



Organization for Security and Co-operation in Europe

Office of the Secretary General
Action against Terrorism Unit

Vienna, 29 August 2008

To: All OSCE Delegations

Subject: Executive Report on the OCEEA-ATU Expert Meeting on
Protecting Critical Energy Infrastructure from Terrorist Attacks

Please find attached the following document:

Executive Report on the OCEEA-ATU Expert Meeting on Protecting Critical Energy Infrastructure from Terrorist Attacks

If you have any questions or comments please contact the Action against Terrorism Unit (ATU):

Mehdi Knani
Tel: +43-1-514-36-6636
Email: mehdi.knani@osce.org

OCEEA–ATU Expert Meeting on Protecting Critical Energy Infrastructure from Terrorist Attacks

17 July 2008, Vienna

Organized thanks to a generous extra-budgetary contribution
of the United States of America

Executive Report

Introduction

Gravely concerned with the growing risk of terrorist attacks on critical infrastructure and recognizing that critical energy infrastructure can be vulnerable to terrorist attack, the OSCE Ministerial Council adopted during its meeting in Madrid the Decision [No.6/07](#) on *Protecting Critical Energy Infrastructure from Terrorist Attack*. The Decision tasked, *inter alia*, “the Secretary General to examine and report to the Permanent Council on opportunities for co-operation with relevant international organizations, including the International Atomic Energy Agency, in the field of protection of critical energy infrastructure from terrorist attack (...)”.

In implementation of this task and in order to effectively identify areas where the OSCE could contribute to the enhancement of critical energy infrastructure protection from terrorist attacks, the Office of the Co-ordinator of OSCE Economic and Environmental Activities organized jointly with the Action against Terrorism Unit an expert meeting bringing together 50 participants, including representatives from 6 international organizations and 18 experts from research institutes and the industry/business community. Several other invited organizations declined to participate due to the absence of relevant activities to report on or the non-availability of their experts.

The expert meeting, organized thanks to a generous extra-budgetary contribution of the United States of America, focused on assessing and discussing the current and emerging threats and challenges in protecting critical energy infrastructure from terrorist attacks, as well as exploring possible OSCE contributions and opportunities for co-operation between the OSCE and relevant international entities in this field.

The OCEEA and the ATU have subsequently compiled the present executive report on the proceedings of the meeting, which have provided substantial and valuable input for the report of the Secretary General to the OSCE Permanent Council as foreseen by MC.DEC.No.60/7.

Welcoming Remarks

Mr. **Bernard Snoy**, *Co-ordinator of OSCE Economic and Environmental Activities (OCEEA)* welcomed participants, outlining the background for and objectives of the expert meeting. He highlighted the role of the OSCE as a platform for exchange and dialogue among different stakeholders and its efforts to promote public-private partnerships (PPP) in countering terrorism.

Mr. **Raphael Perl**, *Head of the OSCE Action against Terrorism Unit (ATU)*, emphasized the high stakes in protecting critical energy infrastructure (CEI), which represent attractive targets for terrorists seeking to disrupt the world economic system and the daily life of people. He observed that the characteristics of the energy infrastructure system make it vulnerable to potential attacks, and that enhancing preparedness, resiliency and recovery capacity is paramount, requiring close international co-operation and PPPs. In this regard, he underscored that preparedness and consequence management measures equally apply to mitigating terrorist attacks, natural disasters or accidents involving CEI.

Joint Opening Keynote Speech

On behalf of the United States of America, Mr. **Michael Ritchie**, *Director for Interagency Engagement at the United States European Command (USEUCOM)*, delivered a joint opening keynote speech together with Ms. **Patricia Hoffman**, *Principal Deputy Assistant Secretary with the U.S. Department of Energy*.

Ms. **Hoffman** introduced the mission of the U.S. Department of Energy (DoE), its Office of Electricity Delivery and Energy Reliability, and in particular the Infrastructure Security and Energy Restoration (ISER) Division which leads US national efforts to enhance energy infrastructure security and reliability. She explained that the DoE is the lead agency for the energy sector under the U.S. National Infrastructure Protection Plan (NIPP), which builds on PPPs in each sector. The DoE has co-ordinated the development of an Energy Sector Specific Plan (SSP) approved in May 2007 which follows an all-hazards approach to CEI security. Ms. Hoffman reviewed the 6 security goals set to the energy sector with respect to information-sharing, physical and cyber security, co-ordination and planning, as well as public confidence. She then presented relevant initiatives of both the industry and the public authorities, stressing that the energy sector is particularly active with regard to the cyber security of CEI. She also emphasized the collaboration of the DoE with other federal agencies and industry sectors, and concluded on the international outreach of the United States for enhancing CEI security overseas.

Mr. **Ritchie** discussed the supporting role of the military in securing access to energy by contributing to the protection of CEI, especially critical nodes in the energy production and distribution system. He emphasized that the military can help develop solutions for effective protection systems, harden possible targets against attacks, and organize response/mitigation capabilities. In conclusion, Mr. Ritchie recalled that in order to counter the terrorist threat to the energy sector, terrorism has to be combated in general, emphasizing that there is a need for better border management, better information-sharing and better co-ordination. In this field as well the military can play a supporting role, assisting with training for better capacity and interoperability, enhanced communication, or provision of technical expertise.

Session 1: Threats and Challenges in Protecting Critical Energy Infrastructure from Terrorist Attacks

The first part of this session was moderated by Dr. **Kevin Rosner**, *Senior Energy Adviser at the Institute for State Craft and Governance*.

Dr. **Vladimir Maroz**, *Deputy Director of the Institute of Training of Judges, Prosecutors and Legal Workers, Belarusian State University*, emphasized the need for both technological improvements and the establishment of an adequate legal framework for strengthening the security of CEI. There is a need for adequate legislation and standards addressing, *inter alia*, construction requirements,

physical security, staff issues, and possibly air space restrictions. When formulating this special regulatory regime, all forms of possible attacks have to be anticipated such as bombings, arson, hostage tacking, seizure of facilities, as well as interference with the operating and control systems. Dr. Maroz also emphasized the need for inter-agency co-operation and co-ordination, and the need for adequate funding to implement security measures. To conclude, he underlined that effective international co-operation is crucial and can be facilitated by international organizations. Possibly, additional international agreements could also help strengthen CEI security.

Professor **Wolfgang Kröger**, *from the Swiss Federal Institute of Technology*, provided a comprehensive assessment of the terrorist threat to CEI, emphasizing vulnerabilities to physical and cyber attacks along the whole transnational energy supply chain. Discussing some criticality criteria, he highlighted the choke points in transnational energy distribution network, and the risk of blackouts/shortage due to the geographical concentration of the production/treatment of energy commodities. Prof. Kröger then discussed possible technical fixes to reduce the vulnerability of CEI to terrorist and cyber attacks. However, referring to a study on CEI security commissioned by Switzerland, he noted that none of the most recent blackouts has been caused by a terrorist attack. Hence there is a need for increased data collection, data exchange and development of analytical methods/capabilities for an adequate assessment of the terrorist threat to CEI and their potential vulnerabilities. Also, possible trade-offs between safety/security concerns and other considerations (e.g. economic liberalization and deregulation) should be further analyzed, and the identification and dissemination of good practices and approaches to securing CEI should be enhanced. The creation of institutional frameworks, processes and multi-stakeholders partnerships can foster progress in these areas, thereby supporting the development of balanced and informed security strategies and measures. In conclusion, Prof. Kröger stressed that since an attack can never be ruled out, such measures should not only harden CEI, prevent attacks, but also increase mitigation and resilience, as well as raise public awareness.

Professor **Nikolay Makhutov**, *Head of the Working Group “Risks and Safety” at the Russian Academy of Sciences*, suggested a classification of terrorist threats to CEI according to the damages aimed at: i) “traditional” attacks for maximum “primary” damages to the facility itself; ii) “technological” attacks for maximum secondary damages (loss of energy commodities), and iii) “intellectual” attacks for maximizing disruption by domino effect (e.g. by interfering with the operating or control system). Prof. Makhutov then presented a theoretical modelization of terrorist attacks against CEI to estimate risks as a function of vulnerability, hazard and possible consequences. He also suggested a theoretical representation of the potential escalation after an initial attack, taking into account the interdependencies in the energy infrastructure system. Prof. Makhutov highlighted that the interconnection of an energy infrastructure with other infrastructures can be a major source of vulnerability, calling for an extension of protection measures to the immediate environment of the said CEI. In conclusion he discussed different forms of protection – rigid, functional, and natural – and their combination, stressing that a security arrangement should be tailored to a specific infrastructure.

Discussion from the floor

Mr. **Bruce Averill**, *Senior Coordinator for Critical Energy Infrastructure Protection Policy with the Office of the Coordinator for Counter-Terrorism of the U.S. Department of State (DoS)*, presented the United States Global Critical Energy Infrastructure Protection (GCEIP) Strategy developed in response to concerns about the security of the global petroleum supply. He observed that over the past few years, some terrorist groups have increasingly called for attacks on energy infrastructure in order to harm the global economy. The GCEIP Strategy is the result of an interagency collaboration co-ordinated by the DoS aimed at assisting foreign countries in improving the security and resilience of overseas petroleum infrastructure identified as critical. Under the GCEIP Strategy, the U.S. pursues bilateral, multilateral and public outreach/co-operative efforts, building on existing initiatives. Bilateral co-operation is established upon request, strictly confidential, and includes provision of interagency expertise, assessments, recommendations, and training.

Mr. **Vladimir Andreev**, *Deputy Director, Department on New Challenges and Threats at the Russian Foreign Ministry*, noted that given the potential damages of a terrorist attack on CEI, the

contribution of international organizations such as the OSCE is very important, but duplication of efforts should be avoided. He felt that the OSCE Ministerial Council Decision No.6/07 provides the basis for an appropriate OSCE involvement, in close co-ordination with other relevant international organizations. Mr. Andreev indicated that the Russian Federation has a rich experience to share in this regard and he reiterated the role of the OSCE as an effective platform for information-exchange and promotion of PPPs in counter-terrorism issues. Mr. Andreev also drew attention to relevant initiatives by the G8 and the Shanghai Co-operation Organization, and informed about an upcoming anti-terrorist drill organized by the Russian company Lukoil in September 2008.

Dr. **Rosner** asked the panellists which possible OSCE contributions they would envisage in light of the needs identified in their presentations regarding the protection of CEI against terrorist attacks. Dr. **Maroz** suggested that in implementation of the existing Ministerial Council Decision, the OSCE could compile a list and facilitate the exchange of best practices and recommendations.

Dr. **Rosner** observed that countries seem to recognize the threat of cyber attacks against CEI highlighted by Prof. Kröger, and also asked him what role the OSCE could play in terms of extending data collection. Prof. **Kröger** suggested the OSCE could promote a comprehensive approach to CEI security along the whole energy supply chain. He felt that there is a need not only to extend data collection but also to conduct more data evaluation and research. He also raised the issue of whether and under which conditions cyber attacks could be regarded as terrorist acts.

At the request of the moderator, Prof. **Makhutov** elaborated on the role of the military and the need for military co-operation in securing CEI, arguing that depending on the infrastructure at stake and potential damages, protection systems have to be elaborated on different complementary levels, including possible military protection.

In response to Dr. Rosner, Mr. **Averill** indicated that the large multilateral framework of the OSCE could be a very effective platform for the United States to share their experience in securing critical infrastructures and establishing high security systems. Mr. **Ritchie** concurred, reiterating the importance of critical information-exchange for effective counter-terrorism.

Ms. **Hoffman** concurred with the presentations by Prof. Kröger and Makhutov, stressing the need for enhanced situational awareness for each infrastructure identified as critical, and assessment of risks as a function of vulnerabilities, degree of threat and potential impact.

Recalling that OSCE Ministerial Council Decision [No.12/06](#) on *Energy Security Dialogue in the OSCE* tasks the OSCE Secretariat with raising awareness and enhancing dialogue on the [G8 Saint Petersburg Plan of Action for Global Energy Security \(2006\)](#), Mr. **Snoy** inquired whether the comprehensive report on securing energy infrastructure called for by the action plan is available to the public. Mr. **Averill** was under the impression that work had been carried out under the German G8 Presidency. Mr. **Andreev** was aware of compilation of different contributions and documents but was not sure whether it is available to the public.

In response to Prof. **Kröger's** observation about the lack of research and data, a representative of the Anti Terrorism Centre of the Commonwealth of Independent States (**CIS-ATC**) informed that several projects already exist in the Russian Federation with risk assessment methodologies and programmes already in use by the private sector and intelligence services.

Concluding the first part of session 1, Dr. **Rosner** highlighted the need for enhanced information-exchange mechanisms, awareness-raising and further promoting PPPs, as areas where the OSCE could make a valuable contribution. In particular, he suggested that the OSCE could look into facilitating the creation of a database in co-operation with other organizations.

Session 1 (continued)

The second part of the first session was moderated by Mr. **Janis Folkmanis**, *Co-founder and Deputy Chairman of the New Security Foundation*.

Mr. **Vladimir Safonov**, *Director of Gazprom Research & Development Centre*, introduced with key facts and figures the Russian company Gazprom, its projects and gas transmission system (GTS).

He then discussed the different factors negatively influencing the performance and development of the GTS, among which illegal acts, including terrorism, represent only a small, although increasing, proportion over the years. Mr. Safonov presented Gazprom's methodology to assess potential risks, which allows for a 5-tier classification of the sections of the GTS depending on the potential impact of their complete failure. Gazprom has developed a series of scenarios based on re-routing and underground storage to ensure the resilience of its GTS in the event of large-scale emergencies such as a terrorist attack on a given section. Since 2005 Gazprom has also developed and implemented specific programmes to enhance both the physical and cyber protection of its facilities against terrorist attacks, including standards, specifications, models and software solutions.

Mr. **Christian Pibitz**, *Chief Executive Officer of Bessentials Groups*, shared his experience as former Chief Security Officer for the Austrian company OMV. He emphasized that appropriate protection of both personnel and facilities is an imperative in ensuring business continuity and should be seen as an investment since preventive measures are more cost-effective. He argued in favour of a long-term and comprehensive approach to risk and threat assessment, underpinned by a good understanding of the socio-economic and political environment where CEI are located. He felt that the complexity of today's security environment for the business sector requires new mindset, methodologies and capabilities. Security systems should aim at reducing vulnerabilities and mitigating risks in general, rather than focusing on a specific threat. Security measures should be decided after cost/benefit analysis, taking into account the impact on the local community. Mr. Pibitz also pointed at the need to discuss the respective roles of the private and public sectors, especially as the importance of private security companies increases.

Mr. **Otto Musilek**, *Senior Executive Adviser at OMV, on behalf of EUROGAS*, presented the activities of Gas Infrastructure Europe (GIE) which has been providing substantial input to the EU-led European Programme for Critical Infrastructure Protection. He also introduced the Energy Security Platform created in 2005 with a view to enhance collaboration within the industry and to facilitate dialogue with European authorities on energy infrastructure security. Discussing the vulnerabilities of European energy infrastructure, including vulnerability to terrorism and cyber attacks, Mr. Musilek explained that GIE follows an all-hazard approach, focusing on the potential damage to CEI rather than the cause. At the political level, GIE lobbies for a European long-term approach to CEI security, based on formal cross-border co-operation, harmonization of basic safety and security standards and a strategic enhancement of the European distribution network. Within the industry, GIE raises awareness and promotes an all-risk long-term security planning, with proactive risk mitigation. In conclusion, Mr. Musilek underlined that a robust energy crisis management strategy depends on co-operation of all stakeholders towards an integrated long-term infrastructure planning and management.

Mr. **Martin van Vianen**, *Deputy Head of Shell's Corporate Security Department, and Chairman of the Security Committee of the International Association of Oil and Gas Producers (OGP)*, emphasized that according to the industry's experience and assessment, terrorism only ranks sixth in terms of the security threats to energy infrastructure, after violent crime, organized crime, militant activism, civil unrest, and political instability. Nevertheless, terrorism is specifically taken into account since the 11 September 2001 terrorist attacks against the United States. Mr. van Vianen underscored that it is in the industry's own interest to assess its possible vulnerability to terrorism and to make the necessary investments for mitigation measures. However, he stressed that governments follow an impact-driven approach in assessing security risks, which leads them to impose on the industry excessive security measures, while the industry's approach is threat-driven and results in flexible, balanced and cost effective mitigation measures. Accordingly, the industry is looking to get threat information from public authorities, and international organizations like the OSCE could facilitate the building of trust and exchange of information between the public and private sector. Mr. van Vianen concluded by cautioning that in order to command the support of the industry in counter-terrorism efforts, governments have to effectively involve stakeholders from the private sector in the formulation of initiatives and legislation.

Dr. **Raul Montaña**, *Project Manager with High Voltage Valley*, briefed from the floor on a research about electro-magnetic terrorism which he felt is underrated as a threat to CEI. He pointed out that the technology is rather simple, affordable and readily available. It only takes a microwave and

some amplifiers for an individual to remotely target, interfere with, and potentially completely disable operating and control systems, without the immediate appearance of an attack. Infrastructure should be modernized accordingly and upgraded with device tested against external electromagnetic interferences. Dr. Montaña felt that the biggest challenge for companies is to co-operate in developing protective solutions, leaving security out the competition field.

Discussion from the floor

Mr. **Folkmanis** asked the presenters about their experience in co-operating with the public sector, how they see the respective roles of the public and private sectors, and what they would suggest to enhance PPPs in securing CEI, including through OSCE facilitation. Mr. **Safonov** explained that within the Russian Federation Gazprom has to comply with both regional and national legislation and regulation, which provide the basis for a close multi-level public-private co-operation with local, regional and federal authorities. Where relevant and appropriate, Gazprom also strives to use and meet the standards developed elsewhere in the international community, such as the European Union. Given the scope of its operations and range of challenges it faces, Gazprom has a vast experience in CEI security that it is ready and willing to share, including through a forum such as the OSCE.

Mr. **Pibitz** noted that in terms of PPP model, computer emergency response networks function very well in Europe and could be replicated with respect to CEI security, possibly at the European level, as a platform for exchanging real-time information, disseminating best practices, but also developing benchmarks and standards for the industry. The OSCE could foster discussions between the public and private sectors on their respective roles; it could promote PPPs, information-exchange and policy discussions, as well as possibly support research, academic exchanges and the creation of a database in the field of CEI protection.

Dr. **Montaña** concurred that one of the biggest challenges is to promote effective co-operation between the academia and the business community, possibly through the creation of specialized research centres.

Mr. **Musilek** felt that there are already several fora and platforms for discussions, but that there is a need for a common framework of minimal binding rules and standards to be developed and adopted at the international level, because so far each company assesses risks differently and implements different security measures which are not always coherent. A set of uniform binding rules and standards to meet would also limit competitiveness/security trade-offs.

Mr. **van Vianen** recalled that a given critical infrastructure is always located in a specific country and that enhanced information-sharing between government agencies and the relevant companies would be mutually beneficial: the industry needs intelligence and threat information that public authorities can provide, and the industry can provide a better assessment of its vulnerabilities. This would improve risk assessment and result in a clearer picture of what the industry and public authorities respectively need to do.

In response to an inquiry of Prof. **Makhutov** about the costs induced by terrorist attacks against CEI and the costs of preventive security measures, Mr. **van Vianen** observed that so far only one such attack has been really successful (against the French oil tanker Limburg in 2002 off the coasts of Yemen) and that the resulting steep increase in the insurance premiums has exacerbated the induced costs. All in all however, security expenses by the industry since 9/11 have been much higher than losses caused by attacks. He stressed that according to the industry's current threat assessment, the stringent regulations under consideration by the EU appear out of proportion and the related costs unjustified.

Mr. **Pibitz** argued that it is hard and impractical to distinguish anti-terrorism related costs from broader security expenses; security enhancement measures should be designed and treated as an investment against security hazards in general. A representative of **NATO** added that besides it is difficult to assess how many attacks and related losses have been prevented thanks to these security measures, which also harden infrastructure against natural hazards.

Mr. **Safonov** indicated that Gazprom's current security expenses exceed potential losses so far, but that they anticipate increasing capabilities and determination of terrorists in the near future. He informed that concrete plans for attacks against Gazprom infrastructure have already been discovered. Mr. **Averill** felt that security budgets within the industry should be increased, but that funding is an issue. He also asked representatives of the industry whether their companies are self-insured or contract insurance policies against terrorist incidents. Mr. **van Vianen** replied that so far security costs for privately owned facilities are still completely incurred by the energy industry, including insurance policies, while for other sectors such as the aviation industry rising costs have ultimately been at least partly covered through public monies. He reiterated that there is a feeling within the energy industry that some security measures and related costs imposed by governments are not warranted by the industry's assessment of the terrorist threat to CEI.

Mr. **Musilek** observed that in order to discuss costs and insurance, one would need to first agree on what critical infrastructure are, noting that the EU has not yet been able to clearly do so. Mr. **Pibitz** concurred that answers to all these issues still vary from one country to another, with some instances where responsibilities between the public and private sectors are quite clear. Prof. **Kröger** argued that a predictive analysis and risk informed regime is the best approach to limit costs. He also raised the issue of how to best involve all stakeholders in the decision-making process, in particular the industry when it is expected to bear high costs.

A representative of the **NATO School** asked to what extent the energy industry relies on public security provision by the military and law-enforcement agencies, what the shortfalls are, what could be done by private security companies, and what role the OSCE could have in this respect. Mr. **Pibitz** answered that the energy industry often opts for a security mix including its own capacity, external private security companies as well as public security provision, depending on the local situation. Private security companies are often contracted to secure the outside and immediate perimeter of CEI. However private security sometimes raises human right concerns and the sector suffers from a lack of transparency, despite improvements over the past few years. Mr. Pibitz also observed that there is a tendency towards unarmed private security.

Mr. **Folkmanis** asked the panellists to summarize what is in their view the greatest priority in terms CEI protection against terrorist attacks. Dr. **Montaño** felt there is need for a comprehensive assessment of vulnerabilities as few infrastructures have actually been designed to face the terrorist threat. These vulnerabilities should be acknowledged and all stakeholders should frankly exchange and better co-operate among themselves. Mr. **van Vianen** reiterated that strengthening the information-exchange between the public and private sector is critical and he added that public authorities should be ready to provide enhanced security in times of crisis, as well as to look into the issue of funding. Mr. **Musilek** highlighted the need to define what is "critical" and to provide the whole sector with an international framework of binding rules and standards for CEI security. Mr. **Pibitz** emphasized the need to promote a threat-driven approach and to clarify roles and responsibilities between the public and private sectors. Mr. **Safonov** emphasized that all countries should co-operate and agree on a common methodology because they are interconnected. He also underlined the need for public-private co-operation, noting that Gazprom successfully co-operates with the Russian authorities thanks to a clear division of responsibilities.

Session 2: Activities of Relevant International Organizations and Structures, and Opportunities for Co-operation with the OSCE

The first part of the second session was moderated by Mr. **Snoy**, *Co-ordinator of OSCE Economic and Environmental Activities*.

Ms. **Anita Nilsson**, *Director of the Office for Nuclear Security at the International Atomic Energy Agency (IAEA)*, presented the activities of the IAEA to protect against acts of nuclear terrorism, pointing at a real risk for nuclear infrastructures to be the target of theft or sabotage. She stressed that nuclear safety and security measures are becoming ever more topical as the demand for nuclear energy is growing, the transport of radioactive materials is increasing and several new nuclear related facilities are under construction. The IAEA provides standards and norms and

promotes their systematic implementation by constructors and operators. Highlighting the contribution of the OSCE in promoting the ratification of the existing relevant legal instruments, Ms. Nilsson also suggested that the OSCE could facilitate their implementation and promote the six Nuclear Security Series guidance materials developed by the IAEA. She stressed that in order to prevent and reduce the threat of nuclear terrorism the IAEA needs the support of the international community in improving the physical protection of facilities, providing training and equipment, including for detection and response. Reiterating that information-sharing is a cornerstone of counter-terrorism, she also briefed on the Agency's Illicit Trafficking Database (ITDB) Programme. In conclusion, Ms. Nilsson explained about the Integrated Nuclear Security Support Plans (INSSPs), each of which sets a predictable work plan for assistance to a given country and help coordinate multilateral and bilateral assistance projects.

Mr. **Ralf Dickel**, *Director of Trade and Transit, Energy Charter Secretariat*, explained that while terrorist attacks against CEI are not explicitly addressed under the Energy Charter (EC), some of its provisions indirectly cover the physical protection of infrastructure. Art.10 on the *Promotion, Protection and Treatment of Investments* and the Art.12 on *Compensation for Losses* could apply to terrorist acts, and Art.7 under the transit provisions implicitly calls for the comprehensive protection of transit infrastructure. Additionally, Mr. Dickel explained that the Legal Advisory Taskforce of the EC Secretariat has developed models for intergovernmental agreements (IGA) and host government agreements (HGA) on cross-border pipelines, as well as an appendix, which address some security issues such as obligation of means to eliminate an eminent threat, establishment of security zone, and prohibition of the use of explosives within an agreed security perimeter. He suggested that the IGA and HGAs for the Baku-Tbilisi-Ceyhan Main Export Pipeline could provide examples of such security provisions for other projects, highlighting that the transit fees implicitly include a compensation of the cost related to the protection of the pipeline. In conclusion, Mr. Dickel informed that a possible role of the EC in the field of CEI protection might be addressed during a review of the EC treaty in 2009.

Mr. **Dmitry Yegorov**, *Head of Information Group at the Anti-Terrorism Centre of the Commonwealth of Independent States (CIS-ATC)*, informed about the relevant activities of the CIS in protecting critical infrastructure, including CEI, on the basis of the 1999 Minsk Treaty for co-operation among CIS member states in combating terrorism. The Minsk treaty classifies take-over, destruction or partial damage of critical infrastructure as "technological terrorism" and foresees CIS co-operation in assessing critical infrastructure protection, developing and implementing security enhancement measures, as well as joint research projects and experiments for improved protection systems. Subsequent Interstate Programmes for CIS counter-terrorism co-operation have developed since 2000 concrete activities, including assessment of vulnerabilities and potential consequences of attacks, classification of infrastructure, random testing of security systems, enhancement of physical protection measures, and drills. Since 2005, CIS member states have conducted joint counter-terrorism exercises aimed at improving interagency and cross-border coordination, focusing in particular on the protection of infrastructure close to borders, including CEI (e.g. KASPI Anti Terror 2005 in Kazakhstan, ATOM Anti Terror 2006 in Armenia). CIS-ATC now develops methodological recommendations for organizing exercises simulating attacks on nuclear/radioactive facilities. To conclude, Mr. Yegorov stressed that all these exercises have testified to the preparedness of CIS member states in the event of a terrorist attack against critical infrastructure.

Discussion from the floor

In response to a question posed by another representative of **CIS-ATC** about possible IAEA activities regarding the threat of radioactive materials in Central Asia, Ms. **Nilsson** indicated that a lot of attention is devoted to the region by the Agency, especially with respect to storage issues, and that specific capacity building and technical assistant projects are already under way to foster compliance with existing security and safety standards.

Mr. **Snoy** noted that the Russian Federation provisionally implements the Energy Charter Treaty, in spite of not having ratified it, and asked whether this includes the Charter security provisions. Mr. **Dickel** explained that with a provisional implementation, only the provisions of the Charter that do not conflict with existing national rules and standards are implemented. He felt that in any case the

protection of CEI is state of the art in Russia and the Russian Federation probably does not need to rely on the EC provisions in this regard.

Prof. **Kröger** raised the issue of the potential psychological impact and panic associated with a terrorist radiological attack. Ms. **Nilsson** concurred that the public perceives the spread of radioactivity as big danger, often disproportionately to the real danger, which can lead to panic and disruption of evacuation efforts, and can potentially result in more long-term casualties by irradiation. This is an important dimension that the IAEA takes into consideration for emergency preparedness and consequence mitigation. Basic emergency preparedness needs to be fostered in all countries, even in those which do not host nuclear facilities. Mr. **Yegorov** noted that exercises have been conducted in this regard within the CIS.

In response to a question by Prof. Makhutov about the issue of radon and its isotopes, Ms. **Nilsson** indicated that the IAEA has no jurisdiction over non-fissile materials but that, upon request, it can facilitate bilateral support and assist in establishing domestic controls.

The representative of **Électricité de France** believed that security expenses to prevent terrorist attacks against CEI will keep increasing as new measures and standards are imposed. He felt that public awareness should be raised about these costs and that this financial burden should be shared. Prof. **Kröger** agreed, noting that the energy industry is often suspected of profiteering.

Recalling the tragedy of Chernobyl, Mr. **Yegorov** argued that damages and losses will always outweigh the costs of preparedness and prevention measures when dealing with the security and safety of critical energy infrastructure. But he agreed that the actual level of threat should be taken into account to formulate balanced security solutions. Ms. **Nilsson** concurred, advocating a proactive rather than reactive approach to security, according to which security is seen as an investment and is integrated from the beginning. In-built security would result in a “normal” way of operating critical energy infrastructure that is safe and responsible. New upgraded norms and standards are needed and should be integrated, especially when designing new infrastructure, just as the aviation industry had to after the 11 September 2001 terrorist attacks.

Session 2 (continued)

The second part of this session was moderated by Mr. **Perl**, Head of the ATU.

Mr. **Michael Gaul**, *Deputy Director of Defence and Security Economics, Directorate for Political Affairs and Security Policy, North Atlantic Treaty Organization (NATO)*, presented the role of NATO in enhancing energy security, as envisaged by the 2008 Bucharest Summit following discussions initiated at the Riga Summit in 2006. He stressed that NATO is not a principal actor and does not aspire to a leading role in CEI protection, but it can make a key contribution as security provider. In this regard, the [Bucharest Summit](#) was a milestone, framing NATO’s involvement in energy security in five areas. Thanks to its specialized bodies and expertise, NATO can support information and intelligence gathering and sharing, providing early and reliable information for long-term threat and risk assessment. It can help project stability through its outreach and partnership programmes as well as its crisis response under exceptional circumstances. NATO can advance international and regional co-operation on relevant energy security issues, including military co-operation, science and technology development programmes, dissemination of lessons learned, organization of topical conferences and seminars. NATO can support consequence management efforts through its Euro-Atlantic Disaster Response Coordination Centre (EADRCC) and Senior Civil Emergency Planning Committee (SCEPC). More specifically, NATO can support the protection of CEI, including through its maritime surveillance operations. Mr. Gaul concluded that early co-ordination with the OSCE is valuable as NATO’s specific initiatives in the field of energy security are being defined.

Mr. **Zakir S. Zaitov**, *Deputy Director of the Department for Countering Threats and Challenges at the Secretariat of the Collective Security Treaty Organization (CSTO)*, emphasized that since their 2006 Minsk Summit, CSTO member states have been strengthening their co-operation and co-ordination in countering new security threats and challenges, including international terrorism. A programme of common measures and activities has been implemented to improve law-enforcement

and intelligence capabilities in the fight against terrorism and drug trafficking, including through strengthening the international legal framework for co-operation, providing specialized training, exchanging experience and information, upgrading technical and technological capabilities, and conducting joint exercises. Accordingly, the Russian Interior Ministry's Institute for Advanced Education and Training of Law Enforcement Officers has become the CSTO's official training institution, and CSTO member states also adopted during their 2007 Summit in Dushanbe a decision setting preferential terms of access to technological capabilities by their law-enforcement and intelligence agencies in charge of the protection of critical infrastructure. In addition, CSTO is elaborating a draft plan for collective action over 2008-2010 in support of the implementation of the United Nations Global Counter-Terrorism Strategy, which foresees enhanced protection of critical infrastructure and other vulnerable targets such as public places, strengthening response capabilities and civil emergency preparedness, as well as identification and dissemination of best practices in protecting vulnerable targets, including PPPs. CSTO is taking concrete steps towards the creation of joint anti-terrorist forces, but there is already the possibility to use its rapid deployment forces for counter-terrorism operations. Besides, CSTO has also organized since 2006 a series of drills and practical training to enhance CEI protection against terrorist attacks, mitigation and consequence management, as well as co-ordination among its member states (e.g. 2006 ATOM Anti Terror in Armenia, 2007 BAIKONOUR Anti Terror in Kazakhstan), which have resulted in concrete regulatory and organizational improvements. Mr. Zaitov concluded by emphasizing CSTO's readiness to further co-operate with other international organizations and interested states in countering new threats and challenges to peace, security and stability in the Eurasian region.

Dr. Heiko Borchert, security and defence consultant, and advisory board member of IPA Network International Public Affairs, made a presentation from the floor on the findings of a research project commissioned by the Swiss Ministry of Foreign Affairs, which identifies the following key issues in terms of securing the worldwide energy infrastructure system: i) lack of cross-border co-operation and transborder emergency management capabilities, ii) complex vulnerabilities including interdependencies with other infrastructure, especially information and communication technologies, iii) underinvestment, as well as iv) lack of common safety and security standards along the whole global energy supply chain. Against this background, Dr. Borchert advocated an integrated and comprehensive approach for energy infrastructure security, identifying four areas where the OSCE could provide value added: i) organizing best practices workshops in particular to advance CEI safety and security, ii) supporting relevant security sector reforms (e.g. promoting investment in dual-use capabilities, interagency co-ordination, and involvement of the industry in decision-making process), iii) fostering community involvement (e.g. promoting integrated community-based security), and iv) promoting dialogue and best practices regarding private security contractors. Dr. Borchert underlined that there is a need for transparency and confidence-building with regard to energy infrastructure security and that the OSCE could serve as platform for co-ordination between all public and private stakeholders towards comprehensive action, as well as facilitation of joint regional initiatives along key infrastructure corridors.

Discussion from the floor

Noting that the cyberspace is virtually ungoverned and that critical infrastructure in general are potentially vulnerable to cyber attacks, a representative of the **Marshall Centre** inquired about NATO's possible role in this regard. Mr. **Gaul** informed that cyber security is a need recognized by NATO which was also addressed by the Bucharest Summit, where the development of NATO's cyber defence capabilities to implement its Policy on Cyber Defence was agreed upon.

Prof. **Makhutov** asked whether there are plans for establishing specialized counter-terrorism forces within NATO and CSTO, which would be organized, equipped and trained to face this specific and increasing threat. Mr. **Zaitov** reiterated that CSTO is considering the creation of special anti-terrorism forces, drawing on the complementary expertise and capabilities of all CSTO members. Tactics, technology weaponry and training would need to be adapted to face different possible situations, including where firearms cannot be used. Mr. **Gaul** indicated that NATO intervenes only upon request in terrorist-induced crisis and that, building on the outcome of the Bucharest Summit, the NATO Response Force will receive special training to deal with attacks involving CEI. Mr. **Averill** added that appropriate special weaponry already exists.

Closing Remarks and Overview of Suggested Options for Possible OSCE Contribution to Enhancing Critical Energy Infrastructure Security

Mr. **Perl** thanked participants for their active contributions and summarized the challenges and needs identified in enhancing CEI protection against terrorist attacks. He also reviewed the suggestions made by participants for possible value-adding OSCE activities (e.g. workshops, training, compilation of materials) in terms of mobilizing political support, promoting co-operation and enhancing national capabilities. Such activities could be conducted on an OSCE wide, sub-regional, or national level, in close co-ordination with, and facilitating the work of relevant other international organizations:

1/. Mobilizing political support

- The OSCE could raise awareness of the threats to CEI, interdependencies between countries and stakeholders, and options for response. Security needs to be mainstreamed in the planning and management of energy infrastructure, with additional investments and enhancement measures to meet new vulnerabilities and threats (e.g. cyber and electromagnetic attacks), which can also increase preparedness against natural disasters or accidents.
- The OSCE could promote the international legal framework for CEI security, including through further promoting the ratification and implementation of existing instruments (e.g. universal anti-terrorism conventions and protocols), as well as supporting the development of new instruments where relevant and appropriate.
- The OSCE could promote compliance with existing guidance materials such as the IAEA Nuclear Security Series.
- The OSCE could promote the development of a uniform cross-border regulatory framework and a comprehensive set of standards for CEI security along the whole energy supply chain.

2/. Promoting co-operation

- The OSCE could promote and possibly facilitate the creation of enhanced mechanisms for international co-operation on CEI protection, such as a CEI Emergency Response Network.
- The OSCE could foster multilateral information-sharing (e.g. lessons-learned, threat information, technological information, situational awareness), as well as the dissemination of good practices for CEI security (e.g. measures to increase resilience and enhance recovery capacity, good practices with regard to private security contractors), for instance through the creation of a secure and restricted Internet portal.
- The OSCE could promote and facilitate public-private partnerships for CEI protection, including by supporting discussions on roles, responsibilities and sharing of costs, building public-private trust, and supporting public-private information-sharing (e.g. facilitating the creation of a PPP CEI Security newsletter, of an international public-private CEI Forum, or of an international public-private CEI security commission).

3/. Enhancing national capabilities

- The OSCE could promote the development of national CEI security strategies following a comprehensive, integrated, all-hazard, balanced and sustainable approach.
- The OSCE could promote the strengthening of analytical methods and capabilities for CEI protection, including through the dissemination of vulnerability, risk and threat assessment methodologies, the promotion of research, data collection-evaluation and sharing. The OSCE could possibly facilitate the creation of a comprehensive CEI protection database.
- The OSCE could facilitate institutional capacity-building, including through the promotion of national inter-agency co-operation and co-ordination, supporting the creation of national agencies for critical infrastructure protection, supporting the enhancement of civil emergency planning and capabilities, including for disaster response, facilitating national and cross-border training.

Closing the expert meeting, Mr. **Snoy** emphasized the value and importance of the input from participants for the report of the OSCE Secretary General on opportunities for OSCE co-operation with relevant international organizations in the field of CEI protection from terrorist attacks. He stressed that the OSCE has a strong track record in raising awareness, building political will and promoting co-operation for a comprehensive approach to security issues, and he recalled in this regard that CEI security cannot be isolated from economic and environmental considerations.