POLICY BRIEF
OSCE Action against terrorism Unit (ATU)

Protecting Critical Energy Infrastructure from Terrorist Attacks

September 2010

Action against Terrorism Unit (ATU) Policy Brief No. 2/2010

"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 (30 NOVEMBER 2007)

Executive Summary

This brief presents key policy recommendations for critical energy infrastructure protection that emerged from an OSCE public-private expert workshop in 2010.

The risk of terrorist and other non-state actor attacks on critical energy infrastructures is growing. The disruption or destruction of these infrastructures would have a serious impact on the health, safety, security or economic well-being of citizens. Countries should review the security vulnerabilities of their energy infrastructures and their policy to address this challenge.

Countries are advised to follow an approach based on regular, all-hazard risk assessment, taking into account cyber vulnerabilities. Their approach should be designed to mitigate risks to an acceptable level while aiming, ultimately, to ensure overall infrastructure resilience and energy reliability. In doing so, countries should flexibly combine prevention, protection and preparedness, and they should build on effective multi-stakeholder co-operation (inter-agency, public-private and international).

Context

Energy security, including energy infrastructure security, is among the most serious security and economic challenges both today and in the future. As economies around the world grow and societies develop, so does the importance of energy and infrastructures producing and supplying energy.

Protecting critical energy infrastructures (CEI) from terrorists has received increasing attention from the international community in recent years. Inflicting maximum economic damage and social disruption is a key goal for many terrorists. Hence CEI, which provide the fuel that keeps the global economy moving and our societies working, are potentially ideal terrorist targets.

The reality of the terrorist threat to CEI is often discussed, especially by private sector owners and operators. It is generally understood that terrorist attacks against CEI are low-probability but high-consequence risks. However, indications exist of an increasing threat of attacks by non-state actors against energy infrastructures, and vulnerabilities still exist despite all efforts undertaken to increase CEI security. Such threats and vulnerabilities should not be ignored, but countries can also not afford to overreact.

Protecting CEI from terrorist attacks is an issue particularly salient for the OSCE, whose 56 participating States include some of the largest producers and consumers of energy as well as strategic transit countries. In November 2007 OSCE participating States adopted a Ministerial Council Decision on *Protecting Critical Energy Infrastructure from Terrorist Attack* [MC.DEC/6/07] whereby they committed to co-operate amongst themselves and to consider all necessary measures at the national level in order to ensure adequate CEI protection from terrorist attack.

The OSCE held a *Public-Private Expert Workshop on Protecting Non-Nuclear Critical Energy Infrastructure from Terrorist Attacks* on 11-12 February 2010 in Vienna, bringing together 200 participants from 50 countries, 12 international structures and 30 private sector organizations. A series of policy recommendations emerged from the workshop which have been consolidated in this Policy Brief. These recommendations do not necessarily imply endorsement by OSCE participating States or by the OSCE Secretariat.

Policy Recommendations

1. Follow a comprehensive risk-based approach. The importance, vulnerabilities and the risk environment of energy infrastructures vary from one infrastructure to the other, from one country to the other, and they vary over time. Arrangements to protect energy infrastructures should be dynamic and informed by an all-hazard and regularly updated assessment, looking at a whole range of man-made (accidental or malicious) and natural risks, rather than focusing on terrorism only. This assessment should also take into account dependencies and interconnections between sectors (e.g. transport and information technology sectors) and between countries. On the basis of the risk assessment, measures in terms of prevention, protection and preparedness should be adequately combined to mitigate risks to an acceptable level.

2. Develop a multi-stakeholder co-operation framework. A comprehensive approach to CEI protection as outlined above requires the co-ordinated involvement of multiple stakeholders, from different state agencies (e.g. ministries for energy, interior/ security, environment, defense), from both the public and private sectors, as well as from stakeholders across borders. Efforts should be devoted early on in the (re) formulation of a CEI protection policy to promote dialogue, common understanding and language, trust and sensitive information-sharing. Efforts to foster a convergence/harmonization of approaches to risk assessment and designation of critical infrastructure will stimulate multi-stakeholder co-operation. Countries should explore which existing or new arrangements would be best suited to facilitate, in their respective case, co-operation on different levels.

3. Design flexible security arrangements ensuring an adequate minimum level of protection. The vulnerabilities and the risk environment of each CEI are specific and dynamic; their protection must take this into account to be commensurate to the risks and cost-effective. Security measures should be tailored to each infrastructure and ideally built in the infrastructure by design. Measures can be implemented to simultaneously serve different Health Safety, Security and Environment purposes. Security should be "scalable", with plans to (des) escalate measures depending on the latest risk level. But "backbone" security measures should be in place because CEI are vital to society, and minimum, preferably international, security standards would provide a level playing field for economic operators as well as consistency across borders. While spending on security should be part of CEI owners and/or operators duty of care and business continuity strategy, a need exists to discuss incentives and cost-sharing.

4. Place greater emphasis on preparedness and overall resilience. Disruptions, accidental or not, cannot be completely ruled out, hence the need to ensure energy infrastructure reliability through preparedness and consequence management. Preparedness requires advanced contingency planning, testing and exercising, including plans for communicating with the public/consumers and energy markets. Countries might envisage establishing specialized agencies with rapid deployment response/recovery capabilities. Regarding resilience, a need exists for more investments in network interconnections and alternative routes, as well as to increase storage capacity/strategic reserves. Ensuring overall resilience and energy reliability requires looking beyond infrastructure to other energy security issues, such as energy solidarity, diversification of the energy mix, diversification of suppliers.

5. Identify and address cyber vulnerabilities of the energy sector. Traditional physical security measures ("guns, gates and guards") are no longer sufficient in today's increasingly computerized and ICT-dependent world. The level of public and corporate awareness and understanding of cyber security issues needs to be dramatically raised and the development of cyber security expertise should be promoted. Cyber security assessment should be integral to infrastructure risk assessment, in particular in the energy sector (e.g. markets, infrastructure process controls, smart power grids). Countries should build up national cyber emergency response capabilities and establish an effective international framework to better respond to international cyber emergencies.

6. Develop effective public-private partnerships (PPPs). Most CEI today are owned and/or operated, in whole or parts, by the private sector. The respective security roles and responsibilities of private stakeholders and state authorities should be clearly defined. But each can benefit in fulfilling its role from the support of the other; effective security, especially preparedness, requires close, tried and tested co-ordination. Platforms should be thus provided to establish and maintain public-private dialogue (possibly through institutionalized mechanisms,) which allow building the trust necessary for timely and reciprocal sharing of sensitive information between public and private stakeholders. Partnerships can be developed for joint CEI security assessment, review of security measures, elaboration of contingency plans, and incident response training. Moreover, PPPs can help leverage the support of communities where CEI are located to enhance preventive security, by creating a community stake in the integrity of the infrastructure.

7. Enhance cross-border / international co-operation. Energy infrastructure security and the challenge of ensuring energy reliability today have a strong and ever growing transnational dimension. National power grids are increasingly interconnected and new cross-border oil or gas pipelines are being built around the world. The disruption of a single energy infrastructure can impact far beyond the national borders of the country where it is located, whether in terms of supply discontinuation, or other damage, including economic (e.g. soaring prices in volatile energy commodity markets) or environmental damage. Countries should take stock of these direct and indirect dependences, which entail a vested interest in co-operating to ensure the integrity of energy infrastructures. A number of options to enhance cross-border and international co-operation exist, including exchange of (confidential) information, development of security standards, co-operation in emergency situations (e.g. technical assistance, energy sharing); their merit should be considered by countries and the international community.

Potential OSCE Role

The OSCE, with its unique membership spanning Eurasia and its comprehensive approach to security, has been mandated since 2007 to facilitate the exchange of best practices and timely sharing of information on CEI protection.

The OSCE, in co-ordination with other relevant organizations, stands ready to assist requesting participating States with raising awareness of CEI challenges and best practices, formulating a CEI protection policy, improving inter-agency co-ordination, developing PPPs, enhancing their cross-border co-operation, notably through the organization of national and sub-regional workshops, table-top simulations, and provision of expert advice / technical assistance.

Contact Information

For more information please contact the OSCE ATU Critical Energy Infrastructure Security Programme Officers:

Reinhard.Uhrig@osce.org or Mehdi.Knani@osce.org

Action against Terrorism Unit (ATU)
OSCE Secretariat
Wallnerstrasse 6
A-1010 Vienna, Austria

Tel: +43 1 514 36 6702
atu@osce.org
osce.org/atu