Organization for Security and Co-operation in Europe

21ST OSCE ECONOMIC AND ENVIRONMENTAL FORUM
"Increasing stability and security: Improving the environmental footprint of energy-related activities in the OSCE region"

CONCLUDING MEETING
Prague, 11 – 13 September 2013

Session I: OSCE Guidebook on Critical Infrastructure Protection

Address by Mr. Thomas Wuchte
Head on Anti-Terrorism Issues, OSCE Transnational Threats Department

Ladies and Gentlemen,

Let me start by thanking the organizers of the 21st OSCE Economic and Environmental Forum for having invited me to address the important topic of "Strengthening policy and regulatory frameworks and fostering international co-operation to prevent adverse environmental impacts of energy activities".

For those who don't know me, as the Head on Anti-Terrorism Issues within the OSCE's Transnational Threats Department, we are working as the focal point for co-ordinating the Organization's anti-terrorism activities, and our Unit is offering a wide range of counter-terrorism assistance to participating States as part of advancing the global counter-terrorism agenda with a number of specific counter-terrorism programmes.

The OSCE, reaching from North America, Europe to Central Asia has developed in the past 40 years its unique comprehensive approach to security. The concept of comprehensive security enables the organization to address transnational threats in a genuine comprehensive way with the aim of translating political commitments into effective and sustainable action.

I would like to approach our discussion topic today from the point of view of security. What I am going to demonstrate today is that smooth and secure running of energy infrastructure is a prerequisite to safe and environment-friendly energy activities of any company or country.

The challenge here is twofold: on the one hand it is important to ensure the secure supply of energy and on the other hand it is not less essential to safeguard the security of the existing energy infrastructure. Any disruption, any breakdown can be a threat either on its own or by triggering a chain reaction with severe consequences, including for the environment.

Ladies and Gentlemen,

The importance of energy security and energy infrastructure security cannot be overstated. It is among the most serious security, economic and environmental challenges of both today, and the future. As the economies of the world grow more homogenous and societies continue to develop, so does the importance of energy; and so does the importance of the infrastructures that produce, refine and transport this energy. The disruption or destruction of these infrastructures would have a serious impact on the health, safety, security and economic well-being of individuals and the world as a whole.

In recent years, protecting critical energy infrastructure from terrorists has received increasing attention from the international community. Since critical energy infrastructure contains the fuel that keeps the global economy moving and our societies working, our dependency on such infrastructure makes it an ideal target for terrorists. Researchers indeed suggest that the threat of terrorist and other non-state actor attacks on critical energy infrastructure is growing.

Protecting critical energy infrastructure from terrorist attacks is an issue particularly salient for the OSCE, whose 57 participating States, as well as Partners for Co-operation, include some of the largest producers and consumers of energy as well as many strategic transit countries. OSCE participating States adopted in November 2007 a Ministerial Council Decision on Protecting Critical Energy Infrastructure from Terrorist Attack [MC.DEC/6/07], whereby they not only reaffirmed 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…"[1].

OSCE participating States agree that efforts "should particularly take due account of identifying, prioritizing, and protecting critical infrastructure as well as addressing preparedness/consequence management issues..."[2]

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

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. There is an understanding of the benefits through an approach focused on co-operation and collaboration – it seeks to use the organization's comparative advantage to best harness 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] Ministerial Council Decision No. 6/07, *Protecting Critical Energy Infrastructure from terrorist attack* (MC.DEC/6/07), 30 November 2007
[2] Ibid.

OSCE Efforts to Protect Critical Infrastructure

I would like to give you some information about the OSCE´s efforts in the field of energy infrastructure protection. I also want to share some details on a project called "Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace[3].

This audience knows well that in today's highly industrialized world, few things can function without energy. Energy resources guarantee our way of life and help to improve our standard of living. The more important the 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 organizations are inspired to cause as much damage as possible, physically as well as economically. Besides physical attacks, cyberspace increasingly appears to be a lucrative tool for them in fulfilling their goals.

OSCE Efforts to Protect Non-Nuclear Critical Infrastructure

In order to implement the already mentioned OSCE Ministerial Council Decision the Action against Terrorism Unit initiated the development of a good practices guide on non-nuclear critical energy infrastructure protection from terrorist attacks focusing on threats emanating from cyberspace, a topic 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 work on the Guide has involved a significant number of public and private experts nominated by interested OSCE participating States, as well as partners from the EU and NATO. The work was done through consultations and recommendations. We are particularly proud of the fact that a high number of industry experts has contributed to the guidebook. A reputable expert company, HiSolutions AG collected good practices and edited the Guide on the basis of expert opinion and recommendations.

The intent of the publication is to raise awareness of the risk of the cyber-related terrorist threat to Non-Nuclear Critical Energy Infrastructure (NNCEI), particularly to industrial control systems and cyber-related infrastructure, among all stakeholders and to promote the implementation of good practices for protecting this infrastructure. This Guide identifies key policy issues and challenges and collects selected good practices as possible solutions. The Guide is to serve as a reference document containing key information for government policy makers, state authorities

[3] A Publication by OSCE/Transnational Threat Department (TNTD)/Action against Terrorism Unit (ATU)

in charge of critical (energy) infrastructure protection, owners and operators of non-nuclear energy infrastructure, and other stakeholders in OSCE participating States and Partners for Co-operation.

The guide provides a framework that encourages the formulation and implementation of appropriate policies and institutional management of cyber security related to NNCEI, based on a co-operative, integrated (all-hazard) and risk-based approach, and with an emphasis on achieving incident response preparedness, overall infrastructure resilience and energy reliability. Issues include: risk assessment, physical security, cyber security, contingency planning, public-private partnerships, community engagement (including the special contributions of women community members), and international/ cross-border co-operation.

This guide describes the significance of non-nuclear critical energy infrastructure (NNCEI) for countries and energy consumers and identifies threats to that infrastructure, focusing on cyber-related terrorist attacks. It is not intended to be a comprehensive threat analysis or to explain all protection measures in detail. Nor does it discuss whether and to what extent a particular country or operator of non-nuclear critical energy infrastructure is actually vulnerable to these threats, as this can only be determined on an individual basis. Rather, the guide highlights methodological issues that need to be taken into account for the protection of non-nuclear critical energy infrastructure and offers suggestions for good practices to mitigate potential vulnerabilities.

Although the aim of the good practices presented is to assist countries with identifying and countering threats to cyber-related terrorist attacks, these measures may be adapted, extended and/or applied to other threats and other sectors. This possibility is taken into account throughout the guide.

Chapters of the guide give an overview on cyber-related terrorist attacks on non-nuclear critical energy infrastructure and provide good practices in Information Communication Technology (ICT) risk management frameworks to address cyber-related terrorist risks as well as in ICT-related security measures to address cyber-related terrorist risks. The guide gives also an overview on good practices in critical infrastructure protection within the OSCE. Each main chapter concludes with recommendations both for governments, regulators and other actors of the industry.

Finally the guide enlists suggestions for future OSCE roles to advance cyber security in non-nuclear critical energy infrastructure. It calls for mobilizing political support through raising awareness on the threat, and for promoting co-operation through multilateral exchange of information as well as enhancing national capabilities.

From among the recommendations given by the Guide, I would like to single out one of special significance to this conference: it suggests that the OSCE could promote and facilitate the formation of public-public, public-private, and private-private partnerships in critical infrastructure protection by organizing good practices workshops, disseminating information, and compiling good practices manuals and handbooks.

And indeed, since both the government and the private sector sides have acknowledged each other's special role in providing security we have witnessed a growing number of examples of forming these types of partnerships, building on recognition, confidence and distribution of responsibilities based on mutual interest. For example, the US Department of Homeland Security recognizes the importance of building effective Public-Private Partnerships in their National Infrastructure Protection Plan (NIPP). The NIPP Partnership Framework enables co-ordination and collaboration between private sector owners and operators and governments at all levels. This is accomplished through the establishment of Sector Co-ordinating Councils (SCCs), consisting of private industry, and Government Co-ordinating Councils, comprised of representatives across various levels of government.

Furthermore, the Good Practices Guide on Non-Nuclear Critical Infrastructure Protection provides a number of additional examples on public-private co-operation in areas related to the security of critical infrastructure, including threat and vulnerability analysis, information sharing, risk management, information exchange etc. Switzerland is bringing together nationwide Critical Infrastructure Protection and Business Continuity Management, thus harmonizing preparedness and resilience issues both on national and business levels. The Swiss approach can be seen as a model in this regard.

Conclusion

Critical infrastructure and especially critical energy infrastructure is of crucial importance for our way of life. The probability that terrorists will be tempted to attack the infrastructure is very high. Our attention should be given to the level of vulnerability and to the protection of energy infrastructure.

When looking for solutions, we should build upon and promote the work of specialized partners. That is why taking stock of best practices in the field of non-nuclear critical energy infrastructure protection as one of the goals of the project. Maximum co-operation and collaboration is crucial and offers the best way to protect against future threats. The OSCE´s support of public-private-partnerships (PPP) programs 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 critical infrastructure, and central to work to improve our standard of living.

It is my pleasure to invite you to the official presentation of the Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace. It will take place after this session in the Mirror Hall during the lunch break.

Thank you for your attention!