Second roundtable: Cybersecurity challenges for Smart Grids

Klaus-Dieter BORCHARDT, Director Internal energy market at EU Commission's DG Energy, explained that monitoring and maintenance, repair and management, are vitals! "***We have no time for an international agreement and institutional discussions, we need actions***". Some States are prepared to scenario A, meanwhile other States are getting prepared for scenario B. How can we be sure that States are prepared for all the different scenario? European energy system will go toward more flexibility, which necessitate more smartness in the grid system. "***Opening the infrastructure to external cybersecurity audit is accepting to be exposed to threats***". Data protection is a major challenge for Smart Grids. Cybersecurity frameworks should be risk-based, outcome focused for common language, within and between organisations.

"***It should be mandatory for the Industry to provide secure digital products and solutions***" stated Jean-Christophe MATHIEU, Products and solutions Security Officer at Siemens. We have to change the process of product creation with cybersecurity. It must be integrated in the conception process, and to the maintenance and training. Training on cybersecurity for everyone in a company "***is a vital matter, we need to strengthen that***". We will need great investment from the Regulator to create a technical resilience, and risk preparedness from member states: if one system fails, it does not stay in one country, it spreads.

Nuno MEDEIROS from EURELECTRIC talked about securing critical infrastructure operators. "***At least two blackouts caused by cyberattacks are substantiate to have occurred in Ukraine in 2015 and 2016***". The Company Board and the Regulator have to be aware of the cyberthreats and cybersecurity challenges. E-learning courses on cybersecurity is one of the action all companies need to work on. We need to address a "***collective, pan-European and cross-industry response toward cybersecurity challenges***". Smart Grids challenges must have a multi actor response. "***We need discussions on Smart Grids, data and risk assessment to elaborate security requirements***". There is a lack of harmonisation at the European level. We need to implement better practices, regarding customers information collected, we need to strengthen training and awareness, and accelerate the sharing of information about risks and responses at EU level.

Marc SMITHAM, from Microsoft, explained how Smart Grids represent a huge number of connected devices, and that number is challenging our cybersecurity capacities. "***Cyber risk management challenges also need a multi-stakeholder approach***". The question is also the security of the Internet of Things (IoT).

"***We have to change our vision of cybersecurity management***" (Lawrence JONES, VP international at Edison Institute). The human cost if an attack is against a hospital or Smart Grids has to be taken into account. What if a cyberattack provoked death? Mortal failures call for preparedness: cyber is one of the multiple crisis scenario. From the European side, we have to promote education to develop new competences.