Minutes - High level Roundtable on Main Challenges for Cyber Security in the Energy System

24. March 2017, Rome,

Terna S.p.A. Piazza Frua n. 2 -00 156 Roma

Organised by the European Commission

Dominique Ristori, European Commission, Director-General for Energy

Mr Ristori welcomed the speakers and the audience and thanked Mr Del Fante and Terna for hosting this important event. He stressed that we have to speak about one of the most important issues regarding energy and security. Additionally, the Ministerial Meeting of G7 will take place in Rome 9-10 April. Europe should not be seen as followers, but as leaders. In this context Mr Ristori passed two main messages. First, cybersecurity and energy security go hand in hand and require a common approach of the energy and digital worlds. They are two sides of the same coin. Energy is vital for all our all economic and human activities. Ensuring energy security is one of the key European energy policy priorities. There is a clear need to increase the capacity to work together. This is an issue of international interest to accelerate the preparation for adequate response to these threats.
Secondly, we need to develop a cyber security response covering all stages of the energy cycle. Priority has to be given to all aspects of the energy grid – transmission and distribution grid. We need an EU power grid prepared to withstand any cyber-attack. We will examine all challenges, having all priorities in mind and build a bridge in this context between Energy Union and Digital Single Market.

Roberto Viola, European Commission, Director-General for Communications Networks, Content & Technology

Mr Viola welcomed speakers and audience and thanked Mr Del Fante for hosting the event. He stressed the importance of cyber security in energy for our society. He reminded the signing of the European Treaties 60 years ago in Rome, starting from a steel and coal Community and being also a community of digital services today. He underlined that there would not be any digital services without energy, and that 8 % of the US energy bill today is used for data centres. In 10 years from now, the energy bill for the US and Europe will be more than 50% for digital devices. Digital needs energy and energy needs digital. Mr Viola linked the digital autonomous driving to energy through e-mobility and stressed that the concept of industry 4.0 has a clear link to energy. He also pointed out the importance to work together on digital skills which are also needed in the energy sector.

Mr Viola explained that cyber security is key in the energy and transport sectors. The cyber risks for these sectors have to be prevented as the consequences could be devastating to our society. We have to take this discussion seriously and cooperate together, and the NIS directive is the key mechanism for such cooperation. In the next two years, the implementation of this directive will translate in various actions. The most important one is cooperation. This year, the main focus lies on the renewal of the ENISA mandate, on certification and labelling, internet of things and the revision of the EU Cyber Security Strategy.

Matteo Del Fante, CEO Terna Rete Elettrica, Italy

Mr Del Fante thanked the Directors General and welcomed the participants. He said the meeting was an important initiative and discussion, and that he was very happy to have Terna experts on cyber security along. His main lines were: The transport sector, the health sector and the energy sector are facing digitalisation. Cyber security has to be one of the top priorities. The multiplication of access points in our networks is creating the need for sharing information and best practices and strong links between companies and states. Terna in collaboration with institutions play a role at national level, but the challenge is a European one. The forum of today is very important. It might maybe easier to tackle and discuss at national level, as well as defending and share best practices at national level, but best practices have to be shared at European level. Establishing new standards and adopting new solutions have to be addressed at European level. Mr Del Fante welcomed Mr Laurent Schmitt and emphasised the importance of ENTSO-E. Referring to Terna, he explained that Terna has a security operational centre which is extremely well regarded, Terna does security monitoring of tangible and intangible assets, monitor incident response activities and continuously monitor the most suitable cyber defence technologies used in Italy and around the world. In order to guarantee the best coverage of Terna assets, information security at Terna defines specific guidelines and strategies in addition, to identifying correct behaviour of all employees. Terna does a lot of simulations of possible cyber intrusions. During 2016, the Terna information security competence centre has completed a review of the information security policies and information security framework aiming for gradual alignment with the NIS directive. Terna has adapted an operational program and information risk management an RIM under the direction of the chief security officer. The coordination belongs to the corporate protection directorate, which has allowed Terna to identify the top cyber security risks. There is a daily cyber report, and whenever there is an event at European level, it gets analysed and a simulation at the Terna network is launched. To conclude, Mr Del Fante emphasised that cyber security is a key issue for critical infrastructures and that Terna is identified in Italy as a critical operator. Mr Del Fante stressed the importance of putting cyber security considerations already at the planning stage of industrial plans – thus cyber security has to be embedded in R&D.

Guido Bortoni, President Autorità per l'Energia Elettrica e il Gas, Italy

Mr Bortoni emphasised that the security of power systems is highly complex and must be addressed without simplification. The Italian experience has brought some distinctions that are useful to be recalled. Firstly, it is important to distinguish between system adequacy and security. Adequacy has a preventive character and relates to the procurement of resources up to the extend to cover demand to a reasonable level. Security is the capability of the

system to stay on, or rather to serve according to certain standards. Concerning risk management towards a secure system, it requires to manage enough resources in a preventive manner, along with operating the system by exploiting in a corrective manner the available resources. 100% security does not exist in nature. The concept of resilience is the capability of the system to serve or to recover from failures to a new equilibrium state. The main element of the resilient power system is the flexibility to adapt to an emergency beyond the security level to get services running or quick-start the service as quick as possible. Adequacy is guaranteed only by preventive measures, security by both – preventive and corrective measures, whereas resilience is merely corrective. For security the proper balance between preventive and corrective measures can only be assessed by the relation to the risk – to the two components of the risks, on the one hand the probability to occur and on the second hand the magnitude of the impact. We need a correct balance upon security that can be only realised with a proper risk assessment that goes beyond regulatory competences and requires further considerations at various political levels. Cyber security is a direct consequence of the present evolution of our power systems, especially in Europe. For the second roll-out of smart meters in Italy (starting end of 2017), cyber security is of utmost relevance. Cyber security introduces a new order of costs, but it also brings benefits to the system. Cyber security is founded on training and know-how of dedicated people involved. To conclude, traditional power systems have always been interconnected among themselves, digital or cyber is a strong dimension, which introduces the need for a cross sectorial connection between power and ICT (information and Communication Technologies).

Massimo Gaiani, Director General, Ministry of Foreign Affairs, Italy

Mr Gaiani stressed that our society is more complex, interconnected and digitalised. All these factors increase the flexibility, the performance of the system, while making it also more fragile and vulnerable. This applies to all sectors, but the energy sector plays a crucial role in our economy and our lives such that energy is vital to the functioning of the system as a whole. Security of infrastructures is a key element of security of supply. Electricity plays a central role, but security of supply must play an important role for all supply carriers including oil and gas pipelines. Cyber security is nowadays not to be merely understood as a defensive mechanism, but as a policy, a behaviour attitude that governments, private entities and citizens have to comply with. Working together is the only possible way for government and private undertakings to effectively address cyber issues. Cyber security is one of the main concerns to be talked by the Energy Union. A pan-European commitment is essential to mitigate cybercrime. Cybersecurity should become part of the most important fora, including IEA, G7 and G20. There is not enough awareness on cyber security, thus training and education must become part of effective forward looking prevention policies in the cyber space.

Rita Forsi, Director General, Ministry of Economic Development, Italy

Mrs Forsi – as the head of the Italian CERT – started with the challenges of cyber security in energy. Cyberattacks are increasingly targeting the energy sector, and we do not know who will be next and what attack will be used. Cyber-attacks could have catastrophic consequences. In 2014 in Rome, it was recalled amongst G7 members to protect the critical

energy infrastructures, including from cyber-attacks. The G7 in Hamburg agreed to improve the commitment on cybersecurity in the energy sector. Last year the G7 in Japan stated that cyber security has become a crucial element for guaranteeing security of energy supply. The G7 countries will facilitate cross-regional and cross sectoral networking on cybersecurity in the energy sector among relevant stakeholders, including national CERTS/CSIRTS. G7 countries announced to share threat information and to cooperate for the improvement of cyber security for critical infrastructure with a specific reference to the energy sector. This commitment is perfectly in line with the NIS Directive. The development of energy specific cyber security solutions and defensive practices are essential. National security, economic prosperity, the well-being of our citizens depend on reliable energy infrastructure. The government should support private companies and private companies should take more responsibility at private-public partnerships. The risk of human factors is of utmost importance when it comes to cyber security. Therefore it is crucial for companies to invest in training of staff. The European Union has a key role to play to take cyber security forward.

Juhan Lepassaar, Head of Cabinet for European Commission Vice- President Andrus Ansip, Digital Single Market

Mr Lephassar gave an overview of the Commission initiatives in the field of cybersecurity highlighting the importance to address cybersecurity in a coherent manner. For this purpose, DG CNECT and DG ENER are cooperating on a number of initiatives related to cybersecurity in the energy sector (e.g. NIS Directive, Energy Expert Cyber Security Platform – Expert, Smart Grid Task Force). He finally announced the review of the EU Cybersecurity Strategy later this year that is expected to include the review of the ENISA mandate and a proposal on ICT security certification, as well as a trusted IoT (Internet of Things) label.

Session 1 - Panel: Expectations from energy operators on cyber security What role for Member States and Europe?

Moderator: Laurent Schmitt, Secretary-General ENTSO-E

The European grids are heading forward on digitalisation, and ENTSO-E is committed to support this trend. The attacks today are of different nature, not only coming from individuals but also from organised entities. A lot of work has already been done by the Smart Grids Task Force. European grids are largely interconnected, thus we have to think on a broad basis.

Boris Schucht, CEO at 50Hertz, Germany

50Hertz is one of the four Transmission System Operators (TSOs) in Germany located north-east of Germany, the region with the highest amount of intermitted renewable energies in the world. 50% of the consumption are covered by solar and wind. This region is also a big export region. In Germany there are 1.7 Million decentralised installations. System security has four challenges. The first challenge is the real time IT and the SCADA system, which is physically disconnected thus not the biggest challenge. Every TSO in Europe has a different real time IT, thus if there is a problem another TSO can support and take over. We are on the right way with the ICT certification and policies that increase the awareness. The Second

part is the business IT. Due to the liberalised market, all schedules are made via the internet. It is a decentralised world where a central dispatch would still work today, but the future will raise challenges (in case the internet would be down). In the year 2012, a dDoS[1] attack hit 50Hertz , blocking the internet access for two weeks. This was not the biggest problem, as they were well prepared. Mr Schucht drew the attention to a recent article he read on the hacking of Tesla. As he drives an electric car and uses remote control from his phone also for charging, he is concerned that this application could get hacked, especially if the number of electric cars increases. If hackers have control over the remote control and charge all cars at once, we will have a problem. The major challenge will be all the applications. He does not think that the smart meter will be the main problem. The question is what happens behind the meter, while increasing appliances will have internet connection (like TVs). For example Samsung can switch off all their applications – thus it is hard to control. Not all attacks are unfriendly, but may stem from simple mistakes. He used the example of the converters of SME, which shut off at 50,2 hertz, not at 52 hertz as they should. This programming mistake was only found after 5 years. The fourth challenge mentioned by Mr Schucht is data protection. The costumer is the owner of the data and it must be clear who collects the data. Nobody should be allowed to use the data for additionally businesses. He concluded with the request to the Commission that while the ongoing certification procedures are good, data protection needs more clarification regarding who can use what data and the big question is the growth of de-central devices behind the meter. The political attention needs to focus on this question to raise society awareness and to call upon the market participants to find solutions.

Philippe Monloubou, CEO of ENEDIS, France

Mr Monloubou explained that risk is inclusively adapted to business and the new boarder of our business (compared to 60 year ago) is cyber security. It is not only a threat, but also a huge opportunity. We have to integrate all dimensions of cybersecurity in our business as it is our core business. We need to address cybersecurity from an offensive perspective, not from a defensive one. In France there are 400.000 photovoltaic (PV) generators on the network. The question is to be able to integrate data, data management and IT systems. Why is it our core business? Nowadays, Distribution System Operators (DSOs) are totally involved in real time, thus time-to-market. From a customer point of view, the way the DSO rolls out smart meters, should be the same the DSO addresses cyber security. Thus it is a DSO core business responsibility. As the president of the Smart Grids association, Mr Monloubou emphasised that this is a worldwide challenge. Other countries are waiting for our knowledge, but we have to be fast as there are also many competitors. We have to address the topic very quickly. We need new skills, certification, innovation, cooperation and talents to be able to address these new markets. Mr Monloubou stated that cyber security can also create jobs and that it needs to be understood as a part of the core business.

Q&A - Session

Erikson: Certification is one way to ensure more resilience, but it does not solve the whole problem. What about certification and formal device management? Regarding the 400.000

[1] Distributed Denial-of_Service

PV generators in France, would it not be that your main assets coming forward would be an intelligent trusted cloud software, etc. that would control these generators?

Answer: Device management does not solve the problem in itself; it only adds another level as a kind of responsible in-between. There is no clear view yet, how this will look in the future. Certification slightly increases the level, but does not solve it completely. We will need to have more control power and that needs to be as safe as possible, e.g. the internet must be completely separated. At the end of the day, it will be a combination of different measures.

The speakers answered that there is also a challenge of sharing of own generation amongst neighbours. Cloud system could be a solution, because they are better than the existing systems. There will be cloud solutions, but cloud systems are not only a French consideration.

What is the importance of data scientists and modelling? Sharing information in the energy sector like it happens in the aerospace sector and if that would be a solution.

Answer: Sharing information is no question anymore, the awareness is there and we have to address it through innovation. The more IT specialists we have, the more hackers we have as well. "Competition on ideas" was raised as a good example – thus to raise standards, but also leave some ideas.

Symantec: the ability to have access and share the information from outside Europe is extremely critical.

Answer: TSO is implementing a new real time IT from Siemens, also the Californian DSO bought this real time IT. In some places penetration tests are conducted, providing capable hacking teams two weeks to get into the system. This approach means companies are on the right track, but this does not mean that they are 100% protected. IoT also means devices on our own networks.

Conclusions Mr Laurent Schmitt: 2-3 years ago, cyber security was more a R&D innovation topic. This has changed now. Mr Schmitt also raised the importance of having in the near future a cyber security network code, which would be joint for DSOs and TSOs and which would basically fit all IoT devices which are critical for energy and which would clearly define what is a requirement from physical energy security point of view.

Session 2: Energy – Key elements for a Cyber Security Strategy
Stephan Lechner, Director Euratom, Moderator

Hubert Tardieu, CEO advisor at Atos, France

Mr Tardieu presented the technology supplier angle. All systems are taking into account the IT (information Technologies) and the OT (Operation Technologies) world. It is a very serious matter to shut 8 Million of smart meters by an IT command. From purely predictive (where

we still are) we will go progressively into the prescriptive world where we will be able to intervene to the final systems. The first point Mr Tardieu stresses is that distributed architecture is not nice to have, but is becoming a must. As a second point he mentioned that it forces to mix the culture of the IT people and the culture of the OT people. Eventually, the OT people will win because they are closer to the real system.
Atos is working closely with Siemens on a SOC (security operations centre) approach, which they manage now to regroup, meaning that the same security management is applicable to both the IT SOC and the OT SOC.
His recommendation to the European Commission to follow the financial sector regulation with PSD2 to have an open API to provide to the user the kind of services they want using data collected by the account holder. This is a good compromise between respecting what is the ownership of the data and it is giving the role to all customers the "vendor-relationship-management". This is a way to unlock the value of the data.

Bernd Kowalski, Head of Department, BSI, Germany

Mr Kowalski emphasised that regulation plays an important role to push cyber security in all vertical sectors. Germany is one of the first nations that has already implemented the NIS directive, including the energy sector.
Digitalisation and the design of new digital technologies have to be considered before deployment. We cannot control the speed with that new technologies are coming to the market. They have inherent risks which need to get prevented. After the Fukushima accident Germany changed its energy policy in favour or renewables and decided to opt out nuclear energy. Already by that time, there were cyber-attacks to the energy grid and at the same time some countries had problems with privacy issues with their smart meters. Thus the German Government decided to have a very secure design on the smart meters. In December 2016, the German parliament adopted the act on the digitalisation of the energy transition to new energies. Government responsibility is a major concern.
The recommendations to the Commissions are to apply principles of security and privacy by design. There is no time to wait, as afterwards the costs will be higher. It is important not to only implement the NIS directive, but to connect to other existing regulations like the eIDAS regulation. We should also use the existing European standards. This would also be cost-effective. The European Commission should encourage the Member States to set up appropriate regulatory frameworks for the energy systems, to have agreements on basic principles using standards that already exist for long time.
30 years ago, a cyber security certification mechanism was created, but the European Commission forgot about this. Twelve Member States are using cyber security certification mechanisms nowadays and have no interest in a fragmented market. The BSI and the German Ministry would like to support the European Commission in bringing cyber security to the energy system.

Philippe Dewost, Deputy Director Investments for the Future Program @ Caisse des Dépôts, France

Mr Dewost invests approximately €3 billion of French taxpayer's money (through the Investments for The Future Program) in digital economy, and raised since 2013 interest in digital sovereignty, cyber security, and related “deep tech”. Such cyber security and deep tech funds are being currently set up and could be announced soon. He observes that in this digital space, speed is of the essence, and that we hence will not be able to cope with cyber

security challenges if we do not accept the shift from centering cooperations around the most powerful (measured by relative GDP or population weight), to following the fast and nimble runners when it comes to structuring joint initiatives. He then noted that decentralisation is a key and core force in technology development : IT is shifting from the core to the edges, Blockchain technologies allows decentralization of transactions and assets tracking, while security now combines thickening dungeon walls with detecting and filling breaches as fast as possible and even sometimes from "outside" the systems: a recommendation to the European Commission could be thus to change the approach legally framing hackers turned into "white hats" and securing their legal. The second advice he gave is to think exponential at any decision level as Moore's Law always leads us to overestimate the short term and underestimate the mid/long term when designing cybersecurity policies especially for IoT and industrial systems. Thirdly, we should no longer be naïve: cybersecurity often relies on mastering the full stack down to the silicon as evidenced by Russian and Chinese efforts to regain independence in terms of chip design. Hardware and microchip development could be mastered by Europe especially if we leverage Open Source architectures such as Risc-V. Regarding cyber security and energy infrastructures, he acknowledged this joint DG Energy / DG CNCT approach as these two domains can no longer remain disjointed, and raised Blockchain as an example and promising technology for operating and securing transactions across microgrids. His final recommendation was to invest in research and development, like blockchain or homomorphic encryption, and to visibly recognize such fields as EU wide sovereign priorities. He estimated that approximately €500 M of R&D funding should be allocated to Blockchain research over the next 3 years, combined with an equivalent €500 M to be deployed through investment vehicles in European Blockchain startups.

Q&A – session:

1) How far can we do a one-size-fits-all approach in terms of certification?
Mr Tardieu answered that there is no difference on what is going on in real time prescriptive analytics and the security platform.
2) Is there any complementing activity in any other EU Member State regarding financial funding?
Mr Dewost answered that there are lots of talents across Europe even if you leave the UK out. We should however pick and choose our battles, thus we should go together – overcome competition issues and learn from each other's best practices in Europe: a national approach will not be sufficient when it comes to compete with the other major world powers. Regarding all the public investments efforts that have been driven in high tech startups including security, these will pay (and be repaid to taxpayers) only if there are, within the next 2-3 years, solid and deep enough exit markets for the best of these tech companies ; exits markets mean both corporate exits and stock markets. Should these conditions not be met in time, we will have to rely on trade sales with non EU acquirers which could result on seeing the best talents leave EU.
3) Mrs Spanou emphasised that the European Commission has not forgotten of certification and is currently working on it.
4) Luigi Rebuffi presented ECSO and the cPPP (contractual Public-Private-Partnership on cyber security).
5) Accenture: What is your point of view that people far away from the market work on frameworks?

Answer: We need education also at CEO level. The workshop on Economy of data was mentioned and we need to be able to explain the concept to our CEOs.
6) Bto: Does it make more sense to cooperate more?
Answer: It is not about the regulation, but who is enforcing the regulation. Talent should always come first, as small teams can make profound changes.

Summary - Stephan Lechner, Director Euratom, Moderator

Mr Lechner summarised the event, underlining that cyber security never stops and we need to stay ahead of the game. He recalled key statements of the speakers: Director General Mr Ristori emphasised that Europe should take the lead and not just follow. Director General Mr Viola said that digital needs energy and energy needs digital. Mr Del Fante told that security needs to be integrated. Mr Bortoni said risk is something that needs to be balanced. Mr Gaiani stressed the international dimension. Mrs Forsi underlined the value of sharing. Mr Lepassaar stated that collaboration is the most important tool. Mr Schucht underlined that viruses could already come from the suppliers and that there are more devices behind the meter moving at a different pace than the part before the meter. The legacy is in and we got all the fast moving digital parts not being able to be formalised certified. The DSO perspective was similar, emphasising that the core business is cyber security. Atos said that we have prescriptive technologies coming in which means IT (information technology) ruling the OT (operations technology) of the grid. Mr Kowalski recalled that the technology solutions are already around and cyber security in the grid is not a research topic any more. Mr Devost emphasised the speed of digitalisation,
Mr Lechner stated that security is a process, and that the issue of cyber security is here to stay. To conclude he identified three findings: firstly, the energy sector has its particularities. In our energy networks, traditional industrial control systems are being more and more connected, exposing them to new cyber threats. In addition, new and smart technologies are pushing in at the consumer end, and not all of them are designed with cyber security in mind. This combination of legacy and future technologies requires specific solutions in the energy system that cannot be copied from other areas with different needs (e.g. the internet). A concrete action on certification was also called.
Secondly, we need to realise the importance of information technology suppliers. Both, power grid operators and consumers are bound to information technologies that are typically not produced by themselves, and very often originate from outside Europe (US, South-East Asia). Suppliers of information technologies to the EU energy system must be bound to clear obligations to provide their products and services at a well-defined, high level of cyber security. Thirdly, we need to strike a good balance between cyber security, data protection and economic growth. Cyber security is not a purpose of its own, but is required to create business opportunities, jobs and growth. Cyber security and data protection requirements must not hinder innovation or prevent businesses from settling in Europe, as data analysis is at the core of the future automated and smart energy system. The European market must be secure without decreasing competitiveness or banning business models based on big data analysis.

Mr Dominique Ristori, European Commission Director-General for Energy and Mr Roberto Viola, European Commission Director-General for Communications Networks, Content & Technology closed the meeting.