Cybersecurity –
a challenge to the new energy system

EU & Cybersecurity
GEODE Spring Seminar 2018

Michaela Kollau
DG ENER, B.4
29.05.2018

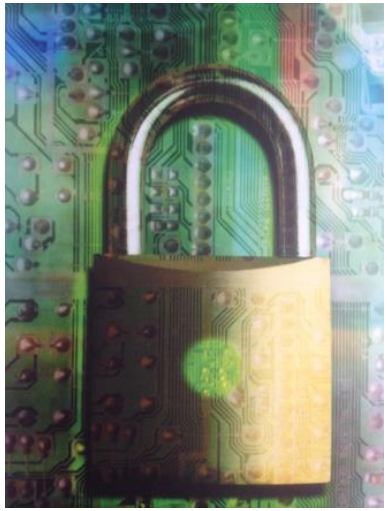
State of the Union 2017

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 Europeans 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;**

Policy Context



Where we are:

- EU Cyber Security Strategy (2013)

*- Network and Information Security Directive (EU) 2016/1148**

- Data Protection: Regulation (EU) 2016/679 - GDPR

- European Program for Critical Infrastructure Protection

*- Cybersecurity Package (2017)**

** More info next slides*

Network and Information Security Directive (EU) 2016/1148

- *Improving national cybersecurity capabilities*
- *Cooperation: NIS Cooperation Group & CSIRT Network*
- *Security and notification requirements for operators of essential services and digital service providers*

TIMELINE FOR IMPLEMENTATION:

- *May 2018 – transposition into national law*
- *November 2018 – MS to identify Operators of essential services*

European Commission

Cybersecurity Package (2017)

- *EU Cybersecurity Act*
  - **Proposal for a renewal of ENISA's mandate**
  - **Rules for the creation of a European certification framework**
- *Joint Communication on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" – JOIN(2017) 450*
- *Blueprint for rapid emergency response*
- *The Cyber Security Package acknowledges the importance of **specificities of different sectors** and refers to **sector-specific requirements**.*

Do we need anything specific for the energy sector?

..YES…

Stakeholder hearings of February 2018 *confirmed that specific considerations of the energy sector in terms of cyber security are needed.*

Stakeholders consulted include ENTSO-E, ENTSO-G, ECSO (European Cybersecurity Organization), Eurelectric, Eurogas, EDSO, GEODE and the Commission Agencies ACER and ENISA (the Agency for network and information security)

European Commission

Key challenges of the energy sector in terms of cyber security

- *Real time requirements*
- *Cascading effects*
- *Legacy technologies connected to digital technologies*

European Commission

How to address these particularities of the energy sector?

Short- and mid-term policy actions for cybersecurity in energy

- ***NIS implementation at energy sector level:***
  - *Guidance via an energy-specific work stream in NIS Cooperation Group*
  - *Kick-off meeting: 18 June 2018*
- ***Specific cybersecurity guidance for the energy sector beyond NIS***
  - *Via Staff Working Document*
  - *until end 2018*
- ***Continue the series of energy cybersecurity events***
  - *Previous: March 2017, High-level roundtable in Rome*
  - *Next: October 2018, Co-organised with AUT Presidency & IW*
- ***Enhanced cooperation with the EE-ISAC***
  - *DG ENER participation at next Plenary Meeting, June 2018*

Mid- and long-term policy actions for cybersecurity in energy

- ***Network code on cybersecurity***
  - Clean Energy for all Europeans Package

- ***Smart Grids Task Force : Expert Group 2***
  - **To prepare the ground for this network code**
  - **Key areas and subgroups:**

  — *European Cybersecurity Maturity Framework*

  — *Supply Chain Management*

  — *European Early Warning System for Cyber Threats*

  — *Cross-Border and Cross-Organisational Risk Management*

Conclusions

- *The energy sector has its particularities in terms of cybersecurity that we need to address*

- *We need to tackle cyber security in energy from all sides to guarantee sufficient progress and minimise the risk*

- *"Security is a process, not a product" (B. Schneier)*