ENERGY INFO DAYS

Brussels, 25 October 2017

Cybersecurity & Digital Privacy in the Energy sector

CNECT.H1 – Cybersecurity & Digital Privacy, DG CNECT
ENER.B3 - Retail markets; coal & oil, DG ENER
European Commission

2013-2017: Evolving threat landscape

- Proliferation of (poorly secured) IoT devices
- Blurring lines between state and non-state actors
- Hybrid attacks on western democracies
- Fake news
- Evolving cybercrime business models
- Cyber espionage on the rise
- Dependence on foreign security technologies
- Persisting critical infrastructure vulnerabilities
- Attempts to promote new internet governance model
- Vulnerabilities of third countries

Policy context

- Digital Single Market Strategy – COM(2015) 192 of 6.5.2015;
- European Agenda for Security – COM(2015) 185 of 28.4.2015;
- NIS Directive – Directive (EU) 2016/1148 of 6/7/2016 concerning measures for a high common level of security of network and information systems across the Union;
- eIDAS – Regulation (EU) 910/2016 of 23.7.2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
- General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679 of 27.4.2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

Policy context (cont.)

- Proposal for an e-Privacy regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - COM(2017) 10 of 10.1.2017;
- Communication on "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry" – COM(2016) 410 of 5.7.2016;
- Contractual Public-Private Partnership on Cybersecurity – July 2016;
- **Cybersecurity package September 2017: Joint Communication on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" – JOIN(2017) 450 of 13.9.2017;**

State of the Union 2017

by Jean-Claude Juncker, President of the European Commission (13 September 2017)

"A Europe that protects, empowers and defends."

"Fourth priority for the year ahead: we need to better protect European in the digital age."

"Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks."

- **Europe must be better equipped for cyber-attacks (no borders, no one is immune);**
- **European Cybersecurity Agency: to help defend against such cyber-attacks;**

Conclusions from the Tallinn Digital Summit (29 September 2017)

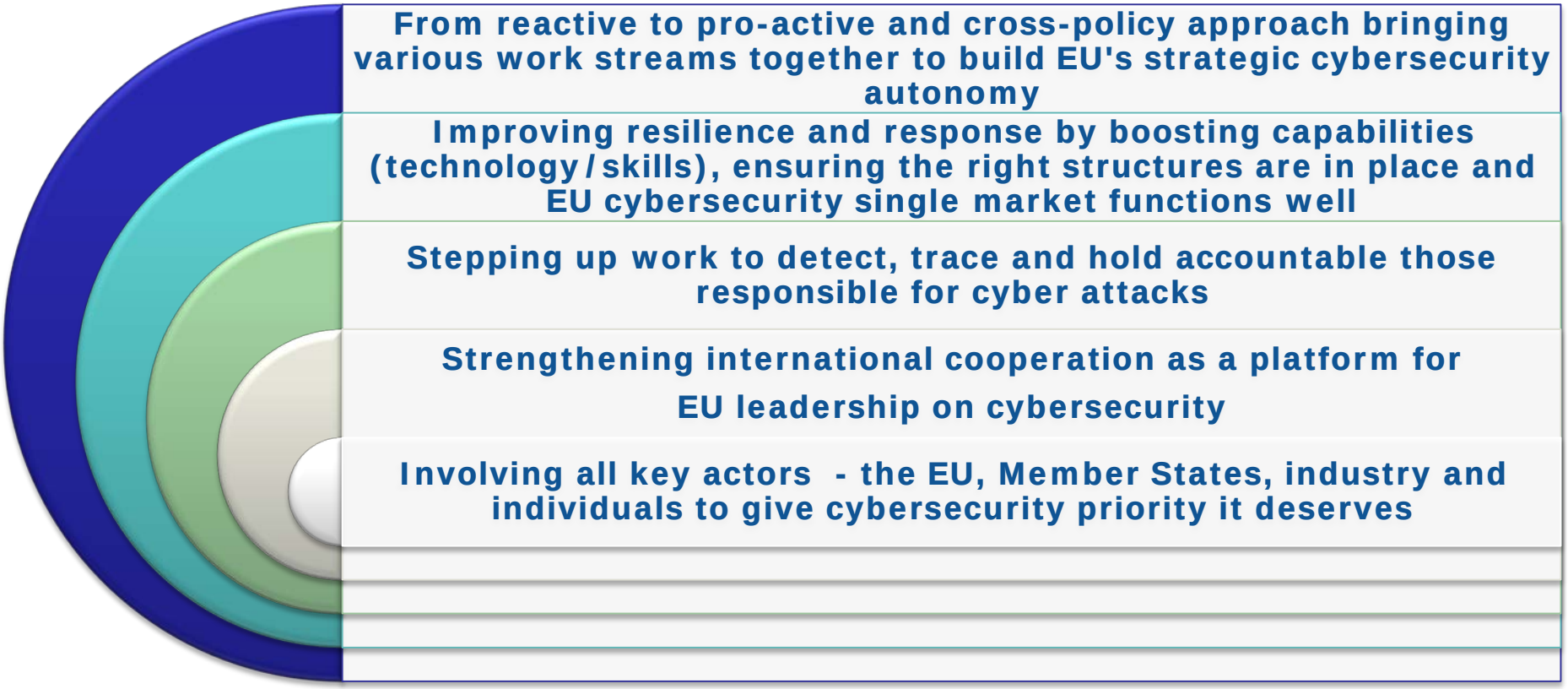
*"We should make Europe a **leader in cybersecurity by 2025**, in order to ensure the trust, confidence, and protection of our citizens, consumers and enterprises online and to enable a free and law-governed internet."*

...

- **"***Europe needs a **common European approach to cybersecurity**. Europe has to function as a **single European cyberspace** and a **single cybersecurity market**, including in terms of world-class and state-of-the-art security certification and joint standards, operational capacity, and collective crisis response."*

...

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



Cybersecurity Package

Highlights of key initiatives

	Building EU Resilience to cyber attacks	Creating effective EU cyber deterrence	Strengthening international cooperation on cybersecurity
Cybersecurity Act	Reformed ENISA	Identifying malicious actors	Promoting global cyber stability and contributing to Europe's strategic autonomy in cyberspace
Cybersecurity Act	EU cybersecurity Certification Framework	Stepping up the law enforcement response	Strengthening cyber dialogues
Communication	NIS Directive Implementation	Stepping up public-private cooperation against cybercrime	Modernising export controls, including for critical cyber-surveillance technologies
Recommendation	Rapid emergency response – Blueprint & Cybersecurity Emergency Response Fund	Stepping up political response	Continue rights-based capacity building model
	Cybersecurity competence network with a European Cybersecurity Research and Competence Centre	Building cybersecurity deterrence through the Member States' defence capability	Deepen EU-NATO cooperation on cybersecurity, hybrid threats and defence
	Building strong EU cyber skills base, improving cyber hygiene and awareness		

A European Energy Union

Why does the energy sector require specific considerations in terms of cyber security?

- *Real time requirements*
- *Cascading effects*
- *Legacy and digital technologies*

How the Clean Energy Package acknowledges cybersecurity?

The legislative proposals put a lot of emphasis on **smarter and more efficient management of the grid**, by using digital technologies and the flexibility of consumers and their electrical appliances -PV, eV, etc

Innovation is at the core of the package, from renewable energy legislation, to energy efficiency and the new market design proposals

The package **acknowledges the importance of cyber security** for the energy sector, and **the need to duly assess cyber-risks** and their possible impact on the security of supply.

It proposes the **adoption of measures** to prevent and mitigate the risks identified as well as the adaption of **technical rules for electricity** (i.e. a Network Code) on cyber-security.

The Commission's proposal for a revised **security of gas supply regulation** acknowledges the importance of cyber security in gas.

Smart Grids Task Force (SGTF)

Working Group on Cybersecurity

- This working group stems from the Commission Communication "Clean Energy for All Europeans" (COM/2016/0860 final) announcing stakeholder working groups under the Smart Grids Task Force to prepare the ground for network codes on demand response, energy-specific cybersecurity and common consumer's data format.

- Set up in spring 2017 and final results by the end of 2018

- Revision of the Electricity Regulation – Article 55 – Establishment of network codes
  - Commission proposes a network code on cyber security

Study

On the Evaluation of Risks of Cyber-Incidents and on Costs of Preventing Cyber-Incidents in the Energy Sector

EECSP-Report: Expert Recommendation
The European Commission should launch an analysis of possible cyber threat scenarios addressing the high-level objectives with their associated risks and to assess how to mitigate respective risks and associated mitigation costs. (S)

Study on the Evaluation of Risks of Cyber-Incidents and on Costs of Preventing Cyber-Incidents in the Energy Sector.

Tasks:

Task 1: **System description & use cases**

Task 2: **Identification of threat scenarios**

Task 3: **Detailed analysis on mitigation measures in place**

Task 4: **Development of a methodology for and carrying out a risk assessment**

Task 5: **Identification of additional mitigation measures and calculation of their costs**

Task 6: **Recommendation**

DRAFT

Digital Security in WP2018-2020

LEIT-ICT:

Draft published on H2020 website

- **Cybersecurity call**
- **Cybersecurity embedded in several other topics**

SC7 – Secure Societies:

Publication: check the Participant Portal on 27.10.2017

- **intends to address: cybersecurity preparedness; digital security, privacy, data protection in critical sectors; cybersecurity in energy; combined physical and cyber threats;**

DRAFT

Cybersecurity in energy

- NIS Directive: "*Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market*."
- Energy sector mentioned in Annex II of the NIS Directive, with 'operators of essential services', to which the Directive applies;

Some of the main challenges:

- Digital technologies playing a more important role in the energy system, which is facing higher risks and vulnerabilities, being exposed to an increasing range of cyber threats;
- Need for new security approaches in detecting and preventing threats, building protection against cyber and privacy attacks;

DRAFT

Cybersecurity in energy

Scope of action could include:

- Development of solutions to make the energy sector more resilient to the cyber and privacy attacks, more cyber secure;
- Development of scenarios for possible attacks, with appropriate counteracting measures, designed, described, tested on a demonstrator, to verify effectiveness;
- Assessment of vulnerabilities and threats, design of adequate security measures;
- Development of security information, definition of cybersecurity design principles, formulation of recommendations, including for policy purposes;

DRAFT

Cybersecurity in energy

Impact expected could mainly include:

- Increased resilience against cyber and privacy attacks;
- Cyber protection policy design and uptake;
- Ensured continuity of critical business energy operations;

Disclaimer:

The views in the slides marked as 'draft' are the views of the services and may not in any circumstances be regarded as stating an official position of the Commission. Only the adopted work programme will have legal value. Information given in this presentation may not appear in the final work programme; and likewise, new elements may be introduced at a later stage.

Thank you for your attention!

More details (revised presentation) after the publication of the Work Programme

Questions?

CNECT-H1@ec.europa.eu

ENER-B3@ec.europa.eu