EUROPEAN CYBER SECURITY ORGANISATION

Healthcare and cyber physical systems: the policy context

Nina OLESEN – Senior Policy Manager at ECSO
Twitter: olesen_nina / LinkedIn: nina-olesen
www.ecs-org.eu

SAFECARE Demo event

1st February 2021

SHORT INTRODUCTION TO ECSO

www.ecs-org.eu

ECSO is the European Commission's partner in implementing the Public-Private Partnership on cyber security (established in 2016)

Today, ECSO federates and represents the European cybersecurity community: industry players (large companies and SMEs – suppliers and users), as well as national public administrations, regions, research centres and academia

Our membership: from 132 members in June 2016 to 266 members across 29 countries in February 2021, connecting more than 2000 organisations in Europe

The ECSO community is cooperating with the different main EU and international actors: European Institutions (EP, EC, Council), European Agencies (ENISA, EUROPOL, EDA, …), Non-EU Public administrations (US, Japan, …); EU Initiatives (PPPs, Jus, Competence centre, …), International Bodies (UN, WEF, …)

Timeline of the European approach to cybersecurity

- 2009: EU stakeholders started to advocate for a specific “ICT security” approach on EU R&D
- 2011: Started the discussion with the EC about a possible Public Private cooperation
- 2013: First EU cybersecurity strategy (“building blocks”)
- **2016: Signature of the cPPP between the EC and ECSO**
- 2017: Update of the EU cybersecurity strategy
- 2018: Adoption GDPR and NIS Directive
- 2019: Adoption of Cybersecurity Act (new ENISA mandate, EU certification)

- 2020: Discussion on the next MFF (2021-2027). Recovery plan for the “new normal” after the COVID crisis. New EU Cybersecurity Strategy (December 2020)
- 2021: European Cybersecurity Centre / Creation of national Cybersecurity Centres; Horizon Europe – Digital Europe Programme; Starting discussions on Digital Service Act and European secure ID; …
- **2021: ECSO continues to support the growth of the European Cybersecurity ecosystem and Community**

We go beyond Research & Innovation (R&I)

In our six working groups, we deal with the different aspects of cybersecurity industrial policy

WG1 - Standardisation, certification, labelling and supply chain management

WG2 - Market deployment, investments and international collaboration

WG3 - Sectoral demand and Users Committee

WG4 - Support to SMEs and Regions

WG5 - Education, training, awareness and cyber ranges

WG6 - SRIA and cybersecurity technologies

WG3

Sectoral demand and Users Committee

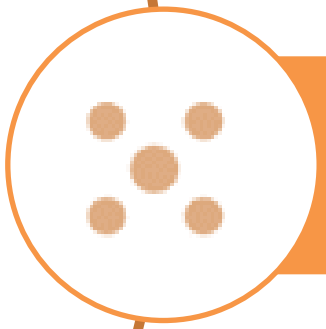
Engage directly with users (operators, companies, governments) to understand cyber threats, share information among trusted peers, link supply and demand, and act as a transversal WG that defines the needs of the following sectors

- ✓ **Industry 4.0**
- ✓ **Energy***
- ✓ **Transport***
- ✓ **Finance***
- ✓ **Public Services / eGov**
- ✓ **Healthcare***
- ✓ **Smart Cities**
- ✓ **Telecom, Media, and Content**

*Priority Sectors

Providing recommendations on policy, technology and strategy capacity / capability for sectors upon request of the European Institutions or other WGs

- Recommendations on the review of the NIS Directive
- Input to WG1 on the definition of certification schemes, WG6 on R&I priorities.
- Establish collaboration with CERT/CSIRT, SOC, ISAC, DG CNCT (EC) and sectoral associations



Mapping Sectoral needs and requirements

- Sector reports on needs and requirements (energy, finance, healthcare, industry 4.0, transport, smart cities)
- ECSO COVID-19 cybersecurity package

Users Committee

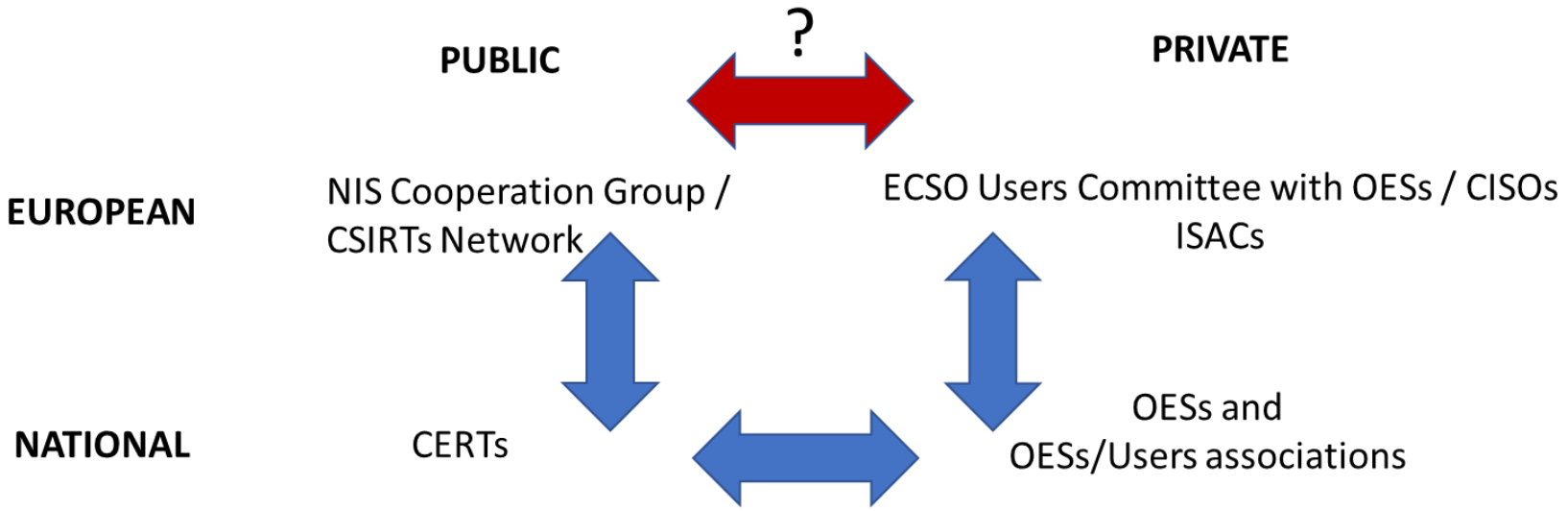
- Establishing trusted environment for information sharing and strategic threat intelligence among CISOs and peers from different sectors

WG3

In Focus: Users' Committee (UC) & EU information-sharing environment

Objectives:

- Provide Users/Operators with a **space to discuss operational and security-related issues** in trust and confidence (understand the risks and threats by sharing non-public and restricted information).
- **Share best practices, lessons learned and strategic intelligence** between C-level executives
- **Raise awareness among Users/Operators** in general with regards to the dangers of cybersecurity and vulnerabilities
- Support sectoral demand and **provide recommendations for specific cybersecurity needs**



WG3

Users Committee: Key outcomes & coming up

Main outcomes so far:

- POSITION PAPER: Review of the NIS Directive
- GREEN PAPER: Challenges for CISO's & Threat Intelligence Sharing

Ongoing task: CISO Survey

- Aimed at CISOs (or equivalent), especially from transportation, health, energy, finance and manufacturing sectors
- Objective: Understand CISO's needs, requirements, challenges, roles and responsibilities, operational / business continuity issues, etc
- 99 responses received from CISOs from different sectors, including healthcare, transport, food, finance, energy, government, water & utilities, telecom
- Currently analysing the data

Coming soon: Analysis Report on CISO Needs: sector by sector & cross-sector

Healthcare will be at the heart of future cybersecurity policies
Here's a few reasons why…

- Impact of the COVID-19 pandemic
- Reliance on network and information systems that are increasingly interconnected
- Increased digitalisation of our society and the number of connected devices (IoT)
- Need for awareness and skilled workforce
- Privacy and access to health services
- Cross-border cooperation and dependencies (CI)
- Medical devices (standardisation)
- Response to threats and operational resilience
- Data breach notification and incident reporting
- Cybercrime (ransomware)
- Sheer criticality (life or death)

By 2030, Global IOT in Healthcare Market to Grow at 24.6% CAGR to Reach USD 491 Billion

A patient has died after ransomware hackers hit a German hospital

This is the first ever case of a fatality being linked to a cyberattack.

by **Patrick Howell O'Neill** September 18, 2020

The EU's Cybersecurity Strategy for the Digital Decade (Dec 2020)

FOCUS: Cyber and physical resilience of network, information systems and critical entities (updating EU-level measures aimed at protecting key services and infrastructures from both cyber and physical risks)

- The proposed **Directive on measures for high common level of cybersecurity across the Union (revised NIS Directive or 'NIS 2')** will cover medium and large entities from more sectors based on their criticality for the economy and society. NIS 2 strengthens security requirements, addresses security of supply chains, streamlines reporting obligations, introduces more stringent supervisory measures for national authorities, and aims at harmonising sanctions regimes across Member States. NIS 2 will also help increase information sharing and cooperation on cyber crisis management at national and EU level.

- The proposed **Critical Entities Resilience (CER) Directive** expands on the 2008 European Critical Infrastructure directive with 10 sectors now covered: **energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, public administration and space**. Under the proposed directive, MS would adopt a national strategy for ensuring the resilience of critical entities and carry out regular risk assessments. These assessments are intended to also enhance their resilience in the face of non-cyber risks, including entity-level risk assessments, technical and organisational measures, and incident notification.

FOCUS: Stronger situational awareness and response to threats

- Proposal to build a **network of Security Operations Centres across the EU**: Goal would be to connect, in phases, as many centres as possible across the EU to create collective knowledge and share best practices. Support would be provided to improve incident detection, analysis and response speeds through state-of-the-art AI and machine learning capabilities.

- A **Joint Cyber Unit** would serve as a virtual and physical platform for cooperation for the different cybersecurity communities in the EU, with a focus on operational and technical coordination against major cross border cyber incidents and threats. The Joint Cyber Unit would be an important step towards completing the European cybersecurity crisis management framework.

“NIS 2” will:

1. Expand the scope of the current NIS Directive by **adding new sectors based on their criticality** for the economy and society and by **introducing a size cap** (all medium and large companies in selected sectors will be included) leaving Member States flexibility to identify smaller entities.
2. **Eliminate distinction between operators of essential services and digital service providers**.
3. Strengthen security requirements for the companies by **imposing a risk management approach** providing a list of basic security elements that have to be applied.
4. Introduce precise **provisions on the process for incident reporting, content of the reports and timelines**.
5. Require **companies to address cybersecurity risks in supply chains and supplier relationships**. Member States and ENISA will carry out coordinated risk assessment of critical supply chains building on the approach taken in the context of the recommendations on cybersecurity of 5G networks
6. Introduce more stringent supervisory measures for national authorities and aim at **harmonising sanctions regimes** across Member States
7. Enhance the role of the **Cooperation Group in shaping strategic policy decisions on emerging technologies and new trends,** and increases information sharing and cooperation between Member State authorities

10 sectors are now covered: energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, public administration and space.

2021	
NEW INITIATIVES (CRITICAL INFRASTRUCTURE)	
Protecting critical infrastructure in the EU – new rules	On 16 December 2020, the Commission published its proposal for a directive on the resilience of critical entities. The proposed Critical Entities Resilience (CER) directive expands the scope of the 2008 European Critical Infrastructure directive: it would cover ten sectors - energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, public administration and space, while the 2008 legislation only applied to energy and transport sectors. It aims to create an all-hazards framework to support Member States in ensuring that critical entities are able to prevent, resist, absorb and recover from disruptive incidents, no matter if they are caused by natural disasters, accidents, terrorism, insider threats, or public health emergencies, including pandemics like the one that Europe faces today. Proposal for a Directive

2021	
NEW INITIATIVES (HEALTH/CYBER PHYSICAL)	
Coronavirus: European Commission launches Next-Generation Internet of Things project for innovative healthcare solutions	Receiving €8 million and comprising of 13 partners from 9 countries, the IntellIoT consortium will drive autonomous and human-centred healthcare solutions by using Artificial Intelligence (AI) and Internet of Things (IoT) systems to provide cardiovascular patients with quicker and higher quality remote treatment, all whilst preserving the privacy and security of patients' data

2021	
NEW INITIATIVES (HEALTHCARE)	
European Health Data Space	European Health Data Space (legislative, including impact assessment Q4). A common European Health Data Space will promote better exchange and access to different types of health data (electronic health records, genomics data, data from patient registries etc.), not only to support healthcare delivery (so-called primary use of data) but also for health research and health policy making purposes (so-called secondary use of data). Public consultation currently open until 3rd February 2021

2021	
UPCOMING (HEALTHCARE)	
EU4Health 2021-2027 – a vision for a healthier European Union	Programme for the Union's action in the field of health for the period 2021-2027 ("EU4Health Programme") – Regulation Aims to boost EU's preparedness for major cross border health threats by creating reserves of medical supplies for crises; a reserve of healthcare staff and experts that can be mobilised to respond to crises across the EU; increased surveillance of health threats. It will strengthen health systems to face epidemics as well as long-term challenges by stimulating disease prevention and health promotion in an ageing population; digital transformation of health systems; access to health care for vulnerable groups. It will also make medicines and medical devices available and affordable **STATUS**: Awaiting Parliament's position in 1st reading

	THEMATIC	LEGISLATIVE DOSSIERS
VERTICAL	EU strategies	Europe's Digital Decade; Europe Fit for the Digital Age strategy; Industrial strategy; SMEs strategy; Recovery Plan for Europe; Security Union Strategy; revision of the IPCEI
	Consumer Protection	AI including safety liability, fundamental rights; NLF; RED; Low Voltage Directive; Machinery; Medical Devices; Electromagnetic devises; revision of the Product Safety Directive
	Market/Competition	Digital Services Act; ex ante competition tool; Foreign Subsidies (levelling playing field + public procurement); Single market barriers
	Sector specific	Review of the NIS Directive; cross sectoral financial services act on operational and cyber resilience; resilience of critical entities
HORIZONTAL	Data/Privacy	ePrivacy Regulation; Data Act; European Health Data Space; review of Database Directive
	Technologies	5G, Trusted ID (eIDAS regulation)
	R&I	Competence Centre; MFF for HE & DEP
	Education	Digital Education Action Plan
	Cybercrime/Terrorism/ Judiciary/LEA	Encryption; digital information exchange; joint investigation collaboration platform; review of EUROPOL Mandate; digitalisation of cross border judicial cooperation

Look out for…

- **Next Generation EU – Recovery plan for Europe:**
  - Preparedness, recovery and resilience, via the Recovery and Resilience Facility, rescEU and a new health programme, EU4Health.
- **The new Medical Devices Regulation and the In Vitro Diagnostic Medical Devices Regulation**
  - The new Regulations will create a robust, transparent, and sustainable regulatory framework, recognised internationally, that improves clinical safety and creates fair market access for manufacturers and healthcare professionals.
  - Date of application of the Medical Devices Regulation postponed until May 2021 with date of application of the In Vitro Diagnostic Medical Devices Regulation May 2022.
- **Joint Cyber Unit**
  - While it will be managed by the European Institutions, it will give cybersecurity stakeholders (incl. private sector) a focal point for sharing information about threats. Further communication from the EC on how the JCU will be set up and operated expected this month.
- **Horizon Europe** (resilient infrastructures, situational awareness, safety-security in cyber physical systems, secure health data,…).
- **Digital Europe Programme** (digital transformation of healthcare / digital solutions, skills & awareness, cyber ranges, European health data space,…).

CONTACT US – JOIN US !

European Cyber Security Organisation
29, Rue Ducale
1000 – Brussels – BELGIUM

E-mail:
nina.olesen@ecs-org.eu

Follow ECSO:

Website: www.ecs-org.eu

LinkedIn: https://www.linkedin.com/company/ecso-cyber-security/

Twitter: @ecso_eu