VIENNA CYBER SECURITY WEEK 2018

Protecting Critical Energy Infrastructure

International Multistakeholder Conference, Training & Exhibition
29 January – 02 February

Jointly organized by the Austrian and international governmental and non-governmental partners and the Energypact Foundation

The second edition of Vienna Cyber Security Week will be held at the Diplomatic Academy in Vienna, from 29 January to 02 February 2018. This annual event aims to engage with key national and international stakeholders in dialogue and cooperation in the field of cyber security for critical infrastructure with a focus on the energy sector. A five-day event will offer a unique forum for both governmental and non-governmental partners to delve into substantive debates over the protection of critical energy infrastructure, combating cybercrime and terrorism, cyber diplomacy and the future of technologic development in the energy sector.

DAY 1 January 29	DAY 2 January 30	DAY 3 January 31	DAY 4 February 01	DAY 5 February 02
PROTECTING ENERGY INFRASTRUCURE AGAINST CYBER CRIME AND TERRORISM	SAFEGUARDING CRITICAL ENERGY INFRASTRUCTURE IN CONTEXT OF REGIONAL AND GLOBAL SECURITY: POLITICAL AND STRATEGIC ASPECTS		SECURING ENERGY ECONOMY: OIL, GAS, ELECTRICITY & NUCLEAR	SECURING SMART CITIES AND EMERGING TECHNOLOGIES

CONFERENCE DAY 1:
PROTECTING ENERGY INFRASTRUCURE AGAINST CYBERCRIME AND TERRORISM

The growing availability of hackers for hire, zero days exploits for sale, availability of hacking toolkits, and the possibility of buying attacks as a service generate a new economy for criminals and terrorists, thus raising the likelihood of sophisticated attacks on our digitalized infrastructures. Based on this trend the lines between these group and their interactions are often blurred and malicious cyber acts are rarely limited by sovereign borders. Thus, information sharing and international governmental action along with strong national frameworks are paramount to developing deterrence, protection, and response measures to counter malicious cyber acts against energy infrastructure.

CONFERENCE DAY 2 & DAY 3:
SAFEGUARDING CRITICAL ENERGY INFRASTRUCTURE IN THE CONTEXT OF REGIONAL AND GLOBAL SECURITY: POLITICAL AND STRATEGIC ASPECTS

Given the importance of critical energy infrastructure to national prosperity and security, as well as an increasing reliance on information and communications technology (ICT) to run them, the likelihood of tensions arising between states over cyber incidents involving them is rising. Consequently, efforts to enhance cyber stability between states, which can prevent tensions and even conflicts, must focus on effectively protecting critical energy infrastructure from cyber/ICT security threats. Exploring the potential threats to critical energy infrastructure and the impact on regional and international peace and security as well as effective mechanisms and processes in the political and strategic sphere to prevent the escalation of events, will be key topics of Day 2 and Day 3 of the Vienna Cyber Security Week 2018.

CONFERENCE DAY 4:
SECURING THE ENERGY ECONOMY: OIL, GAS, ELECTRICITY & NUCLEAR

Low and zero-carbon energy generation represents a diverse collection of technologies including but not limited to solar, wind, geothermal, hydro, and nuclear. While individual energy sources rely on unique technologies, they are also often bound by similar equipment and components. Day 4 of the conference will examine the cyber security of not only power generation, but also of energy management and transmission through “smart grids.” The infrastructure that supports agile and dynamic energy production, distribution, and consumption of energy on a micro-scale basis will present a core topic in terms of skills, processes, and common strategies for a more sustainable energy economy.

CONFERENCE DAY 5:
SECURING SMART CITIES AND EMERGING TECHNOLOGIES

More and more elements of everyday life are becoming “smart”, whereby devices are incorporating functions of sensing, actuation, control, and communication to support predictive or adaptive decision making. The Internet of Things (IoT) architectures, consumer devices, and consumer control functions require new approaches to building resilient systems for our society. Examining cyber risks and consequences for state-of-the-art technologies and promising research will be on the agenda for the last day of Vienna Cyber Security Week 2018.