DRAFT

EUROPE INTEGRATION FOREIGN AFFAIRS
FEDERAL MINISTRY
REPUBLIC OF AUSTRIA

energypact

FEDERAL MINISTRY OF DEFENCE AND SPORTS

International Multistakeholder Conference

CYBERSPACE, ENERGY & DEVELOPMENT

Protecting Critical Energy Infrastructure

February 16, 2017

CSP AUSTRIA

National Defence Academy
Vienna

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

supported by

IEC

UNODC
United Nations Office on Drugs and Crime

ITU

Cyberspace, Energy & Development Protecting Critical Energy Infrastructure

This international conference will be co-organized with the Federal Ministry for Europe, Integration and Foreign Affairs of Austria, the Federal Ministry of Defence and Sports of Austria, the AIT Austrian Institute of Technology, the CSP Austrian Cybersecurity Platform and the EnergyPact Foundation and hosted by the Austrian National Defence Academy.

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 clear 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 underlying infrastructure of cyberspace. However, if a cyberattack were to result in the deterioration in the supply of energy means such as electricity, it could also impair the availability of other critical infrastructures like telecommunications, finance, health, transport, etc. Many areas of energy systems are exposed to damage originated in cyberspace, and include energy mining and production centers, 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 the potential damaging of key infrastructures, market impacts, the theft of 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. Cybersecurity, just like Energy and Telecommunications are cross-border topics and therefore require exchange and cooperation between the national level and the international level, as well as cross-industries. This interaction is a prerequisite for safe and sustainable economic development.

Session 1

International Dialogue: Promoting Awareness and Collaboration in the Energy Sector

It is vital to a State's interests and socio-economic wellbeing that its critical energy infrastructure is secure, resilient to threats, and also has the ability to recover from attack. The increasing reliance on digital technologies within the energy sector has resulted in the convergence of both physical and digital security concerns. Energy infrastructure includes a vast array of interconnected systems and multiple levels of interdependence that extend beyond national borders. Security concerns originating in one State may indeed have international consequence. An attack against digital systems of a State's energy infrastructure could provide indication of pending attack or vulnerabilities within other States' infrastructure. Likewise such an attack could have political and socio-economic consequence across an entire international industry. This session will engage international/national leadership and senior level experts in discussing the key challenges but also strategies and good practices for promoting information sharing, confidence building, and partnerships in enhancing energy sector sustainability and resilience to cyber threats. It seeks to leverage experiences and good practices from multiple energy sector constituents: fossil fuels, nuclear, and renewables.

Session 2

Developing capacity in the fight against cyber threats to critical energy infrastructure

Countries are putting special emphasis on the importance of human capacity development in their national critical information infrastructure protection programmes. The lack of sufficient human capacity in the form of trained computer security professionals increasingly has become a pressing issue for all critical infrastructure sectors. The energy sector is further challenged to find security experts that understand the operational environment of energy networks as well as industrial control systems specific to the energy industries including oil, gas, nuclear and renewable. This shortage, while prevalent in both developed and developing countries, is felt particularly acutely in the latter, thus putting them at a greater risk. This session examines these challenges, but also looks at the strategies for human capacity development within the energy sector, especially in developing countries, to support greater security awareness and skill sets.

Session 3

Public Private Partnerships for Sustainable and Secure Critical Energy Infrastructure

Energy infrastructure is composed of complex network of stakeholders that include government authorities, business investors, facility operators, technology providers, network operators, service providers, technical support organizations, contracted parties and end users. Stakeholders often additionally exist across international boundaries. Developing and implementing a sustainable and secure environment for the energy sector cannot be achieved without the involvement of all stakeholders. Further, much can be learned from the lessons of other critical infrastructure sectors in implementing security across cyberspace. Hence, public/private partnerships are necessary for the design and management of a systemic security approach in the face of cyber-attacks on national and cross-border infrastructures. This session provides discussion on the role and contributions of the different stakeholders of Public Private Partnerships in enhancing energy sector security and sustainability.