VIENNA CYBER SECURITY WEEK 2018

Protecting Critical Energy Infrastructure

International Multistakeholder Conference, Training & Exhibition

diplomatische akademie wien
Vienna School of International Studies
École des Hautes Études Internationales de Vienne

SECURITY & DIPLOMACY
29 - 30 January

TECHGATE

ENERGY, TECHNOLOGY & SECURITY
31 January - 02 February

SECURITY & DIPLOMACY		ENERGY, TECHNOLOGY & SECURITY		
DAY 1	DAY 2	DAY 3	DAY 4	DAY 5
CYBERSECURITY FOR CRITICAL (ENERGY) INFRASTRUCTURE: A GLOBAL CHALLENGE	**SAFEGUARDING CRITICAL ENERGY INFRASTRUCTURE IN THE CONTEXT OF REGIONAL AND GLOBAL SECURITY: STRATEGIC AND DIPLOMATIC ASPECTS**	**TRENDS IN TECHNOLOGY AND CYBERSECURITY**	**SECURING ENERGY ECONOMY: OIL, GAS, ELECTRICITY & NUCLEAR**	**SECURING SMART CITIES AND EMERGING TECHNOLOGIES**
Official opening	Session 1: Operational considerations for responding to the threat of cyber-attacks on critical energy infrastructure	Cyber Range Tutorial: Concept, Demonstration, Exercises, Training and the Cyber Research Project	Session 1: Emerging and Future Threats to Digitalized Energy Systems	Session 1: Making Smart Cities Cyber Secure
Session 1: Implementing the EU Strategy for Safe, Open and Secure Cyberspace	Session 2: Reducing the Risks of Conflict Stemming from the Use of Cyber-Capabilities	Cyber Security Cluster Austria (CSCA) Day 2018: Exhibition on leading-edge cybersecurity technologies	Session 2: Cybersecurity Standards in Critical Energy Infrastructure	Session 2: Austrian IoT Safety & Security light house initiatives
Session 2: Cyber-Threats to Critical Energy Infrastructure	Session 3: Cyber-Diplomacy: Developing Capacity and Trust Between States	Reception of the organizers of the CSCA Day 2018	Session 3: Cybersecurity & Resilience in Transport Infrastructure	Session 3: The Promise and Challenge of New Technologies
	Concluding Statements		Session 4: Public sector, industry, and research cooperation in cybersecurity	Concluding Statements
Diplomatic Academy of Vienna 15A Favoritenstraße, 1040 Vienna U1 Taubstummengasse		Tech Gate Vienna 1 Donau-City-Straße, 1220 Vienna U1 Kaisermühlen VIC		

The second edition of Vienna Cybersecurity Week will be held 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 cybersecurity 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, cyber-diplomacy and the future of technologic development in the energy sector.

DAY 1 - January 29

CYBERSECURITY FOR CRITICAL (ENERGY) INFRASTRUCTURE: A GLOBAL CHALLENGE

The growing availability of hackers for hire, zero days exploits for sale, 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 infrastructure. Based on this trend, the lines between these groups and their interactions are often blurred. Further, malicious cyber-acts are rarely limited by sovereign borders. Thus, information sharing and international action along with strong national frameworks are paramount to developing deterrence, protection, and response measures to counter malicious cyber-acts against energy infrastructure.

Session 1:
Implementing the EU Strategy for Safe, Open and Secure Cyberspace

In September 2017 the European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy published the joint communication "*Deterrence and defence: Building strong cybersecurity for the EU*", taking stock of the implementation of the EU's Cybersecurity Strategy "*An Open, Safe and Secure Cyberspace*". Welcoming this communication the Council of the EU called in November 2017, for the strengthening of European cybersecurity and enhancing cyber-resilience across the EU, i.a. by formation of a European research and competency Centre for Cybersecurity; the establishment of a Europe-wide crisis-response mechanism to deal with future large scale cyber-attacks and the creation of a cybersecurity emergency fund and the development of common projects in military cyber-defence.
This session will address the progress made by the EU and its member states in achieving cyber-resilience, reducing cyber-crime, developing cyber defence policy and capabilities and industrial and technological resources for cybersecurity as well as establishing a coherent international cyberspace policy for the European Union and promoting core EU values.

Session 2:
Cyber-Threats to Critical Energy Infrastructure

The protection of critical energy infrastructure against cyber-attacks is a process and not a single endpoint. The protection involves elements of prevention, mitigation, detection, and response.
As the migration towards digital technologies continues, infrastructure owners must seek to enhance protection, but also greater resilience in systems against the impact of cyber-attacks. Enhancing resilience within a multi-stakeholder environment is the topic of this session. Specific areas of interest include:

- Governments, private sector and civil society measures to prevent cyber-crime and terrorism
- Security challenges that new technologies introduce and possible solutions
- National and international strategies and initiatives for protecting critical infrastructure against cyber-attacks
- Tools and techniques for risk monitoring and management that have been proven to be effective
- Experiences in cyber-exercises as an efficient tool to test and improve the resilience of critical information infrastructure

DAY 2 - January 30

SAFEGUARDING CRITICAL ENERGY INFRASTRUCTURE IN THE CONTEXT OF REGIONAL AND GLOBAL SECURITY: STRATEGIC AND DIPLOMATIC 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 of the Vienna Cybersecurity Week 2018.

Session 1:
Operational considerations for responding to the threat of cyber-attacks on critical energy infrastructure

The threat of cyber-attack continues to grow as potential adversaries continue to develop or acquire cyber skills. In this environment, how do States and organizations address a dynamic cyber-threat, specifically:

- What measures can be taken to reduce or contain the cyber-threat? How can response to the growing threat be organized and implemented?
- What are the roles and responsibilities of national stakeholders and critical infrastructure owners and operators?
- What is the role and capability of international organizations of mitigating such threats?
- What additional resources are needed?

Session 2:
Reducing the Risks of Conflict Stemming from the Use of Cyber-Capabilities

Cyberspace and consequently cyber-attacks are not limited by national borders. The cross-border nature of many attacks and the often limited ability to positively identify the responsible attacker may result in friction between States. International instruments and measures can assist in promoting uniform and predictable response that may assist in preventing undesired side effects including conflict escalation. This session will examine among other areas,

- The role of international legal frameworks in promoting cyber-stability between States;
- Processes to reliably establish attribution and identify proportionate countermeasures;
- Methods to ensure crisis communication on cybersecurity incidents is possible on all levels of authority including both policy and technical representation; and Mediation between States in the case of cyber-conflict

Session 3:
Cyber-Diplomacy: Developing Capacity and Trust Between States

This session examines the need for confidence building and information-sharing between States with regards to cyber-incidents, especially those with cross broader implications. While national interest will always dictate information-sharing limitations, meaningful discussion and exchange between States can be achieved for enhancing cybersecurity of energy infrastructure globally. Areas of interest for discussion include but are not limited to:

- Approaches for effective capacity building especially in light of the national security sensitivities regarding critical energy infrastructure
- Perspectives on information sharing from the viewpoint of national security interests
- Potential capacity builders: who are they and how to engage with them?

DAY 3 - January 31

TRENDS IN TECHNOLOGY AND CYBERSECURITY

On this day the organizers of the Vienna Cybersecurity Week 2018 host cyber range tutorials and the Cyber Security Cluster Austria (CSCA) Day 2018. The cyber range tutorials offer insight into the hot topic of cyber ranges and showcase the CSCA Day 2018, a cybersecurity exhibition on the latest technology.

Cyber Range Tutorial:
Concept, Demonstration, Exercises, Training and the Cyber Research Project

The Cyber Range Tutorials introduce into the concept of cyber ranges and how they improve cybersecurity capabilities. Three cyber range case studies will be presented by giving an indication of how they are beneficial to an organization. Further, an example threat scenario will be presented, which can be realized on a cyber range and used for training and exercises. Finally, the cyber range tutorials showcase how the AIT cyber range is being used to support research activities in the IAEA Cooperative Research Project (CRP) on computer security incident response and analysis.

Cyber Security Cluster Austria Day 2018:
Exhibition on leading-edge cyber security technologies

Within the course of the Vienna Cybersecurity Week 2018, AIT Austrian Institute of Technology together with WKO Austrian Economic Chamber, ASW Austrian Defense and Security Industry, and the Austrian Cyber Security Cluster invite to a technology exhibition of latest solutions and products as well as R&D projects. Visitors have the opportunity to see state-of-the-art of next generation solutions and meet key experts in the field of cybersecurity for protecting critical infrastructure to fight against cyber-crime and -terrorism.

DAY 4 - February 01

SECURING 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.

Session 1:
Emerging and Future Threats to Digitalized Energy Systems

We are in the process of digitalizing our energy systems, be those nuclear facilities, oil refineries, or electrical distribution systems, for example. This digitalization introduces several operational benefits and efficiencies; however, it introduces a much larger cyber-attack surface than ever before. Meanwhile, there is a general trend that cyber-attacks to critical infrastructure are becoming more targeted and sophisticated. Moreover, these attacks are targeting operational and safety-critical systems, using a range of attack techniques. In this session, there will be a discussion regarding the nature of this emerging threat landscape, identifying broad trends that are being seen across the energy sector and elsewhere. Following-on from this discussion, the panel will provide hypotheses about how they see these trends evolving in the future. The aim is to support organizations with their cybersecurity preparedness, by having a sound understanding of the emerging threat landscape.

Session 2:
Cybersecurity Standards in Critical Energy Infrastructure

In response to the need to secure our critical energy infrastructure from cyber-attacks, several cybersecurity standards and guidelines have emerged from organizations such as the IEC, IEEE, ITU-T, and the IAEA. For example, these standards provide specific guidance on how to secure industrial control systems, from conception to operation. An overall aim is that these standards will support organizations to improve their security posture in response to an increasingly sophisticated threat (see the previous session). In this session, the cybersecurity standards landscape will be explored, with the aim of addressing questions, such as are further standards required and in what area; are standards being correctly applied by operators and vendors; in which ways could certification schemes be useful to ensure standards compliance? The aim of the session is to inform session participants about current standards, their state of application in the field, and to identify gaps that need to be addressed in the future.

Session 3:
Cybersecurity and the Resilience in Transport Infrastructure

Digitalization is not limited to energy systems, but also affects other areas of critical infrastructure. Intelligent public transport, smart transport-hubs or smart cars are increasingly becoming part of the daily lives of millions of citizens. This session will look at cybersecurity in the area of transport infrastructure by exploring their commonalities. This includes an analysis of critical assets threats, of liabilities, and of safety and security process integration. This will be done in relation to technical standards, information sharing processes among different actors and regarding security by design with other areas of critical infrastructure.

Session 4:
Public Sector, Industry, and Research Cooperation in Cybersecurity

This session focuses on the interrelations between European, international and national research programs and efforts, and how they are intertwined with the interactions of industries and the public-sector stake holders in critical infrastructure cyberspace security. The session will give insights into the EU´s Horizon 2020 and FP9 project, Austria´s efforts in FFG and Kiras, including discussions on defence and the future of funding.

DAY 5 - February 02

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 Cybersecurity Week 2018.

Session 1:
Making Smart Cities Cyber Secure

This session examines the challenges and strategies for building protection and resilience in smart cities against cyber-attacks. Smart cities integrate numerous technologies to create advanced and more efficient processes for accomplishing everyday tasks. At the same time this creates a target rich environment for cyber-attacks. Topics of interest include:

- Threats and vulnerabilities of smart cities
- Engineering security – how to build more resilient systems
- Detection and response – what to do when under attack

Session 2:
Austrian IoT Safety & Security light house initiatives

Austrian industry and research institutions are on the technological forefront in cyberspace. This session offers an insight in some national best practice topics and projects in these terrains.

Session 3:
The Promise and Challenge of New Technologies

The development and integration of new digital technologies and software continues at a rapid pace. This session examines the value and impact of new technology trends from a cybersecurity prospective. Discussion in this session will centre on:

- Projected trends and emerging areas of technology
- Approaches and methods for verifying and securing new technologies
- State of the art and future security designs, methods, and tools
- The future of cyber-threats