


VIENNA CYBER SECURITY WEEK 2018

Protecting Critical Energy Infrastructure


International Multi-stakeholder Conference, Training & Exhibition



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

SECURITY & DIPLOMACY
29 - 30 January
15A Favoritenstraße, 1040
 Taubstummengasse



ENERGY, TECHNOLOGY & SECURITY
31 January - 02 February
1 Donau-City-Straße, 1220
 Kaisermühlen VIC

Program

Monday - 29 January

Diplomatic Academy of Vienna

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 infrastructures. 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.

08:45 – 09:30 Coffee & Registration

09:30 – 11:00 Official Opening

11:00 – 11:30 Coffee break

11:30 – 13:15 Session 1: Implementing the EU Strategy for Safe, Open and Secure Cyberspace

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.

13:15 – 14:45 Lunch

14:45 – 15:15 Special Session: Austrian Cyber Security Exercise

15:15 – 16:45 Session 2: Cyber-Threats to Critical Energy Infrastructure

The topic of this session focuses on enhancing critical infrastructure resilience within a multi-stakeholder environment. Specific areas of interest include:

- Security challenges that new technologies introduce and possible solutions
- National and international strategies and initiatives for protecting critical infrastructure against cyber-attacks
- Experiences in cyber-exercises as an efficient tool to test and improve the resilience of critical information infrastructure

Tuesday - 30 January Diplomatic Academy of Vienna

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 Cyber Security Week 2018.

08:45 – 09:30 Coffee

09:30 – 11:00 Session 1: Operational considerations for responding to the threat of cyber-attacks on critical energy infrastructure

The threat of cyber-attacks continues to grow as potential adversaries continue to develop or acquire new cyber-skills. In this environment, how should 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?

11:00 – 11:15 Coffee break

11:15 – 12:45 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 limited ability to 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.

12:45 – 14:15 Lunch break

14:15 – 14:30 Special Session: Securing the future together

What does the current trend in threats, attackers and cybercrime tell us? Where would we want to be in a few years? In a decade? What concrete initiatives could we design today to ensure the knowledge and the capabilities to protect critical infrastructure from cyber-attacks exist and is available to the relevant stakeholders?

14:30 – 16:15 Session 3: Cyber-Diplomacy: Developing Capacity and Trust Between States

This session examines the need for confidence building and information sharing among States in regards to cyber-incidents, especially those with cross-border implications. While national interest will always dictate information-sharing limitations, meaningful discussions and exchanges between States can be achieved in order to enhance the cybersecurity of the global energy infrastructure.

Closing Remarks 16:15-16:30

**Wednesday - 31 January
Tech Gate**

TRENDS IN TECHNOLOGY AND CYBER SECURITY

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

[Cyber Range and Policy Table Top Tutorial: Concept, Demonstration, Exercises, Training and the Cyber Research Project](#)

The Cyber Range Tutorials introduce into the concept of cyber ranges and cyber security policies and how they improve cyber security 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.

10:00 – 12:00	Cyber Range Tutorial	Policy Table Top Tutorial
10:00 – 10:30	Introduction into the Cyber Range (CR) Concept	<p style="text-align: center;">10:00 – 12:00</p> <p>A mini tutorial/training on designing security policy – organized by the Energypact.</p>
10:30 – 10:45	CR Case Study – Training: – CR supporting IAEA programs	
10:45 – 11:00	CR Case Study – Exercises: – Austrian cyber exercises	
11:00 – 11:15	CR Case Study - Research (CRP – IAEA): Analysis & response	
11:15 – 12:00	CR Scenario Demonstration: Attacks to energy systems	

12:00 – 13:00 Lunch for the participants of Cyber Range and Policy Table Top Tutorials

Exhibition on leading-edge cyber security technologies

Within the course of the Vienna Cyber Security Week 2018, AIT Austrian Institute of Technology together with WKO Austrian Economic Chambers, 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 cyber security for protecting critical infrastructures to fight against cyber-crime and terrorism.

Cyber Security Cluster Austria Day (CSCA) 2018 – Technology Expo		
13:00	Opening of the CSCA Day – Technology Expo 2018	
13:00 – 17:00	Registration	Sign-up for sessions on Thu 01 Feb & Wed 02 Feb at CSCA Day site at Tech Gate
15:00 – open end	Reception	Official welcome by the VCSW 2018 organizers
16:30 – 17:00	Presentation on Offensive Security Testing	

Thursday - 1 February

Tech Gate

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.

08:30 – 09:00 Coffee & Registration

09:00 – 10:30 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. Digitalization introduces several operational benefits and efficiencies; however, it introduces a much larger cyber-attack surface. Cyber-attacks to critical infrastructures are becoming more targeted and sophisticated and they are targeting operational and safety-critical systems, using a range of attack techniques. In this session, we will talk about the nature of the emerging threat landscape, identifying broad trends that are being seen across the energy sector and elsewhere.

10:30 – 11:00 Coffee Break

11:00 – 12:30 Session 2: Cyber Security Standards in Critical Energy Infrastructure

In this session, the cyber security 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.

12:30 – 13:30 Lunch

13:30 – 14:30 Session 3: Public Sector, Industry, and Research Cooperation in Cyber Security

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 stakeholders in critical infrastructure cyberspace security.

14:30 – 15:00 Coffee Break

15:00 – 16:45 Session 4: Securing Critical Energy Infrastructures by Understanding Global Energy Markets

In order to understand how to implement the necessary cyber policies and cyber technologies to protect critical energy infrastructures, it is key to understand how the global energy markets work. In this session, energy experts give a short overview on the stakeholders and the markets of global energy.

16:45 – 17:00 Closing Remarks

Friday - 2 February

Tech Gate

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.

09:15 - 09:45 **Welcome Speeches**

09:45 – 11:00 **Session 1: Making Smart Cities Cyber Secure**

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. This session examines the challenges and strategies for building resilient smart cities. 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

11:00 – 11:30 **Coffee Break**

11:30 – 12:30 **Session 2: Austrian & International 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.

12:30 – 13:30 **Lunch**

13:30 – 15:30 **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 focus 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 the cyber threat

15:30-16:00 **Closing Statements**

With the support of



With courtesy of

