CYBERSPACE, ENERGY & DEVELOPMENT: Protecting Critical Energy Infrastructure

October 10, 2014
Popov Room, ITU Headquarters, Geneva
(Update: 11 September 2014)

This one day international conference will be co-organized and co-hosted by the ITU and Energy Pact Foundation with the support of the International Atomic Energy Agency (IAEA) and the World Economic Forum (WEF). The conference will focus on the different aspects of the interaction of cyberspace, energy & development based, on key findings on security issues.

There is a need for greater international cooperation among nations regarding cyberspace especially concerning the risks related to critical infrastructure such as conventional energy systems. The early initiatives in this area have mainly focused on the safety of telecommunication and information networks, as these are the very infrastructure of cyberspace. However, if a cyber-attack were to result in the deterioration in the supply of electricity, it could also impair the operational protection of the telecommunications infrastructure at large. Apart from this ubiquitous role of the electricity system, itself unique compared to all other critical infrastructures, many areas of energy systems are exposed to damage originated in cyberspace, and include energy mining and production centres, logistics or trading platforms, transport infrastructures of primary resources, such as oil, gas and coal, or processed electricity, such as smart grids, processing units, such as for uranium, consumption meters, such as smart metering, control systems, such as drones and e-mobility environments, including electric cars.

Obviously, the stakes go well beyond ensuring the security of supply, and also involve the constantly shifting national and transnational flows of resources and power grids, the potential damaging of key infrastructures, market impacts, the theft of general as well as customer data and other dormant risks. This interaction of risk issues between cyberspace and energy is in fact the umbrella under which effective cyber security should be designed for such critical infrastructure. It requires an exchange between the national level, responsible for critical domestic infrastructures, and the international level, as the extreme inter-connectedness in the telecommunications industry and in that of electricity infrastructures will only increase over time. Furthermore, taking into consideration the interaction between cyberspace and energy is a prerequisite for effective and safe economic development.

A dialogue for building consensus: from awareness to action

The program of this conference will focus on policy and strategic issues, and is intended for all stakeholders working in the area including governments, private sector, civil society and international organizations.

Because of their growing connection to cyberspace, the protection of critical infrastructures requires new relations between national and international realms. Crisis management has undergone fundamental change, as can be seen from the conduct of a number of recent international operations. This feedback from the latter, as well as from the various cyber-attacks carried out between 2000 and 2013, which have assaulted energy infrastructures several times, has generated

new needs for cooperation, with the intrinsic difficulty of protecting national interests, all whilst pooling international resources.

Rules and standards limited to the interoperability of equipment and organisations are not sufficient in order to deal with cyber-attacks on energy systems. This is mainly due to differences of conceptual strategic and perspectives leading to the choice of potential rules and standards, as to preserve a cyber-ecosystem representing a market of several trillion dollars, that focuses on swift globalisation of connectivity. In this context, how can government departments, national or regional cooperate to ensure a comprehensive management of the significant risks generated by cyberspace to critical infrastructure such as energy infrastructure? What should be the allocation of roles and responsibilities between different stakeholders, globally as well as regionally, to protect energy infrastructures along with the protection of telecommunication industry infrastructures? Would these solutions be resilient enough if all countries linked to cross border infrastructures are not involved in the process of cooperation?

Agenda

9:00- 10:00 - Coffee

10:00 – 11:30 - Official Opening and Introductive Key Note Speeches

11:30– 13:00 - Session 1

Cyber space and critical energy infrastructure protection: national and international strategies

It is vital to a nation's interests and socio-economic wellbeing that its critical energy infrastructure must be secure, resilient to threats, and also have the ability to recover from any attacks. With the increasing reliance on ICTs by designers of such critical infrastructure systems, and therefore the convergence of physical and digital security concerns, security concerns can emerge at national, regional and international levels. Therefore, key questions include - what safeguards are needed at these levels, especially in terms of improved cooperation frameworks? What are the hurdles to establishing these safeguards, and what are the related mitigation measures?

Supporting Organization: International Atomic Energy Agency (IAEA)

13:00 – 14:30 - Lunch

14:30 – 15:45 - Session 2

Priority public-private partnerships in the fight against cyber threats to critical energy infrastructures

Although the protection of critical infrastructures and related public/private coordination are a national responsibility, cyber security requires a comprehensive inventory of them at the regional level, even if the national/regional distinction is not always easily achieved, as deregulation has widely encouraged mergers and cross-border cooperation between private operators. Beyond such an inventory, the implementation of a transnational cyber security cooperation framework is vital, when it comes to critical infrastructure such as energy systems. The transnational nature of energy systems is itself justified by other vital needs, such as securing supplies and regional market integration. These critical infrastructures are therefore prime targets for cyber-attacks, potentially threatening people's lives and endangering national economies. This could be most damaging, as the impact could transcend industry sectors and spill over a country's borders. Hence, public/private partnerships are necessary for the design and management of a systemic approach in order to ensure a sustainable defence in the face of cyber-attacks on cross border infrastructures. Especially so as the maintenance of security is more difficult to achieve in the context of overlapping public/private responsibilities, interdependent centralised/decentralised issues and crisis management which is both the responsibility of civil society as well as of governments. But how is all this to be prioritised?

Supporting Organization: World Economic Forum (WEF)

15:45 – 17:00 - Session 3

Protecting the energy ecosystem: Designing and managing technology for critical energy infrastructure

Energy infrastructure is composed of complex industrial environments usually underpinned by ICT systems (Industrial control systems or ICS), sometimes not designed with security in mind. While the use of ICTs in operating critical systems such as power control enables better management and increased productivity, it also creates new sources of vulnerabilities and potential exploits that can be used for targeted cyber-attacks. Since the energy sector is so diverse, ensuring business continuity and securing control systems is not a simple matter. As technology evolves, so does the sophistication in exploiting the vulnerabilities. For example, corrupted information sent by intelligent electronic devices or remote terminal units could affect negatively the processes related to energy provision. Denial of Service attacks would cause loss of availability and generate unacceptable delays and down time for critical energy services and related infrastructures, such as the power grids.

Cybersecurity for the energy sector therefore requires the use of preventive and reactive security measures as well as the deployment of capabilities to proactively manage the risks. *How can the technology sector contribute to managing risks in the energy infrastructure?*

Standardization has a key role to play and some standards already directly address industrial control system security, but these need to be pushed for wider adoption at the industry level. *What role can Standards Development Organizations play in this regard? What steps need to be taken to ensure the interoperability of products and services from the early design stage?*

17:00-17:30 – Official Closing

17:30 onwards – Cocktails