NEWSLETTER

Vienna, April 2017

energypact foundation

THE NEED

The development, security, and sustainability of energy are key components of national and international growth and stability. Energy production is often a mixture of fossil fuels, hydropower, nuclear, wind, solar, and other sources. Technological advances are essential to further energy efficiencies and to reduce the carbon footprint of production. The same technology that furthers energy production and delivery can at the same time create vulnerabilities that can be exploited by malicious actors. Recent events within the energy sector are vivid reminders that cyber-attacks represent an ongoing operational risk with potentially devastating consequences.

THE VIENNA PROJECT

The Energypact Foundation was established in 2007 in Switzerland as a non-profit and non-political organisation. Since its inception, the Energypact Foundation has engaged the international energy community through activities aimed at raising the global awareness on issues related to energy development and sustainability. These activities have included coordination and sponsorship of multiple international conferences for information exchange and confidence building.

Relocating to Vienna, Austria in 2017 to be at the centre of international energy discussions, Energypact has launched the "Vienna Project" to promote and launch activities supporting awareness and dialogue on energy security with specific focus on cyber security for the energy sector.

EUROPE
INTEGRATION
FOREIGN AFFAIRS
FEDERAL MINISTRY
REPUBLIC OF AUSTRIA

energypact foundation

FEDERAL MINISTRY OF DEFENCE AND SPORTS

VIENNA CYBER SECURITY WEEK 2017

Protecting Critical Energy Infrastructure

February 14, 16 & 17

CSP AUSTRIA

National Defence Academy
Vienna

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

courtesy of

EY OMV

VIENNA CYBER SECURITY WEEK 2017

PROTECTING VITAL ENERGY INFRASTRUCTURE

The Vienna Cyber Security Week is the centrepiece annual event co-organised by the Energypact Foundation and Austrian governmental and non-governmental actors to engage with key national and international stakeholders in dialogue and cooperation in the field of cyber security for critical infrastructure in general and the energy field in particular.

February 2017 saw the inaugural event co-organised by the Energypact Foundation, the Federal Ministry for Europe, Integration and Foreign Affairs of Austria, the Federal Ministry of Defence and Sports of Austria, the AIT Austrian Institute of Technology, the CSP Austrian Cybersecurity Platform and hosted by the National Defence Academy on 14, 16 and 17 February 2017 in Vienna, in the margins of the Conference of the Austrian OSCE Chairmanship on Cyber Security for Critical Infrastructure – Strengthening Confidence Building in the OSCE, which took place on 15 February 2017.

- Days of Discussion & Exchange: **3**
- Participants: **> 200**
- Represented States: **26**
- International Organizations: **8**
- Expert Speakers/Panellists: **> 70**

Feb 14

International Intergovernmental High Level Panel

PROTECTING CRITICAL INFRASTRUCTURE FROM CYBERATTACKS

A Global Challenge

Feb 16

International Multistakeholder Conference

CYBERSPACE, ENERGY & DEVELOPMENT

Protecting Critical Energy Infrastructure

supported by:

IEC UNODC United Nations Office on Drugs and Crime ITU

Feb 17

International Business High Level Panel

DIGITAL SECURITY

Protecting Strategic Business Leadership

energypact foundation

DAY 1: 14 FEBRUARY 2017 INTERNATIONAL INTERGOVERNMENTAL HIGH LEVEL PANEL: PROTECTING CRITICAL INFRASTRUCTURE FROM CYBER ATTACKS - A GLOBAL CHALLENGE

Cyber-exploitation and cyber-attacks have become tools for crime, terrorism and international conflict. Attack trends show an increase in attacker sophistication and an increased capacity of cyberattacks to do physical damage. Additionally the number of potential adversaries gaining cyber skills continues to grow.

The Intergovernmental High Level Panel provided a venue for dialogue among leading governmental representatives and experts on the needs and challenges related to the protection of the cyberspace and the growing risk which cyber-attacks pose to national critical infrastructure.

Austrian government and EU representatives opened the day with a discussion of the Austrian and the EU cyber security strategy. Panel discussions and engagement with the participants provided insight into sector- and organisation-specific cyber security strategies. A brief highlight of the discussion follows.

Cyberspace - being the new emerging ***"battle field"*** - today enables adversaries to reach across great physical distances with relative anonymity to affect critical services and processes. Moreover, as Maj.-Gen. Johann Frank, the Director for Security Policy of Austrian Federal Ministry for Defence and Sports put it, ***"monitoring of Critical Infrastructure is increasingly done remotely; this domain hosts a range of systems including electric grid, IoT, making our lives more convenient but by allowing any system to be accessed remotely internet we're causing these systems to be vulnerable. However, security is somewhat an illusion: You can't eliminate cyber threats, you must manage risks".***

CONVENTIONAL ARMS CANNOT FIGHT IN CYBER SPHERE...

The number of cyber incidents targeting energy infrastructure has significantly increased over the last years. A well-planned and motivated cyber-attack to energy infrastructure could inflict severe damage to a nation. The Director of Security Policy at the Austrian Federal Ministry for Europe, Integration and Foreign Affairs, Gerhard Jandl stated that security today required a new mind-set: ***"Conventional arms won't ensure security in the future; cyber specialists will! Policymakers often are not familiar with the technical necessities and are therefore often experiencing great difficulties in drafting and – more importantly - continuously updating the appropriate legislation, which enables an adequate response to cyber-attacks to Critical Infrastructure."***
While the technical challenge of attribution and legal challenges with regards to prosecution remain remarkable barriers in creating a common action agenda for addressing cyber security, Mr Jandl's

remarks highlighted the importance raising awareness and knowledge among the leadership. As Energypact's President Alexandre Dimitrijevic stated: ***"For every nation's safety, we urgently need to initiate an international dialogue to protect vital energy infrastructures against growing cyber threats, whether they are purely criminal or are driven by terrorism."***

INTERNATIONAL COOPERATION; IMPLEMENTING HOLISTIC APPROACH

Today, the digitalisation of critical infrastructure is an inevitable process. Therefore, ***"the protection strategy of these systems must not be static; it must be responsive to change"*** as the Director of Euratom Safeguards in the European Commission, Stephan Lechner, said and added ***"the real challenge is getting all these minds together to discuss the future of cyber in terms of threats, defence, offense, etc. Public and private actors have a shared responsibility and a common interest in protecting Critical Infrastructure".***

In that sense, while cooperation seems as the key step in providing a holistic approach in securing cyber space, international organisations play a crucial role. Mr Aldo Lale-Demoz, UNODC's (United Nations Office on Drugs and Crime) Deputy Executive Director highlighted: ***"we provide tech assistance to governments to plan and implement response to particular needs; today, critical infrastructure protection is no longer uniquely a nation-state's capability".***

DIFFERENT SECURITY SPHERES OF IT AND OT

What are the challenges and real cyber threats for energy infrastructure where information technologies (IT) and operational technologies (OT) are increasingly computer-based? Marcus Frantz, the CIO of OMV stated that ***"there are large issues and challenges in the IT and OT".*** Additionally, even though security in IT (Information technologies) systems are familiar for cyber defenders, operational part/OT systems poses real hidden vulnerabilities which makes security of ICS (Industrial Control Systems) an increasingly crucial topic.

Concerns with regards to cyber-attacks span across the energy sector and include initiatives by the IAEA to support the nuclear industry. Donald Dudenhoeffer, Nuclear Security Information Officer of IAEA, underlines that ***"there is a great interest in ensuring computer security for nuclear facilities; IAEA's focus is on helping to develop a holistic approach to the protection of nuclear facilities against cyber-attacks"*** and, he added, ***"one of the best measures of protection is investing in people. Technology can only do so much; it's people who ultimately decide the outcomes. An informed and trained workforce is one of the measures of protection against cyber-attacks."***

ENGAGEMENT OF PRIVATE SECTOR IS THE KEY

National and regional initiatives to secure infrastructure against cyber threats were discussed by Austrian and EU representatives, but experts also underlined the crucial role of the private sector as Roland Ledinger, CIO of Federal Chancellery, put it.
"We must acknowledge the experience needed to address threats from cyber space comes from the private sector, so we must engage with the private sector."
In addition to engaging the private sector into the security layer, cooperation is a must and ***"is necessary between public/private agencies, economic and scientific institutions"*** as emphasised by the director of the Austrian Federal Agency for State Protection and Counter Terrorism, Peter Gridling.

PUBLIC INVOLVEMENT AND AWARENESS HAS A VITAL ROLE

What is the developing nature of cyber threats and how can effective strategies for protection be developed? Aapo Cerdeberg, Executive Advisor of the Finnish Information Security Cluster, stated that, ***"the future is more unpredictable, targets of hybrid operations could be found all over society; adversaries will be looking to attack elements of critical infrastructures that could create the greatest impacts."*** In addressing the threats, public involvement and awareness plays a vital role. International organisations, such as the International Telecommunication Union (ITU), have significant programmes and activities with their respective Member States. This includes the development of international standards for ICT. ITU along with the IEC, and ISO are the main governing standards bodies for IT and OT. Like ITU, UNODC has a crucial responsibility in capacity building. For Neil Walsh, UNODC's Chief Cyber and Emerging Crime officer, ***"Awareness is key"***. He reported on UNODC's efforts in working with Member States to build cyber incident response capabilities.
Cyber space is a rapidly expanding domain. Research is essential for identifying vulnerabilities, developing mitigation strategies, and developing cyber resilient systems. Research is often conducted in partnership between many stakeholders. In Austria, the Federal Ministry for Transport, Innovation and Technology is responsible for 70% of the public R&D funds. As the deputy director-general responsible for Technology, Transfer and Security Research, Gernot Grimm said, ***"Our task is to optimise and intensify the cooperation in R&D related to cyber security."***

THE ROLE OF GOVERNMENT AGENCIES

Khammar Mrabit, Director General of the Moroccan Agency for Nuclear and Radiological Safety and Security, discussed the development of a computer security regulatory framework and the associated need to develop capabilities.

He relayed that Morocco has embraced the concept of a Nuclear Security Support Centre (NSSC) with the aim of providing a national and also regional resource for building nuclear security skill sets including those for computer security.

Nebojsa Jokic, Head of the CERT at the Serbian Ministry of Internal Affairs, likewise described capacity building efforts in Serbia.

"As a result from cyber incidents, new social networks were created and these communication lines could help build the collaborative community in cyber security".

Laura Crespo, Political Affairs Officer in the Department of Foreign Affairs of Switzerland, re-affirmed the need for capacity building and community engagement stating that ***"dialogue is important due to the decentralised nature of cyber."*** Bodo Meseke, EY Cyber Forensic Leader EMEIA also highlighted the critical nature of strategic information and added that, ***"the paradigm shift is no longer to prevent and protect, but to detect and respond, so we must have the information exchange"***.

Mohamed Mekerba, IT Development Officer of OPEC, also discussed the need for a paradigm shift: ***"In the future, there will be a greater need for smart grids to facilitate the 20% of passenger cars that will be hybrids fuelled by natural gas and renewables which is a serious challenge for cyber security."*** Therefore the operational model for security must adapt to the changing technologies and threats.

Concluding the first day, Helmut Leopold, Director for Digital Safety & Security at the Austrian Institute of Technology AIT, underlined that research and development would push the bounds on existing concepts of business, but also of security. Policy, programmes and procedures relating to security issues must be adaptive towards such disruptive technologies.

DAY 2: 16 FEBRUARY 2017 INTERNATIONAL MULTISTAKEHOLDER CONFERENCE: CYBER-SPACE, ENERGY & DEVELOPMENT – PROTECTING CRITICAL ENERGY INFRASTRUCTURE

supported by:

IEC

UNODC
United Nations Office on Drugs and Crime

ITU

The energy sector contains many activities and respective stakeholders that can be exposed to damage originating from cyberspace. The activities include but are not limited to mining and fuel production centres, multi-dimensional transport infrastructures for oil, gas, coal, uranium, and electricity, logistics or trading platforms as well as distribution- and "smart"-use-systems. Energy is a cross-border industry. Similarly, cyber security must be a cross-border discussion between national and international stakeholders, industry and government. This interaction is a prerequisite for safe and sustainable economic development.

Day two focussed on stakeholder engagement including the need for collaboration, capacity development, and the importance of Public-Private Partnerships.

RESPONSE TO EVENTS IN CYBERSPACE IS A CROSS-BORDER CHALLENGE

Gerhard Jandl, Security Policy Director, Austrian Federal Ministry for Europe, Integration and Foreign Affairs opened the day's discussion by stating the reality that ***"it's not a matter of if, but of when there will be a large scale conflict related to the compromise of critical infrastructure and that there is still an uncertainty over who has the responsibility for managing risks in cyber security"***. With respect to the borderless nature of cyber space, developing a collective response is therefore vital.

For Muna Duzdar, State Secretary at the Austrian Federal Chancellery for the Public Service and Digital Information of Austrian Federal Chancellery, ***"the main role is to promote digitalisation for everyone's benefit"***. Benefits, however, cannot be had without taking account of related security issues. Suleiman Jasir al-Herbish, DG and CEO of the OPEC Fund for International Development (OFID) further stated that, ***"as we're living in a highly interconnected world, it's important to have dialogue and have effective training, capacity building and technology transfer channels"***.

The rapid growth of digital technologies and the associated cyber threat has resulted in a situation of limited resources and capabilities to respond to all challenges. Anton Mair, deputy director general for Development Cooperation at the Austrian Federal Ministry for Europe, Integration and Foreign Affairs, stressed the need for partnership, but also of the need for prioritisation of efforts on the most pressing or impactful challenges.

Jose Luis Martins, Counsellor at the EU Delegation to the International Organisations in Vienna, spoke of the EU challenges, and questions that should be taken into account in implementing cyber security approaches, such as ***"how distributed operators will respond to a (cyber) crisis or how equipped legacy systems are to bear cyber events"***.

Understanding the nature of information is also a crucial step in building awareness. The ***"flow of information is not constrainable"*** mentioned by Mohamed Mekerba, IT Development Officer of OPEC, who added that there should be a continuous flow of information from bottom to top.

SHARING THE INFORMATION IS NOT AN EASY TASK

One of the most heavily discussed topic of the conference was the question of "information sharing" in cyber security. Jordan Georgiev, Managing Director of JKG Advisory, highlighted a key issue: ***"Trust is an important challenge in the future of information sharing"***. It is clear that pursuing a custom solution and creating comfort level between information holders and sharers is not an easy goal to be achieved.

Ferenc Suba, Executive Director of Energypact, stressed that in an interconnected world with such a broad range of stakeholders, a trust environment is critical for expert-exchange on cyber security issues. This trust must also include acknowledgement of different approaches to cyber security including recognising the importance of understanding the culture of respective stakeholders.

PUBLIC PRIVATE PARTNERSHIPS (PPP)

Developing and implementing a sustainable and secure environment for the energy sector cannot be achieved without the involvement of all stakeholders. Furthermore, much can be learned from the lessons of other critical infrastructure sectors in implementing security across cyberspace.

Hence, public/private partnerships are necessary for the design and management of a systemic security approach in the face of cyber-attacks on national and cross-border infrastructure.

The definition and scope of critical infrastructure among States varies and ultimately it is a State's responsibility for developing its critical infrastructure protection strategy. Developing awareness of the cyber threat and associated risk in policymakers is vital for developing this strategy. Part of this process requires understanding the connectedness of IT and OT including the possibility for cascading impact across sectors many of which may be owned by industry and not under direct control of government agencies.

According to Aapo Cederberg, Executive Adviser of the Finnish Information Security Cluster, it is also key to understand, that ***"buying and implementing the most cutting edge technology does not inherently mean cyber security"***. Cyber security is a process of multi-dimensional measures and controls that includes technology, but also the human element. Additionally as Helmut Leopold, Director for Digital Safety & Security at the AIT Austrian Institute of Technology, points out ***"we shouldn't use the problems and information of the past to measure the complex digital future."*** Innovation, adaptiveness, and responsiveness are all needed characteristics for computer security.

Computer security cannot be a solitary effort, but requires PPP engagement. Implementing a PPP structure in the layers of cyber security is thus an emerging point of focus. It is important to encourage engagement and provide both informal and formal mechanisms for fostering these relationships. Thomas Stubbings, Chairman of the CSP Austrian Cyber Security Platform, has found by experience, that ***"establishing platforms for dialogue, ensuring cooperation, and information exchange are important for the efficacy for public private partnerships."*** Preetam Maloor, ITU, provided closing remarks for day two and stressed the essential nature of public private partnerships within computer security. He likewise re-iterated that cyber security is not just a security issue, it is a developmental and sustainability issues for States. Partnership across the range of stakeholders is needed.

DAY 3: 17 FEBRUARY 2017 INTERNATIONAL BUSINESS HIGH LEVEL PANEL: DIGITAL SECURITY – PROTECTING STRATEGIC BUSINESS LEADERSHIP

Digital technologies are impacting the way we do business today. New technologies and changing business processes offer an abundance of opportunities, but also an array of new threats. Day three of the conference focused on strategic leadership and digital change management.

DIGITAL TECHNOLOGIES THE WAY FOR DOING TODAY'S BUSINESS

Strategic leadership, today, is faced with managing digital transformation to maximising opportunities while at the same time minimising threats. These two objectives do not always exist without conflict. As new technologies are promoted for introduction into both IT and OT, ***"we need ways to validate new technology"*** from a security focus as stated by Helmut Leopold, AIT. Industry standards are a powerful tool in ensuring a level of quality and performance. Eyal Adar, IEC Conformity Assessment Board; Founder and CEO of White Cyber Knight Ltd., stated that ***"cyber security standards are the core of digital elements"***. The application of cyber security considerations in the development and implementation of technologies is a much more effective strategy in terms of costs and protection than adding security afterwards.

LEGAL AND REGULATORY CHALLENGES

States are starting to implement cyber security regulatory requirements for critical infrastructure including in the energy sector. Implementing clear and binding requirements can be a starting point, but ***"there are a lot of issues with what can and can't be bound by law in the realm of cyber space"*** as stated by the Head of Information Security Compliance Center, University of Applied Sciences Upper Austria, Ingrid Schaumüller-Bichl. Wilhelm Wimmreuter from VP International Operations, InCharge Systems, acknowledged the government's role in developing regulation, but also recommended that the regulatory development process ***"also incorporates the feedback and participation of industry throughout the (development) process"***. Creating requirements without ***"Proper information results in poor decision-making, thus poor performance and overall negatively impacts to the entire organisation"*** warned Jerry Holdsworth, Director of AMCL Europe. Engagement by all respective parties should be both recommended and encouraged.

"COST" THE KEY WORD FOR BUSINESS

Experts stressed the need for business leadership to understand cyber risks – the potential impact of a cyber-attack. Risk management is often a business driven decision of which security can be one of many contributing inputs. Implementing cyber security comes with a cost. Energypact's Executive Director, Ferenc Suba discussed the range of factors that shape decision-making with regards to cyber security and resource allocation. This often brings to bear the question ***"how much computer security do I need, and how much will it costs"***. Unfortunately, these are not trivial questions nor are the answers often straightforward.

A CHANGING DYNAMIC FOR BUSINESS

In the migration to digital technologies, core business processes, such as communications, are evolving. Such technologies include cloud services and virtualisation. Reinhard Posch, CIO of the Austrian Federal Government, brought up key security issues with this technology migration: Who holds the data, where does the data exists, where do the programs that process originate, and what are the cyber and physical protection measures for the data?

Various security practices exist in business to meet the new challenges. For instance, as Yochai Corem the VP EMEA of Cyberbit stated, ***"cyber regulation is executed using a "business permit" with a security section and it is updated annually according to risks, best practices and technologies available."*** But in addition to technical measures, practical activities such as crisis management exercises are also crucial, because ***"no one really knows how employees will react in a cyber emergency, unless you've run through an exercise"*** as stressed by Benjamin Weissmann, Senior Manager of EY Austria.

While cost is often the major business driver, it should not be considered as a permanent barrier for cyber security as mentioned by Hansjoerg Kalcher the CISO of OMV. ***"Even companies with a tight budget can find money to put toward cyber security; it was just a matter of finding the right expert to but in front of the c-suite to appropriately explain the risks and need for cyber security."***

SECURE THE PRODUCT, SECURE THE SYSTEM AND THE SECURED HUMAN.

"The holistic view of security in business includes secure products, secure system design, and the secured human" said Walter Wutzl who is the Head of Digital Grid Automation Products Siemens Austria. Implementation of at least a baseline security policy, such as incident management, is essential in today's digital environment. While cyber threats represent one of the top business risks for corporations, it might be too early to be pessimistic. ***"Corporations in fact have the opportunity to change the game in how we all deal with cyber criminals"***, said Harald Reisinger, Managing Director, RadarServices Smart IT Security and he added: ***"You can't prevent a threat actor from acting against you, but you can enable your organisation to detect and mitigate threats before they have a chance to take effect."*** Often, the best cyber security investment an organisation can make is an investment in the awareness and training of its employees.
In conclusion, the rise and integration of digital technologies (i.e. the digital market) continues to be the highest growing business area. Digital technologies are integrated into almost every aspect of information and operational technologies, propelling industry in previously unreachable levels of productivity and effectiveness. Cyber threats have also identified this transformation as a target rich environment. Business leadership must possess an awareness of this cyber threat the potential impact of cyber-attack. While business must be driven by cost considerations, the investment in cyber security measures should be a risk-informed decision and such investments can be a strategic business differentiator.

VIENNA CYBER SECURITY WEEK CONCLUSIONS AND ACTIONS FORWARD

Information exchange and the development of cyber security solutions for the energy sector cannot occur in a vacuum. Venues for frank and open discussion are vital for building awareness, trust, and confidence among international stakeholders in energy security and in cyber security.

This inaugural Vienna Cyber Security week was a success in bringing together a community of experts to begin an important discussion. It was only the beginning, however, of an ongoing dialogue that is needed as digital technologies grow in use for the energy sector and a growing cyber threat continues to develop greater capabilities.

Energypact seeks to build upon this conference and the discussion points brought forward by the array of international experts. Plans are already in place for Vienna Cyber Security week 2018. Additionally multiple smaller awareness building events are planned for 2017. More information will follow in future newsletters.

MARK YOUR CALENDARS

VIENNA CYBER SECURITY WEEK 2018

29 JANUARY – 02 FEBRUARY 2018

ADVANCED ANNOUNCEMENT – SAVE THE DATE

ORGANIZED JOINTLY BY AUSTRIAN GOVERNMENTAL AND NON GOVERNMENTAL ACTORS AND THE ENERGYPACT FOUNDATION

energypact foundation

VISION

An international collaborative community of technologically and risk informed leadership, researchers, implementers, and stakeholders for the development, sustainability, and security of energy production, transmission, and delivery addressing today's challenges and tomorrow's needs.

MISSION

The Energypact Foundation has directed its efforts toward three mission areas:

AWARENESS:
promoting dialogue and international co-operation on security issues for the energy sector.

TRAINING:
establishing the Industrial Control Systems Security Centre (ICS Security Centre) in Vienna, Austria and regional training centres around the world for providing human resource development activities for leadership, management and employees.

RESEARCH:
nurturing a collaborative research network for the energy sector.

energypact foundation

Become a Collaborating Member of the Vienna Project

Energypact Foundation
viennaproject@energypact.org
www.energypact.org