European Cybersecurity in Public Private Partnership

VIENNA CYBER SECURITY WEEK 2018

Protecting Critical Energy Infrastructure

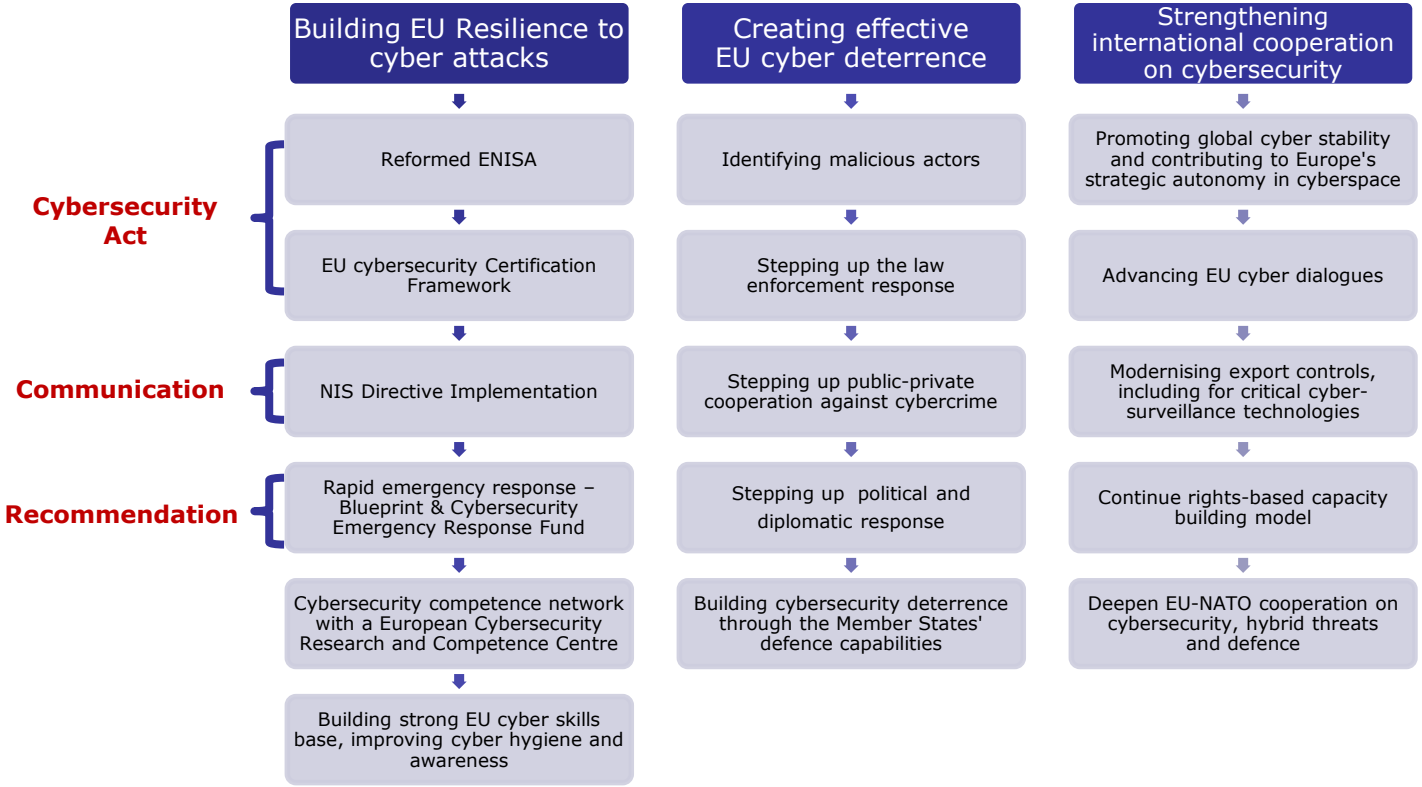
29 January 2018

www.ecs-org.eu

Europe and cybersecurity: now evolving faster. Overview of the context

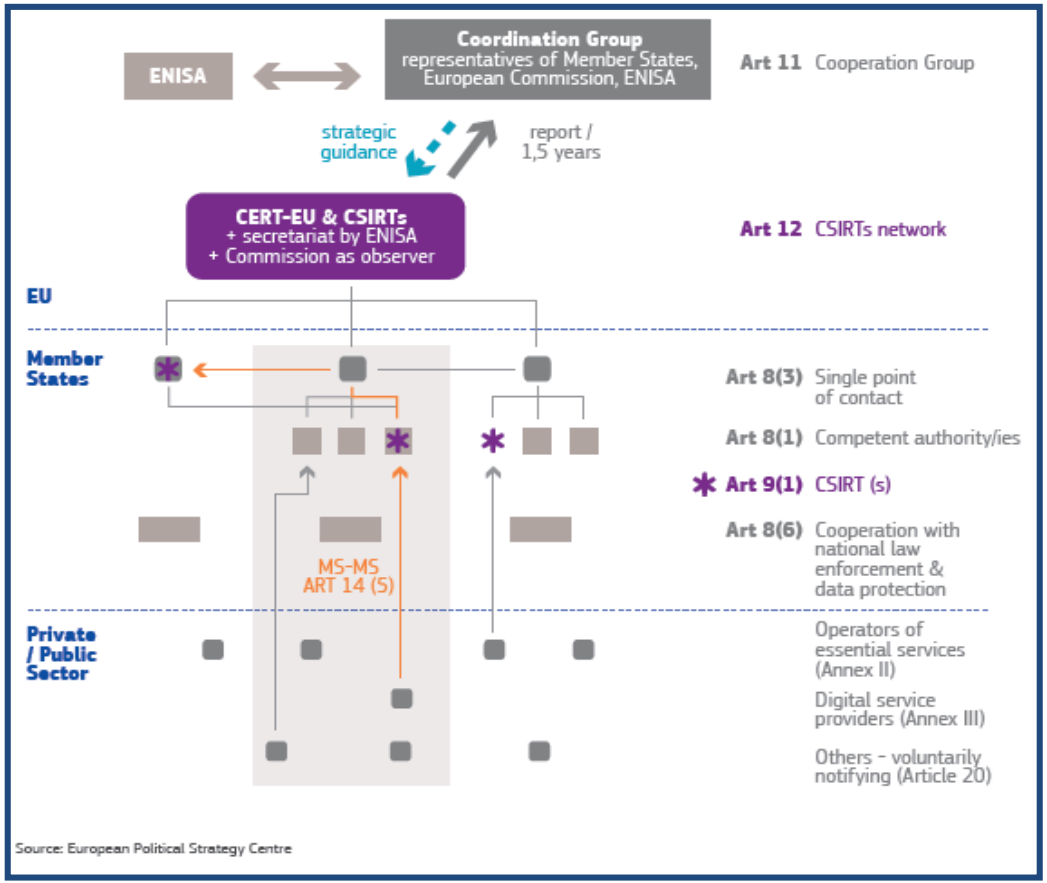
- 2013: EU Cybersecurity Strategy
- 2014: Digital Single Market / Digitalisation
- 2016: cPPP on Cybersecurity
- 2017: Joint Communication on EU strategy Review and Cybersecurity Act (“New” EU Cyber Security Agency: ENISA + EU Certification Framework)
- New technologies: Artificial Intelligence / Big Data Analytics; IoT; High Performance Computing…
- Still large number of Bodies and fragmentation at EU and MS level
- Creation of a Network of Cybersecurity Competence Centres (pilots starting in 2018) with a European Cybersecurity Research and Competence Centre
- EC proposal for the next MFF (2020 – 2026): May 2018
- Transposition of the NIS Directive and application of the GDPR Regulation: May 2018
- Possible evolution of the cPPP (after 2020) towards a more ambitious governance and objectives (e.g. JU)

Building strong cybersecurity for the EU: Resilience, Deterrence and Defence



NIS operating schema

Overview of the multilayer architecture under the NIS Directive



Each **Member State** shall:

- Designate a competent National Authority to manage the NIS;
- Designate a national Computer Security Incident Response Team (CSIRT);
- Define national NIS strategy and a Network Information Security cooperation plan.

ENISA shall:

- Have a key role in coordinating with other CSIRTs.

The **Coordination Group** shall:

- Create, among the Member States, cooperation with information regarding warnings and notifications of potential risks and incidents.

NIS Directive vs the blueprint

Open issues w.r.t. large-scale cybersecurity incidents and crisis

ECS
EUROPEAN CYBER SECURITY ORGANISATION

INFOSHARING	INCIDENT REPORTING	CRISIS MANAGEMENT

The **EU cyber resilience relies upon the three pillars: Infosharing, Incident Reporting and Crisis Management**.

The NIS Directive shall foster the development of the Digital Single Market enabling the coordinated deployment of these tools across sectors and across Member States. Some questions arise from this Directive, namely:

Sectorial vs Cross Industries	***Time constraints and time based cyber fight VS Reporting and escalation multi-layers hierarchy***	***National vs European vs International***

It's time for a collaborative approach, involving private and public institutions, to harmonise information exchange, incident reporting and crisis management procedures.
ECSO and the public-private cooperation will be beneficial to the proper implementation of cross-sectorial regulatory requirements

About the European Cybersecurity 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 up to €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

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.

A peculiarity of ECSO is to include among its members (also at Board of Directors level and within the working groups*) **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.
- **to increase the quality of the ECSO recommendations** to the European and national institutions → allowing 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 working groups are dealing with the different aspects of what we call "cybersecurity industrial policy"**

ECSO - Purpose & objectives

- **Short term**
  - R&I priorities for H2020 (2018-2020 work programme); coordination with other cPPPs
  - EU Certification & Labelling Framework
  - European HR Network (EHR-4CYBER) to foster education and training and support job growth in cybersecurity
  - Increase membership (users & operators), improve operational governance
  - Develop dialogue and harmonisation of objectives
  - Suggestions for the revision of the EU Cybersecurity Strategy and future investments (in the 2020 – 2026 MFF)
- **Medium Term**
  - Prepare for post H2020 ("FP9")
  - Standardisation
  - Regional approach (smart specialisation & regional funds)
  - Support to SMEs (SME Hub / Platform; investments in start-ups; …)
  - Develop with concrete actions, education, training, awareness and cyber ranges
  - Development of trusted components, systems, services strategic for Europe
  - Support to implementation of NIS Directive; GDPR; …
  - Build International dialogue / cooperation
- **Long Term**
  - Possible cPPP evolution into a new governance (e.g. “Joint Undertaking – like”) for competences and capabilities
  - European industry among cybersecurity market leaders in targeted sectors
  - Support to business development and global competitiveness

ECSO membership overview (end of December 2017)

132 founding members: now we are **230 organisations from 28 countries and counting**

AUSTRIA	6	LATVIA	1
BELGIUM	11	LITHUANIA	1
BE - EU ASSOCIATIONS	10	LUXEMBOURG	4
CYPRUS	4	NORWAY	4
CZECH REP.	3	POLAND	7
DENMARK	3	PORTUGAL	5
ESTONIA	7	ROMANIA	1
FINLAND	9	SLOVAKIA	3
FRANCE	23	SPAIN	31
GERMANY	21	SWEDEN	1
GREECE	4	SWITZERLAND	4
HUNGARY	2	THE NETHERLANDS	16
IRELAND	3	TURKEY	3
ISRAEL	2	UNITED KINGDOM	10
ITALY	30	BULGARIA	1

- Associations : 21
- Large companies and users: 71
- Public Administrations: 17 - AT, BE, BG, CY, CZ, DE, EE, ES, FI, FR, IT, SK, FI, NL, NO, PL, UK + observers at NAPAC (DK, HU, IE, LT, LU, LV, PT, RO, SE, SI, MT, …)
- Regional clusters: 6
- RTO/Universities: 56
- SMEs: 58

Austrian Members

- Austrian Institute of Technology GmbH
- JOANNEUM RESEARCH Forschungsgesellschaft mbH
- Kuratorium Sicheres Österreich (KSÖ)
- RadarServices Smart IT-Security GmbH
- SBA Research GmbH
- VÖWG - Verband der öffentlichen Wirtschaft und Gemeinwirtschaft

ECS - cPPP Partnership Board
(monitoring of the ECS 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

WG 1	WG 2	WG 3	WG 4	WG 5	WG 6
Standardisation / certification / labelling / supply chain management	Market deployment / investments / international collaboration	Sectoral Demand (Industry 4.0; Energy; Transport; Finance; eGov; Health; Smart Cities; Telecom/media)	Support to SMEs and REGIONS (in particular East EU)	Education, training, cyber ranges, awareness	Strategic Research & Innovation Agenda Technologies, Products & Services

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

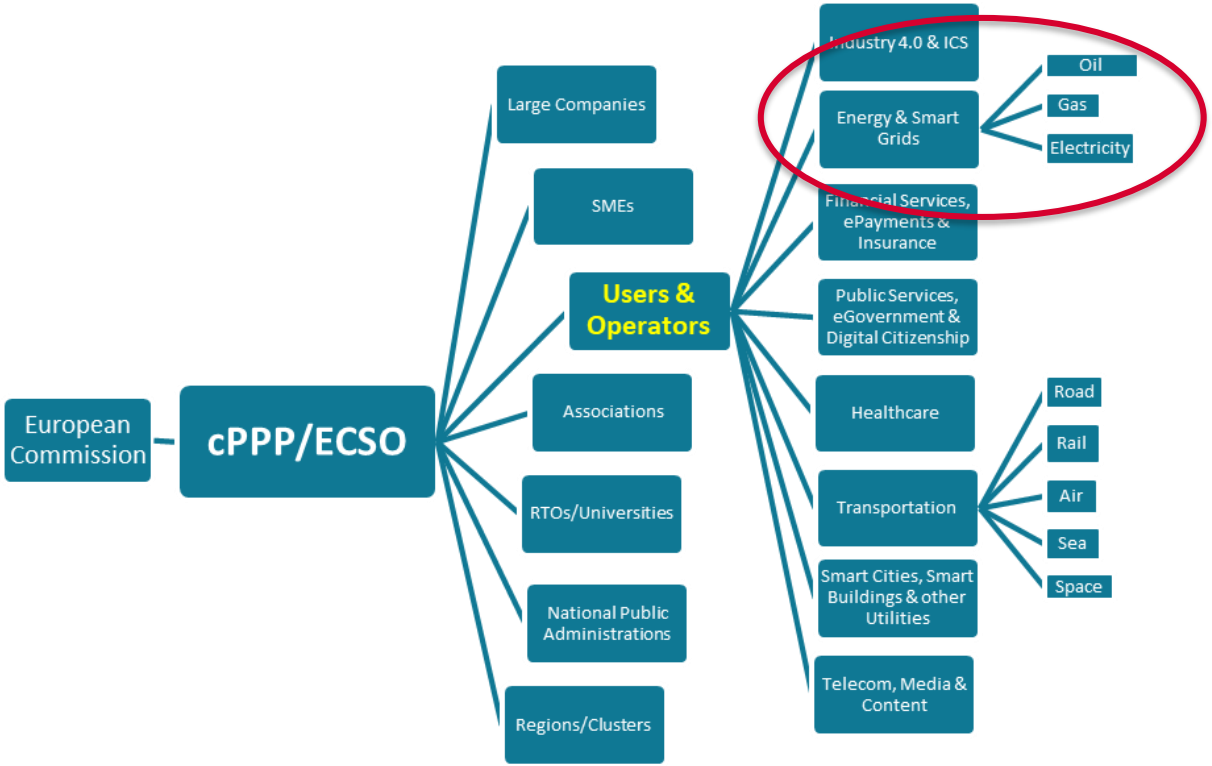
WG activities: achieving wider objectives in a wider dialogue across public – private stakeholders

- **WG1 - standards / certification / label / trusted supply chain (133 members with 280 experts):** Initial positions for an EU certification framework: State of the Art (SOTA), Challenges relevant to the industrial sector (COTI), Meta-Scheme for EU certification. Initial cooperation (MoU) on standards with CEN/CENELEC – ETSI. Contact: roberto.cascella@ecs-org.eu
- **WG2 - market / funds / international cooperation / cPPP monitoring (80 members with 152 experts):** Market analysis: Support Cybersecurity Industry Market Analysis (EC funded CIMA project). Market investments: initial discussions with banks, insurances and investment funds. Investments for start-ups: support to national public and private bodies to understand and develop an EU approach. International cooperation: dialogue with US admin.; involvement via members in EC CSA projects (Japan and US). Contact: danilo.delia@ecs-org.eu
- **WG3 - verticals: Industry 4.0; Energy; Transport; Finance / Bank; Public Admin / eGov; Health; Smart Cities; Telecom/Content/Media (120 members with 253 experts):** Sector reports under finalisation; initial dialogue with ISACs (finance, energy) for exchange of information across operators; support to NIS Directive implementation. Contact: nina.olesen@ecs-org.eu

WG activities: achieving wider objectives in a wider dialogue across public – private stakeholders

- **WG4 - SMEs, Regions, East EU (78 members with 136 experts):** SME – Position paper (role of SMEs in the cybersecurity ecosystem); suggestion for an SME hub / Platform and a EU "ECSO Quadrant" scheme; REGIONS: – partner in proposals for INTERREG and Interregional cooperation in cybersec domain; EAST EU REGION: just started – envisaging how to better support users and suppliers in East EU. Contact: danilo.delia@ecs-org.eu
- **WG5 - education, training, awareness, cyber ranges (96 members with 197 experts):** Initiation of a EHR-4CYBER Network to share best practices on training, harmonise courses, identify job needs; mapping of educational and professional training courses; started tackling gender issue on education & training to increase number of cyber experts. Contact: nina.olesen@ecs-org.eu
- **WG6 - Strategic Research and Innovation Agenda (151 members with 332 experts):** Identification of research priorities for EC programmes: SRIA (Strategic Research & Innovation Agenda) priorities well incorporated in the 2018-2020 work programme of H2020. Analysis to review technology and needs evolution in the next 10 years. Link with other PPPs to coordinate objectives (BDVA, EFFRA, 5G). Contact: roberto.cascella@ecs-org.eu

WG3: Verticals / Sectoral Demand



Purpose and Approach

- Identification of user/market needs
- Assess vertical sectors challenges and impact
  - Understand market needs (e.g. demand driven requirements, threats, functional requirements, ecosystem impact etc.)
  - Influence EU instruments on research and/or policy issues by input to other ECSO WG's and other means as appropriate in the scope/constitution of ECSO
  - Drive well founded sector impact into other ECSO WGs

WG3 : Objectives for 2018

Deliverables:

Sector-specific reports (chapters 1-4 of SOTA's)

Report on transversal assessment of functionalities (matrix)

Report on NIS implementation and harmonisation of incident reporting (following SWG 3.4 workshop)

Sector-specific guidelines on implications of GDPR on cybersecurity and privacy

Report on ISAC's (assessment of needs by ECSO members)

Internal working documents:

Sector specific recommendations on:

- Standardisation/certification/labelling (with WG1)
- Education & Training (with WG5)
- Research needs beyond H2020 (with WG6)

Workshops:

Q1-Q2: SWG 3.1 Industry 4.0/ICS workshop (with EFFRA), SWG 3.2 Energy workshop (with DG ENER), SWG 3.4 Finance, ePayments and Insurance workshop

Q3-Q4: SWG 3.3 Transportation, SWG 3.5 Public services, eGov, and Digital Citizenship, SWG 3.6 Healthcare, SWG 3.7 Smart cities and smart buildings

General:

- Assessment of needs for ISAC's (based on survey results) and discussions with ENISA on creation of ISAC's.
- Further exchanges with WG1 on sector-specific requirements Further exchanges with WG2 on taxonomy
- Discussions on GDPR (sector-specific guidelines)
- Cooperation with sectoral associations, DG's, and agencies
- Identify "concrete projects" to raise interests of users: e.g. information sharing platforms (on threats)
- Support to members on NIS implementation (pilot scenario analyses similar to SWG 3.4 analysis on harmonised incident reporting)
- Transversal assessment of IoT implications
- Cooperation with sectoral associations, DG's, and agencies
- User engagement

Strategic priorities, areas and recommended actions of the Energy Expert Cyber Security Platform (EECSP) - Expert Group (2017)

Strategic Priorities		Strategic Areas	Areas of Actions
I	Set-up an effective threat and risk management system	European threat and risk landscape and treatment. Identification of operators of essential services Best practice and information exchange Foster international collaboration.	1) Identification of operators of essential services for the energy sector at EU level. 2) Risk analysis and treatment. 3) Framework of rules for a regional cooperation. 4) EU framework for vulnerabilities disclosure for the energy sector
II	Set-up an effective cyber response framework	Cyber response framework Crisis management	1) Define and implement cyber response framework and coordination. 2) Implement and strengthen the regional cooperation for emergency handling.
III	Continuously improve cyber resilience	European cyber security maturity framework Supply chain integrity framework for components Best practice and information exchange Awareness campaign from top level EU institutions	1) Establish a European cyber security maturity framework for energy. 2) Establish a cPPP for supply chain integrity 3) Foster European and international collaboration.
IV	Build-up the required capacity and competences	Capacity & competence build-up	1) Capacity and competence build-up.

JOIN US TODAY AND HAVE YOUR SAY ON

ECS
EUROPEAN CYBER SECURITY ORGANISATION

- Increasing the use of cybersecurity solutions in the different application areas
- 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
- Developing employment in cybersecurity sectors (supply and users/operators)
- Facilitating the process for information-sharing between national administrations, CERTs and users to increase monitoring and advice on threats, as well as a better understanding of risk management and metrics
- Coordinating work with the future projects envisaged by the European Commission as announced in the “European Union Cyber Security Strategy”, as well as the activities of relevant networks, such as ISACs, and EU policies and regulations specific to each sector
- Investing in the entire supply chain and bringing innovative results to market via the systematic use of the whole set of available funding tools (at European and national level; public and private)

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