Reflections on Cybersecurity for Energy

Veli-Pekka Saajo, CEER DS Vice Chair

Florence Forum 2018 (agenda item 4.5)

- **Markets are mature enough to adopt/implement cybersecurity rules to protect long-term investments, under the condition that directions are clear**

- **Barriers to the implementation of cybersecurity:**
  - Unclear targets and unclear expected standards
  - Too many signals, i.e. Directives and Regulations, to implement with a number of parallel proposal (NIS, GDPR, Clean Energy for All Europeans, the Cybersecurity Act); we need a holistic and consistent approach
  - Lack of knowledge on the economics of cybersecurity for the energy sector: we only know that each sector has different objectives and different approaches
  - Lack of competence among executive and managerial staff, making the communication on the risks very difficult and creating the need for situational awareness campaigns
  - The costs of cybersecurity for the energy sector have not been sufficiently monitored by regulators, but a regular monitoring is needed to meet short, medium and long-term objectives at national, regional and European level

Recommendations and Future Work

- **Key Recommendations on Regulation:**
  - In order to align all stakeholders, create an energy cyber security strategy to set basic principles, then spread a common culture and work on the implementation, in agreement with other sectors
  - Make use of momentum and use incentives only for those regions/operators which may be the weakest link, measuring improvement and prioritising activites based on the criticality of the assets or the clusters of assets
  - The EU should create mandates for cybersecurity-specific competent authorities: different governance and approaches in different MSs creates risk for shared energy networks
- **CEER Future Work:**
  - CEER Public Report on Cyber Security for the Energy Sector, providing a regulatory overview of the situation and recommendations. CEER will organise a presentation followed by a roundtable for Autumn 2018
  - Monitor the markets for technological trends, strengthen the relationships with standards developers to help have the right technical standards to enable implementation (Meeting between Regulators and IEC in Korea – October 2018)
  - A workshop putting together Operators/Associations (ENTSOs, TSOs, DSOs, and others) and Regulators to define a shared strategy – in planning for 2019

Annex: CEER Initial Answers to European Commission Questions

I. Wide use of technology to overcome intermittence of energy resources and fast digitalisation with technologies is not used in any other sector (with the exception of the manufacturing sector, which is not so critical) is another point to add as a specificity of the Energy Sector.

II. Lack of trust in a competitive market is the main obstacle to free information sharing: the fear that sensitive information may be used against others. The inability to offer a shared and homogeneous response to an emerging threat because of different cybersecurity capabilities among operators (with the potential of a cascade effect) may be another obstacle in the future to a consistent information sharing.

III. Setting and enforcing a minimum level of cybersecurity measures may be a first step to build trust. Information exchange with the central role of CSIRTs is probably the best way to share information under the current conditions. The possibility to have a specific European Energy ISAC may be an additional step to tackle specificities of the energy sector.

IV. Guidelines should be based on shared principles and having in mind a common strategy. The definition of a strategic level through a European Energy Cybersecurity Strategy, followed by a tactical level with high-level guidelines setting the protection principles and explaining them in simple terms, may be a good way forward and may justify the need for guidelines. We may need to consider who should issue those guidelines.

V. There is no way to determine the right security level, but there are ways to estimate if the current risk level of the grid is acceptable. Investments in cybersecurity must be oriented to meeting principles established at a high level. Cybersecurity may not need incentives, except in some cases: most of the operators will need to protect and secure their cyber assets if they want to update regularly: incentives may just accelerate the process. We need to start monitoring cybersecurity activities and try to understand leverage which may better drive desired policy objectives. Only then may we analyse the need to use incentives and/or subsidies to foster an higher level of cybersecurity for the energy sector.