First roundtable: Cybersecurity of critical energy infrastructure

We are so dependent on the energy sector, that if we experienced a three-day long outage, people would start killing each other to survive. In the opinion of Pierre CALAIS, CEO at Stormshield, there are no major players of cybersecurity in Europe because they all stay on a local market perspective. That is why, in his opinion, the key of the future is that National Agencies talk to ensure cybersecurity at European level. We are experiencing in this idea a sovereignty challenge, due to interconnections: do we trust the technology and products we use, do we put all our trust in software and hardware? Talking about the future, there is a new revolution in Industry: Data Driven and connected systems. How can we ensure the data is secure?

The European Union is engaged in Europol's E-crime Project, that aim at evaluating the economic costs of cybercrime. We need a third party to evaluate the costs. In France, Stormshield works closely with ANSSI, the National Agency in charge of information system security, to answer a continuous certification for each release code impact, etc, but those are not recognized outside of France. There is no harmonisation, so today it is time-consuming, costly and is not efficient. Creating an EU restraint certification could be quite easy, by recognizing a certification common to two countries.

Lawrence JONES, VP international at Edison Institute, talked about how private and public sectors can cooperate to instore more cybersecurity, with cooperation between different industries and agencies. How do we build trust for cybersecurity? It's necessary to work on this. It is necessary to create an opportunity of trust, by a step by step approach. We need to share practices, and cooperate with good faith.

The discussion was also about the Certification and the standards used, in term of trust: maybe the idea of a transatlantic cooperation could help? But unfortunately, going global takes a lifetime in software development, even if Marc SMITHAM, from Microsoft, called for the recognition of a global standard, to avoid today's problems of borders and national standards. Cooperation for international standards can be a great idea, but there is no need of a new organization for that.

Francesco MORELLI from Terna, stated that supply chain must be opened to certification authority, but a good and trustworthy certification authority is hard to find. Transparency in the cybersecurity field is very important. Distributed solutions are maybe not the solution we thought, they are maybe a greater challenge for cybersecurity.

Stefan MOSER, head of Unit Security of supply from DG Energy at EU Commission pointed out that new requirements in NIS directive about sharing information in the eventuality of cyberattacks can be very useful. Confidentiality is crucial for this.

"***Cybersecurity is a very specific risk: some actors are playing across borders and avoid security measures***".

Reliability depends on cybersecurity in the energy sector. We shall not deny sovereignty of member states in their cybersecurity strategy, but it can't be a pretext to refuse to work at European level for more cybersecurity, not only for energy sector but for all economic sectors.