VIENNA CYBER SECURITY WEEK 2019
Protecting Critical Infrastructure

International Multi–Stakeholder Conferences, Training & Exhibition

11–15 March 2019

Austrian Federal Economic Chamber (WKÖ)

Vienna, Austria

Digital systems have become a workhorse of today's business and society. It is no longer the Internet of Things or the Internet of Industrial Thing, it has become the Internet of Everything. The security of digital systems against both malicious and non-malicious events has become vital to the sustainability of societal essential processes. The advancement of digital technologies will continue to grow as will our reliance on them. This is especially true with regards to critical infrastructure.

This, the third annual Vienna Cyber Security Week (VCSW) brings together over 700 national and international stakeholders representing over 75 States and International Organizations to conduct information exchange, confidence building, and enhance awareness of the risks and state of practice for critical infrastructure and digital system protection against malicious cyber actions. During the five days of the conference, over 115 experts will discuss topics ranging from national cyber security and CIP strategies to the promising new technologies.

Included in the conference are a special panel discussion and training on "The Role of Women in Cyber Space". The panel discussion and training will focus on raising awareness about the importance of gender equality in the online space and as a career choice.

The Vienna Cyber Security Week is organized by the EnergyPact Foundation, the AIT Austrian Institute for Technology GmbH and the Austrian Chamber of Commerce (Wirtschaftskammer Österreich- WKÖ). Conference co-organizers include the International Telecommunication Union (ITU) and the International Electrotechnical Commission (IEC). Additionally, the conference has the support of the Slovak OSCE Chairmanship and Austrian Federal Chancellery together with Austrian Ministries.

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	**Welcome by the Conference Scientific Secretary** - Donald Dudenhoeffer, Director of Operations of the EnergyPact Foundation/ Cyber Security Research Engineer, AIT Austrian Institute for Technology GmbH (USA)
	Opening Remarks from Conference Organizers - Alexandre Dimitrijevic, President & Executive Director, EnergyPact Foundation (EP) - Helmut Leopold, Head of Center for Digital Safety & Security, AIT Austrian Institute for Technology GmbH (Austria) - Matthias Grabner, Sector Manager Technology, ADVANTAGE AUSTRIA / WKÖ AUSSENWIRTSCHAFT AUSTRIA (Austria)
	10 – Conference Official Opening - Ambassador Thomas Greminger, Secretary General, Organization for Security and Co-operation in Europe (OSCE) - Lukáš Parízek, State Secretary of the Ministry of Foreign and European Affairs of the Slovak Republic, Special Representative of the OSCE Chairperson-in-Office for the Slovak OSCE Chairmanship 2019 - Ambassador Andreas Riecken, Director General, EU and Multilateral Affairs, Federal Ministry of Europe, Integration, and Foreign Affairs, Republic of Austria - Frans Vreeswijk, General Secretary and CEO at International Electrotechnical Commission (IEC) - Kemal Huseinovic, Chief of Infrastructure, Enabling Environment and E- Applications Department International Telecommunication Union (ITU) - Michael Otter, Director General, ADVANTAGE AUSTRIA / WKÖ AUSSENWIRTSCHAFT AUSTRIA (Austria) - Robert Bodenstein, Chairman, Information and Consulting Division, Austrian Federal Economic Chamber (Austria)
12:30	Lunch provided by WKÖ
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. - Rasa Ostrauskaite, Co-ordinator of Activities to Address Transnational Threats at OSCE (Moderator) - Ambassador Károly Dán, Permanent Representative of Hungary to OSCE (Hungary) - Camille Gufflet, Policy Officer for Cyber Security, European External Action Service (EEAS) - Shohin Samadi, Secretariat, Shanghai Cooperation Organization (SCO) - Nemanja Malisevic, Senior Security Strategist, Microsoft (Germany) - Orhan Osmani, Cybersecurity Coordinator, ICT Applications and Cybersecurity Division International Telecommunication Union (ITU)
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. Introductions: Ambassador Véronique Roger-Lacan, Permanent Representative of France to the OSCE - Baudouin Carrard, Permanent Representation of France to the OSCE (France) (Moderator) - Desroches Vincent, Deputy Head of Division, French National Cybersecurity Agency (France) - Cristian Iordan, Head of International Cooperation, National Cyberint Center, SRI (Romania) - Bibiana Andújar, Head of International Relations, National Centre for Critical Infrastructure Protection (CNPIC) (Spain) - Martin Vereš, Head of Unit, Cybersecurity, Ministry of Foreign and European Affairs of the Slovak Republic (Slovakia)
17:00	Adjourn
17:00	Reception hosted by the Slovak OSCE Chairmanship.

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)** - Alexandre Dimitrijevic, President & Executive Director, EnergyPact Foundation (EP) - Kemal Huseinovic, Chief of Infrastructure, Enabling Environment and E- Applications Department, International Telecommunication Union (ITU) - Gabriela Ehrlich, Global Head Public Affairs & Advocacy, International Electrotechnical Commission (IEC)
	20a – Special Session *"Critical Infrastructure Protection and Human Capacity Development – Challenges & Chances for Austria"* - Antonella Mei-Pochtler, Special Advisor to the Federal Chancellor of Austria & Head of Strategy Unit (Think Austria)
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. - Mike Mullane, International Media Executive (IEC) - David Hanlon, Secretary of the IEC Conformity Assessment Board (IEC) - Eyal Adar, Advisor to McKinsey & Company, Member of IEC CAB WG 17 Cybersecurity
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. - Moreno Carullo, CTO & Co-Founder, Nozomi Networks (Italy) - David Hanlon, Secretary of the IEC Conformity Assessment Board (IEC) - Prokopios Drogkaris, Expert in Network and Information Security, European Union Agency for Network and Information Security (ENISA) - Mike Mullane, International Media Executive (IEC)
13:00	Lunch provided by the International Electrotechnical Commission (IEC)
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. - Orhan Osmani, Cybersecurity Coordinator, ICT Applications and Cybersecurity Division International Telecommunication Union (ITU) (Moderator) - Csaba Virág, Head of Cybersecurity Competence Center, Cyber Services Zrt (Hungary) - Aleksandar Vratonjić Gligorijević, Director of TeleGroup Innovation Team, TeleGroup, (Serbia) - Luca Tenzi, Resilience Strategy Consultant at UN - Prokopios Drogkaris, Expert in Network and Information Security, European Union Agency for Network and Information Security (ENISA) - Eyal Adar, Advisor to McKinsey & Company, Member of IEC CAB WG 17 Cybersecurity

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

15:15	**Special Session 24 – The Role of Women in the Cyberspace (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. - Carla Licciardello, Policy Analyst, International Telecommunication Union (ITU) (Moderator) - Denise Mazzolani, Deputy Head Strategic Police Matters Unit/Transnational Threats Department, (OSCE) - Anett Mádi-Nátor,Vice President (Operations and Strategic Business Development), Cyber Services (Hungary) - Ivana Kojadinović Žižić, Corporate Counsel, TeleGroup (Serbia) - Rhonda Evans, Head of the WINS Academy, World Institute of Nuclear Security, (WINS) - Karsten Simons, Regional Manager Corporate Affairs Europe, CIS, Russia & Israel, CISCO (Germany) - Valerie Khan, Consultant and Founding member, Digital Equity (UK)
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. - Cristina Bueti, ITU Focal point on Smart Sustainable Cities & Environment", International Telecommunication Union (ITU) (Moderator) - Birgit Ginzler, Head of Communications, Smart City Wien Agency (Austria) - John Smiciklas, Director, Building Owners and Managers Association (BOMA), (Canada) - Kari Aina Eik, Secretary General, Organization for International Economic Relations (OiER) - Javier Llavador Piqueras, City of Valencia (Spain)
18:00	Adjourn
Day 2 – Women's Cyber Forum (Parallel Session)	
16:30	**Session 25b – Training on Career Transition to Cybersecurity' provided by CyberWayFinder and contributions by EQUALS**
18:00	Adjourn
18:00	Reception hosted by the ITU and the EnergyPact Foundation

Day 3 – Energy Security and Critical Infrastructure Protection from Cyber Exploitation	
08:30	Registration
09:00	**30 – Welcome and Keynote(s)** - Donald Dudenhoeffer, Director of Operations of the EnergyPact Foundation/ Cyber Security Research Engineer AIT Austrian Institute for Technology GmbH (USA) - Esti Peshin, General Manager of the Cyber Division, Israel Aerospace Industries Ltd. (Israel) - Michaela Kollau, Policy Officer, Cybersecurity in the Energy Sector, European Commission
09:30	**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. Keynote: Dr. Jan Ban, Senior Research Analyst, Research Division (OPEC) - Michaela Kollau, Policy Officer, Cybersecurity in the Energy Sector, European Commission (Moderator) - Simon Uzunov, Energy Community Secretariat Electricity Expert / Deputy Head of Unit, Energy Community (EC) - Ayhan Gucuyener, Doctoral Candidate and Project Specialist, Kadir Has University; Center for Cybersecurity & Critical Infrastructure Protection (Turkey) - Marcela J. Lozano Luna, Master Student, Technische Universität Wien (Mexico) - Nadejda Komendantova, Senior Research Scholar, Advanced Systems Analysis Program, International Institute for Applied Systems Analysis (IIASA) - Jan Ban, Senior Research Analyst, Research Division, OPEC.
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. - Esti Peshin, General Manager of the Cyber Division, Israel Aerospace Industries Ltd. (Israel) (Moderator) - Alexander Janda, Secretary-General, KSÖ Austria, (Austria) - Stefan Schachinger, Senior Consulting Engineer, Barracuda Networks AG (Austria) - Florin Galaftion, Information Security Manager, Comprehensive Nuclear-Test-Ban Treaty Organization (CTBTO) - Nebojsa Naric, Head of Business Development, Khaoticen (Serbia)
13:15	Light 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. - Clifford Glantz, Senior Staff Scientist/Project Manager, Pacific Northwest National Laboratory, (USA) (Moderator) - Joerg Nachbaur, Committee Manager, Austrian Standards International (Austria) - Rainer Eisenkirchner, CEO, ERM-Consult, (Austria)
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. - Christina Lekati, Social Engineering Security Consultant & Trainer, Cyber Risk GmbH (Switzerland)(Moderator) - Sajad Abedi, Resident Research Fellow at the National Security and Defense Think Tank (Iran) - Roger Howsley, Executive Director, World Institute for Nuclear Security (WINS) - David Lambert, Senior Security Specialist, Gregg Protection Services, LLC (USA)
17:30	Adjourn

Day 3 – Cyber Security Incident Planning and Response and Planning. (**Parallel Session)**	
14:15	**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. - Stefan Wagenhofer, Chairman of the Austrian Energy CERT Supervisory Board, (Austria) - Ivan Dragnev, Principle Technical Leader Europe, Cyber Security, Electric Power Research Institute (EPRI) - Alexander Janda, Secretary-General, KSÖ Austria, (Austria) - Edith Huber, Bettina Pospisil, and Walter Seböck, Danube University Krems (Austria)
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. - Thomas lozanobings, Chairman, Cybersecurity Platform of the Austrian Government (Austria) (Moderator) - Harald Wenisch, Spokesperson of the Experts Group IT Security of the Federal Chamber of Commerce Austria (Austria) - Walter Fraißler, Head of Information Security, Verbund (Austria) - Wim Hafkamp, Deputy head of NL Cybersecurity Center (Netherlands)
17:30	Adjourn

Day 3 – Tutorials and Demonstration (Parallel Session)	
11:45	**Session 32c – Quantum Computer – why is it a cyber security threat?** - Training Leader, Hannes Hübel, AIT Austrian Institute of Technology GmbH (Austria)
13:15	Lunch
14:15	**Session 33c – Artificial Intelligence & Security** - Training Leader, Alexander Schindler, AIT Austrian Institute of Technology GmbH (Austria)
15:30	Coffee Break
16:00	**Session 34c – AIT Cyber Range: training and simulation for securing critical infrastructures** This session includes a interactive strategic cyber security simulation game. Please bring your own web-enabled device (e.g., laptop, mobile phone). No technical knowledge is required for participation. - Training Leader, Maria Leitner, AIT Austrian Institute of Technology GmbH (Austria)
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** - Gernot Blümel, Federal Minister within the Federal Chancellery for the EU, Arts, Culture and Media (Austria) - Patrick Sagmeister, Deputy Director General, ADVANTAGE AUSTRIA / WKÖ AUSSENWIRTSCHAFT AUSTRIA (Austria)
	40 – Keynote(s) - Mika Lauhde, Vice-President, Cyber Security & Privacy, Global PACD, Huawei Technologies Co., LTD. (Finland)
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. - Nicole Samantha van der Meulen, Senior Strategic Analyst at the European Cybercrime Centre (EC3) (EUROPOL) (Moderator) - Hans Holmer, Director, Noetic International (USA) - Christina Lekati, Social Engineering Security Consultant & Trainer, Cyber Risk GmbH (Switzerland) - Holger Sontag, Senior Cyber Security Consultant, CyberTrap Software GmbH (Austria) - Komitas Stepanyan, Deputy Head of Internal Audit, Central Bank of Armenia, (Armenia)
12:00	Lunch provide by WKO ARGE Sicherheit / Austrian Defense Industry Cooperation
13:00	**Special Keynote:** - Brig. Gen.(res). Danny Bren, CEO and Co-founder OTORIO; Former CIO and Military Cyber Defense Commander, IDF (Israel)
13:20	**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. Special Presentation by the Spanish National Police - Maroto Domínguez, Police Commissioner, HQ CT (Policía Nacional) (Spain) - Miguel Ángel Cortes Ruberte, Police Inspector, HQ CT (Policía Nacional) (Spain) - Jonathan Darby, Head, Cyber Growth & Innovation, Department of Digital, Culture, Media and Sport (UK) - Reinhard Marak, CEO, Austrian Defence and Security Industry Group (Austria)
14:30	Coffee Break

[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. - Alexander Duchac, Nuclear Safety Officer, International Atomic Energy Agency (IAEA) - Christian Flachberger and Andreas Gerstinger, Chief Information Security Officer / Safety Manager, Frequentis AG (Austria) - Sascha Böhm, Senior Consultant, softScheck GmbH (Germany) - Aurelian Buzdugan, ICT Infrastructure Security & Operations Expert, UNIDO (Moldova) - Adolf Schmidthuber, Director of Corporate Development, DESOMA GmbH, (Austria)
12:00	Lunch
13:00	**Session 42b – Cyber Security in Industry** Technologies, products and organizations are currently under constant threat of cyber-attacks on different levels. Not only does an attack on a digital manufacturing site have consequences for the on-going production, like a stand-still causing delay, but it can also have severe business impact caused by loss of trust by partners, customers, etc. This session covers three talks on different perspectives on the possibilities and implications to secure industrial manufacturing and a final panel discussion. - Corinna Schmitt, Researcher and Laboratory Supervisor, Universität der Bundeswehr München, Research Institute CODE (Germany) (Moderator) - Omar Veledar, Project Manager R&D, AVL List GmbH (Austria) - Violeta Damjanovic-Behrendt, Senior Researcher, Salzburg Research (Serbia) - Nikolaus Dürk, Founder and Managing Director, X-Net Services GmbH (Austria)
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. - Ambassador Ali Asghar Soltanieh, International Security Consultant (Iran)(Moderator) - Janos Eiler, Scientific Secretary, International Atomic Energy Agency (IAEA) - Guy Landine, Senior Cyber Security Specialist/Analyst, Pacific Northwest National Laboratory (USA) - Kathryn Rauhut, Vienna Nonresident Fellow, The Stimson Center (USA) - Paul Smith, Senior Scientist, AIT Austrian Institute for Technology GmbH (AT)
17:00	Adjourn

Day 4 – SBA Research (Parallel Session)	
13:00	**Session 42c – Cyber Security Challenge – how to grow IT-Security Excellence** - Joe Pichlmayr, IKARUS Security Software GmbH (Austria)
14:30	Coffee Break
15:00	**Session 43c – Rethink Cyber Security** Rethink Cybersecurity is co-hosted by Anovis – Member of CymbiQ Group, Kuratorium Sicheres Österreich (KSÖ), SBA Research and the Eventpartner Forcepoint.
	15:00 **Welcome** *Jimmy Heschl, Head of Digital Security, Red Bull* *Stefan Jakoubi, Head of Professional Services, SBA Research* 15:05 **Opening Address: Opening Address: Cyber challenges of the future** *Udo Helmbrecht, Executive Director, ENISA* **Impulse Speeches** 15:20 **Cyber Resilience – If the worst case is not bad enough** *Tom Köhler, CSO & Vice Chairman, CymbiQ Group* 15:35 **Human-Centric Security For The Era of Digital Transformation** *Emiliano Massa, VP EMEA Sales, Forcepoint* 15:50 **Media manipulation in the digital age** *Markus Klemen, CEO, SBA Research* 16:05 **Panel: New joint approaches to cyber security. The next level of innovation – Security made in Europe?** *Udo Helmbrecht, Executive Director, ENISA* *Tom Köhler, CSO & Vice Chairman, CymbiQ Group* *Helmut Leopold, Head of Center for Digital Safety & Security, AIT* *Emiliano Massa, VP EMEA Sales, Forcepoint* 16:50 Coffee Break 17:10 **The rising cybersecurity stars: Security Rockstars - promising security startups from Austria and beyond** *Startup representatives* 17:40 **Panel: Developing a cyber resilient business world and society** *Jan-Peter Kleinhans, Stiftung Neue Veranwortung* *N.N. BMDW representative* *Markus Klemen, CEO, SBA Research* *Corinna Schmitt, Researcher and Laboratory Supervisor, UniBW* *Jimmy Heschl, Head of Digital Security, Red Bull* *Moderation: Oliver Rolofs, Director Communications, CymbiQ Group & Managing Partner, connecting trust* 18:25 **Farewell Speech: Digital Society – Lost in Complexity?** *Alexander Schatten, Senior Researcher, SBA Research* 18:50 **Get together and networking**

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)** - Ludmila Georgieva, Public Policy and Government Relations Manager, Google (Belgium) - Martin Stierle, Head of Competence Unit Security & Communication Technologies, Center for Digital Safety & Security AIT Austrian Institute for Technology GmbH (Austria) - Philipp Agathonos, Director, Office of Science and Technology (OSTA), Embassy of Austria - Beijing (Austria)
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. - Philipp Agathonos, Director, Office of Science and Technology (OSTA), Embassy of Austria - Beijing (Austria) (Moderator) - Wensheng Wang, Vice-General Manager, CETC Institute 30 (China) - Manuel Koschuch, Researcher and Teacher, FH Campus Wien (Austria) - Marcus Kottinger, Solution Architec, Axians (Austria) - Corinna Schmitt, Researcher and Laboratory Supervisor, Universität der Bundeswehr München, Research Institute CODE (Germany)
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. - Robert Haider, Managing Director, Vienna International Underwriters - Vienna Insurance Group (Austria) - Christopher Leder, CEO, Satellite Telecom (Austria) - Herbert Saurugg, Experte für die Vorbereitung auf den Ausfall lebenswichtiger Infrastrukturen (Austria) - Corinna Schmitt, Researcher and Laboratory Supervisor, Universität der Bundeswehr München, Research Institute CODE (Germany) - Roxana Albisteanu, Global Information Security Policy Counsel, UiPath (Romania)
12:50	**Conference Closing Remarks** - BM a.D. Dr. Friedhelm Frischenschlager, Vice President of the Energypact Foundation (Austria) - Martin Stierle, Head of Competence Unit Security & Communication Technologies, Center for Digital Safety & Security AIT Austrian Institute for Technology GmbH (Austria)
13:00	Adjourn