Cybersecurity Considerations for Energy

Charles Esser, CEER Secretary General

Florence Forum 2019 (agenda item 6.3)

Reaction EC Guidance

- It is important that incident handling capability is stressed and improved: incident handling activities should be coordinated taking into account the different maturities of the Member States, and also in respect to interconnected systems. A harmonised approach to have consistent handling is important.

- There is a need for gathering and analysing “early warnings” related to cybersecurity and energy. On this point, gathering of early warning and their possible analysis will require the involvement of intelligence and security corps of the Member States in order to contextualise and properly assess the gathered warnings.

- There is a need for more analysis capability in respect to all information gathered in the context of the NIS Directive and by the Energy Operators (sometimes not shared outside their company boundaries). Research, awareness, knowledge building and training is needed for all actors.

- In regard to the cascade effect, there is a need for “real time” yet widespread use of legacy devices in the current infrastructure that create a vulnerability. Hence, we should possibly define priorities to address investments and allow regulatory authorities to approve investments respecting commonly agreed strategic priorities.

Cybersecurity Considerations for Energy

Charles Esser, CEER Secretary General

Florence Forum 2019 (agenda item 6.3)

Reaction EC Guidance

- **Supply chain (and its vulnerabilities) and certification is a key issue: certification is a crucial point in the supply chain of the cyber-secure energy sector, but the use of certification should not increase complexity for administrative procedures and/or costs for consumers and it should make use of already existing experiences.**

- **Operators and experts continue to stress the importance of distinguishing between Operational Technology and Information Technology when talking about cyber security: a specific research stream may help in increasing the potential for cybersecurity concepts which fit better with the energy sector's needs (and which may be extended to other sectors, such as manufacturing which are less critical but still financially impactful).**

- **Important to distinguish between cybersecurity and cyber-resilience: resilience is mentioned in 8(c) but also useful to frame it in terms of information and operational technology. We need to address both.**

- **In 12 (f), tender formulations are described, but perhaps this needs to be to be politically aware – this connects to Commission Recommendation on Cybersecurity of 5G networks (C(2019) 2335 final), recital 20.**