Organization for Security and Co-operation in Europe

To Protect Critical Energy Infrastructure:

Gaining Critical Insights and Discussing the Role, Strategic Objectives and Practical Measures Initiated by the Organisation for Security and Co-Operation in Europe via Their Action against Terrorism Programme

Oil & Gas Critical Infrastructure & Asset Security Forum
19-21 September 2012

Address by Mr. Thomas Wuchte
Head/Action against Terrorism Unit
Transnational Threats Department
OSCE

Dear Ladies and Gentlemen,

Let me start by thanking the organizers of the Oil & Gas Critical Infrastructure & Asset Security Forum for having invited me to address the important topic of critical energy infrastructure security. It is a pleasure and a great honour for me to address such a distinguished audience.

The OSCE, consisting of 56 participating States and its 12 Partners for Co-operation in the Mediterranean Region, Asia and Australia, is the world´s largest regional security organization and it is based in Vienna, Austria. The organisation is working to ensure peace, democracy and stability for more than a billion people. The OSCE, reaching from North America, Europe to Central Asia, serves as a forum for political negotiations and decision-making and deals with early warning, conflict prevention, crisis management and post-conflict rehabilitation. In addition to its Secretariat, the support of its members, and other partners, the OSCE in particular “puts the political

will of its participating States into practices through its unique network of field missions."[1]

Among the 56 participating States, we count some of the biggest producers of energy commodities, as well as large consumers of energy crossed by many strategic transit countries.

In its Ministerial Council Decision from 2007, *Protecting Critical Energy Infrastructure from Terrorist Attack,* OSCE participating States not only reaffirm the commitment to prevent and combat terrorism in all its forms and manifestations, but also expressed their grave concerns about the "… growing risk of terrorist attack on critical infrastructure, which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens…"[2].

Vulnerable Critical Energy Infrastructure

As this audience certainly knows, infrastructure, in all its form, is a vulnerable and a valuable target for any kind of attacker. Therefore, one of the highest priority for state authorities is to protect these targets against attacks and to minimize "… serious impact on the health, safety, security or economic well-being of citizens …"[3] as underscored by our participating States.

We agreed as an organisation that efforts "should particularly take due account of identifying, prioritizing, and protecting critical infrastructure and addressing preparedness/consequence management issues..."[4]

The OSCE participating States have a very broad perception of the expression "critical energy infrastructure". It reaches from nuclear power-plants, dams of hydroelectric power plants, oil and gas producers, refineries, transmission facilities, supply routes and facilities, to energy storage as well as hazardous waste storage facilities.[5]

One of the great comparative advantages of the OSCE is that it "… seeks to connect different actors inside and between States and across regions. This includes strengthening local government, building partnerships between the private and public sectors and working with civil society."[6] We value cooperation and collaboration. There is an understanding of the benefits through an approach focussed on co-operation and collaboration – it seeks to use the organization's comparative advantage to best harnass resources. Collaboration has meant to us that we seek the broadest number of partners in a cost effective way – to include private companies and state authorities.

---

[1] http://www.osce.org/who, retrieved 3 August 2012
[2] Ministerial Council Decision No. 6/07, *Protecting Critical Energy Infrastructure from terrorist attack* (MC.DEC/6/07), MC15EW24, 30 November 2007
[3] Ibd.
[4] Ibd.
[5] Ibd.
[6] Factsheet: What is the OSCE? http://www.osce.org/secretariat/35775, retrieved 3 August 2012

OSCE Efforts to Protect Critical Infrastructure

I would like to give you some information about the OSCE´s efforts in the field of infrastructure and energy infrastructure protection. I also want to share some details on an OSCE/Transnational Threat Department (TNTD)/Action against Terrorism Unit (ATU) project called "Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks" focusing on threats emanating from cyberspace.

This audience knows well energy resources guarantee our way of life and help to improve our standard of living. The more important access to these resources becomes, the more we seek ways to address the consequences after a potential interruption in any form.

One common challenge nearly all energy producers or companies face is the challenge of transporting or delivering energy via secure routes. As consumers want to use these products without any interruption, there is a need to constantly monitor all these processes. Such monitoring and maintenance includes using Internet connections or radio transmitters.

At the same time, we are confronted with actors interested to destroy or disrupt such systems. Motivations for such attacks can range from financial to political reasons. A sobering thought in this connection is that terrorist organisations are inspired to cause as much damage as possible, physically as well as economically. Cyberspace increasingly appears to be a lucrative tool for them to fulfil their goals.

To give you an example: In a statement of the Security Guidelines developed by the American Petroleum Institute in 2005, it says that "... computer technology has become pervasive throughout the entire organisation, including network access to plant equipment to allow vendors to maintain systems remotely, and remote access connections to process control systems (SCADA) to allow engineers to trouble-shoot problems."[7]

There are plenty more open source examples which can give us an idea how Critical Infrastructure could be affected via cyberspace: For instance in 2003 several newspapers reported that a private network of the U.S. nuclear power station, Davis Besse, became infected with the slammer worm, which resulted in a five hour loss of safety monitoring.[8] Other examples include two BBC news stories: In November 2011, hackers were alleged to have destroyed a pump used to pipe water to thousands of homes in a U.S. city in Illinois by turning it on and off repeatedly. It later turned out that it was local water district employee on vacation who logged into the system remotely.[9] Moreover, in August this year the BBC reported that a virus called “Shamoon” was able to render several computers on a network unusable affecting

[7] American Petroleum Institute: Security Guidelines for the Petroleum Industry, April 2005, p.31;
SCADA: Supervisory Control and Data Acquisition used for the remote control and monitoring of a pipeline system, p. 43
[8] www.theregister.co.uk/2003/08/20/slammer_worm_crashed_ohio_nuke/; retrieved 28 August 2012
[9] www.bbc.com/news/technology-19293797, retrieved 18 August 2012

operations of an oil producer. [10] There are many more similar news items which raise important questions, most importantly how air-gapped networks of critical infrastructure really are from the Internet?

OSCE Efforts to Protect Non-Nuclear Critical Infrastructure

The OSCE Secretary General´s mandate and Ministerial Council Decision No. 6/07 on *Protecting Critical Energy Infrastructure from Terrorist Attack* are the basis for the current project on *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure (NNCEIP) from Terrorist Attacks*. This topic was identified as a possible follow-up activity during an OSCE-wide *Public Private Workshop on Protecting Non-Nuclear Critical Infrastructure from Terrorist Attacks* organized by the OSCE Action against Terrorism Unit (ATU) in Vienna on 11-12 February 2010.

The objective of the project is to compile and publish a Good Practices Guide on protecting non-nuclear critical energy infrastructure from attacks particularly on cyber-related infrastructure. The purpose of the OSCE project is "… to raise awareness of the risk of terrorists threatening the security of Non-Nuclear Critical Energy Infrastructure Protection, particularly industrial control systems and cyber-related infrastructure, among all stakeholders and to promote the implementation of good practices for protecting this infrastructure."[11]

The proposed guide is intended to share and promote good practices for government policy makers, state authorities in charge of critical (NNCEI) infrastructure protection, owners and operators of Non-Nuclear Critical Energy Infrastructure, and other stakeholders in OSCE participating States and Partners for Co-operation. The publication also encourages the formulation and implementation of appropriate policy and institutional frameworks for managing Non-Nuclear Critical Energy Infrastructure cyber security that relies on a co-operative, risk-based and public-private approach. It will also place emphasis on practices to promote incident response preparedness, overall infrastructure resilience and energy reliability.

The collection of good practices is planned to draw from outreach activities, with a wide range of stakeholders across the OSCE area, including state authorities, industry, academia/research institutes and international organizations. Information will be collected through open source research, written contributions, teleconferences, face-to-face interviews and expert meetings and will rely on and disseminate non-confidential information. Public-Private Partnerships (PPP) play an especially important role in the project.

The guide will be available online at the OSCE website by April/May 2013. The publication will made available in English and Russian language, with the possibility of other languages.

[10] source: http://www.bbc.co.uk/news/technology-15817335, retrieved 21 November 2011
[11] OSCE/TNTD/ATU project overview on *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks* focusing on threats emanating from cyberspace.

Conclusion

Critical Infrastructure (CI) and especially critical energy infrastructure is of crucial importance for our way of life. The probability that terrorists will be gravitated towards infrastructure is very high. Our entire attentiveness has to be geared to the vital vulnerability and to the protection of this energy infrastructure. Previous examples show that attacks against CI are an existing threat to our global world and it can be expected that attacks against CI will be considered.

When looking for solutions, we should build upon and promote the work of specialised partners. That is why we take stock of best practices in the field Non-Nuclear Critical Energy Infrastructure Protection as one of the goals of the project. Maximum co-operation and collaboration is crucial and the best way to prepare against future threats. The OSCE´s Private-Public-Partnership (PPP) program is an excellent prerequisite to achieve this objective. We can best protect our investments by enhancing resilience and thereby minimizing the consequences of attacks. Comprehensive co-operation and collaboration is the best and most cost effective way to protect our CI, and central to work to improve each other´s standard of living.

I am convinced that the OSCE with its 56 participating States and its 12 Partners for Co-operation in the Mediterranean Region, Asia and Australia will add to the value of your work in the field of Critical Energy Infrastructure Security.

Thank you very much for your attention!