The Vienna Project

Cyber Security for Critical (Energy) Infrastructure

Information Sheet

The protection of critical infrastructure is of vital importance for interconnected societies. Governments as well as providers of critical infrastructures need to create a socio-economic infrastructure which protects the cyberspace and all dependent infrastructures. The Vienna Project initiated by the Energypact Foundation[1] in collaboration with the Federal Ministry for Europe, Integration and Foreign Affairs, the Federal Ministry of Defence and Sports, the CSP Austrian Cybersecurity Platform and the AIT Austrian Institute for Technology aims at engaging with key national and international actors in dialogue and cooperation in the field of cyber security for critical infrastructure in general and the energy field in particular.

The International Multi-Stakeholder Conference “Cyberspace, Energy and Development - Protecting Critical Energy Infrastructure”, which takes place on 16 February 2017 at the National Defence Academy in Vienna marks the start of the Vienna Project. It is organised back-to-back with the Conference of the Austrian OSCE Chairmanship “Cyber Security for Critical Infrastructure Strengthening Confidence
Building in the OSCE”, which takes place on 15 February 2017 and is complemented by an international High Level Panel on Digital Security on 17 February 2017 and an International Intergovernmental High-Level Panel on “Protecting Critical Infrastructure from Cyber Attacks” on 14 February 2017, to which a number of countries actively engaged in the Cyber-domain, the IT-sector and/or the energy sector have been invited.[2]

These events form the first pillar of the Vienna Project and aim primarily at awareness raising and confidence building, by providing a platform for dialogue and cooperation. The two other pillars of the Project are training and research.

Through the establishment of an Industrial Control Systems (ICS) Security Centre the Vienna Project aims at improving information technology security awareness and contributing to capacity building for the management and operational personnel.

The research pillar will be used to nurture a Collaborative Research Network, which can lead, inter alia, to the development of methodologies to determine and assess their security and associated risks, the development of protective measures for both new and legacy systems, the detection of cyber-attacks as well as the monitoring of system resilience.

The main communication platform of the Vienna Project is the Energypact website: www.energypact.org

---

[1] The Energypact Foundation was established in 2007 in Switzerland as a non-profit and non-political organisation, and is now in the process of relocating to Vienna, Austria. Its mission is to promote the balanced use of energy sources with the objective of reconciling innovation, economic development and the protection of the environment. In order to better respond to threats to energy infrastructures, during the last two years, the EnergyPact Foundation has increasingly focused on cyber security for the energy sector.

[2] Algeria, Brazil, China, the European Union, France, Germany, India, Indonesia, Iran, Italy, Japan, Nigeria, the Russian Federation, the Republic of Korea, the UAE, the UK and the USA

Vienna Cyber Security Week

14-17 February 2017

14/2 International Intergovernmental High Level Panel Protecting Critical Infrastructure from Cyberattacks: A Global Challenge (restricted access)

Session 1: Austrian/EU Cyber Security Strategy for Critical Infrastructure Protection

Session 2: Impact of Cyberattacks and Suitable Strategies for Enhancing Cyber Resilience

Session 3: The Role of Cyber Awareness and Dialogue for Safeguarding Critical Infrastructure

15/2 Conference of the Austrian OSCE Chairmanship Cyber Security for Critical Infrastructure: Strengthening Confidence Building in the OSCE

Working Group 1: Cyber-attacks on Critical Infrastructure: Facts or Fiction?

Working Group 2: Who Provides for Security? Division of Responsibilities between State and Private Sector in Protecting Critical Infrastructure

Working Group 3: What should States do to Promote an Open Internet?

16/2 International Multistakeholder Conference Cyberspace, Energy and Development: Protecting Critical Energy Infrastructure

Session 1: International Dialogue: Promoting Awareness and Collaboration in the Energy Sector

Session 2: Developing Capacity in the Fight against Cyberthreats to Critical Energy Infrastructure

Session 3: Public Private Partnerships for Sustainable and Secure Critical Energy Infrastructure

17/2 International Business High Level Panel Digital Security: Protecting Strategic Business Leadership

Session 1: Legal and Regulatory Frameworks

Session 2: Critical Infrastructures Session

3: Business Enablement