Organization for Security and Co-operation in Europe

Protecting Critical Energy Infrastructures Against Terrorist Attacks: Threats, Challenges and Opportunities for International Co-operation

Reinforced NATO Economic Committee Meeting
22 September 2008, Brussels

Address by Dr. Raphael F. Perl
Head of the OSCE Action against Terrorism Unit*

Ladies and Gentlemen,

Dear Colleagues,

Let me start by thanking NATO's Defence and Security Economics Directorate for having invited me to address the important topic of energy security. It is a pleasure and a great honor for me to address such a distinguished audience.

The importance of energy security, and energy infrastructure security, cannot be overstated. Think about what would be the potential consequences of a terrorist attack against the energy infrastructure system. Think about the consequences of a successful terrorist attack on a nuclear power plant – radioactive clouds spreading across borders, very much like the Chernobyl disaster in 1986. Or think of a successful terrorist attack against a super tanker in the Strait of Hormuz – wreaking havoc in the oil market

Clearly, energy security is among the most serious security and economic challenges both today, and in the future. As the economies of the World grow and societies develop, so does the importance of energy. And so does the importance of the infrastructures that produce and supply this energy. Critical energy infrastructures provide the fuel that keeps the global economy moving and our societies working.

Disruptions of energy distribution, natural or manmade, are likely to have cascading effects on the entire system, in fact on all aspects of society. And the destruction or disruption of critical energy infrastructure such as nuclear power plants, dams of hydroelectric power plants or major pipelines, would have a potentially serious, if not catastrophic impact on the health, safety, security and economic well-being of citizens.

For the international community, energy security and critical energy infrastructure security presents both challenges in terms of the threats we face, and opportunities in terms of how we can respond to those threats. Enhancing energy security, very much like combating terrorism, is a complex, multifaceted and interdisciplinary challenge. It requires a comprehensive approach and all countries have a stake in it. Important contributions can be made by all of us, in our different fields of expertise.

* Prepared with the assistance and substantive input of Mr. Mehdi Knani

And let me stress that the topic of energy security is particularly relevant for the OSCE. My organization spans North America and Eurasia, including Central Asia, the Caucasus, the Caspian Sea, and the Black Sea. We have 56 participating States, among which are found some of the biggest producers of energy commodities, and some of the largest consumers of energy, as well as strategic transit countries. And the OSCE, like NATO, is considering how it can add value to enhancing energy security. OSCE participating States have adopted in November last year a Ministerial Decision on *Protecting Critical Energy Infrastructure from Terrorist Attack* (MC.DEC/6/07). In implementation of this decision, we are examining opportunities for co-operation with relevant international organizations in this field, and we will soon report to our participating States for further deliberation on an appropriate OSCE involvement.

So what I suggest to you in my remarks today is first that I share some of my thoughts on the terrorist threat to critical energy infrastructures. And then I will attempt to identify some needs and options for response, including opportunities for international co-operation.

Assessing the terrorist threat to critical energy infrastructure and vulnerabilities

The reality of the terrorist threat to critical energy infrastructure is often discussed, especially by the private sector: the companies owning and or operating these infrastructures. As a case in point, the International Association of Oil and Gas Producers (OGP) ranks terrorism only in 6th position in terms of threat to the industry, behind violent crime, organized crime, militant activism, civil unrest and political instability. But such assessment of the threat may well be underestimated.

I would suggest that terrorists, particularly Al Qaeda inspired terrorists think different in terms of targets and target priorities. An avowed goal of Al-Qaeda inspired terrorists is to inflict damage of catastrophic proportions, not only physical but also economic damage. Disruption of the global economic system and of the western lifestyle has become a goal and a rallying call for Al-Qaeda inspired terrorists. From this perspective, energy infrastructures, given their economic importance, could be particularly attractive as targets for terrorists.

If one wants to cause economic damage, attacks on energy infrastructure are clearly an attractive option for terrorists. The economic impact of such attacks, even if they are localized, has the potential to be greatly amplified given the volatility of the energy market and other economic implications. Think for instance of the consequences of the failed Al Qaeda suicide attack against Saudi Arabia's largest oil refinery in Abqaiq, early 2006 – oil prices jumped $2 a barrel on news of the attack. And following the terrorist attack on the French super tanker Limburg in 2002 off the coast of Yemen, oil maritime transportation costs tripled!

Moreover, as the energy infrastructure system is highly networked, a potential exists for a cascade of disruptions, thereby multiplying the impact of a single localized attack. Just think of the massive blackout experienced by the United States and Canada in the summer of 2003, which affected some 50 million people in the Northeast. And this started with a single generating plant unexpectedly shutting down in Ohio, sparking a cascade of failures across the whole grid.

Much of Al Qaeda leadership are engineers – they think in term of systems and networks. We need do the same, and we need to think in terms of multiple attacks.

I would also suggest to you that energy is often perceived as being at the core of some controversial decisions, policies, and attitudes of western countries. Hence, some energy infrastructures could also be attacked for their symbolic value.

So the terrorist threat is real, but how vulnerable are we? I would suggest that despite all our commendable efforts, vulnerabilities still exist. These vulnerabilities derive from a number of different factors. Overall, the system today is complex, highly networked along a transnational supply chain, from extraction/production to local distribution, with thousands of km of pipelines and power lines, cutting across wide open areas, or dense urban environments. Critical junctions, nodes, choke points and bottle necks exist along transportation routes and transmission grids. Important single facilities exist, like hydroelectric dams or nuclear power plants

In addition, these energy infrastructures are connected and/or dependent upon other infrastructures, such as transportation networks and facilities, but also information and communication infrastructures, which represent yet another source of vulnerability. Many experts argue indeed that the threat of cyber attacks against energy infrastructures today is underestimated.

Some researchers also point to the potential employment of Electro-Magnetic Pulse (EMP) technology by terrorists. It only takes a microwave and some amplifiers for an individual to remotely target, interfere with, and potentially disable operating and control systems, without the immediate appearance of an attack.

Globalization and de-regulation also create vulnerabilities. The energy infrastructure system today is profit oriented and arguably suffers from under investment, especially in terms of security enhancement. The drive for profit and optimal efficiency has resulted in decreased resiliency and decreased redundancy in back up in the sector. The industry itself recognizes the existence of competitiveness / security trade-offs, but arguably still favors competitiveness.

Needs and options for response

So the threat is potentially great, arguably increasing, and vulnerabilities abound. But what can we do? To put everything in a nutshell: we need to foster a proactive – comprehensive – inclusive and cooperative approach to securing the energy infrastructure system. We need to take a holistic approach, thinking in terms of securing the entire energy supply chain – not in fragmented terms – not just security of some physical infrastructures.

Moreover, I suggest to you that rather than focusing specifically on the terrorist threat, security enhancement measures should be designed, promoted and treated as an investment against security hazards in general. We should not think of this as a costly response to a threat, but rather an investment opportunity.

The security measures we take to protect energy infrastructures from terrorist attacks also apply to mitigating other criminal threats, as well as possible accidents or natural disasters.

Clearly, as we cannot protect everything to the same extent we need to prioritize our efforts and allocation of resources. The approach followed by most countries here is to identify the "critical" component of their energy infrastructure systems, the Critical Energy Infrastructures located on their territory. However, these criticality criteria vary from one country to another, thus perhaps, it could be useful to strive towards an harmonized definition of what is critical.

A need also exists for comprehensive and regular assessments of vulnerabilities and threats to the energy infrastructure system. For this, analytical methods and capabilities must be strengthened, ideally again on a harmonized basis. A broad range of energy infrastructure protection issues must be addressed, including cyber threats, electromagnetic threats. Infrastructure situational awareness should be enhanced to the maximum extent possible and private owners and operators should be compelled, to the maximum extent possible, to regularly report to state authorities on the status of their infrastructures. In addition, state authorities could arguably do more to share threat information with the private sector.

Developing public-private partnerships (PPPs) is a potentially effective tool here. This is an area where my organization, the OSCE, is particularly active. Effective PPPs require clarifying roles and responsibilities, building mutual trust, as well as highlighting mutual benefits and the shared valued outcome of co-operation. These are results we want to achieve. To maximise the effectiveness of such partnerships, a variety of stakeholders, public and private, must be involved to discuss their needs, concerns and priorities, to identify compromise approaches and joint actions, and first of all to share information.

Building on this honest exchange of information and assessment of vulnerabilities, threats, and risks, we must aim at cost-effective mitigation measures, to enhance both physical and cyber security. Importantly, security arrangements should be tailored to take into account the specific characteristics of a given infrastructure. For example, when dealing with nuclear power plants, hardening and military protection seems only reasonable. When addressing the security of other infrastructures, it might simply be desirable to build more redundancy into the system and prepare for the eventuality of acceptable, perhaps inevitable or unpreventable losses.

As we cannot protect everything, preparedness, resiliency and recovery capacity are paramount to ensuring continuity of service. It is quite telling in this regard that the division of the United States Department of Energy that deals with energy infrastructure security is called the *Infrastructure Security and Energy Restoration* (ISER) Division.

And with this, I come to the issue of institutional capacity-building. The approach to securing the energy infrastructure system that I am promoting here is very much a strategic approach. For such a strategically-oriented comprehensive strategy to be adequately devised, let alone implemented, institutional capacity is *sine qua non*. National inter-agency co-ordination has to be strengthened and this could take the form of special national inter-agency bodies or taskforces for instance. A need also exists to maintain and/or to enhance civil emergency planning and disaster response capabilities in the event of a successful attack.

Conservation can also do much to reduce efforts required to bring energy supplies up to speed and to backfill supplies or compensate for decreases in supply in wake of a terrorist attack. Arguably, this is an area where we need to do more.

Opportunities for international co-operation

I would now argue that international co-operation is essential with respect to most, if not all needs and action areas that I have just identified. Given the transnational character of the energy supply chain, countries have a vested interest in co-operating to ensure the integrity of the energy infrastructure system. More experienced and resourced countries have a vested interest in sharing their expertise and providing assistance to other less resourced or experienced countries.

As energy security of a particular country is closely linked to that of others, each country needs to know what others are doing. Compliance with existing international safety and security standards is a key element of transparency and essential to regional energy stability. International co-operation is obviously indispensable to further promote such compliance, including through the provision of assistance, expert advice and training.

Besides, many actors of the energy sector feel that as the energy infrastructure system is transnational, a need exists for international efforts towards development of a uniform cross-border regulatory framework and comprehensive set of international standards for energy infrastructure security.

But we need not wait for such a comprehensive framework to take action. There is already a wealth of experience, good practices and lessons learned that are waiting to be disseminated. Countries would also benefit from more exchanging data and information, as well as from pooling resources to promote further research on energy infrastructure security.

Due to their particular location or importance, some critical energy infrastructures arguably require targeted cross-border co-operation. In this regard, I would like to recognize here the ongoing efforts of the European Union towards the identification of *European* Critical Infrastructures. The United States Global Critical Energy Infrastructure Protection (GCEIP) Strategy is a model one might also want to draw from, which aims at assisting foreign countries in improving the security and resilience of overseas petroleum infrastructures identified as critical for the United States.

International co-operation could also be specifically enhanced with initiatives focusing on key energy corridors or areas. Establishing a *Critical Energy Infrastructure Emergency Response Network* might also be an option worth considering as a possible mechanism for enhanced international co-operation.

And at the confluence of objectives between counter-terrorism and energy security, we might want to put more emphasis on the need for further international co-operation in terms of enhancing maritime security, transport security, and cyber security.

Finally we should not overlook the role of international organizations such as the OSCE and NATO. International organizations have also an important role to play here, in their different field of expertise, where they can add value to existing efforts. My organization,

the OSCE, has the potential to play a key role in raising awareness and mobilizing political support; it could promote intergovernmental as well as public-private co-operation; and it could support the enhancement of national capabilities. The OSCE, with its 56 participating States, has a comprehensive security mandate with a soft power focus, as opposed to the specialized mandates of other organizations. It is arguably therefore well positioned to serve as a platform to promote a comprehensive approach to critical energy infrastructure protection.

Conclusion

I would like now to briefly conclude by reiterating a few thoughts. The economic importance of the energy infrastructure system and interdependencies in the energy supply network leave us vulnerable to terrorist attacks on major facilities, nodes or routes, aimed at paralyzing the whole system by cascade effect.

The threat is potentially great, increasing. But we must not over react. We cannot protect everything – we must protect wisely and ensure against potential losses. Excessive redundancy and back up are generally not perceived as cost effective. But major damage to the energy infrastructure system, where supplies remain disrupted for long periods of time, is even less cost effective. And clearly, as we cannot protect everything, building resiliency and recovery capacity must be emphasized.

Energy security like terrorism is a truly global issue in which we all have a stake. Hence international co-operation is indispensable – we are all on the same boat. And we all need to work together to maximize our ability to effectively protect the energy infrastructure system from attacks and to maximize our resiliency and ability to recover in the wake of such attacks.

I thank you again for this opportunity to offer my thoughts on this important and timely topic. Thank you for your attention.

Office of the Secretary General
Action against Terrorism Unit

Wallnerstrasse 6
A - 1010 Vienna

Tel: +43 1 514 36 6702
Fax: +43 1 514 36 6687
Mail: atu@osce.org

osce.org/atu