European Cybersecurity cPPP and ECSO
The role of IoT

Roberto Cascella

Senior Policy Officer (ECSO)

IoTWeek

6 June *2018 – Bilbao*

Europe and cybersecurity: now evolving faster
Overview of the context

2013: EU CYBERSECURITY STRATEGY "Open safe and secure cyberspace"

2015: DIGITAL SINGLE MARKET (EC COMM, envisaging a cybersecurity cPPP)

2016 (7 July): EC COMM "STRENGHTENING EU's CYBER RESILIENCE SYSTEM & FOSTERING A COMPETITIVE AND INNOVATIVE CYBERSECURITY INDUSTRY" announcing the creation of the cPPP

2017 (13 September): EU cybersecurity package – Joint Communication on EU strategy Review and Cybersecurity Act ("New" EU Cyber Security Agency: ENISA + EU Certification Framework)

- Still large number of Bodies and fragmentation at EU and MS level
- Creation of a Network of Cybersecurity Competence Centres (pilots starting by end 2018) with a European Cybersecurity Research and Competence Centre
- New technologies: Internet of Things; Artificial Intelligence / Big Data Analytics; High Performance Computing…
- Transposition of the NIS Directive and application of the GDPR Regulation: May 2018
- EC proposal for the next MFF (2021 – 2027): May 2018 (details for cyber expected mid June)

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 (UPDATE: now over €500 mln), 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 (UPDATE: total beyond €2000 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.

The uniqueness 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"**

INDUSTRY OBJECTIVES for the cPPP strategy

Industry looks for

- Increase competitiveness at global level supported by a European cybersecurity industrial policy
- Rapid reaction capabilities in case of attacks
- Development of innovative cybersecurity technologies
- Validation of the solutions in key infrastructures and applications
- The development of a sustainable ecosystem that will facilitate innovation uptake including
  - European certification framework
  - Capability building at regional, national and EU level also to increase European digital autonomy
  - Education and harmonised training for increased needs in job creation
  - Increased leverage upon SMEs
  - Development of cybersecurity services

23 months after: Update of the analysis of the situation

Evolutions in the latest months

- Evolution of the awareness on cybersecurity at national and EU level
- Evolution of threats (e.g. Petya; Mirai/ IoT; WannaCry; Spectre & Meltdown) and priorities (political: interferences in democratic processes)
- Evolution in the dialogue between public and private stakeholders thanks to the cPPP / ECSO (but still limited exchange of information due to sovereignty or competition issues)
- Revised objectives / actions of the EU cybersecurity strategy
- Definition / implementation of new legislations (NIS Directive, GDPR, ePrivacy, …)

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

- Impact on all levels: societal and economic
- Strongly increased need for skilled experts (c.f. EC Joint Comm: 350.000 by 2022)
- Need for improved control / ownership / security of data in Europe
- Growth of pervasive and distributed IT infrastructure (secure 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); increased use of blockchain (DLT)

ECSO membership overview

132 founding members: now we are **236 organisations from 29 countries and counting (included 6 new provisional membership – in brackets) and 3 new demands**

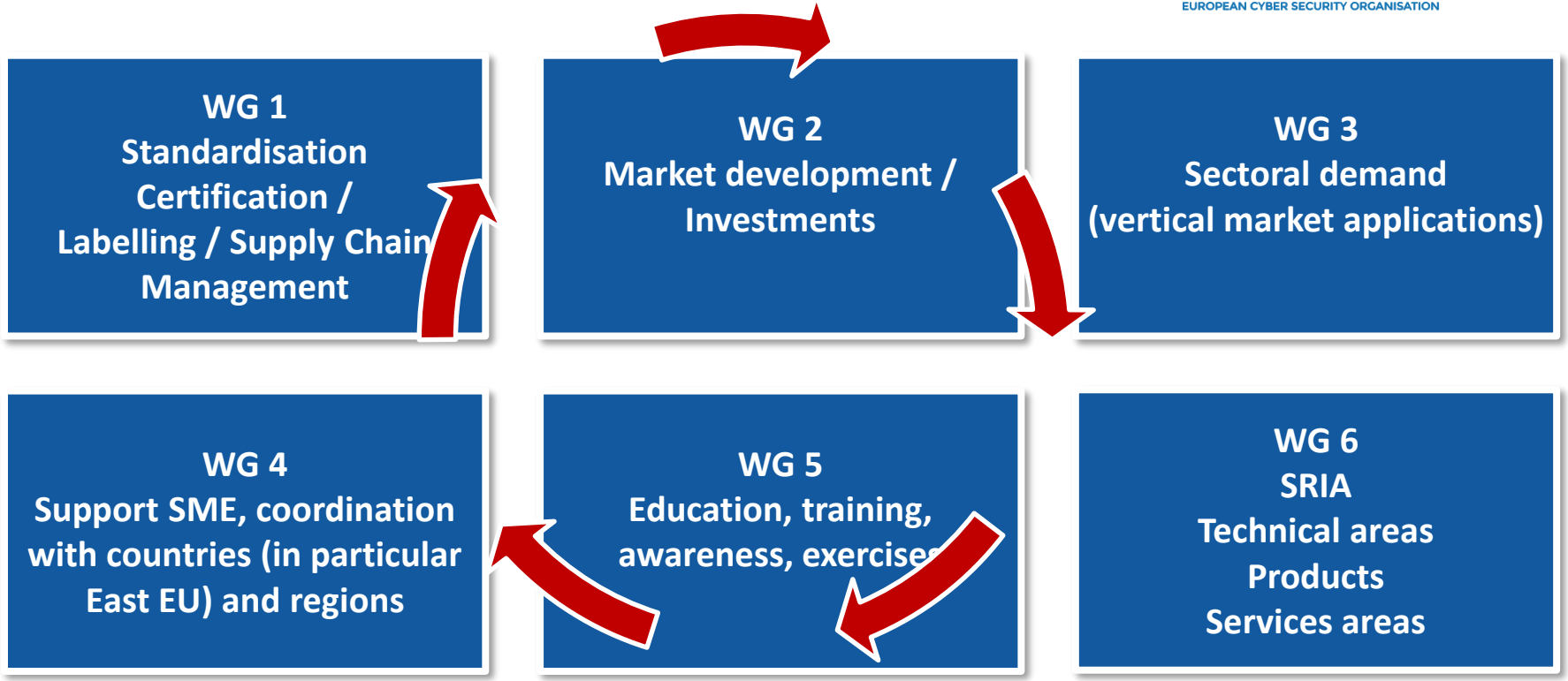
AUSTRIA	7	ITALY	26 (+2)
BELGIUM	13	LATVIA	1
BE - EU ASSOCIATIONS	9	LITHUANIA	1
BULGARIA	1 (+1)	LUXEMBOURG	4
CYPRUS	4 (+1)	NORWAY	4
CZECH REP.	3	POLAND	6
DENMARK	5	PORTUGAL	3
ESTONIA	7	ROMANIA	1
FINLAND	8	SLOVAKIA	2
		SLOVENIA	1
FRANCE	24 (+1)	SPAIN	32
GERMANY	21	SWEDEN	2
GREECE	5	SWITZERLAND	5
HUNGARY	3	THE NETHERLANDS	17
IRELAND	3	TURKEY	3 (+1)
ISRAEL	2	UNITED KINGDOM	8

- Associations : 21
- Large companies and users: 70
- Public Administrations: 20

  AT, BE, CY, CZ, DE, EE, ES, FI, FR, IT, SK, FI, NL, NO, PL, UK, BG, SE, GR +

  observers at NAPAC (DK, HU, IE, LT, LU, LV, PT, RO, SI, MT, …)
- Regional clusters: 6
- RTO/Universities: 62 (+1)
- SMEs: 52 (+5)

Working Groups



Impact of IoT technology

Internet of Things (IoT) will have a significant impact in the daily life of citizens in addition to have a relevant role in the digitization of the European Industry ➔ new security challenges that needs to be addressed to ensure a safe ecosystem

Where we stand now ➔ the adoption of IoT has raised many new legal, policy and regulatory challenges

- DSM Strategy emphasises the importance of legal certainty for the rollout of the Internet of Things (IoT)
- The September 2017 Joint Communication recognises the importance and relevance of IoT technology and the need to address cybersecurity challenges to ensure trust of consumers in emerging technologies and protect critical infrastructures
- The "Liability for emerging digital technologies" study (April 2018) provides a first mapping of liability challenges also for IoT technology

Importance of IoT devices for the industry:

- **Consumer**: addressing the mass, thus having the need for lightweight security solutions that can deployed in large scale and with limited impact on the cost of the device for the end-users while guaranteeing trust in the IoT products and services
- **Industrial**: meant for the digitisation of the industrial sectors and enabling the automation of the processes
- **Critical infrastructure**: deployed in critical infrastructures and requiring a high degree of trust and enabled security features

What are the relevant aspects for ECSO WGs

- **WG1**: certification schemes and baseline security standards ➔ Ensure a trustworthy supply chain
- **WG2**: IoT market is significantly growing
- **WG3**: impact in several sectors (c.f. transport, eHealth, industry 4.0, energy, …) ➔ import to deploy secure IoT on the market
- **WG4**: development of local ecosystem and new business opportunities for SMEs
- **WG5**: simulation and cyber range tools that address IoT technology
- **WG6**: wider deployment of IoT will have an impact on the needed EU strategic capabilities ➔ key to invest in future disruptive technologies

BECOME MEMBER!
CONTACT US

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

www.ecs-org.eu

Phone:
+32 (0) 27770252

E-mail:
Dr. Roberto G. Cascella
Senior Policy Officer
roberto.cascella@ecs-org.eu

Follow us
Twitter: @ecso_eu