Organization for Security and Co-operation in Europe

Developing Resilient Infrastructure for a Secure Future

Bangkok, Thailand, 5-6 October 2016

Remarks by Mr. Thomas Wuchte on

Emerging & Future Threats Detection & Management

Acting Director & Head on Anti-terrorism

Transnational Threats Department

OSCE

Introduction

Ladies and Gentlemen, I would like to thank the organizers of the 2016 Critical Infrastructure Protection & Resilience Asia (CIPRAsia) for having invited me to address the important topic of critical energy infrastructure and cyber security. It is a pleasure and a great honour for me to address such a distinguished audience. I note that your focus on securing critical infrastructure across ASEAN fits well with recent work in our organization with ASEAN.

The OSCE's Comprehensive and Co-operative Role as a Regional Organization

For those not familiar with the OSCE, let me briefly note that it is the world's largest regional security organization, gathering 57 participating States and 11 Mediterranean and Asian Partners for Co-operation, with a strong mandate to work on preventing and countering violent extremism and radicalization that lead to terrorism, while promoting human rights based approaches along with supporting public-private partnerships such as today's conference on critical infrastructure protection.

Our OSCE comprehensive concept recognizes that security is multi-dimensional and that its politico-military, economic and environmental as well as human dimensions are closely inter-linked. And this concept also underscores that to achieve comprehensive security;

co-operation is indispensable on multiple levels, between countries, within countries, and among international organizations.

OSCE's Efforts on Developing Resilient Infrastructure for a Secure Future

CBMs -- Confidence Building Measures

Now, I would like to talk about OSCE's efforts to make our vast critical energy infrastructure safer and more resilient against potential attacks from cyberspace. These efforts are part of the wider OSCE work in the field of cyber security. To this end, 57 OSCE participating States have agreed to a series of confidence building measures (CBMs) that promote transparency, co-operation and stability between States in this field. Importantly, the CBMs are designed to avoid misunderstandings between States and to make cyberspace more predictable. CBMs also promote due diligence as a mechanisms to build trust between States, such as developing shared crisis management procedures in case of widespread or transnational disruption of Information Communications Technology (ICT) – i.e., ICT-enabled critical infrastructure; or to protect national and international ICT infrastructure including their integrity.

PPP – Public-Private Partnerships

In addition OSCE participating States committed to promote public private partnerships and develop mechanisms to exchange best practices of responses to common security challenges stemming from the use of ICTs. While the CBMs are primarily designed for national policy makers, their effective implementation requires the constructive engagement with other non-state stakeholders. For instance, the protection of critical infrastructure (CI) from cyber-attacks is not only in the interest of the many private CI operators, it is also a prime national security concern. The key words for us are collaboration and partnership among all the stakeholders as a guarantee of effectiveness in the common strive for cyber security. I look forward to tomorrow's panel discussion where this will be discussed in more detail.

NNCEIP -- Non-nuclear Critical Energy Infrastructure Protection

Consistent with the UN Counter-Terrorism Global Strategy, and guided by the December 2012 "OSCE Consolidated Framework for the Fight against Terrorism" and subsequent decisions, the OSCE participating States have adopted a strong mandate to counter terrorism. In this context they have addressed the issue of protection of critical infrastructure giving guidelines also for the OSCE executive structures in their activities in this field.

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. In recent years, protecting critical energy infrastructure from terrorists has received increasing attention from the international community. Since critical energy infrastructure encompasses the fuel that keeps the global economy moving and our societies working, our dependency on such infrastructure makes it an ideal target for terrorists. The disruption or destruction of this infrastructure would have a serious impact on the security, safety, economic well-being and health of individuals and the world as a whole.

The OSCE participating States have a very broad perception of the expression "critical energy infrastructure" or Non-nuclear Critical Energy Infrastructure Protection. It reaches from 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. We value co-operation and collaboration.

Good Practices Guide on NNCEIP

Based on the experiences of OSCE workshops on Protecting Critical Energy Infrastructure from Terrorist Attacks and a Public-Private Expert Workshop on the same topic in Vienna, expert knowledge and as an implementation of relevant OSCE decisions, the OSCE (Action against Terrorism Unit) started to develop a good practices guide on Non-nuclear Critical Energy Infrastructure Protection (NNCEIP) from terrorist attacks focusing on threats emanating from cyberspace.

The work on the Guide involved a significant number of public and private experts nominated by interested OSCE participating States, as well as international partners. The work was done through consultations and recommendations. We are particularly proud of the fact that a high number of industry experts have contributed to the guidebook.

From among the recommendations given by the Guide, I would like to single out one of special significance to this meeting: 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.

The Guide has received attention both from governments, international organizations and the private sector. We have already had the opportunity to introduce it at a number of workshops and conferences organized by international organizations as well as non-governmental organizations and business communities – with this being our first opportunity to present with one of our Asian Partners for Co-operation – Thailand.

.

The English version of the Good practices guide can be downloaded from the ATU's website: http://www.osce.org/atu/103500 . The Russian translation is also available on this website www.osce.org/ru/atu/110472 .

Series of National Table-Top Exercises (TTXs)

In more concrete terms, in order to promote national co-operation between public agencies, owners and operators of non-nuclear critical energy infrastructure in response to targeted cyber-attacks, the OSCE (Action against Terrorism Unit) has developed a project on a series National risk-assessment and crisis situation management exercises based on the recommendations of the Good Practices Guide on NNCEIP for interested countries.

The objectives of the project are to strengthen the protection of critical infrastructure from terrorist attacks emanating from cyberspace and to raise awareness and advance the capabilities of OSCE participating States to respond to a targeted cyber-attack aiming at their industrial control systems; and to disseminate knowledge building on the "Good

Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace" developed by the OSCE.

What we offer is a series of table-top risk-assessment and crisis situation management exercises on the national level for interested OSCE participating States. For each interested participating State, a dedicated national training and exercise will be provided. The type of activities expected to be conducted include crisis situation management simulations based on entirely fictitious scenarios.

The benefit of the hosting country is that participants of the table-top exercises will gain a hands-on experience on the possible consequences and vulnerabilities terrorist attacks might have on non-nuclear critical energy infrastructure. They will also have better awareness of the risk, better understanding of the cyber security vulnerabilities and possible consequences of cyber-attacks for the entire infrastructure and the society. During these exercises participants will be able to test the effectiveness of their existing protection and crisis management systems as well as the efficiency of interfaces to external crisis management instances. These exercises also aim to facilitate and invigorate better working partnership between the public and private sectors thus contributing to better protection and higher resilience of national energy infrastructures.

The target audience of the exercises is representatives of state authorities – regulators, law enforcement agencies – and the private sector – operators, providers and owners. The aim is to increase their ability to respond to cyber related incidents by sharing experience and improving public-private and private-private co-operation and also to facilitate dialogue and collaboration among national stakeholders.

The project will contribute to achieving better risk awareness, preparedness, response-standards, mutual assistance, situation/crisis management on the national and sector level.
The exercises and trainings will build upon lessons learned and recommendations collected in the OSCE Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection. OSCE participating States have already hosted at the national level and we have several more in 2016/2017 – I have detailed material for those interested.

TTX: Assessing the Readiness to Mitigate Cyber Attacks – National/Sectoral Level

Usually experts carry out a survey / questionnaire among the participants representing different sectors in order to assess and evaluate the readiness to mitigate cyber attacks. The results of the evaluation is presented as a spider net figure showing five key dimensions of co-ordination/collaboration related to early detection and escalation of issues, information sharing between public-public, public-private and private-private sectors.

Lessons learned from TTXs (OSCE participating States)

As mentioned, we have organized now two national table top exercises (TTX). In both exercises the great engagement of the host authorities and the involvement of representatives from private companies in the energy sector and information and communication sector resulted in the successful delivery of the training material developed together with the experts (HiSolutions AG).

The exercises were designed to test the effectiveness of the procedures and tools available for energy infrastructure protection against terrorist cyber attacks. Exercise scenarios were described as "difficult and complex" as they combined three of the greatest threats: terrorism, large scale cyber attacks and the vulnerability of critical infrastructure.

The exercises tested the effectiveness of protection and management systems including coordination of the private sector with state management mechanisms, in a case of cyber attacks against energy infrastructure. The conclusions of the exercises were that the degree of development of the regulatory and strategic framework to tackle a crisis caused by a cyber attack on critical energy infrastructure is appropriately developed. However, it was considered that there is room for improvement in terms of communication/coordination between business and government, as well as between sectors, emphasizing the need to report cybersecurity related incidents through appropriate national authorities and subsequently manage the eventual crisis through government mechanisms as planned.

The exercises were both informative and also interactive – making it possible for all participants to understand the level of practical preparedness of countries to meet the challenges. Participants confirmed the importance of preparedness both on the corporate

and national level and underlined the need to create and effectively operate responsive and co-ordinating frameworks involving all stakeholders.

Conclusions

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 was one of the goals of the OSCE. Maximum co-operation and collaboration is crucial and offers the best way to protect against future threats. The OSCE´s support of public-private-partnership (PPP) programs is an excellent prerequisite to achieve this objective. The OSCE Secretariat, its Executive Structures and the field operations play an active role in promoting such partnership initiatives: by raising awareness, providing expertise, building capacity while also promoting the ratification and implementation of the international legal counter terrorism framework and the protection of human rights.

To conclude my remarks, let me reiterate that the OSCE through a broad range of decisions and commitments has a solid basis for supporting its participating States in counter-terrorism, and a long experience in building capacity and fostering co-operation on cyber security.

Support and interaction among States, the public and private sector, as well as international and regional organizations is paramount in tackling threats posed by terrorism and/or cyber security. There is a need to strengthen the sharing of best practices between public and private sectors. Recognizing each other's roles and responsibilities and stronger joint collaboration will benefit all stakeholders in countering terrorism in all its forms.

Thank you for your attention.