NEWSLETTER

Vienna, April 2018

energypact foundation

VIENNA CYBER SECURITY WEEK 2018

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

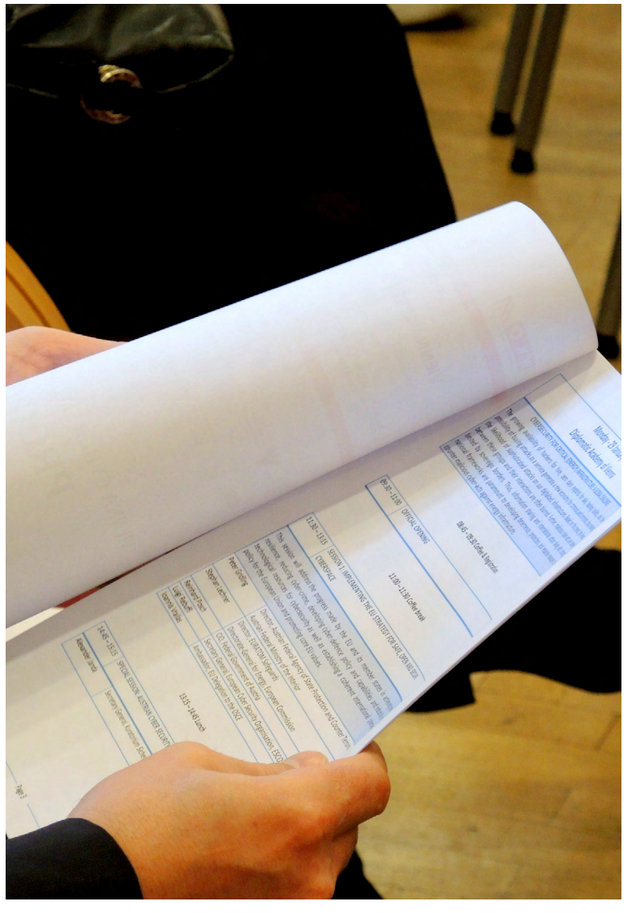
2018

Foreword

This issue presents the second Energypact Newsletter publication in 2018. As such, it aims to highlight the themes discussed at the Vienna Cyber Security Week held from 29 January to 02 February 2018 at the Diplomatic Academy of Vienna and the Tech Gate Tower in Vienna. The conference covered key topics in the sphere of Cyber Security of critical energy infrastructure. Beside the reports and interviews from our five-day event, this issue brings you the articles and discussions written *post festum* by some of our speakers.

Contents

Articles



Briefs

Facts & Figures

THE SECOND EDITION OF
VIENNA CYBER SECURITY WEEK 2018
FACTS & FIGURES

- 5 DAYS
- 18 PLENARY SESSIONS
- 5 SPECIAL SESSIONS
- 2 VENUES
- MORE THAN 550 PARTICIPANTS AND SPEAKERS
- FROM 41 COUNTRIES WORLDWIDE
- 2 TRAINING AND TUTORIAL SESSIONS
- 21 EXHIBITING COMPANIES

The 2018 edition of Vienna Cyber Security Week was jointly organized by Energypact Foundation, Austrian Institute of Technology - AIT, Cybersecurity Platform of Austrian Government - CSP, and Austrian Federal Chamber of Commerce - WKÖ.

It was supported by international organizations: Organization for Security and Cooperation in Europe - OSCE, International Electrotechnical Commission - IEC, and International Telecommunication Union - ITU, as well as by the Austrian Federal Chancellery, the Austrian Federal Ministry for Europe, Integration and Foreign Affairs - BMEIA, the Austrian Federal Ministry of Defence - BMLV, the Austrian Federal Ministry of the Interior - BMI, and the Austrian Federal Ministry of Transport, Innovation and Technology - BMVIT.

Vienna Cyber Security Week 2018

29 January–02 February

DAY 1

OFFICIAL OPENING

SESSION 1:
IMPLEMENTING THE EU STRATEGY FOR SAFE, OPEN AND SECURE CYBERSPACE

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

SPECIAL SESSION:
AUSTRIAN CYBER SECURITY EXERCISE

Alexander Janda, Secretary General, Kuratorium Sicheres Österreich, KSÖ

SESSION 2:
CYBER-THREATS TO CRITICAL ENERGY 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

DAY 2

SESSION 1:
OPERATIONAL CONSIDERATIONS FOR RESPONDING TO THE THREAT OF CYBER-ATTACKS ON CRITICAL ENERGY INFRASTRUCTURE

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

SPECIAL SESSION:
SECURING THE FUTURE TOGETHER

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

SESSION 2:
REDUCING THE RISKS OF CONFLICT STEMMING FROM THE USE OF CYBER- CAPABILITIES

Ben Hiller, Cyber Security Officer, OSCE SecretariatSecurity, ENISA

Mikhail Konarovskiy, Advisor, Shanghai Cooperation Organisation, SCOFederal Ministry of Defence

Nemanja Malisevic, Senior Strategist, Microsoft

Andreas Stadler, Minister Plenipotentiary, OSCE Directorate, Austrian Federal Ministry of Europe, Integration and Foreign Affairs

Yazici Deniz, SSenior Adviser,
Austrian Federal Ministry for Europe, Integration and Foreign Affairs

SESSION 3:
CYBER-DIPLOMACY: DEVELOPING CAPACITY AND TRUST BETWEEN STATES

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

DAY 3

CYBER RANGE TUTORIAL

Maria Leitner, AIT
Donald Dudenhoeffer, IAEA
Maria Leitner, AIT
Paul Smith, AIT
Mislav Findrik, AIT
Paul Smith, AIT

POLICY TABLE TOP TUTORIAL

Eyal Adar, White Cyber Knight
Andrea Cavina, Energypact Foundation
Donald Dudenhoeffer, IAEA

SPECIAL SESSION:
OFFENSIVE SECURITY TESTING
Ron Peeters, Synack

DAY 4

SESSION 1:
EMERGING AND FUTURE THREATS TO DIGITALIZED ENERGY SYSTEMS

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

SESSION 2:
CYBER SECURITY STANDARDS IN CRITICAL ENERGY INFRASTRUCTURE

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.Contact

SESSION 3:
PUBLIC SECTOR, INDUSTRY, AND RESEARCH COOPERATION IN CYBER 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

SESSION 4:
SECURING CRITICAL ENERGY INFRASTRUCTURES BY UNDERSTANDING GLOBAL ENERGY MARKETS

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

DAY 5

SESSION 1:
MAKING SMART CITIES CYBER SECURE

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

SESSION 2:
AUSTRIAN & INTERNATIONAL IOT SAFETY & SECURITY LIGHT HOUSE INITIATIVES

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

SESSION 3:
THE PROMISE AND CHALLENGE OF NEW TECHNOLOGIES

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

SPECIAL GUEST SPEECH

Karoly Dan, Ambassador, Permanent Mission of Hungary to the OSCE

VIENNA CYBER SECURITY WEEK 2018

The second edition of Energypact Foundation`s annual flagship event Vienna Cyber Security Week, was held from 29 January to 02 February 2018, at the premises of Diplomatic Academy of Vienna and the Tech Gate Tower in Vienna.

Our renowned international multistakeholder event has gathered more than 550 high-level participants and speakers from various areas and professional backgrounds. As an original concept developed by the Energypact Foundation, Vienna Cyber Security Week is a unique opportunity for representatives of governments, companies, experts and academics to discuss on the most pressuring global issues, in cyber & energy infrastructure. This year`s event covered various topics under the umbrella of protection of critical energy infrastructure and cyber threats.

After the successful launch of the first Vienna Cyber Security Week last year, this international dialogue platform has again succeeded in positioning Vienna as a global centre for energy security and the cyber threat. This year the five-day conference was co-organized in a joint effort between the Austrian Institute of Technology - AIT, Austrian Government's Cybersecurity Platform - CSP, Austrian Federal Chamber of Commerce - WKÖ and the Energypact Foundation, which works to raise global awareness of cyber security. International experts from the public and private sectors in over 41 countries and from international authorities discussed the challenges and opportunities created by digitalising critical infrastructures, and the need for global cooperation.

Our event was split into two segments, held consecutively at the Diplomatic Academy of Vienna (29-30 January), and then, in Tech Gate Tower (31 January - 02 February). The first segment was focused on national and global diplomatic cooperation and efforts in bringing these topics to political agenda. It gathered representatives from governments and international organizations such as the Organization for Security and Cooperation in Europe - OSCE, the International Telecommunication Union - ITU, the International Electrotechnical Commission - IEC, the Shanghai Cooperation Organization (SCO), the Organization of American States - OAS, the European Union - EU and many others. The second segment beside the professional and business talks, compounded the exhibitions and cyber range tutorials and trainings as well.

Vienna Cyber Security Week 2018 was supported by the Austrian Federal Chancellery, the Austrian Federal Ministry for Europe, Integration and Foreign Affairs (BMEIA), the Ministry of Defence (BMLV), the Ministry of Internal Affairs (BM.I), and the Ministry of Transport, Innovation and Technology (bmvit). Beside institutional support coming from Austria, this edition of Vienna Cyber Security Week was supported by the OSCE, the ITU and the IEC.

Our event would not be successful without an inevitable support coming from our sponsors - the OMV Group, the KPMG, Fortinet, Ikarus Security Software, KSO Austria and Digital City Vienna.

DAY 1

The first day of Vienna Cyber Security Week, "Cybersecurity For Critical (Energy) Infrastructure: A Global Challenge", was held at the Diplomatic Academy of Vienna, on 29 January 2018. It pointed out the growing availability of hackers for hire, zero days exploits for sale, hacking toolkits, and the possibility of buying attacks as a service generates a new economy for criminals and terrorists. As malicious cyber-acts are rarely limited by sovereign borders, 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.

The official opening was hosted by Mr. Philipp Agathonos, Minister Plenipotentiary from the Austrian Federal Ministry of Europe, Integration and Foreign Affairs.

The first session, "Implementing the EU Strategy for Safe, Open and Secure Cyberspace", addressed 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.

Between the first two sessions, there has been held a special one, hosted by Mr. Alexander Janda, Secretary General of Kuratorium Sicheres Österreich - KSÖ, who presented the Austrian Cyber Security Exercise.

It was followed by "Cyber-threats to Critical Energy Infrastructure", which was the second session of the first day, focusing on enhancing critical infrastructure resilience within a multi-stakeholder environment.

SPEAKERS AT OFFICIAL OPENING

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 UN, 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

Zoran Predić
State Secretary, Ministry of Energy and Mining, Republic of Serbia

Matthias Grabner
Special Announcement B2B
Advantage Austria / WKÖ Aussenwirtschaft Österreich

DAY 2

The second day of a five-day event, "Safeguarding Critical Energy Infrastructure In The Context Of Regional And Global Security: Strategic And Diplomatic Aspects", was held on 30 January at the Diplomatic Academy of Vienna. 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, were the key topics of this day.

"Operational Considerations for Responding to the threat of Cyber-Attacks on Critical Energy Infrastructure", was the first session, and dedicated to recognition of the measures which could be taken to reduce or contain the cyber-threat. It also addressed a response to the growing threat organized and implemented and the roles & responsibilities of national stakeholders and critical infrastructure owners and operators.

Following these issues, the second session "Reducing the Risks of Conflict Stemming from the use of Cyber-capabilities", introduced international instruments and measures that can assist in promoting uniform and predictable response in preventing undesired side effects including conflict escalation.

A special session - "Securing the Future Together", hosted by Mr. Andrea Cavina, Director for Training and Education Development of Energypact Foundation gave an insight into concrete initiatives that we could design today to ensure the knowledge and the capabilities to protect critical infrastructure from cyber-attacks exist and is available to the relevant stakeholders.

The last session of the first segment of Vienna Cyber Security Week, was "Cyber-Diplomacy: Developing Capacity and Trust between States", and it examined the need for confidence building and information sharing among States in regards to cyber-incidents, especially those with cross-border implications.

With eight sessions in total, the first segment of the five-day event, gathered more than 280 participants and speakers in total.

DAY 3

After successful first segment of the conference, the experts, governmental and international organizations` representatives, academics, practitioners and entrepreneurs, moved to the Tech Gate Tower to discuss on Trend in Technology and Cyber Security. On the third day, organizers of the Vienna Cyber Security Week 2018, simultaneously hosted cyber range and policy table top tutorials and the Cyber Security Cluster Austria (CSCA) Day 2018.

The Cyber Range Tutorial introduced the concept of cyber ranges and cyber security policies and how they improve cyber security capabilities. Three cyber range case studies were presented by giving an indication of how they are beneficial to an organization. Some of 50 participants took an active participation within the Cyber Range Tutorial.

At the same time, Policy Table Top Tutorial was held as a parallel training. It was 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. This training was taken by 40 participants.

After the trainings were finished, the Reception & Official welcome by the CSCA 2018 organizers from AIT, FEEI, KSÖ, WKÖ/ASW, was held, followed by "Offensive Security Testing", introduced by Mr. Ron Peeters from Synack.

This special session presented a revolutionary security testing platform and managed security solutions which typically can find serious exploits in a matter of hours in any IT asset. It was concluded with a case study on the Pentagon where Synack was able to break in within only 4 hours' time.

DAY 4

The fourth day of Vienna Cyber Security Week 2018, "Securing the Energy Economy: Oil, Gas, Electricity & Nuclear", was held at the Tech Gate Tower, on 01 February. It gathered more than 100 participants and speakers. It examined 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 presented a core topic in terms of skills, processes, and common strategies for a more sustainable energy economy.

The first plenary session "Emerging and Future Threats to Digitalized Energy Systems", was dedicated to critical infrastructures, which are becoming more targeted and sophisticated and target operational and safety-critical systems, using a range of attack techniques. In this session, emphasis was given on the nature of the emerging threat landscape, and on the identification of broad trends which are being seen across the energy sector and elsewhere.

"Cyber Security Standards In Critical Energy Infrastructure", was the key topic of the second session, which aimed to inform participants about current standards, their state of application in the field, and to identify gaps that need to be addressed in the future.

The third session "Public Sector, Industry, and Research Cooperation in Cyber Security", focused 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.

This day was closed by the last session on "Securing Critical Energy Infrastructures by Understanding Global Energy Markets", in which energy experts give a short overview on the stakeholders and the markets of global energy.


Copyright Raimund Appel

DAY 5

The last day of the second edition of Vienna Cyber Security Week 2018, "Securing Smart Cities And Emerging Technologies", was held at the Tech Gate Tower, on 02 February 2018. It examined the Internet of Things (IoT) architectures, consumer devices, and consumer control functions that require new approaches to building resilient systems for our society, as well as cyber risks and consequences for state-of-the art technologies and promising research. It gathered 100 participants and speakers in total, and consisted of three regular and two special sessions.

This day started with the special session in which Chief Information Officer, Mrs. Urlike Huemer, presented the Digital City Vienna.

It was followed by the first plenary session "Making Smart Cities Cyber Secure", which pointed out the threats and vulnerabilities of smart cities, engineering security – how to build more resilient systems, and the detection and response – what to do when under attack.

The second session "Austrian & International Iot Safety & Security Light House Initiatives", introduced that Austrian industry and research institutions are on the technological forefront in cyberspace. It offered an insight in some national best practice topics and projects in theses terrains. The very last plenary session for the Vienna Cyber Security Week 2018, "The Promise And Challenge Of New Technologies", initiated a discussions on projected trends and emerging areas of technology, approaches and methods for verifying and securing new technologies, the state of the art and future security designs & methods, and ultimately, to the future of the cyber threat.

The second edition of Vienna Cyber Security Week, was closed by the official address of H.E. Amb. Karoly Dan, from the Permanent Mission of Hungary to the OSCE, and concluding remarks from the representatives of the AIT and Energypact Foundation.

Copyright Energypact Foundation

I am very pleased that we as the CSP are invited to be the co-organizers of this event which is happening now for the second time in Vienna, and which made Vienna the capital of cyber for at least one week in this year. I am really overwhelmed by the broad participation here in terms of participants but also of countries represented here which is the sign that people that have come here to discuss this topic in an unbiased and uncompetitive way, to progress the topic in the interest of our society. Cyber and Digital is the future and we have to make the decisions to bring them now to the agenda. I hope that this format will continue in the next years.

Thomas Stubbings
Chairman, Cyber Security Platform of the Austrian Government, CSP

This event is an important platform to discuss the cyber issues, and more importantly, cyber issues in the sector of the energy. Therefore, we encourage all stakeholders to join our regional efforts in work on cyber security, not only to develop the policies and strategies, but also to look for the practical solutions hoe to address the incidents, which are harming our lives, and the economic development. These are our priorities for the coming years, and we will work with the governments, civil society and other partners.

Jaroslaw Ponder
Head of the Office for Europe, International Telecommunication Union, ITU

Roger Bertozzi
Vice-President, Energypact Foundation

CYBER-SECURING THE WORLD: RESILIENT ORDERS IN AN ERA OF DISORDERS

We must conduct a copernician revolution where security, in a holistic multi-dimensional vision, is valued as a common good, and subsequently, cybersecurity is governed as a public good.

> *"Cybersecurity has to evolve from a security perspective into a societal grand vision where it is recognized and managed as the ultimate guarantor of peace, stability, prosperity…*

With its intrinsic cooperative and transnational nature, and with its universal reach in a smart world in the making, cybersecurity embodies the very essence of resilience in the XXI century: the ability to tackle emerging threats, asymmetric aggressions, rapid change and the fragmentation of the international system through the build-up of a collective intelligence.

The interconnected nature of threats and the interdependence of international actors accentuate the impact of the perils as the weakening of multilateral disciplines and solidarities makes powers less and less powerful actually when they face systemic and existential risks such as climate change, major pandemics, or cybercrime.

The world is becoming a cyber-ecosystem, from the internet of things to the 4.0 Industry, from the spread of Artificial Intelligence to the immersion of social life in the flow of digital contents and networks.

Cybersecurity therefore gains a central and unique status in global governance with profound implications for politics, diplomacy and social transformation: it has to evolve from a security perspective into a societal grand vision where it is recognized and managed as the ultimate guarantor of peace, stability, prosperity and fundamental multilateral rights such as the right of universal access to energy and all other rights defined in multilateral Agreements and Declarations which are more and more threatened by the risks of massive disruptions and attacks.

In an era of growing disorders, a new paradigm for convergence and contribution in international relations can emerge from the innovative governance of cybersecurity seen as a public good.

It is important for public diplomacy to make sure that beyond political and business circles, the issue of cyber security is better understood by civil society, because today cyber security is a holistic issue on which almost every aspect of our life depends.

Roger Bertozzi
Vice-President, Energypact Foundation

Zoran Predic
Deputy Minister,Ministry of Mining
and Energy of the Republic of Serbia

OPENING SPEECH

Ladies and gentlemen, distinguished participants, good morning to all of you. It is a great pleasure for me to attend this meeting on behalf of the Ministry of Mining and Energy of the Government of Serbia and get the opportunity to address you. It is very important that we, all together, joined this extremely important forum for discussion of energy security and especially the challenge of improving cyber security in the energy sector from a national and international perspective. First of all, I would like to sincerely thank the organizers (the Energypact Foundation, WKO, CSP Austria, and the Austrian Institute of Technology) for organizing such a conference and providing the opportunity for expert discussion and information exchange about extremely important issue of the protection of the energy sector from cyber attacks.

Energy security has many dimensions. The advancement of technology has enabled tremendous steps in all aspects of production, transport, distribution and end-use of energy. The importance of energy and the inability to live without it in everyday life is something needless to talk. Modern IT and related technologies have created increasing opportunities that were previously visible only in science fiction. ***We are currently witnessing the development and implementation of smart sensors, smart systems and smart cities that are changing the paradigm of business and everyday life.*** However, new technologies come with new challenges and new risks. Each digital device, each smart sensor, each new computer is a potential target for a cyber attack.

This new environment has not gone unnoticed by many potential adversaries. They continue to grow not only in number, but also in their capability and sophistication. While in the past, the targets of the attack were information systems, now these are also the operational technologies that drive critical energy infrastructure. The time we live in, is marked by almost every day pictures and reports of terrorist attacks all around the world. The extremists of all kinds, political and religious beliefs, do not choose the way to kill dozens, hundreds or thousands of innocent people, to achieve their goals. Unlike these physical attacks, cyber attacks are not limited with barriers, or national borders. They can be carried out at any moment and at any place from a vast distance, and material destruction as well as the number of victims could be much higher.

In Serbia the awareness of the potential danger of cyber attacks is growing up every day. ***We are fully convinced that the energy sector represents a serious potential target because it is the heart of every state, every economy.*** Our energy companies are making great efforts to provide the most up-to-date protection of their infrastructure and thus protect millions of end-users from possible consequences. In October last year, in cooperation with the OSCE (Organization for Security and Co-operation in Europe) and domestic institutions, a very useful practical exercise was held in Belgrade. The results show that in addition to the technical and technological strengthening of cyber security, additional attention must be paid to improve and upgrade the regulatory and institutional framework, both nationally and internationally. In addition, one of the key challenges is the lack of qualified security professionals to meet growing needs. ***We should all think about the available number of cyber specialists, first of all those who have operational experience in the systems that run our energy infrastructure.***

Cyber security is not only a matter of the state: it is an international issue that requires cooperation, partnership and unity of efforts not only between governments, but also industries and organizations. In the future, a number of activities are needed to promote awareness and partnership to develop protection against cyber attacks. ***Cyber security as well as energy security are a processes that needs to be constantly evolving and adapted to new technologies, in order to have an adequate response at any time for a credible and dynamic adversary.***

We must continue to promote and support activities such as today's event in order to achieve common understanding, and to find answers to new challenges in front of us. In addition, I believe that a hard work is ahead of us in order to improve our capacities to develop more cyber-security experts in the energy sector.

In conclusion, I would like to thank the conference organizers for providing this opportunity to share information and experiences in order to build international confidence in this area.

I am convinced that by working together and sharing our experience, all of us can help in improving the protection of critical energy infrastructure from the impact of cyber attacks.

I wish everyone an interesting and fruitful conference.

Thank you.

H. E. Amb. Mikhail Konarovsky
Advisor, Secretariat of Shanghai Cooperation Organization, SCO

PROVIDING INTERNATIONAL CYBER SECURITY: THE SCO EXPERIENCE

The Shanghai Cooperation Organization's principal activity aims at strengthening of mutual trust, friendship and neighbourness among member states, amid their broad cooperation in various areas. This objective fully applies to countering terrorism and extremism. SCO nations' main point is that ICT should serve to bring cultures and civilizations together and to promote exchanges among them, but not to divide them.

In early 2000th the Heads of SCO member states issued a Statement expressing serious concern over the use of ICT for purposes that could damage the security of individuals, society and the states in violation of the principles of equality, mutual respect and non-interference in internal affairs. In 2006, the ad-hoc Working group on information and telecommunication technologies was established with core attention on identifying ways and means of addressing all aspects of the concerned issues. A number of international seminars have also been held. Their attention was focused on the exchange of experience in using and developing of current information and telecommunication technologies.

The 2009 Intergovernmental Agreement on cooperation in ensuring international information security defines such concepts as information security, information wars, weapons and crime, information terrorism, unauthorized interference in information resources, etc. Simultaneously, special bodies responsible for the implementation of the document were identified. International cyber security issue is being discussed at regular consultations of the SCO member states' Foreign Ministries.

In 2015 a new SCO ten year Development Strategy has been approved, with its significant part dedicated to the international information security as well. The document reaffirmed the readiness to continue close cooperation in countering crimes in the sphere of ICT and noted intention for further cooperation in Internet control to prevent its use focused on undermining of regional security and stability.

In order to do this, the SCO Summit in last June adopted the Statement on terrorism. In this context, the member nations reaffirmed the significance to prevent the spread of terrorist ideology and propaganda. They confirmed as well the determination to promote efforts to prevent the radicalization of societies that could lead to utmost extremism, first of all, among the young.

These provisions were elaborated as well in the Convention on Countering Extremism, also adopted at the Astana Summit. It reaffirms the obligation to take necessary legislative measures to establish liability of failure of the person who provides the access to information and telecommunication systems and the demands of the authorized agency to restrict access to extremist materials.

The SCO fully supports the United Nations' activities in examining existing and potential threats in information security and possible joint measures to eliminate them as well as in researching concepts to promote security of global information and telecommunication systems. The SCO member states resolutely stand for drawing up in the UN framework of a universal code of principles regulating behavior in the information space.

The new edition of the Code of Conduct for International Information Security had been, issued in 2015 on behalf of the SCO member states as an official UN document. The SCO welcomes the UN General Assemblies' resolutions on Achievements in the field of information and telecommunications in the context of international security.

Just recently the SCO reaffirmed expediency to enhance overall interactions in this sphere and reviewed a draft resolution "Achievements in the field of information and telecommunications" due to be presented to the 73th GA Session on behalf of the SCO member nations.

Taking in consideration the ever growing importance of all aspects of ICT and cyber security the SCO is ready to work together with other members of the international community on the elaboration of a unified international regulation of this field.

This expectation fully corresponds with its policy which aims at enhancing the Organization's transregional political profile as a result of its recent enlargement and expansion of international contacts.


WKO
AUSSENWIRTSCHAFT AUSTRIA
AUSSEN
WIRTSCHAFT
Austria's Official Trade Promotion Organisation
AUSTRIA BUILDING BRIDGES
AIT
AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY
JAN SCHUBERT

Reinhard Posch,
CIO – Federal Government of Austria

CYBER SECURITY WEEK - DIGITAL FIRST – EMERGING GAPS

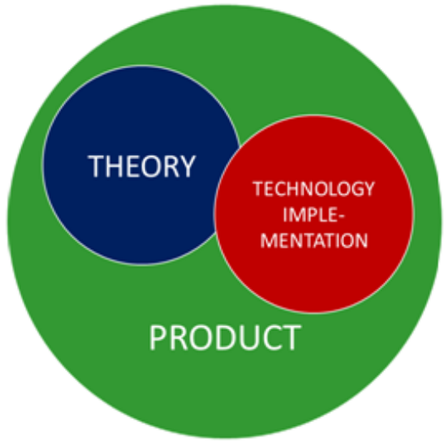
We are all aware of the gaps existing due to the security divide and gradually this is taken on board on one hand and getting smaller and smaller as digital native and digital adopted/converted people are the ever-growing majority. ***What we are not aware of is that volume matters and changes quality.***

Just think about pictures. As long as technology was only able to generate and display pictures at a rate below 5 in a second movies were nothing that came in our mind. As the barrier of 10 per second was doable, a very new facet came in.
In addition, it is common knowledge that bigger entities are in many situations more efficient and productive. Search engines; Cloud … all this is a perfect proof of this fact. This also is underpinned with an argument of greater stability and reliability. What is sometimes overlooked in this context is the aspect of the single point of failure. This is usually beaten with the argument of multiple locations, redundancy etc. With this regard, we might want to learn from evolution of the society. ***It is common understanding that distribution of powers in a community (democracy) outperforms a centralistic regime with this aspect of "single point of failure"*** – the Second World War being the perfect example.

What does this tell us in terms of new technologies?
The perception that monopolies with search engines exhibits the potential of such danger has arrived at our minds. With other technologies, we still have to sharpen awareness. The following gives a few examples that these aspects are not minor.

A Crypto: For the general public crypto is associated with a strange flair of conspiracy and dubious secrets. This perception is even used in the political debate for example with legal interception and the argument that the good people have nothing to hide. However, crypto is at this moment the only way to efficiently secure digital values. Webpages, bank accounts, identity management – like everything depends on the quality of cryptographic algorithms and implementations. Quality being taken on board by complexity of problems in informatics and implementation by manufacturers.

As concerns algorithms we are living in a monoculture depending on NP-Completeness. We know quantum computers might challenge this. Research and implementation being limited to large institutions give us some certainty of having this under control as concerns timing and the need to change to post quantum. We can easier face a problem as we can imagine the problem.



The situation becomes ways more difficult when we face with a problem that was not within our imagination. Basically this might happen if there was a flaw in the theory or when the model of having a theory which is technically implemented in a proper way resulting in a good product is no more applicable. We have to work with assumptions of the linearity of time when it comes to criticality of systems and attacks. However, even if very rarely it turns out that sometimes the assumptions need a revision.

When in 1996 Paul C. Kocher came up with its timing attack to RSA etc., he did not find a flaw in the theory but in the assumption, you cannot extract information without tapping into memory or instructions.
Side channel attacks made a whole generation of smartcards obsolete even if they were physically perfectly secured beforehand. The specific property of the timing attack is that it is not using standard processing scenarios. Countermeasures therefore are only possible by changing the design.

Cloud & Intel:
Differential analysis that became famous with the idea of Paul Kocher and was soon extended from timing to other side channel effects challenged the industry but covered a limited area as smartcards were in coverage and application still limited at that time. More than 20 years later 2018 an equally the Meltdown attack (https://meltdownattack.com/) shocked the Intel world as the assumption of the industry applied for over 15 years needs a revision. Unlike the timing attack on keys Meltdown affects all situations where information is assumed to be safely locked away by keeping it within a process. This ranges from the laptop executing a JavaScript from a web page to virtual machines running in clouds virtualized on the same kernel. Like with the timing attack standard behavior as designed is used to retrieve storage information that should only be available to users with super user access rights. The attack not only theoretically extracts such information and this is done with rather high speed at minimum cost. Having a de facto monopoly of basic processor design structures makes this aspect and order of magnitude more important.

IoT and Security:
Internet of things has specific properties. One being the potential of extremely high numbers of devices on the internet. While there is hardly any use for one person to have more than one or perhaps two mobile phones. IoT devices do not have these limits. It is e.g. perfectly imaginable that each switch in a private home for lights etc. sits on the internet and can be addressed for actions.
In addition, anyone can buy a fully equipped device (including persistent storage and Wi-Fi as well as analog and digital IO) for under 2€. The entry barrier into the market is virtually nonexistent from this point of view. This also means that already now systems are

offered that do not care for security and protection of data at all. The functionality counts.
In case we stay where we are in terms of regulation and control we soon will have a huge number of devices in the field and this will be a perfect environment for criminal activities like detecting when and where breaking into an private home is from the viewpoint of the criminal effective at minimum risk. This might even be offered as a service. Devices come from all over the world so that we do not have a fair chance to influence the source. In addition, ***functionality beats security – at least for the broad public.***

We still need to close this gap as it might cause huge security weakness. One possible successful avenue would be to hold the supply chain liable if something happens. As a first step, sharing damage between users and vendors might be the opportunity to prevent vendors from selling completely broken devices as concerns security and even lead to the situation that vendors start to educate users in order to avoid them to get liable. What we would have to do is to install and keep up to date a set of effective minimum-security standards which, when followed, would free vendors from liability – a mechanism which is not unusual when we look e.g. at payment system based on smart cards.

Dr. Reinhard Marak
Chief Executive of the Austrian Defence and Security Industries Group,
Austrian Federal Economic Chamber, WKÖ

EUROPEAN CYBER DEFENCE FUND

One does not have to be a rocket scientist to understand that our security environment is constantly changing and we nowadays face threats of a different nature than some decades ago. On one hand, the kinds of threats have changed, on the other the origins of threats have changed as well. Today governments often find themselves in the so-called hybrid threat situations, meaning that neither their adversary nor the threat is clearly identifiable. Particularly in the Cyber domain, it is not necessarily clear whether a governmental organisation or some nerds with a specific affection to their political elites execute an attack.

Copyright Raimund Appel

At the same time, ***in today's conflicts a Cyber-attack on, let's say, critical infrastructure of a state can potentially cause more harm to the security situation of that nation than a conventional one.*** Therefore, it does not come as a surprise that recently Cyber entered the scene as the "fourth service" besides the traditional three military services Army, Navy and Airforce. ***As any of those services need an industrial base that prove them with the necessary means to counter threats, Cyber has as an important industrial dimension as has any other service.***

On a national Austrian and especially on a European level the awareness of the importance of Cyber security and defence within the public sector is increasing. In June 2017, the European Commission has launched the European Defence Fund (EDF), which has a dedicated budget for collaborative defence research and for collaborative development of defence capabilities. Starting in 2021 and as a part of the EU's Multiannual Financial Framework (MFF) from 2021 to 2027, a budget of 500 million Euros per year will be allocated to the future European Defence Research Programme (EDRP). The European Defence Industrial Development Programme (EDIDP), which promotes the development of defence technology as well as the cross-border building of consortia, will have an annual budget of 4 billion, starting in 2021. The EDIDP's budget is composed of the European Commission's funding (around 20 percent), and the member states' budget (around 80 percent). The EDIDP offers great chances for both, the industries operating in the defence sector and the public-sector stakeholders trying to strengthen their capabilities to counter threats to their territory and people. It should be in the interest of each EU member state to maintain and strengthen its national defence industry base as an integral part of the European Defence Technological and Industrial Base (EDTIB).

The EDF supports defence research and industrial defence development programmes already before the start of the next MFF in 2021. The Preparatory Action on Defence Research (PADR) is focused on research and is funded with 90 million Euros until 2020, whereas the EDIDP has a preliminary funding of 2 billion Euros - 500 million Euros funded by the Commission, about 1.5 billion by the member states. In addition, the European Defence Agency (EDA) and the European Investment Bank (EIB) recently signed a cooperation agreement that strengthens the EIB's support for Research, Development and Innovation (RDI) for dual-use technologies, Cyber security and civilian security infrastructure. ***An early dialogue between the governmental demand side and the private entrepreneurs on the supply side is essential for the maintenance of the strategic security and defence sector.*** In order to promote and strengthen this dialogue, the Austrian Security and Defence Industries Group of the Federal Economic Chamber puts a special focus on Cyber security. Within a Cyber Security Cluster, target group industries shall build cooperations, get access to information on recent grants and research programmes, and present their products and companies to public-sector stakeholders in their home market and globally.

As Austria introduced a defence research programme only recently, this is a new chance for industry to access new funding programmes, be it on a national basis or in cooperation with the EU.

When it comes to Cyber threats and Cyber security, there is little difference between industry and the public sector as a target. Industries have similar security requirements as states and both have a severe vulnerability towards external Cyber-attacks. Thus, companies could develop defence products not only for the public sector, but also as spin-offs for the private sector and vice versa.

The public as well as the private sector need innovative and well-functioning companies that conduct research and work on identifying Cyber challenges in order to defend the state and critical infrastructures against possible Cyber-attacks. The Austrian Security and Defence Industries Group is designed to be the interface between the defence and security industry and the public sector, with the objective to ease mutual communication and understanding.

Copyright Raimund Appel

Ron Peeters Synack

POWERED SECURITY WITHOUT COMPROMISE

In 2016, cyber incidents were up 1512% compared to the decade prior. Traditional methods of security simply aren't holding up against the modern adversary, which has led CISOs across the world and across industries to try "hacker-powered security". Ethical hackers are now rightfully seen as the only hope against the threat of unethical hacking that has exposed millions of consumer records, caused irreparable monetary and brand damage to companies around the world, and captured countless news headlines.

In just one year, Synack and the US Government have taken a disruptive idea and made hacker-powered security an invaluable reality. It all started last year when the US Internal Revenue Service approached Synack looking for a more effective and efficient way to conduct security testing. They had heard about Synack's crowdsourced penetration testing solution, and they were interested in leveraging the diverse skillsets of a crowd of ethical hackers in a private, managed model. The US Department of Defense quickly followed, partnering with Synack to launch our "Hack the Pentagon" program. A domino effect continued, and US agencies began to realize that they could find more impactful vulnerabilities with less burden on their internal resources by harnessing the power of a highly vetted group of security researchers.

> *We believe in enabling organizations around the world to utilize trusted, ethical hackers to find and fix vulnerabilities in their digital assets before criminal hackers exploit them.*

• We opened internal, mission-critical government systems for external hackers to test.

•We discovered critical vulnerabilities in hardened, mission-critical assets (i.e. zero days). If exploited, these vulnerabilities could have let an attacker send a tank to the White House or derail a critical message being sent to warfighters on the frontlines.

• We shortened the time from vulnerability discovery to remediation to 24 hours and the time from patch to verification to <72 hours.

• We increased their security teams on-demand by over 10 times.

Using a hacker-powered approach to security testing quickly proved to be more effective and efficient than traditional methods. Synack consistently provides >53% ROI over a traditional penetration test. Because of these results, the Synack solution has spread rapidly within the federal government and beyond to the private sector. We believe in "hacker-powered" security, and our experience proves that it always has to be done in the right way.

We believe in enabling organizations around the world to utilize trusted, ethical hackers to find and fix vulnerabilities in their digital assets before criminal hackers exploit them. And in so doing, we can't allow any form of compromise.

There's a reason why we are seeing a swift uptake of programs on Synack's platform. These programs are:

• Trusted and controlled, using only the most skilled, trustworthy ethical hackers with complete audibility

• On-demand, offering the ability to launch a program within 24 hours and receive real-time analytics and reporting on the actionable results

• Efficient, augmenting and scaling internal security teams to completely remove the burden of vulnerability discovery, triage, and remediation

• Effective, uncovering vulnerabilities unknown to an asset owner and highly coveted by the adversary

We are passionate about making the world more secure and that's why we are always putting our heads together to imagine what it will take. When Synack launched in 2013, we set out to redefine traditional security testing through revolutionary technology and innovative thinking. Synack's private, managed hacker-powered security solution arms clients with access to the world's most skilled, highly vetted ethical hackers who provide a truly adversarial perspective to clients' IT environments. Whether it's Responsible Disclosure, Vulnerability Discovery, Crowdsourced Penetration Testing or Continuous Testing, Synack offers the same high standards and quality. Synack Hacker-Powered Security is enabling organizations everywhere to go on the offensive and utilize the most qualified and trusted group of people from around the world to become stronger against criminal cyber attacks.

Here's to the future:
Security Testing — Powered by Hackers — Without Compromise.

> *We are passionate about making the world more secure and that's why we are always putting our heads together to imagine what it will take.*

Copyright Raimund Appel

Andreas Stadler
Minister Plenipotentiary&Deputy Head of Mission
Permanent Mission of Austria to the OSCE

THE OSCE AND CYBER DIPLOMACY IN 2018 MAKING „CYBER“ A CROSS-DIMENSIONAL FOCUS OF SECURITY

We are challenged with the biggest security crisis in Europe since the end of the Cold War as we face negligence and violations of OSCE principles and commitments that were created and solemnly celebrated with the Helsinki Final Act in 1975 and the “Charter of Paris for a New Europe” in 1990. The last unifying and leading OSCE document on the level of Heads of States and Governments is called the “Astana Commemorative Declaration Towards a Security Community”, adopted in Kazakhstan in 2010, already under the worrying shadow of the Russia-Georgia War of 2008 and the evolving world financial and economic crisis. Ever since Astana we need to soberly acknowledge that this so-called “Security Community” has become more and more defined by mutual distrust and confrontation. Since 2014 we have witnessed war in Ukraine and large-scale military exercises outside the so-called OSCE Vienna Document which is the main agreement supposed to build military confidence by exchanging relevant information on armed forces, their doctrines, strengths and calendar of exercises. We are also going through economic sanctions and counter-sanctions and noticing a shrinking space for democracy, the rule of law and the once so praised civil society. But democracy is not only under attack by repressive or illiberal states, but also by the parallel rise of organized crime and terrorism. Beyond the borders of the OSCE we are challenged by civil wars in the Middle East and North Africa, leading to significant movements of refugees and migrants. This is why Austria as the OSCE Chairmanship 2017 decided to focus on three main goals, priorities that we will continue to pursue in 2018 and probably beyond: 1) we want to contribute to defusing existing conflicts and to rebuild trust and confidence 2) we need to address the dangers of radicalization and terrorism 3) we want to strengthen the OSCE both politically and in terms of structure and organisation, to make it “fit for purpose”. Cyber security poses a challenge in all these three priority areas and it needs to be addressed in all three dimensions of the OSCE that form the OSCE´s unique concept of so-called “comprehensive security” which comprises military, economic and environmental and human rights aspects of security. 1) Regarding conflicts, we are facing real risks of conflict stemming from the use of information and telecommunication technologies (ICT): we have witnessed cyber-attacks in Ukraine on critical energy infrastructure (2015, 2017), following attacks in Estonia (2007), Georgia (2008) and indeed also on the OSCE itself (2016)! Furthermore, we are all aware of the mutual accusations by the USA and Russia on cyber interference and espionage. The uncertainty about the origin of hostile cyber- action, the so-called “problem of attribution” is a common characteristic that introduces suspicion, mutual distrust, and open accusations in international affairs. 2) As to the fight against terrorism: the Internet is being abused on a large scale to radicalize and recruit people for violent extremism. States therefore need to work with the providers of ICTs, the media and social media networks to guarantee that the same rules for hate speech, defamation and instigation to extremism and terrorism that apply to traditional “offline” communication are also enforced online. This requires close cooperation between states and the private sector, academia and civil society, also with a view to ensuring respect for human rights and freedom of speech. 3) And this brings me to the third dimension of the OSCE’s comprehensive concept of security: the protection of human rights “online” as well as “offline”, including the right to privacy. The 2013 disclosures of Edward Snowden revealed numerous global surveillance programs, many run by the USA’s NSA and the so-called “Five Eyes Intelligence Alliance,” with the cooperation of numerous governments. It raised serious questions as to data integrity and security of regular citizens. Snowden´s leaks were picked up by the Austrian lawyer and activist Max Schrems, who became famous for his campaigns against Facebook for privacy violation. Schrems accused the Irish Data Protection Commissioner and the European Commission of violating European privacy laws and illegally transferring personal data to the NSA’s PRISM program.

He won this highly visible case before the European Court of Justice in 2015. These cases show that internet and ICTs have become a target for disproportionate and often illegal surveillance everywhere; however, we are particularly concerned with the reports of the Moscow-based writers and activists Irina Borogan and Andrej Soldatov about how the Russian state instrumentalizes the internet and ICTs internally and internationally. We do not share the view that cyber security can be achieved through state censorship of the content of information. There must be no doubt that the freedom of speech and the right to privacy are protected both offline and online. Faced with these cross-dimensional challenges, we need to continue to 1) work towards a common understanding for norms, rules and principles of responsible state behaviour in cyber space; 2) promote confidence and trust between states; and 3) undertake efforts to increase cyber-resilience by promoting capacity-building.

Let me begin with the first point: to establish a universal understanding of rules, norms and principles of responsible state behavior in cyber space, we first must turn to the United Nations. The UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, known as the UN Cyber GGE, had the following task: - to study, with a view to promote common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them. There have been five GGEs so far (2004-05, 2009-10, 2012-13, 2014-15, and 2016-17). Although the 2016-17 Cyber GGE could not agree on common recommendations for the UN, the previous substantial reports offer a rich basis for rules, norms and principles of responsible state behavior for all states. In particular the 2015 report recommended, for example, that states should not conduct or knowingly support ICT activity that intentionally damages critical infrastructure. It also called for an increased exchange of information and assistance to prosecute terrorist and criminal use of ICTs. The report requests states to not knowingly support ICT activity contrary to international law and it goes even further to stipulate that states must not allow their territory to be used for intentionally wrongful acts using ICTs. In doing so, the UN Group of Governmental Experts emphasized that states should guarantee full respect for human rights, including privacy and freedom of expression. Furthermore, the United Nations General Assembly has confirmed that international law, and in particular the UN Charter, is applicable in cyberspace. All these UN recommendations provide vital guidance to continue cooperation on cyber policies, norms and rules with a view to build trust and confidence between states. This is where the OSCE can be of great added value. With its comprehensive approach to security, it has the tool box to play a key role in promoting cyber security. OSCE participating States have adopted 16 confidence-building measures to reduce the risks of conflict stemming from the use of ICTs. Let me just mention some of them:

1) a general commitment to cooperate in the field of ICT to prevent incidents and mitigate tensions (CBM 3);

2) the nomination of official contact points in all participating States for this purpose (CBM 8);

3) measures to counter terrorist or criminal use of ICTs in line with OSCE commitments (CBM 6);
4) a commitment to protect critical infrastructure from malicious ICT activities(CBM 15); and
5) a commitment to an open, interoperable, secure and reliable Internet which in the interpretation of Austria encompasses all aspects of human rights on the internet (CBM 4). While there is an OSCE-wide consensus on the great potential of these CBMs, these agreements are yet to be implemented which is why all OSCE participating States need to redouble efforts to translate rhetorical declarations into honest and practical cooperation. And here the OSCE can also learn from the example of the European Union (EU) which has made enormous progress in terms of enhancing cyber-resilience through cooperation of its Member States. Cyber security was one major theme of the 2017 State of the Union address by EU President Jean Claude Juncker who emphasized the need for the EU to be better equipped to face evolving threats from cyber. The European Union had already agreed on the so-called "Network and Information Systems Directive" (NIS) and the "General Data Protection Regulation" 2016, two important regulatory frameworks that will enter into force in 2018 and that address important questions of cyber and data security.
Building on the EU cyber security strategy, the European Commission and the High Representative proposed the Joint Communication on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" last September.
It also emphasizes international cooperation and the need to support capacity building in third countries which will in turn help raise the level of cyber security globally. Also last year the Political and Security Committee of the Council of the European Union adopted the so called "Cyber Diplomacy Toolbox" pulling together all the possible tools for a collective response on a global level that range from joint declarations to sanctions and further. And here the OSCE comes in again: ***despite the overall grim atmosphere and security situation, 28 EU members out of the 57 OSCE participating States have demonstrated that they can actually work together, develop trusted communication and co-operation networks and even reach out to third countries to support their cyber security efforts. It might possibly sound naïve and overly optimistic, but if 28 states can work together, why should we not also strive for better cooperation in the world´s largest regional security organization, the OSCE?*** Last December in Vienna, all 57 Ministers of Foreign Affairs managed to agree on a OSCE Ministerial Council decision which aims to reduce the risk of cyber conflicts. It endorsed previous commitments to implement confidence building measures in a specially created "Informal Working Group". It is imperative to use this OSCE "Informal Working Group" to effectively address threat perceptions, suspicions, and accusations. This organization is as a regional organization under Chapter VIII of the Charter of the United Nations made to discuss questions of attribution, norms and rules of state behavior. Moreover, the OSCE´s comprehensive concept of security dealing with 1) politico-military questions of arms reduction and disarmament, 2) economic, technological and educational cooperation and 3) human rights offers the right toolbox for cyber cooperation as well. And it has a lot of experience in improving relationships between states and civil society, including the private sector and academia. The OSCE might not, due to the lack of political will of opposing sides, be a very strong and effective international organization. In fact, it is really only a permanent conference of ministers of foreign affairs and their diplomats, with a few thousand people working in its Secretariat and Institutions and the field missions. However, the OSCE is the only platform left where all stakeholders can come together on an equal footing. We need to use it better.

In the international arena, the OSCE is playing the unique pioneer role in enhancing cyber security among its participating states. We focused on increasing transparency among our states, and enhancing cooperation with the aim to mitigate the effects on cyber attacks and cyber incidents on critical infrastructure.
The OSCE confidence building measures (CBMs), may be considered as cyber security at the international level. Italy as current chair of OSCE is deeply committed to that. We encourage analyses on how to improve the implementation the CBMs, and we will organize the cyber security conference in autumn in Rome.

Isa Ghivarelli
Counsellor, Deputy Head of Delegation for the Politico-Military Dimension,
Permanent Mission of Italy to OSCE, 2018 Italian OSCE Chairmanship

Dr. Petar Stanojevic
Full Professor, University of Belgrade

NEW ENERGY SECURITY PARADIGM - ELECTRIC VEHICLES (AND REGIONAL HINTS)

Sale of electric vehicles (EVs) in the world grows with exponential trajectory. In 2010, fewer than 700 EVs were sold across the EU and today roughly 700,000 per year. Half of all new vehicles in Norway are fully-electric or plug-in hybrids today. Earlier in 2017, Norway opened the world's largest fast-charging station, which can charge up to 28 vehicles in about half an hour.

"All new cars sold in Europe will be electric within less than two decades, driven by government support, falling battery costs and economies of scale, a Dutch ING bank has predicted" ("The Guardian" 13/07/2017). The forecast of the UK's National Grid said it expects 90% of new cars in Britain to be electric by 2050. The ING bank said that it believed pure electric cars would "become the rational choice for motorists in Europe" sometime between 2017 and 2024, as their car showroom prices fall, their ranges increase and charging infrastructure becomes more widespread.

> ***The longer term objectives of the new strategy are to decrease oil import dependency, increase innovation and competitiveness and faster opportunities for growth and jobs.***

Situation in EU is such that the Netherlands is planning to phase out all internal combustion engine vehicles by 2035 and has the highest ratio between public charging points and electric vehicles. France's committed to ban combustion car sales by 2040. The European Commission has published the European strategy for low emission mobility (EC, 2016). The longer term objectives of the new strategy are to decrease oil import dependency, increase innovation and competitiveness and faster opportunities for growth and jobs. The transport sector's GHG emission reduction targets are, for example, designed to contribute to the EU's overall goal to reduce GHG emissions by 80–95 % by 2050. EVs incentives are widely in place...

Copyright Raimund Appel

EVs have several advantages over conventional combustion engines: a) this includes their higher efficiency (an electric vehicle converts around 80 % of the energy it uses to usable power, compared with around 20% for a conventional vehicle), b) high durability, c) lower maintenance costs and d) quieter noise levels at low speeds. With regard to the wider transport sector, electric vehicles are a ready technology only at the light-weight end. The aviation, shipping and haulage industries had to make big efficiency gains in the short term. That is why zero – emissions solutions in those areas remained in process of development.

If the world is to stand any chance of staying within the 1.5C0 warming limit set by world leaders in Paris, electric vehicles must replace traditional combustion engines entirely by 2035. To reach the secondary goal of the Paris agreement – keeping warming below 2C0 – electric vehicles will still need be to hugely mobilized. By 2050 half of all cars would need to be "zero-emissions". The electric vehicles come with their own challenges, most importantly, the increased demand for electricity. The emissions gains won by electric vehicles will be undermined unless the electricity sector is decarbonized. Oil companies like Shell or Saudi ARAMCO and the International Energy Agency (IEA) dismissed the idea that electric vehicles will hurt oil demand. Existing known oil & gas deposits are more than enough to satisfy the future consumption and price will not fly up high. At the same time Shell and other petroleum companies hurriedly install chargers on existing petrol stations.

Almost every car manufacturer has now included electric vehicles in its range, with each producer launching at least one new plug in hybrid electric model each year. More than 30 models are currently available in Europe. Small petrol & diesel cars are still significantly cheaper and are small fuel consumers (cost of ownership is low) and are one of the development directions.

Despite the huge investments in the battery's development progress is not as fast as expected and some producers (like Toyota) are working in parallel on more efficient engines development. Development of "intelligent car" is also a trend in the car industry. Cost of ownership (including fuel cost) will be the main market driver in the future as it was in the past. Battery is still expensive and charging infrastructure still need significant development. Critics argue the EU car industry is highly profitable and will need to invest heavily in electric vehicles to remain in business. "European car companies will suffer the same catastrophic collapse Nokia experienced for failing to embrace new technologies".

At the same time, we see a little reluctance or slight support from the energy sector. The electricity utilities are more interested in electric vehicles as an energy peak solution than anything else. With renewable energy not always generating power when it is needed, using it to charge electric vehicles overnight would help to even out the distribution of power that they generate. Recent findings from the EEA show that, if a hypothetical 80% of cars in 2050 were electric, an additional 150GW of additional electricity generation capacity would be needed across the EU (assuming no reduction of demand from other sectors) (EEA, 2016a). Contemporary EU total capacity is about 980GW so required increase should be cca. 15% driven only by the EVs. Distribution grid and interconnections have to grow accordingly. The Balkan region and Italy, is in deficit (the deficit was 40TWh (15-75TWh up to 2020), which is the equivalent to 9 GWh of power). By 2020, due to inefficiency, exploitation due dates and noncompliance with EU environmental demands, numerous providers (power plants) will be shut down in the region. There are almost no incentives for EVs and only couple out of dozens EVs operate. Region sees slow generation capacities development in both fossil or renewable area.

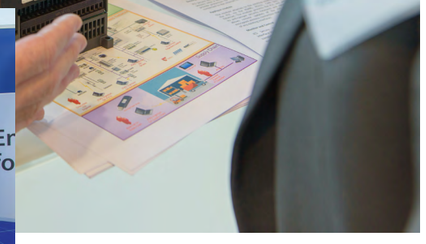
If to make calculation based exclusively on energy prices all regional countries fall in the group where is cheaper to drive on electricity than on fuel (if calculate on EPA (US Environmental Protection Agency) gallon gasoline equivalent and current electricity and fuel prices). The region is to expect Inflow of: cheap second-hand petrol & diesel cars, second-hand EVs and new luxurious EVs. For example, Serbia has 258 cars per 1,000 inhabitants. Similar are the regional figures. EU average is 460-500. If socio-economic development would not be interrupted the vehicle numbers should be doubled in no more than 20 years in case of 3% steady growth of GDP. If to calculate additional load based on the assumption of duplication of car numbers and fleet new structure in years up to 2040: 5-600,000t of petroleum products (or 25% increase) and 450-500MW of generation (7% capacity increase) will be needed only for the transport sector without satisfying needs of mega projects like "Silk road".

General scarce of energy in the region combined with increased consumption growth and slow development of production capacities and grid infrastructure can lead only to electricity price hike. This hike can be dangerous for overall economic growth and have social impact as well. To achieve goals in introduction of the renewable energy sources further digitalization and decentralization of electricity production and distribution system has to be achieved (smart grids). Lack of security of energy production and transmission infrastructure, including cyber security can just worsen the situation.

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 invited leading companies to a technology exhibition of latest solutions and products as well as R&D projects. Visitors have had 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 infrastructure to fight against cyber crime and terrorism.

Over three days of Expo, exactly 21 companies presented their products and services, while more than 250 participants had the chance to get introduced with their solutions, and to establish B2B relations.



WKO AUSSENWIRTSCHAFT AUSTRIA

CSP AUSTRIA

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

energypact foundation

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

With the support of

ITU OSCE IEC

EUROPE INTEGRATION FOREIGN AFFAIRS
FEDERAL MINISTRY
REPUBLIC OF AUSTRIA

REPUBLIC OF AUSTRIA
FEDERAL MINISTRY OF DEFENCE

BUNDESKANZLERAMT ÖSTERREICH

BM.I REPUBLIC OF AUSTRIA
FEDERAL MINISTRY OF THE INTERIOR

bmvit
Federal Ministry for Transport, Innovation and Technology

With courtesy of

WKO WIRTSCHAFTSKAMMER ÖSTERREICH ARGE Sicherheit & Wirtschaft

DIGITAL CITY WIEN

KURATORIUM SICHERES ÖSTERREICH

FORTINET

OMV

KPMG

FEI

IKARUS security software