energypact

VIENNA CYBER SECURITY WEEK 2018

Protecting Critical Energy Infrastructure

International Multi-stakeholder Conference, Training & Exhibition

SECURITY & DIPLOMACY
29 - 30 January

ENERGY, TECHNOLOGY & SECURITY
31 January - 02 February

With the support of

With courtesy of

VIENNA CYBER SECURITY WEEK 2018

PROGRAM

Speakers by speaking order

29 January 2018

Philipp Agathonos	Minister Plenipotentiary, Austrian Federal Ministry of Europe, Integration and Foreign Affairs

H.E. Emil Brix	Ambassador, Director, Diplomatic Academy of Vienna
H.E. Svetoslav Spassov	Ambassador, Permanent Representative of the Republic of Bulgaria to the United Nations, the Organization for Security and Cooperation in Europe and the other International Organisations in Vienna, Austria
Alexandre Dimitrijevic	President and Executive Director, Energypact Foundation
Helmut Leopold	Head of Center for Digital Safety & Security, AIT, Austrian Institute of Technology
Rudolf Thaler	Regional Manager Africa and Middle East, Advantage Austria / WKÖ Aussenwirtschaft Österreich
Thomas Stubbings	Chairman, Cybersecurity Platform of the Austrian Government, CSP
Isa Ghivarelli	Counsellor, Deputy Head of Delegation for the Politico-Military Dimension, Permanent Mission of Italy to OSCE, 2018 Italian OSCE Chairmanship
Jaroslaw Ponder	Head of the Office for Europe, International Telecommunication Union, ITU
Senol Yilmaz	Cybersecurity Programme Manager, UN Office of Counterterrorism, **Statement on behalf of Vladimir Voronkov** Under Secretary General, United Nations Office of Counterterrorism, New York
H.E.M. Faouzia Boumaïza Mebarki	Ambassador of Algeria to Austria and Permanent Representative to the International Organisations in Vienna
Wolfgang Ebner	Deputy Directorate-General, Austrian Federal Ministry of Digitalisation and Economy
H.E. Friedhelm Frischenschlager	Former Austrian Federal Minister of Defence and Former MEP, Vice President, Energypact Foundation
H.E. Zoran Predić	State Secretary, Ministry of Energy and Mining, Republic of Serbia

Matthias Grabner	Special Announcement B2B Advantage Austria / WKÖ Aussenwirtschaft Österreich

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.	
Reinhard Posch	CIO, Federal Government of Austria
Stephan Lechner	Director, EURATOM Safeguards Directorate-General for Energy, European Commission
Ioannis Vrailas	Ambassador, EU Delegation to the OSCE
Luigi Rebuffi	Secretary General, European Cyber Security Organisation, ESCO
Marie Holzleitner	Researcher, Energieinstitut, JK Universität Linz
Peter Gridling	Director, Austrian Federal Agency of State Protection and Counter Terrorism, Austrian Federal Ministry of the Interior

13:15 – 14:45 Lunch

14:45 – 15:15	SPECIAL SESSION: AUSTRIAN CYBER SECURITY EXERCISE
Alexander Janda	Secretary General, Kuratorium Sicheres Österreich, KSÖ

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	
Svetoslav Spassov	Ambassador, Permanent Mission of Bulgaria to the OSCE
Pavol Adamec	Director, KPMG Slovakia
Kurt Hager	Head of Department for Security Policy, Austrian Ministry of the Interior
Don Dudenhoeffer	Senior Information Security Officer, International Atomic Energy Agency, IAEA
Thomas Stubbings	Chairman, Cyber Security Platform of the Austrian Government, CSP

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 break

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?

Udo Helmbrecht	Executive Director, European Union Agency for Network and Information Security, ENISA
Peter Deckenbacher	Brigadier General, Deputy Commander, Computer Information Systems & Cyber Defence, Austrian Federal Ministry of Defence
Ralf Mutzke	Senior Manager, KPMG Austria
Preetam Maloor	Strategy and Policy Advisor, International Telecommunication Union, ITU

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.

Ben Hiller	Cyber Security Officer, OSCE Secretariat
Mikhail Konarovskiy	Advisor, Shanghai Cooperation Organisation, SCO
Nemanja Malisevic	Senior Strategist, Microsoft
Andreas Stadler	Minister Plenipotentiary, OSCE Directorate, Austrian Federal Ministry of Europe, Integration and Foreign Affairs
Yazici Deniz	Senior Adviser, Austrian Federal Ministry for Europe, Integration and Foreign Affairs

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?	
Andrea Cavina	Director for Training and Education Development, Energypact Foundation

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.	
Gerhard Jandl	Security Policy Director, Austrian Federal Ministry of Europe, Integration and Foreign Affairs
Hadewych Hazelzet	First Counsellor, EU Delegation to the OSCE, European External Action Service, EEAS
Alison August Treppel	Executive Secretary, Inter-American Committee against Terrorism, Organisation of American States, OAS
Philipp Agathonos	Minister Plenipotentiary, Austrian Embassy of Beijing, Austrian Federal Ministry of Europe, Integration and Foreign Affairs
Roger Bertozzi	Vice President, Energypact Foundation
Alexander Klimburg	Director, Cyber Policy and Resilience Program, The Hague Centre for Strategic Studies, HCSS

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 TUTORIALS:

CONCEPT, DEMONSTRATION, EXERCISES, TRAINING AND THE CYBER RESEARCH PROJECT

10:00 – 12:00	**CYBER RANGE TUTORIAL**
The Cyber Range Tutorial 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 – 10:30	**Introduction into the Cyber Range (CR) Concept:** What are CRs good for? *Maria Leitner, AIT*
10:30 – 10:45	**CR Case Study – *Training:*** CR supporting IAEA programs *Donald Dudenhoeffer, IAEA*
10:45 – 11:00	**CR Case Study – *Exercises:*** Austrian cyber security exercises *Maria Leitner, AIT*
11:00 – 11:15	**CR Case Study - Research (CRP – IAEA):** Analysis & response *Paul Smith, AIT*
11:15 – 12:00	**CR Scenario Demonstration:** Attacks to energy systems *Mislav Findrik, AIT* *Paul Smith, AIT*

10:00 – 12:00	**POLICY TABLE TOP TUTORIAL**
Cyber Security Scenario-based Exercise Developing an effective computer security strategy is key in developing protection against cyber-threats. Scenario-based exercises are a proven method for developing insight into the threat, protection, and associated response. Energypact will lead participants on a mini-exercise based on a realistic scenario in the development of crucial aspects of policy and regulation to address the growing cyber-threat to the energy sector. Adopting realistic roles in a fictional setup, participants will be lead in team through a scenario to challenge their knowledge and assumptions about the role of cyber security in the industry.	
10:00 – 10:30	**Briefing**
10:30 – 11:30	**Main Session**
11:30 – 12:00	**Debriefing**
Eyal Adar White Cyber Knight Andrea Cavina Energypact Foundation Donald Dudenhoeffer IAEA	

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 Defence 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.

13:00 – 17:00 Registration: Sign-up for sessions on Thu 01 Feb & Wed 02 Feb

CYBER SECURITY CLUSTER AUSTRIA DAY (CSCA) 2018 – TECHNOLOGY EXPO Leading Austrian & international cyber security businesses	
13:30 – 17:00	CSCA Day – Technology Expo 2018 / Exhibition & talks w/technology experts, B2B & B2G
15:00 – open end	Reception & Official welcome by the CSCA 2018 organizers: AIT, FEEI, KSÖ, WKÖ/ASW
16:30 – 17:00	**Presentation: Offensive Security Testing** Ron Peeters, Synack
Offensive Security Testing with a Hacker Mindset: A revolutionary security testing platform and managed security solution will be presented which typically can find serious exploits in a matter of hours in any IT asset. It will be concluded with a case study on the Pentagon where Synack was able to break in within only 4 hours' time.	

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.	
Enrico Frumento	CEFRIEL, Politecnico di Milano
Donald Dudenhoeffer	Senior Information Security Officer, International Atomic Energy Agency, IAEA
Jan Schubert	Corporate Information Security Officer, OMV
Nigel Mackie	MASS, Cambridgeshire
Wolfgang Rosenkranz	Manager, Repuco
Jan Schubert	Corporate Information Security Officer, OMV
Timo Wiander	Enoro Company

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.	
Jordan Georgiev	Managing Director, JKG Advisory
Ingrid Schaumüller-Bichl	Professor, Head of Information Security Compliance Center, University of Applied Sciences Upper Austria
Eyal Adar	Conformity Assessment Board Member, International Electrotechnical Commission, IEC
Gregory Herdes	Project Manager, National Nuclear Security Administration, NNSA, Department of Energy, USA
Erich Kronfuss	Industrial IoT-Security Specialist, Phoenix Contact
Wilhelm Wimmreuter	Vice President, International Operations, InCharge Systems Inc.

12:30 – 13:30 Lunch

13:30 – 14:45	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.	
Martin Stierle	Head of Competence Unit Security and Communications Technologies, AIT
Wolfgang Rosenkranz	Manager, Repuco
Reinhard Marak	Chief Executive of the Austrian Defence and Security Industries Group, Austrian Federal Economic Chamber, WKÖ
Thomas Stubbings	Chairman, Cybersecurity Platform of the Austrian Government, CSP
Helmut Schnitzer	Head of Security Policy Department, Federal Chancellery of Austria

14:45 – 15:15 Coffee Break

15:15 – 17:00	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.	
Andrea Cavina	Director for Training and Education Development, Energypact Foundation
Gulmira Rzayeva	Senior Research Fellow, Center for Strategic Studies, Azerbaijan
Petar Stanojevic	Professor, Faculty of Security Studies, University of Belgrade
Jordan Georgiev	Managing Director, JKG Advisory
Mohamed Mekerba	Senior IT Advisor, OPEC

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	**PRESENTATION DIGITAL CITY VIENNA**
Ulrike Huemer	CIO, City of Vienna

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	
Philipp Agathonos	Minister Plenipotentiary, Austrian Embassy of Beijing, Austrian Federal Ministry of Europe, Integration and Foreign Affairs
Kai Rannenberg	Professor, Goethe University Frankfurt
Josef Pichlmayer	CEO, Ikarus Security
Ulrike Huemer	CIO, City of Vienna
Zhihong Rao	Chief Expert of Cyberspace Security, China Electronics Technology Group Corporation, CETC

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 theses terrains.	
Martin Stierle	Head of Competence Unit Security and Communications Technologies, AIT
Mario Drobics	Senior Research Engineer, Center Digital Safety & Security, AIT
Franz Dielacher	Senior Principal Engineer, Infineon Technology Austria
Kay Römer	Professor, Director, Institute for Technical Information, Graz University of Technology

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

Helmut Leopold	Head of Center for Digital Safety & Security, AIT
Ezio Bartocci	Assistant Professor, Faculty of Informatics, Vienna University of Technology
Ron Peeters	Managing Director, Synack Inc.
Holger Sontag	Cyber Security Consultant, Cyber Trap
Moritz Lipp	PhD-Student, Secure Systems Group, Institute of Applied Information Processing and Communications, Graz University of Technology
Andreas Poppe	Head, Experimental Group of Quantum Cryptography, Huawei Europe
Daniel Slamanig	Center for Digital Safety & Security, AIT

15:30-15:45	SPECIAL GUEST SPEECH
Karoly Dan	Ambassador, Permanent Mission of Hungary to the OSCE

15:45-16:00	CONCLUDING REMARKS