CTN Newsletter Special Bulletin
Protecting Critical Energy Infrastructure from Terrorist Attacks

January 2010

"Effective co-operation among participating States to protect critical energy infrastructure from terrorist attack would enhance security and stability in the OSCE region", *OSCE Ministerial Council Decision No.6/07*

➲ Contents by affiliation and authors

The contact details of the contributors to this Special Bulletin can be obtained through the OSCE Action against Terrorism Unit

➲ Contents by subject

➲ Contact

Reinhard Uhrig
Adviser on Anti-Terrorism Issues
Reinhard.Uhrig@osce.org

Mehdi Knani
Assistant Programme Officer
(Editor of this Special Bulletin)
Mehdi.Knani@osce.org

Tel: +43 1 514 36 6702
Fax: +43 1 514 36 6687
E-mail: atu@osce.org
www.osce.org/atu

"Effective co-operation among participating States to protect critical energy infrastructure from terrorist attack would enhance security and stability in the OSCE region", *OSCE Ministerial Council Decision No.6/07*

We believe that professional activities of national intelligence agencies, although critically important, are not sufficient any longer. Now it is essential to also focus on cooperation among States that supply, transit and receive energy resources, including strengthening counterterrorist collaboration among intelligence agencies. The CIS state participants share grave concerns regarding the security of their most valuable economic assets and consider that to this effect regional stability need to be secured on a permanent basis.

***NOTE**: Unofficial translation from Russian*

Protecting Critical Energy Infrastructures: How to Advance Public-Private Security Cooperation

Dr. Heiko Borchert and Ms. Karina Forster

There is no energy security without energy infrastructure security, but today's global energy infrastructure (EI) is fragile. This situation is most likely to aggravate in the future because our nations' energy demands are growing. As a result pressures on existing EI will grow. Consequently this paper makes the case for a public-private approach to critical energy infrastructure security (CEIS) and suggests concrete action for public-private security cooperation in the energy sector.

There are serious risks…

Significant underinvestment, regulatory differences and specific vulnerabilities caused by physical or cyber risks all affect global EI. The critical situation is further aggravated by the fact that some countries shield off their energy resources and energy markets, thus hampering competition and deterring the transfer of technology to the detriment of EI efficiency. Current problems will be reinforced by new EI challenges such as climate change, political demands for carbon capture and transport/storage, pan-regional infrastructure interconnection, and the introduction of smart grids depending on information and communication technologies (ICT).

Right now, there is neither a uniform regulatory environment nor an adequate governance structure to address security issues along the global energy supply chain that originates in countries of production, travels through transit countries and ends with consumer markets. This is problematic, because the world's dependence on resilient EI is most likely to grow because of raising energy needs. Therefore the most fundamental CEIS challenge is the need to set up and manage a multi-stakeholder process involving different public and private actors along the global energy supply chain.

…that require public-private security cooperation

At the beginning of the 21st century, close public-private security cooperation has become indispensable. Due to new security challenges, the globalization of markets and societies, and the outsourcing of traditional state functions to the private sector national security and corporate security have become closely intertwined. Shortfalls in one sector will inevitably affect the other. This, however, has major implications for security planning that must encompass many different actors and span across various policy domains.

In terms of CEIS, the public sector needs to interact with EI owners and operators, constructions companies, the ICT community and defense and security companies all offering security solutions, as well as the financial and insurance community that helps providing investment stimuli. The private sector must cooperate with political decision-makers, economic regulators, environmental watchdogs, public investors, emergency responders, military/security forces as well as intelligence services. In this complex web of relations public-private security cooperation for CEIS refers to the necessary public-private interaction:

- to coordinate, harmonize and possibly integrate
- goals, strategies, processes, structures, capabilities, and capacities
- in different areas of cooperation
- in order to advance the safety and security of EI at all stages along the global energy supply.

"Effective co-operation among participating States to protect critical energy infrastructure from terrorist attack would enhance security and stability in the OSCE region", *OSCE Ministerial Council Decision No.6/07*

Public-private security cooperation should not be confined to single areas of cooperation such as risk analysis, planning, training and education, research and development, procurement, or emergency operations. Rather it should be designed as a continuous process involving all areas outlined in Figure 1.

Figure 1: Building Blocks for a Public-Private Approach to Critical Energy Infrastructure Security

Strategies and concepts

EIS is not the only issue that public and private stakeholders need to address. Therefore it is important to harmonize EI-specific strategies with other security programs.

On the public side this puts a premium on policy coherence. EIS programs need to be aligned with national critical infrastructure security strategies. These strategies, in turn, need to be properly integrated into overall national security strategies. For example, several countries use national security scenarios to advance interagency cooperation to prepare for the likely consequences. This can also help coordinate public expectations vis-à-vis EI owners and operators. In addition, public stakeholders should scrutinize existing safety- and security-relevant regulation/legislation with a view on the extra requirements that EI owners and operators are expected to meet.

The most important strategic task for the private sector is to embrace corporate security as a competitive advantage and an indispensable building block of national security. By raising awareness for corporate security, companies should not only focus on their own core business processes. Rather there is a growing need for Business Continuity Management along the global energy supply chain and supply chains in other critical infrastructure sectors. This requires a much more intensive strategic upstream and downstream dialogue on security issues among EI owners and operators and with cooperation partners beyond the energy sector.

Risk and vulnerability analyses

When it comes to risk and vulnerabilities the main task is to provide joint situational awareness and joint situational understanding of the key threats faced by different stakeholders along the global energy supply chain. This also entails thorough analyses of intra- and inter-sector dependencies at national and international levels.

The public sector can support risk and vulnerability analyses by creating a trustworthy environment that helps exchange classified risk and threat information based on intelligence assessments. This can provide a significant incentive for the private sector to cooperate. Common methodologies that help identify, classify and assess risks are of further help, in particular for smaller EI owners and operators that operate under

tight market conditions. Together with corporate partners the public sector should also discuss possible safety and security implications of EI unbundling and the sale of EI to financial investors. EI owners and operators play a key role in broadening the scope of risk and vulnerability analyses beyond the energy sector. Energy companies and ICT providers, for example, should join forces to analyze mutual dependencies and develop standards to address respective vulnerabilities. EI owners and operators could also enter into dialogue with key clients, for example, in the chemicals, health, transport and financial sectors in order to identify cross-sector dependencies and vulnerabilities.

Identification and designation

Identifying and designating EI as nationally, European, or globally critical is challenging, because the designation is most likely to have a direct impact on EI owners and operators. There is thus a need for transparent processes and criteria that help identify and designate CEI at national and international levels.

Many governments avoid legislation when it comes to CEI identification and designation. Instead they opt for a dialogue with private operators. This, however, can be tricky. Different ministries might have diverging philosophies when it comes to security. If these differences are played out in front of corporate partners they might be deterred and take a step back. It is thus important for the public sector to find common ground on how to identify CEI components before interacting with the private sector.

The public sector's offer not to legislate gives EI owners and operators significant discretionary power that should be used responsibly. They should seriously engage with the public sector in exchanging information and should think about corporate CEI, for which they bear the prime responsibility. In addition, EI owners and operators involved in multinational infrastructure projects could cooperate with supply and transit countries to develop common methodologies to identify cross-border EI dependencies and to agree on the division of tasks and responsibilities across borders.

Goals and standards

There are several challenges for CEI standards. The growing reliance on ICT prompts a need for cyber security standards in the energy sector. Interdependencies between energy and other infrastructure sectors translates into the need for a security-related level playing field across all critical infrastructure sectors in order to avoid unfair competitive advantages for companies operating under different market conditions. Overall standards must evolve commensurate with a dynamic risk environment. Here, environmental change can be seen as one of those factors most likely to put EI under serious strain.

One of the main issues that the public sector must address is the adequacy of industry standards in light of today's and the most likely future security challenges. Public supervisory bodies need a methodology to evaluate the appropriateness of existing industry standards. In addition, the public sector might also see a need to review the tasks of economic regulators. If value for money is the only task, economic regulators are most likely to set regulatory incentives in a way that will be detrimental to corporate security investments. Security is a public good that economic regulators should consider when deciding about the appropriateness of investments submitted by EI owners and operators to justify their prices.

Among other things, EI owners and operators could acknowledge that generic industry standards might not always fit the public sector's security expectations. Advocating holistic concepts to advance Business Continuity Management standards beyond the energy sector, for example, could be a concrete step for the energy community to embrace in order to demonstrate that public fears of supply interruptions across different sectors are taken seriously. In addition, private EI owners and operators could also enter into dialogue with government-owned or government-controlled energy companies in supply and transit countries over safety and security standards.

Safety and security programs

When it comes to safety and security programs and measures to make EI more resilient, the main responsibility is with the private EI owners and operators. But the public sector can provide valuable incentives. Onsite inspections combined with safety and security advice that benefits from intelligence assessments, for

example, would be a significant service offered to private EI owners and operators. The public sector could also consider regulatory incentives for safety and security investments. In certain countries there are public budgets for specific measures required by national civil protection plans. Other options could include preferential tax treatment for safety and security investments into CEI. In particular in the energy field, the public sector will also have to take into account the relationship between multinational and regional/local energy providers. Safety and security programs must reflect these differences in order to avoid market distortions due to requirements that are too demanding to be met by everyone.

EI owners and operators in turn could increase transparency with regard to CEI-related safety and security investments. For example, they could disclose information on investments in operations and maintenance, infrastructure upgrades, training, and ICT safety and security. In addition, the specific needs of smaller EI owners and operators and smaller companies depending on energy supplies could be addressed by "Supply Chain Mentoring" programs to define common approaches to energy supply security. The exchange of good practice (e.g., on ICT security) with energy supply chain partners and partners from other critical infrastructure sectors would be helpful as well.

Incident management

Pan-regional energy markets are created by connecting national EI. However, without adequate precautionary measures and investments into incident management capabilities, risks will grow exponentially, because current EI was mainly designed to serve national markets. Today, there is a serious lack of information on available capabilities to deal with cross-border incidents.

Many countries run civil protection exercises that also involve EI owners and operators. The scope of these exercises should be broadened in order to train cross-border incident management. In support of these exercises thought should be given to the idea of joint public-private operational pictures that fuse information from public and private domains into an integrated command and control approach. In terms of regulation, the public sector should also discuss compensation schemes for cross-border assistance.

EI owners and operators could support the public sector by investments into modeling and simulation (M&S). M&S is important to capture the complexities of CEI and to understand dependencies among EI components as well as between EI and other critical infrastructure sectors. In case of incidents M&S is needed to make informed decisions about intervening in a fragile EI system in order to avoid unintended cascading effects. Finally, M&S can be used to evaluate the appropriateness of EIS standards. In addition, multinational EI owners and operators could support capacity building for incident management in energy supply and transit countries.

Reviews

The CEIS framework must evolve continuously. But it is well known that every security framework is only as good as the effort that goes into training and reviewing. This is an issue that public and private actors should address jointly as well. It might make sense, for example to think about a graduated approach to CEIS reviews. Self assessments either based on paper audits or self inspections could form the basis. At the next stage third-party assessments, for example with mixed teams consisting of public and private stakeholders, could be envisaged. On top of these layers joint exercises could be conducted. In parallel good practice awards can stimulate corporate innovation. And discussions with financial rating agencies and insurance companies on how to evaluate corporate security investments could provide further incentives.

A holistic governance system

Overall, the successful implementation of the proposed CEIS framework will depend on a holistic governance system. This is important because today most countries lack an adequate institutional set up to manage public-private security cooperation. The governance system includes regular gatherings of public and private stakeholders to create personal networks and to build trust. It also covers mutual identification of points of contacts to exchange information. Last but not least, a collaborative working environment should also entail state of the art ICT equipment that supports the creation of joint situational awareness and joint situational understanding that is at the heart of the public-private security partnership.