Associations : 21
- Large companies and users: 70
- Public Administrations: 15
  AT, BE, CY, CZ, DE, EE, ES, FI, FR, IT, SK, FI, NL, NO, PL, UK + observers at NAPAC (BG, DK, HU, IE, LT, LU, LV, PT, RO, SE, SI, MT, …)
- Regional clusters: 3
- RTO/Universities: 55
- SMEs: 54

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		

EUROPEAN CYBER SECURITY ORGANISATION

Governance



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

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

EUROPEAN COMMISSION

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 deployment / investments / international collaboration

WG
Sectoral Demand (market applications)

WG
Support to SMEs and regions

WG
Education, training, exercise, raising awareness

WG
SRIA
Technical areas
Products
Service 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

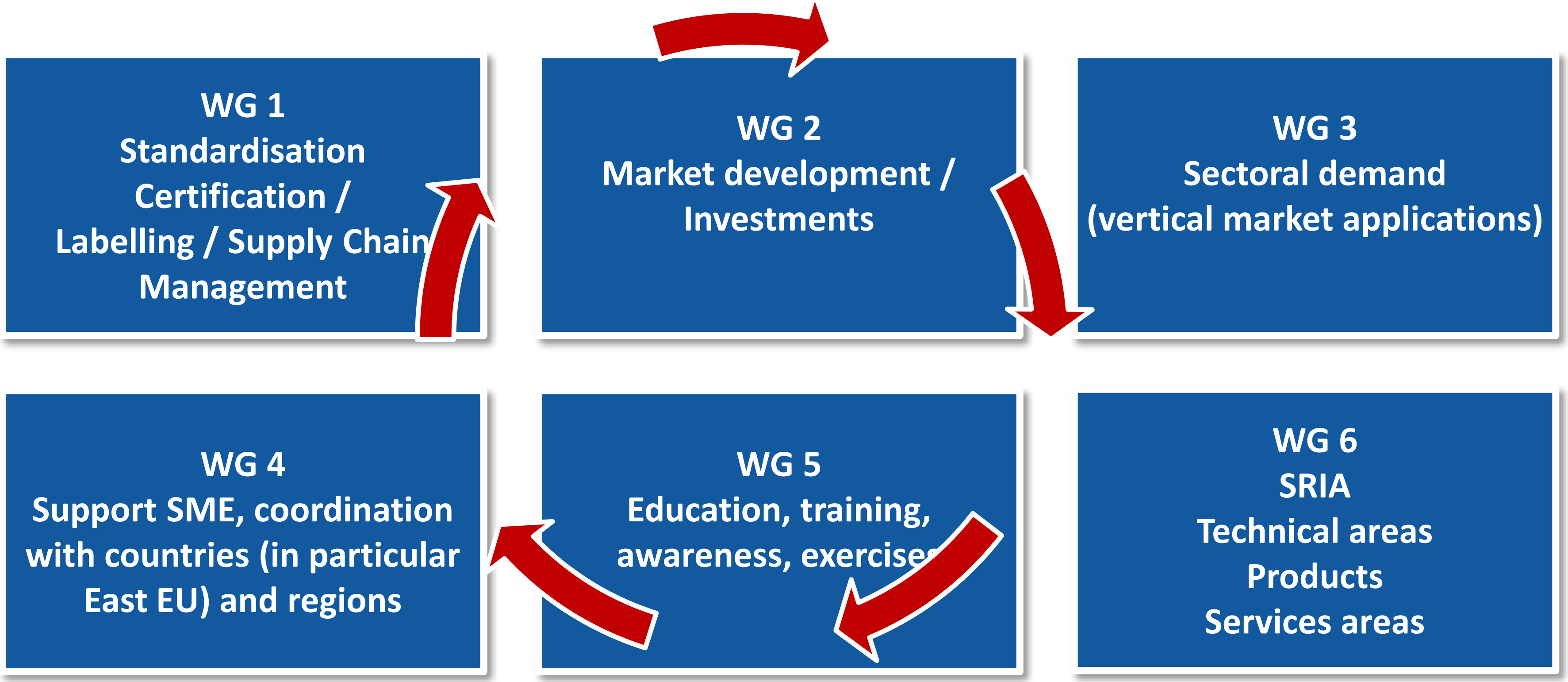
National Public Authority Representatives Committee
R&I Group / Policy Advisory Group (GAG)

Research Centers (large and medium / small), Academies / Universities and their Associations

ECSO General Assembly

WORKING GROUPS & TASK FORCES

ECS
EUROPEAN CYBER SECURITY ORGANISATION



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

Update of WGs activities

ECS
EUROPEAN CYBER SECURITY ORGANISATION

- **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

- **WG2 (market / funds / international cooperation / cPPP monitoring)**

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

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

State of the Art deliverable under definition, 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
Contact: nina.olesen@ecs-org.eu

Update of WGs activities

- **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

- **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)**

Informal suggestions delivered to the European Commission for the 2018 – 2020 H2020 Work Programme: organisation of the priority topics identified by ECSO in the SRIA (good acceptance of suggested priorities). Contacts with other PPPs and similar EU activities to coordinate objectives.
Contact: roberto.cascella@ecs-org.eu

WG1 – Standardisation, certification, labelling & supply chain management : Update

Mission and Objectives

The WG will focus its work around the following topics:

- EU cybersecurity certification framework (liaise with the Commission and contribute to the European cybersecurity certification framework proposal).
- Standards for interoperability
- EU cybersecurity labelling
- Increased digital autonomy
- Testing and validation of the supply / value chain in Europe

Cooperation

CEN/CENELEC (already defined) and ETSI (preparation started)

WG1 – Subworking groups

EUROPEAN CYBER SECURITY ORGANISATION

SWG 1.1. “Manufacturing of Subcomponents, Components, Devices and Products”

- Manufacturing of cyber secure products (from IC components up to cars, aircraft and others that require the integration of several components) including the respective supply-chain during integration of components. Software as a product is also covered by this SWG.

SWG 1.2. “ICT infrastructure providers and other cloud based services”

- Delivering of cyber secure services but with a big effort on the privacy of data handling in Telco or other ICT infrastructure providers, but also cloud -based ones.

SWG 1. 3. “IT Integrators, Critical Infrastructure Operators, End Users and Supply Chain Management”

- Organizations and their IT infrastructure, end users and the organizational and IT infrastructure changes needed to have a market of companies and suppliers able to deliver their services (ICT or non) to citizen in a secure way.

SWG 1.4. “Base Layer”

- Delivering required specific capabilities to other SWGs as advanced research, definition of common terms, structures and procedures.

WG1 – Current activities

EU should further provide **harmonisation** of requirements, certification and standards **to defragment the market**, increase industry competitiveness and enhance security of connected systems and services.

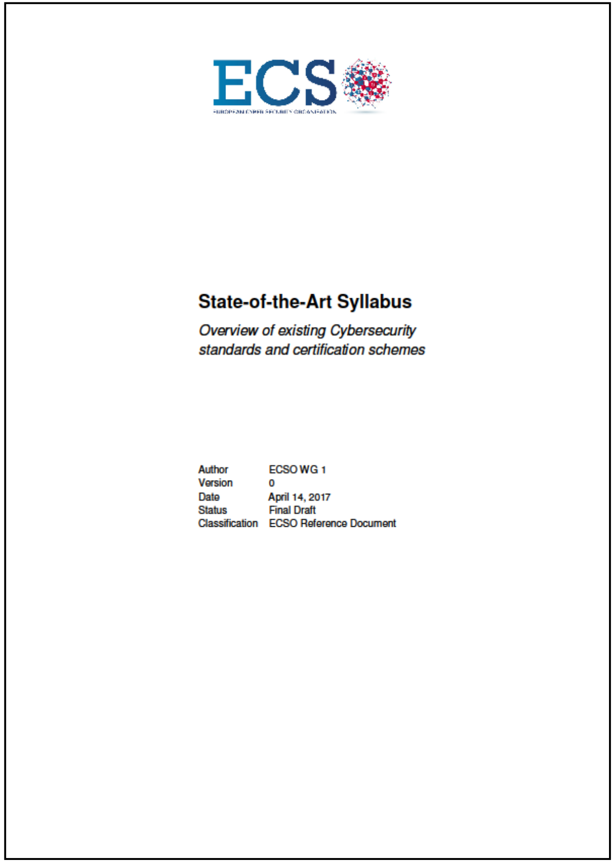
Stage 1

- State_of_the_Art (SOTA) records all available cyber security standards, initiatives and certification schemes to deliver a good understanding of the existing landscape. The purpose is to have a comprehensive way to evaluate what can be used (if existing) to address the challenges expressed in a second document (COTI).
- Challenges_Of_The_Industry (COTI) integrates of all comments received from ECSO members regarding the challenges that the industry is facing so far. The document, is designed to be a compilation of problems, to be used to understand the main driving topics that can be considered as common challenges.

➢ Some of the most frequent topics: Harmonisation; Privacy; Patching & Updating; Connected devices; Time to market; Innovation speed; Trusted products; …

Rising importance of patching and updating as a consequence to latest attacks (e.g. WannaCry)

WG1 – State of the Art (SOTA)



State-of-the-Art Syllabus

Overview of existing Cybersecurity standards and certification schemes

Author	ECSO WG 1
Version	0
Date	April 14, 2017
Status	Final Draft
Classification	ECSO Reference Document

- 178 pages.
- 97 contributions
- 290 standards and certification schemes listed
- Scheduled revision every 6 months, in order to maintain representativeness of the document.

WG1 – Challenges of the Industry (COTI)

MOST FREQUENT TOPICS	
Harmonisation	9
Privacy	9
Patching & Updating	9
Connected devices	6
Time to market	5
Innovation speed	5
Base line	4
Trusted products	4
Brand protection	4

- All inputs have been merged into a single database with all contributions.
- The contributions have been analyzed and additional keywords and data analytics tools, in order to be able to track, in a fast way similar statements and inputs.
- The database (using an excel sheet) will be distributed in an integrated document, in order to be used as the gasp, to be addressed by the meta framework we are tasked to create.
- 292 inputs received from 65 contributors
  - 165 description of solutions
  - 99 challenges to manage
  - 125 criteria's to comply
  - 21 general comments about the process

WG1 – Objectives identified from COTI

- **Threat analysis** and **risk assessment** shall be the **source to determine security requirements** that are used as the basis for security evaluation & certification of items
- The evaluation of the risk should involve the **risk owner** (e.g. user of a product)
- A **minimum required baseline** shall be defined against which items are assessed to significantly reduce the deployment of unsecure items (product, services, infrastructure, …) into the European market
- The **burden for manufacturers w.r.t. to certification**, such as bureaucracy, costs, time to market, shall be **minimized** in the context of its usage while ensuring adequate trust in security claims
- Security evaluation & certification shall confirm the **security strength of items** under evaluation against state-of-the art attacks
- **Regular lean re-assessments** shall be part of the governance procedure to reduce the risk of undiscovered vulnerabilities w.r.t. to new attacks that are found in the field; the frequency and methodology should depend on the application field and type (product, service, …)
- **Patching** shall be considered as a **standard process** in the certification flow (devices are mostly online in future) rather than as an exception (in the past devices where mostly offline) and shall incorporate delta-assessments
- **Fragmentation** of the market **shall be reduced** by means of **harmonization** while **not reinventing the wheel** (maximum re-use of existing schemes)
- **Security by Design** and **Privacy by Design** shall be explicitly taken into account

WG1 – Current activities

Stage 2

- Merging elements from both documents, to understand the gaps and create a first meta-schema model by crossing current challenges (COTI) with existing standards and certification schemes (SOTA) present in the market to:
  - Identify gaps / non-covered challenges
  - Propose new approaches and requirements only if needed: e.g. If a gap is not covered by any standard or best practice

  ➢ Main objective is to rely on existing requirements and standards and bodies (e.g. SOG-IS) – do no reinvent the wheel!
- Consider current mature initiatives in a development or deployment state – e. g. EU 5G initiative, French IoT standardisation working group, etc. – for smooth future compatibility
- Involve relevant End User participation in the verticals
  - Integrate ECSO WG3 vertical needs contributions
  - Consults and surveys via sectorial groups
  - Contact key local / national players
- Coordinate with National Public Administrations: many already members of ECSO and directly participating in WG1 activities or via the NAPAC (ECSO Committee of National Public Administrations)

Elements from the EU Cybersecurity strategy review

EUROPEAN CYBER SECURITY ORGANISATION

BUILDING EU RESILIENCE TO CYBER ATTACKS: Towards a Single Cybersecurity Market

- **EU cybersecurity certification framework:** procedure for the creation of EU-wide cybersecurity certification schemes, covering **products, services and/or systems**, which **adapt the level of assurance to the use involved** (be it critical infrastructures or consumer devices). **Certificate of conformity** to inform and reassure purchasers and users about the security properties of the products and services they buy and use. ICT **products and services** would be formally **evaluated against a defined set of cybersecurity standards**, which could be developed in close connection with the broader ongoing work on ICT standards.
- The **Framework's schemes would be voluntary and would not create any immediate regulatory obligations on vendors or service providers**. Three priority areas:
  - ➢ **Security in critical or high-risk applications**: systems that we depend on in our daily activities, from our cars to the machinery in factories, from the largest of systems such as airplanes or power plants to the smallest such as medical devices. Core ICT components in such products and systems would require rigorous security assessments.
  - ➢ Cybersecurity in **widely-deployed digital products, networks, systems and services used by private and public sector alike to defend against attacks and apply regulatory obligations –** such as email encryption, firewalls and Virtual Private Networks.
  - ➢ **Use of "security by design" methods in low-cost, digital, interconnected mass consumer devices which make up the Internet of Things**

Elements from the EU Cybersecurity strategy review

BUILDING EU RESILIENCE TO CYBER ATTACKS: Towards a Single Cybersecurity Market

- Take particular account of the evolving cybersecurity threat landscape, as well as the importance of essential services such as **transport, energy, health care, banking, financial market infrastructures, drinking water or digital infrastructure.**
- “Security by design" approach could be part of the "**duty of care" principle to be further developed together with the industry**, which could reduce product/software vulnerabilities by applying a range of methods from design to testing and verification, including formal verification where applicable, long term maintenance, and the use of secure development lifecycle processes, as well as developing updates and patches to address previously undiscovered vulnerabilities and fast update and repair.
- At the same time, **specific sectors** face specific issues and should be encouraged to develop their own approach. In this way, **general cybersecurity strategies would be complemented by sector-specific cybersecurity strategies in areas like financial services, energy, transport and health.**
- **Liability**: cybersecurity raises issues around the attribution of damage for businesses and supply chains and failure to address these issues will hamper the development of a strong single market in cybersecurity products and services.
- The effect of foreign acquisitions on critical technologies is a key aspect in the framework for **the screening of foreign direct investment in the European Union**, which aims to enable the screening of investments from third countries on the grounds of security and public order.

ECS
EUROPEAN CYBER SECURITY ORGANISATION

Become member of a unique pan-European cyber security organisation and give your direct contribution to the PPP!

www.ecs-org.eu

- Industry Proposal
- SRIA
- ECSO Statutes
- ECSO Bylaws
- cPPP contract
- ECSO Membership Application Form

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