VIENNA CYBER SECURITY WEEK 2019

Protecting Critical Infrastructure

International Multi–Stakeholder Conference, Training & Exhibition

11–15 March 2019

Austrian Federal Economic Chamber (WKÖ)

Vienna, Austria

Day 1 – Diplomacy and Regional Approaches to Enhancing Cyber Security Globally A cyber–attack is often an exploitation of a technical vulnerability, but the solution space for protection against such attacks extends far beyond technical measures. Diplomacy and international cooperation are key elements in enhance both State and Global security against malicious cyber actions.	
08:30	Registration
10:00	**10 – Conference Official Opening**
12:30	Lunch
13:30	**Session 11 – Effective multilateralism in cyberspace: developments in international cyber diplomacy** In an age of global interconnectedness, the challenges stemming from cyberspace can easily transcend national borders, necessitating multilateral discussions, co-operation and co-ordination. Accordingly, international organizations, such as the United Nations (UN), the Organization for Security and Co-operation in Europe (OSCE), the European Union (EU) and many others around the world have taken the lead in creating voluntary and binding mechanisms aimed at effectively promoting global cyber stability. The session will give diplomats, policy makers, security experts and representatives from international organizations an opportunity to inform the audience on the most recent developments in multilateral cyber/ICT security efforts, discuss opportunities for synchronizing on-going activities and promote practical international measures for reducing tensions stemming from the use of ICTs.
15:00	Coffee Break
15:30	**Session 12 – Implementation of OSCE efforts to enhance the protection of critical infrastructures (CBM 15)** Critical infrastructures form the backbone of national economies and systems of government by ensuring the timely and seamless circulation of energy, information, goods, services and other necessities. This also makes them a prime target for threats stemming from cyberspace, and an important consideration for policy and decision makers dealing with cyber/ICT security and resilience in the OSCE area. Recognizing this, OSCE participating States, as part of a series of cyber/ICT security Confidence-Building Measures (CBMs), created CBM 15, which encourages efforts for the protection of critical infrastructure, such as by developing shared responses and crisis management procedures, raising awareness on the protection of industrial control systems and classifying ICT incidents according to scale and severity. During the session, the panelists will discuss on national and international efforts and good practices, in particular those from the OSCE, for enhancing the protection of critical infrastructure, the role that different sectors can play, and current developments and future plans for the meaningful implementation of CBM 15.
17:00	Adjourn

Day 2 – Critical Infrastructure Protection and Human Capacity Development Critical infrastructure (CI) is an asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may have a significant negative impact for the security of the State and the well–being of its citizens.[1] CI, however, does not exist in isolation, but is often part of an interconnected and interdependent network. The migration to ICT has additionally increased CI vulnerability to cyber–attack and manipulation.	
08:30	Registration
09:00	**20 – Welcome and Keynote(s)**
09:30	**Session 21 – Critical infrastructure: threats and vulnerabilities (IEC)** This session will outline the difference between critical infrastructure OT and IT systems in the face of cyber threats. It will present an impact assessment of cyber attacks on critical infrastructure and highlight the differences between the two.
11:00	Coffee
11:30	**Session 22 – Building trust and resilience (IEC)** This session outlines cyber security strategies in a systems approach including testing and certification, risk assessment and management. It presents a regulatory perspective and a new regulatory framework for cyber security, which is being prepared together with UNECE.
13:00	Lunch
13:45	**Session 23 – Digital Transformation and Cyber Security (ITU)** This session examines the evolution of ICT centric innovation and integration into all aspects of information and operational technologies. This includes the need to encourage and embrace emerging technologies while at the same time understanding the risks and the need for security considerations.
15:15	**Special Session 24 – The Role of Women in the Cyber Space (ITU)** The panel discussion will focus on raising awareness about the importance of cyber security as a career choice for young women in particular. The discussion will stress the importance of doing better marketing of selling jobs to young women but also more importantly, that a great number of cybersecurity jobs require more interpersonal skills than technical ones. They also require analytical thinking, teamwork skills, communication skills, and leadership skills, all of which can be learned in fields other than technology.
16:15	Coffee Break
16:30	**Session 25a – Connecting Smart Sustainable Cities with the Sustainable Development Goals (ITU)** Sustainable urban development is crucial in ensuring that there is adequate housing and infrastructure to support the growing populations and creating more liveable spaces globally. International standards hold the key in leveraging IoT systems and other emerging technologies that are making cities smarter and more sustainable as well as in ensuring that such technologies are inclusive, safe and accessible to all. This session will discuss the role of international standards in shaping emerging technologies in smart sustainable cities (SSC) and in connecting SSC with the United Nations' Sustainable Development goals (SDGs). This session will provide also an opportunity to present the outcomes of the United for Smart Sustainable Cities (U4SSC) Initiative.
18:00	Adjourn
Day 2 – Women's Cyber Forum (Parallel Session)	
16:30	**Session 25b – ITU EQUALS Training**
18:00	Adjourn

Day 3 – Energy Security and Critical Infrastructure Protection from Cyber Exploitation

[1] Modified definition of CI from https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-andterrorism/critical-infrastructure_en

08:30	Registration
09:00	**30 – Welcome and Keynote(s)**
09:45	**Session 31 – Energy Security** Energy Security entails protecting the uninterrupted availability of energy sources at an affordable price. In today's environment this also requires addressing evolving technology and an evolving threat.
11:15	Coffee
11:45	**Session 32a – Critical Infrastructure, Energy Security, and the Digital Society – Challenges and Solutions** The rise in digital technologies and connectivity across all sectors of critical infrastructure have increases the challenge of protection against both natural hazards and malicious cyber acts. This session examines the challenges and initiative to address them.
13:15	Lunch
14:15	**Session 33a – International Standards, Guidelines, and Directives – Status, Usability and Lessons Learned** Significant efforts are in place at both the international and national level to develop and implement cyber security guidance for the protections of critical assets and sensitive sites. This session discusses the state of guidance development and lessons learned.
15:30	Coffee Break
16:00	**Session 34a – Building and Sustaining a Credible Cyber Security Workforce** One of the largest international challenges facing cyber security is the availability of cyber security expertise and associated skill sets for identifying and managing cyber risks. This session discusses current efforts and lessons learned in developing a sustainable workforce in cyber security.
17:30	Adjourn

Day 3 – Cyber Security Incident Planning and Response and Planning. (**Parallel Session)**	
14:00	**Session 33b – Developing Operational Technology Focused Cyber–Attack Response Capability** Given all the protection mechanisms in place, cyber compromise will occur. The development of national and organizations response plans and organizations is essential in maintaining safety, security, and operations at sensitive industrial sites. This session examines national and organizations strategies and experiences in cyber security incident response planning.
15:30	Coffee Break
16:00	**Session 34b – Cyber Incident Response Lessons Learned** Given all planning and preventions attempts, cyber incidents will occur. This session provides a forum for discussing strategies and lessons learned in responding to cyber–attacks.
17:30	Adjourn

Day 3 – Tutorials and Demonstration (Parallel Session)	
11:30	**Session 32c – Quantum Computer – why is it a cyber security threat?**
13:00	Lunch
14:00	**Session 33c – Artificial Intelligence & Security**
15:30	Coffee Break
16:00	**Session 34c – AIT Cyber Range: training and simulation for securing critical infrastructures**
17:30	Adjourn

Day 4 – Countering Cyber Conflict, Terrorism and Crime The boundaries between cyber terrorism and cybercrime continue to blur as terrorist groups become more involved in criminal activities[2] (including cyber activities) to both support and enable their objectives. Protection against malicious cyber–attacks requires international cooperation and collaboration between an array of government and non–government stakeholders.	
08:30	Registration
09:00	**Official Session Opening**
09:10	**40 – Keynote(s)**
10:00	Coffee
10:30	**Session 41a – Trends and Forecast on Threats, Technology, and future Defense against Cyber–Crime** This session examines the current state and projected trends for cyber–crime and associated efforts and resources to combat it.
12:00	Lunch
13:00	**Session 42a – National and International Efforts to Counter Cyber–Terrorism and Cyber–Crime** Cyber–Terrorism and cyber–crimes continue to be growing threat as terrorist groups and criminal organizations develop great cyber capabilities. This session examines the current threat and strategies for countering cyber–terrorism and cyber–crime.
14:30	Coffee Break
15:00	**Session 43a – Cyber Conflict in Today's Age** Cyber–attacks have become a common tool of conflict. National defense strategies must now consider defense against and response to cyber–attacks. This session examines current challenges, international instruments, and lessons learned combatting cyber–attacks.
17:00	Adjourn

[2] "With boundaries blurring between crime and terror, international cooperation's vital, UN highlights", https://news.un.org/en/story/2018/10/1022552

Day 4 – Sector Specific Cyber Security Experiences (Parallel Session)	
10:30	**Session 41b – Security by Design** Security in the past has not been a strong consideration in the design and development of operational technologies. This has often resulted in the costly requirement to back fit security controls on operational technologies. Security should be a design requirement. This session examines the challenges, the progress, and lessons learned.
12:00	Lunch
13:00	**Session 42b – Security and the Internet of Everything** In the evolution of digital systems, it seems like everything seeks to connect to something else. This includes business systems, industrial systems, and personal systems. With this connectivity comes increased efficiency, convenience, and often insecurity. This session examines the future of security in a connected society.
14:30	Coffee Break
15:00	**Session 43b – The Convergence of Nuclear and Cyber Security** One of the most physical secure and regulated industries is nuclear (including other radioactive materials). The consequence of security failure is enormous. The threat has evolved, however, and now has cyber–capabilities. Nuclear security must now consider malicious cyber–attacks as a threat vector. This session examines the efforts of the nuclear sector to address cyber–capable adversaries.
17:00	Adjourn

Day 4 – SBA Research (Parallel Session)	
13:00	**Session 42c – Cyber Security Challenge Workshop**
14:30	Coffee Break
15:00 – 19:35	**Session 43c – SBA Research Symposium** SBA Research is a research center for Information Security funded in part by the national initiative for COMET (Competence Centers for Excellent Technologies). Within a network of more than 70 companies, 15 Austrian and international universities and research institutions, and many additional international research partners SBA Research jointly works on research challenges ranging from organizational to technical security to strengthen Europe's Cybersecurity capabilities.

Day 5 – Security Implementation Today's reality and Tomorrow's promise Research and development seek to build a future of infrastructure resistant and resilient to cyber–exploitation. While at the same time we are faced with the implementation of security with legacy systems, minimal budgets, and a lack of human resources. What can practically be achieved today and tomorrow in terms of cyber secure systems.	
08:30	Registration
09:00	**50 – Welcome and Keynote(s)**
09:30	**Session 51 – The future of cyber security: research and expectations** This session examines current research in cyber security and in the development of resilient systems.
11:00	coffee
11:20	**Session 52 – Cyber Security Practical Implementation** This session examines the reality between desired and actual security implementation. It looks to provide a discussion on the challenges of cyber security implementation, lessons learned, and good practices.
12:50	**Conference Closing Remarks**
13:00	Adjourn