



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

Governments

- Mr. Stephen Caldwell, U.S. Government Accountability Office, [LINK](#)
- Dr. Felix Kwamena, Natural Resources Canada, [LINK](#)
- Romanian Intelligence Service, [LINK](#)
- Ministry of Internal Affairs of the Republic of Georgia, [LINK](#)

International Structures

- Mr. José Hoyos Pérez, European Commission, [LINK](#)
- Col. Andrei Novikov, Anti-Terrorism Centre of the Commonwealth of Independent States (CIS-ATC), [LINK](#)

Research Institutes

- Dr. Heiko Borchert and Ms. Karina Forster, International Public Affairs Network, [LINK](#)
- Ms. Jennifer Giroux, Centre for Security Studies (CSS), [LINK](#)
- Prof. Wolfgang Kröger, Swiss Federal Institute of Technology (ETH) of Zurich, [LINK](#)
- Dr. Kevin Rosner, Institute for the Analysis of Global Security, [LINK](#)
- Dr. Frank Umbach, Centre for European Security Strategy (CESS), [LINK](#)

Industry/Businesses

- Dr. Bruce Averill, Strategic Energy Security Solutions LLC, [LINK](#)
- Mr. David Baker, IOActive, [LINK](#)
- Mr. Umberto Saccone, Corporate Security Manager, ENI spa, [LINK](#)
- Mr. David Taylor-Smith, G4S, [LINK](#)

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

Contents by subject

Threat Assessment

- Ms. Jennifer Giroux, Centre for Security Studies (CSS), [LINK](#)
- Romanian Intelligence Service, [LINK](#)

National Approaches

- Dr. Felix Kwamena, Natural Resources Canada, [LINK](#)
- Ministry of Internal Affairs of the Republic of Georgia, [LINK](#)

Regional Co-operation

- Mr. José Hoyos Pérez, European Commission, [LINK](#)
- Col. Andrei Novikov, Anti-Terrorism Centre of the Commonwealth of Independent States, [LINK](#)
- Dr. Kevin Rosner, Institute for the Analysis of Global Security, [LINK](#)

Public-Private Partnerships

- Dr. Bruce Averill, Strategic Energy Security Solutions LLC, [LINK](#)
- Dr. Heiko Borchert and Ms. Karina Forster, International Public Affairs (IPA) Network, [LINK](#)
- Mr. David Taylor-Smith, G4S, [LINK](#)

Oil and Gas Infrastructure Protection

- Mr. Stephen Caldwell, U.S. Government Accountability Office, [LINK](#)
- Mr. Umberto Saccone, Corporate Security Manager, ENI spa, [LINK](#)
- Ministry of Internal Affairs of the Republic of Georgia, [LINK](#)

Electric Infrastructure Protection

- Mr. David Baker, IOActive, [LINK](#)
- Prof. Wolfgang Kröger, Swiss Federal Institute of Technology (ETH) of Zurich, [LINK](#)

Cyber Security

- Mr. David Baker, IOActive, [LINK](#)
- Dr. Frank Umbach, Centre for European Security Strategy (CESS), [LINK](#)

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



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

Editorial

The importance of energy security and energy infrastructure security cannot be overstated. It 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.

In recent years, protecting critical energy infrastructure (CEI) from terrorists has received increasing attention from the international community, and rightly so. A key goal for an increasing number of terrorists is to inflict maximum economic damage and social disruption. And since CEI provides the fuel that keeps the global economy moving and our societies working, our dependency on such infrastructure makes it an ideal terrorism target.

The reality of the terrorist threat to CEI is often discussed, especially by private sector owners and operators. But strong evidence exists of the level of damage that terrorist attacks on energy infrastructure can cause. And despite all efforts undertaken vulnerabilities still exist.

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.

OSCE participating States adopted in November 2007 a Ministerial Council Decision on *Protecting Critical Energy Infrastructure from Terrorist Attack* [MC.DEC/6/07], whereby they committed to co-operate amongst them and to consider all necessary measures at the national level in order to ensure adequate CEI protection from terrorist attack.

In line with the decision, the OSCE Action against Terrorism Unit (ATU) will organize on 11-12 February 2010 in Vienna, at the initiative of the United States of America, a *Public-Private Expert Workshop on Protecting Non-Nuclear Critical Energy Infrastructure from Terrorist Attacks* [see invitation package circulated on 17 November 2009 as SEC.GAL/188/09, and reminder circulated on 19 January 2010 as SEC.GAL/8/10].

The purpose of the present CTN Special Bulletin is to facilitate the exchange of information and stimulate reflection in view of this upcoming workshop. Participating States, through their OSCE CTN contact points, have been invited to contribute articles and a number of international structures, private sector stakeholders and researchers were invited to share their views.

The contributions received by the ATU and compiled in this Special Bulletin are meant to provide food-for-thought on different issues in the field of CEI protection from terrorist attacks, including:

- Risk assessment methodologies, including identification of *critical* infrastructures and interdependencies;
- Physical and cyber vulnerabilities of CEI and corresponding prophylactic and preparedness measures;
- National approaches, capabilities and measures;
- The need for public-private partnerships (PPPs);
- Opportunities for cross-border and international co-operation;
- The potential contribution of international structures, and in particular that of the OSCE [in this regard, see the OSCE Secretary General's report SEC.GAL/202/08]

CEI security presents challenges in terms of the threats we face and opportunities in terms of how we can respond to those threats. The ATU looks very much forward to working with you in this field. Please do not hesitate to contact us to share information and ideas on possible initiatives to protect CEI from terrorist attacks.

I hope that you will enjoy reading this Special Bulletin,

Sincerely,

Raphael F. Perl

Head on Anti-Terrorism Issues

OSCE Action against Terrorism Unit

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

Maritime Infrastructure: Challenges in Protecting Energy Tankers

*Mr. Stephen L. Caldwell, Director of Maritime Security Issues
U.S. Government Accountability Office (GAO)*

Energy Tankers Critical to Many Economies

Many developed nations are highly dependent on tanker vessels to import oil, gas and other energy commodities from overseas. This already extensive reliance on imported energy commodities is expected to increase, in some cases dramatically. For example, the import of Liquefied Natural Gas (LNG) into the United States is forecast to grow by more than 400 percent by 2015. Transporting these often hazardous commodities by sea involves a global supply chain originating in a number of nations in the Middle East, Africa, Latin America and the Caribbean—depending on the commodity—and ending in various developed nations in Europe, North America, and Asia. Transporting these commodities also involves tankers owned by many different companies, as well as routes across international waters that no government controls. There are more than 3,000 registered crude oil tankers and more than 200 LNG tankers.

There Are Many Threats against Energy Tankers

The energy tanker supply chain, while critical, is also vulnerable to disruption by terrorists and pirates. Port terminals (at both origin and destination nations) are inherently vulnerable, because they must provide access by land and sea and because they are sprawling installations, often close to busy populations centers. Likewise, the tankers that transport the products are vulnerable because they travel on direct routes that are known in advance and, for part of their journey, they may have to travel through narrow straits (known as chokepoints) that do not allow them to maneuver away from possible attacks. Since so many different players are involved, terrorists have room to probe the supply system for the weakest link. Despite an often heavy security presence, terrorists have attempted—and in some cases succeeded—to attack energy tankers and terminals. Successful examples include the 2002 attack on the tanker *Limburg* near Yemen, the 2003 hijacking of the tanker *Penrider* near the Straits of Malacca, the 2004 attack on offshore terminals near Iraq, and the 2006 assault on a gas terminal in Nigeria. In addition to terrorists attacks, pirates have recently and successfully targeted tankers to include the *Sirius Star* and *Longchamp* near Somalia.

As the above examples have demonstrated, there are several types of attacks that tankers face that could have serious consequences. The scenarios of most concern include suicide boat attacks (to ram and explode the side of a tanker), standoff attacks (to launch a rocket or other weapon at a tanker), or armed assault (to board and hijack a tanker). Other potential types of attacks include internal crew conspiracies, and collisions with other vessels piloted by terrorists. While attacks on energy tankers and terminals have been rare, successful attacks could have substantial public safety, environmental, and economic consequences—which would vary by commodity. For instance, highly combustible commodities like LNG have the potential to catch fire, or possibly explode. Less combustible commodities like crude oil have the potential for environmental damage as they do not disperse and might require costly removal. Finally, the economic consequences of a major attack could include a temporary price spike reflecting fears of further attacks and supply disruptions. While the loss of one tanker might not have a significant impact, if an attack results in port closures for multiple days or weeks, price responses and higher costs could mean losses in economic welfare to consumers, businesses, and governments amounting to billions of dollars.

Key Security Measures Are Being Implemented

Much is being done, at both the international and national level, to protect energy tankers and their attendant port facilities from attack. The International Maritime Organization and its ISPS Code set baseline requirements for maritime security. National governments and terminal operators are taking such actions as improving physical security at port facilities and conducting offshore patrols. For example, port facilities report compliance with the ISPS Code requirements, and tanker operators report strengthening their security posture while loading and at sea. Many navies are patrolling threatened waters, such as the Persian Gulf and Gulf of Aden. In the United States, additional actions are being taken beyond those required in the ISPS Code

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

to protect the energy supply chain. These actions include monitoring the arrival of tankers and crews, boarding selected vessels before they reach port, escorting selected tankers into port, and providing waterside security patrols at energy terminals. In addition, officials responsible for port security have developed response plans to address a successful attack and mitigate the consequences. Finally, officials have conducted exercises to test their operational capabilities and their response plans. Such exercises help determine the strengths and weaknesses of various plans and the ability of multiple agencies or communities to respond to an emergency incident related to energy-related maritime infrastructure.

Providing Security Still Presents Challenges

Despite the protective measures in place, maritime security officials face continued challenges in protecting energy tankers and related port infrastructure. For tankers transiting international waters, the primary challenge involved patrolling the lengthy travel routes and frequent danger spots with only a limited number of naval vessels. For port infrastructure, some facilities are having challenges complying with the ISPS Code. GAO visits to energy facilities abroad showed that some port facilities had put extensive security measures in place, while other facilities had such problems as unattended gates and downed fences. Other protective measures, such as boarding and escorting tankers, require expensive resources such as boats and appropriately trained law enforcement personnel. Ports also face challenges in planning, exercising and executing responses to an attack on energy tankers or terminals. Part of the problem is that there can be multiple stakeholders responsible for planning and executing different parts of the response—for example law enforcement, environmental protection, and firefighting. And again, resources are an issue with many of these stakeholders. In some ports, for instance, local firefighters do not have enough fire boats or are not sufficiently trained for maritime firefighting. Finally, given the resource challenges, it is important that security-related decisions and activities to protect tankers and other maritime infrastructure are executed in the context of risk management. No amount of money can totally insulate vessels and ports from attack by an enemy with resources and determination.

NOTE: The Article is based on the report: *Maritime Security: Federal Efforts Needed to Address Challenges in Preventing and Responding to Terrorist Attacks on Energy Commodity Tankers* (GAO-08-141). See www.gao.gov/cgi-bin/getrpt?GAO-08-141.



Photo: U.S. Coast Guard enforcing a security zone around LNG tanker (source GAO)



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

Critical Energy Infrastructure Protection from Terrorist Attacks: a Canadian Approach

*Dr. Felix Kwamena, Director/Special Advisor, Energy Infrastructure Security, Energy Sector,
Natural Resources Canada (NRCan)*

The framework for the protection of Canada's energy infrastructure systems is based on three fundamental and inter-related elements.

First, is prevention – ensuring that the vulnerabilities are well understood, the commendable practices are shared, and the best intelligence and the communication network are in place to respond to the risks, whatever the sources, natural disasters, malicious attacks, internal threats, etc. Second, is response in times of an emergency – the ability to respond in a timely fashion and effectively. Third, is resilience – the ability to bring infrastructure systems or strategic assets back on line to restore energy supply.

The basis for the framework is the National Security Policy of 2004, Securing an Open Society: Canada's National Security Policy; the 2007 Emergency Management Act, and the 2008 Working towards a National Strategy and Action Plan for Critical Infrastructure Draft Paper.

In addition, there are other drivers that underpin the framework. Canada's energy infrastructure system is vast, complex, and intertwined, comprising oil and gas, electricity, hydro-generation, and other energy facilities across the country; each with its unique challenges.

Energy Infrastructure systems are also widely dispersed geographically, and subject to multiplicity of jurisdictional and legislative requirements. There is also the large array of stakeholders ranging from owner-operators, security and intelligence agencies, regulators, representatives of federal, provincial, territorial departments, academia, industry associations, etc.

The Energy and Utilities Sector Network is the forum that brings all the energy sector stakeholders together to discuss issues of common interest – discussion of methodologies for risk profiles, identification of interdependencies, emergency management programs, and communications plans.

Another important aspect of Canada's approach is the hosting of twice-a-year classified information sharing sessions at the Secret level. A selected number of energy infrastructure systems owner-operator representatives, industry association and academia attend these classified briefings. In addition, Natural Resources Canada also hosts other information sharing sessions at the "for-official-use only" level.

These forums provide excellent opportunities for energy sector stakeholders to develop ongoing trusting relations which facilitate the exchange of pertinent information "off the record", with the understanding that it will not be attributed.

Through partnership with academia, Natural Resources Canada commissioned a number of studies on Critical Infrastructure protection policy research. These studies have provided a very useful theoretical and empirical research contribution to guide policy development.

Critical energy infrastructure protection initiatives have also been supported by scientific modeling and analysis work carried out by the Canadian Explosives Research Laboratory. Scientists and engineers from the laboratory have also participated as members of a multi-disciplinary team of experts that carried out site-specific vulnerability and security assessments of critical energy facilities.

Thus, Canada's approach to critical energy infrastructure protection could be characterized as "comprehensive, proactive, collaborative and intelligence-led" based on a national security policy, legislation and regulation. It involves all major stakeholders. Meaningful information sharing, including classified briefings for those with the "need-to-know" is at the core of the framework. All sourced analytical and policy expertise are supplemented by scientific modeling and analysis and academic policy research studies.

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

The Management of Risks in the Process of Defining and Protecting Critical Infrastructure, as a Key-Factor of Regional Stability and Security

Romanian Intelligence Service (SRI)

The global trade-related economic development generated by the accelerated progress of technology and the striking effects of globalization has revealed the close interconnection of the systems which ensure the safety and welfare of society.

The need to interconnect systems – linked to the global trends towards the dissolution of administrative barriers, access to emerging markets and integration of the infrastructure networks – induces changes regarding world-wide security and stability.

The sum of asymmetrical risks, likely to amplify in the future, reflects the role and importance of critical infrastructure, as a **material** element (equipment, installations, art works, transportation facilities, etc), an **organizational** one (transportation networks, energetic systems, production and distribution of oil and natural gas products etc) and also **informational** (data flows and transmissions, procedures, etc), which are vital to an appropriate social life and support economic evolution, in a stable and secure climate.

Its weak point – the increase value of this indicator is intensified by the importance of the attended system, basically the level of protection to threats – represents a key spot of security strategies and policies.

The complexity of the critical infrastructure protection has determined the association of strategies initiated at state-level, and that of great alliances, with the needs to identify and increase its safety levels, as **reactive element to threats**, but also as a main **bearer of internal/external threats**.

The definition and identification of the critical infrastructure

Infrastructure (as a single element or as a whole) may be considered **critical** from the point of view of its **unique condition** and **complementary nature** within a system, its major **role** in ensuring the stability, feasibility, safety, operation and security of the whole, its increased **exposure** to direct threats, but also to those aimed at the processes it is a part of, or from that of the special **weaknesses** towards condition variation and, especially, sudden changes of the state of facts.

Classification criteria result from the sectorial/intersectorial effects and have the following **elements of assessment**: **physical** (or criterion of this, where among other facilities, size, dispersion, endurance reliability), **functional** (or criterion role - what "makes" such infrastructure), **security** (what are the safety and security infrastructure, measured in terms of effects that can be generated by violating the basic conditions), **flexibility** (which shows that there is a certain dynamic and flexible in terms of critical infrastructure, some of those included in the category of being able to become common in certain conditions, critical infrastructure and vice versa), **unpredictability** (what looks like some regular or special facilities may become contextual critical infrastructure) etc.

Therefore, the protection of the critical infrastructure represents a major interest in the globalization-related evolution, as the concern to identify risks, weak spots, threats and dangerous situations related to it (*mainly caused by religious convictions, or subsequent to terrorist acts and extreme weather conditions*) is decisive, together with the initiation of prevention and counteract measures meant to maintain a secure and stable environment.

Risks related to the critical infrastructure in the energy field

Taking into account the international outbreak of terrorism, the critical infrastructure in the energy field deserves a special attention, as it could be a potential target to the terrorist groups, because of the severe effects that may be caused by its destruction (**at a multi-national/statal level**, due to the interconnection of its components). Furthermore, the issue of designating critical infrastructure has become increasingly significant, given the context of the growing number of infrastructure failures (including black-outs), extreme weather conditions and unauthorized physical intrusion acts.

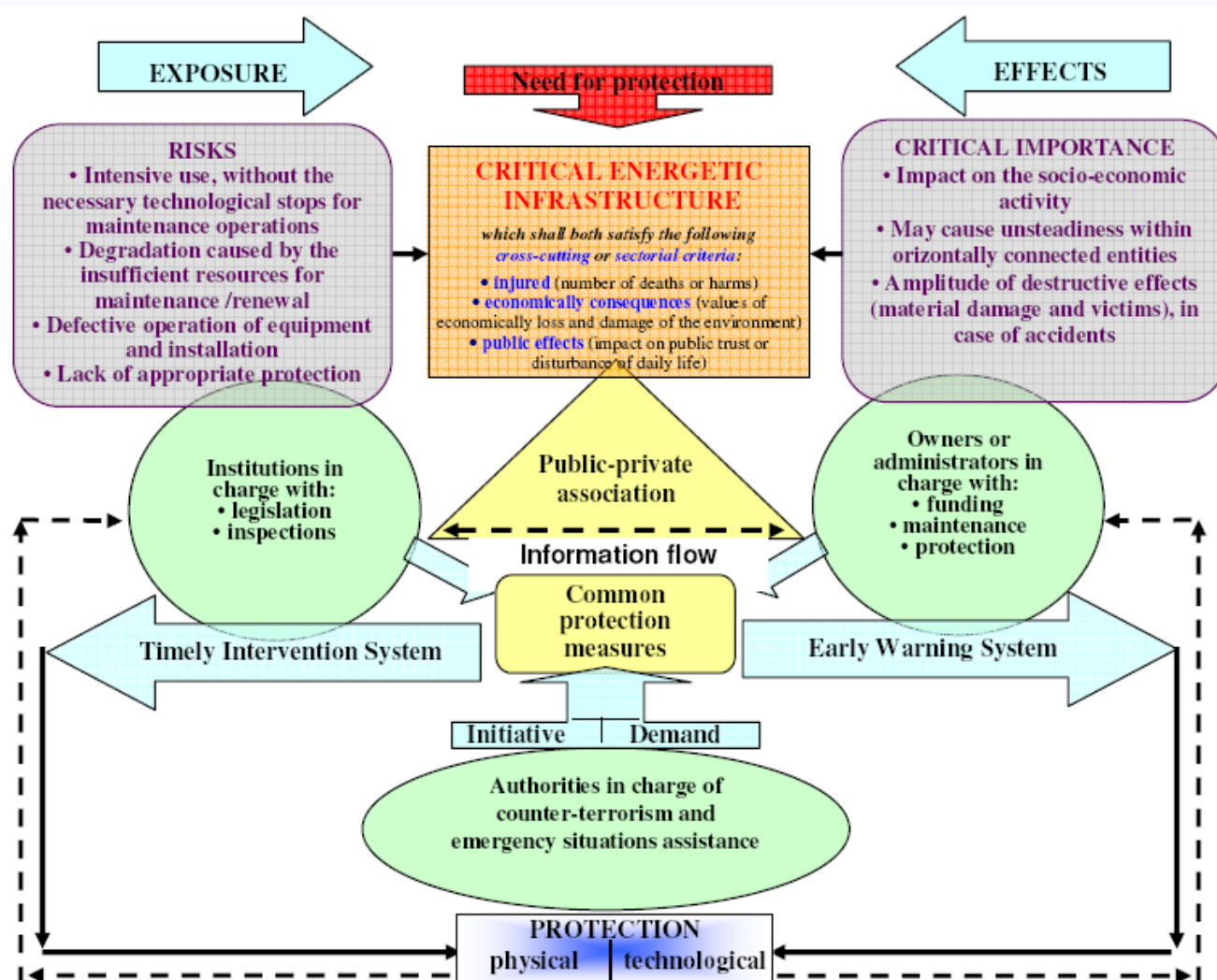
CTN Newsletter Special Bulletin

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

| ASSOCIATED RISKS | FORMS | EFFECTS |
|--|---|---|
| Intensive use , without the necessary technological stops for maintenance operations State of degradation caused by the insufficient allocation of resources for maintenance /repair or for the renewal of the physically and morally exhausted equipment Defective operation of equipment and installation, caused by human error Lack of safety/protection measures | <ul style="list-style-type: none"> • Use of certain practices mainly oriented towards profit maximization, without taking into account the real capacity of installation • Insufficient involvement of the infrastructure administrators, in order to provide the sums necessary for maintenance/repair/renewal • Defective handling of the equipment and installation, as a consequence of human error or lack of trained personnel • Lack of correlation between operations and the real technological requirements of the installation • Use of untrained staff to provide security/protection, and inefficient fulfillment of the contract provisions by security companies | <ul style="list-style-type: none"> • Decrease of the installation feasibility, leading to the impossibility to reach the designed technical parameters • The continuous degradation of the equipment and installation, with impact on their functional security • Inducing technical malfunctions which cause sudden technological stops and failures in the process, with negative consequences to the efforts of maintaining a stable national/regional energetic system • Neglecting the role played by these critical elements to their attended economic objectives • Accidents ended in significant material damage and/or that of the environment • Enabling unauthorized physical intrusions, mainly for theft purposes |





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

Conclusion

From the point of view of the process and applicability, reaching the protection-related objectives of critical infrastructure has significant implications over the strengthening of both inter-state and institutional collaboration, and it also has powerful cross-border connotations, related to setting-up a unitary legislation framework, closely connected to the preservation of economic and security interests, and to the enforcement of consistent, integrated protection measures.

Therefore, starting from the global context of risks and the European authorities' interest towards the issue (according to their national need), it is highly necessary to adopt, at the level of each state, a complex measure framework, able to achieve, in the end, the alignment of the infrastructure systems to safe exploitation requirements.

Following this goal represents a high priority, although it implies consistent economic and financial efforts (subsequent to infrastructure identification, rehabilitation, modernization and protection), and a strengthened communication between the public and private sectors.

REFERENCES:

1. Marian, Rizea; Mariana, Marinică; Alexandru, Barbăsură; Lucian, Dumitrache; Cătălin, Ene, *Protecția infrastructurilor critice în spațiul euroatlantic*, Editura ANI, București, 2008;
2. McLaughlin, J.; Colinson, R.; Patten, D., *Director's briefing – SWOT analysis*, Business Hotline Publications Ltd., London, 2000.
3. Mintzberg, H.; Quinn, J. B., *The strategy proces. Concepts, contexts, cases*, Prentice Hall, New York, 1996.
4. Popescu, M. D., *Globalizarea și dezvoltarea trivalentă*, Editura Expert, București, 1999

Pipelines on Georgian Territory as a Part of the Euro-Atlantic Energy Infrastructure and the Issue of their Security

Ministry of Internal Affairs of Georgia

Pipelines located on Georgian territory (Baku-Tbilisi-Ceyhan and South Caspasia Pipeline) are part of the critical energy infrastructure of Western, Euro-Atlantic region. Traditional threats and possible risks regarding these pipelines are conditioned by the current processes occurring in South Caspasia. This situation generally influences the world energy market and geopolitical conditions of the Caucasus region, as well as internal and foreign affairs of Georgia, risks and dangers to its energy infrastructure.

The majority of countries in the Euro-Atlantic area depend on the energy resources, which are located in unstable regions; therefore, there are various factors, which can affect energy security:

1. Global energy market – According to data provided by International Energy Agency (IEA), demand for energy resources will increase by 50% in 2005-2030; therefore an energy deficit can be expected. This problem can also be prompted by constant price changes on energy resources and products, as well as the unstable situation of the energy market.
2. Danger of terrorist and sabotage acts against energy infrastructure. Such acts can cause serious delays in resource supplies to the international market thus increasing strain. For that reason, this type of attacks becomes more and more attractive to terrorists. Georgia has already suffered from such acts carried out on its soil:
 - ♦ The explosion of a radio transmission station serving the oil pipeline near the village of Chorchana in Georgia on November 17, 2004. The threat of armed groups entering from the territories beyond the control of government of Georgia and carrying out subversive acts against pipelines still exists;
 - ♦ In August 2008, during the armed conflict in Georgia, 27th kilometer of Baku-Supsa oil pipeline on Georgian territory was bombed on August 12, 2008; it also should be emphasized that this was a first precedent when operational-tactical rockets "Iskander" (NATO reporting name SS-26 Stone) had been used. The SS-26 type rocket exploded on the 26th kilometer of the oil pipeline. Fortunately it missed its target by 40 meters;

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

As a result of the deliberate attack against the pipeline, the functioning of the pipeline had been stopped for a certain period of time.

Security plan of energy infrastructure unit is traditionally created base^d on means and tactics worked out after risk identification, evaluation and analysis.

"Risk is generally defined as a factor of the likelihood of a threat to the infrastructure, of vulnerability of this infrastructure, and of the expected consequences or impact on the infrastructure, should that threat materialize." According to this statement, evaluating risk involves identification of a possible ^{un}it that can be attacked, how successful the attack can be, and what potential outcome it has. Therefore, security system consists of several elements: technological; constructional; electronic; and tactical.

Evaluating risk in a right, realistic way, gives us an opportunity to establish an adequate tactical element; using right, technical, constructional and electronic elements while creating a project and building a unit, can avoid successful attack and negative potential effect.

On January 1st, 2006 Strategic Pipeline Protection Department (SPPD) was established and since that, it has been operating as one of the departments of the Ministry of Internal Affairs (MIA) of Georgia.

Due to abovementioned threats, SPPD activities are based on the operational principles of counter-terrorist groups. The patrol groups carry out the following intelligence and security measures on the pipeline route and its adjacent territory:

- ◆ Patrolling territory of the pipelines 24 hours a day (foot and vehicle patrol);
- ◆ Controlling access roads to the pipelines;
- ◆ Checking and registering all persons and vehicles moving on territory of the pipelines;
- ◆ Covert observation of the territory adjacent to the pipelines;
- ◆ Rapid and effective reaction in case of emergency;
- ◆ Gathering intelligence information;

Operational activities according to the Georgian law on "Operational-Investigation Activities."

SPPD operates in accordance with the Georgian legislation, namely: while carrying out its duties and responsibilities the Department acts in compliance with the following legal rules:

- ◆ The Constitution of Georgia;
 - ◆ Georgian Law on Police;
 - ◆ Georgian Law on Operational-Investigation Activities;
 - ◆ The MIA regulations endorsed by the order N 614 issued by the Minister of Internal Affairs of Georgia on December 27;
 - ◆ The regulations of MIA Strategic Pipelines Protection Department endorsed by the order of the Minister of Internal Affairs of Georgia;
 - ◆ Various documents approved by the order of the Head of MIA Strategic Pipelines Protection Department;
- Host Government Agreement signed on November 18, 1999;

In the framework of the NATO program, since September 2006, International Course Eternity is being conducted annually in Ankara, Turkey. Representatives of the Ministries of Defense and Internal Affairs of Azerbaijan, Georgia and Turkey participate in the sessions every year.

Strategic Pipelines Protection Department maintains a close relationship with the Gendarmerie and the Defense Ministry of Turkey, as well as the State Protection Service, the Ministry of State Security and the Defense Ministry of Azerbaijan.

Tactics used by the SPPD can protect pipelines from "usual" terrorist attacks. But, existing threats creates a need for collective actions and cooperation in the activity of critical energy infrastructure security. The current situation prompts us to think about the creation of a collective energy infrastructure security system for Europe, also in the framework of the OSCE.

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

European Commission Initiative on Critical Energy Infrastructure Protection: an Overview

*Mr .José Antonio Hoyos Pérez, Policy Officer, Unit C1 on Energy Policy and Security of Supply,
Directorate-General Energy and Transport (DG TREN), European Commission*

In June 2004 the European Union launched a policy initiative relating to the protection of those infrastructures that are critical in ensuring values such as the well being of European citizens, the operations of the governing bodies or the functioning of the internal market.

In this connection, the European Commission adopted [1] on 20 October 2004 a Communication *on critical infrastructure protection in the fight against terrorism*, which put forward proposals for the prevention of, preparedness for and response to terrorist attacks on critical infrastructures.

Open dialogue with the general public has been at the centre of every development in this process, in order that the Commission could ensure that any legal or financial initiatives that might be taken were commensurate with the needs and expectations of the parties involved. To that end the Commission issued, on 17 November 2005, a Green Paper on a European programme for critical infrastructure protection.

This consultation process led to the Communication [2] from the Commission of 12 December 2006 on a *European Programme for Critical Infrastructure Protection* and consequently launched *the programme* (EPCIP), embracing a wide range of actions which have one ultimate objective, namely to ensure the integrity and functionality of critical infrastructures. On the same date, the Commission submitted to the Council a proposal for a *Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, which was adopted in December 2008 [3].

Although EPCIP was aimed at all sectors from the outset, by the time the Commission decided to step up into policy making certain sectors had been given priority. This was the case for the Energy and Transport, in respect of which the Commission had adopted a Communication on 2 February 2007 [4] entitled "*Protecting Europe's Critical Energy and Transport Infrastructure*".

EPCIP action lines

As formulated in 2006, EPCIP consists of several action lines, which can be summarized as follows:

- ◆ Information exchange: Critical Infrastructure Warning Information Network (CIWIN), the use of Critical Infrastructure Protection (CIP) expert groups at EU level, CIP information sharing processes and the identification and analysis of interdependencies;
- ◆ Protection of National Critical Infrastructures (NCIs). While acknowledging that the protection of NCIs is the responsibility of owners, operators and the Member States themselves, the Commission does provide support in this area at the request of Member States. Each Member State is encouraged to draw up a national protection programme;
- ◆ External dimension, implications for third countries. Collaboration with international organisations active in the area of CIP also falls under this heading;
- ◆ Accompanying financial measures and, in particular, the proposed EU programme on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013, which provides funding opportunities for CIP related measures that have the potential for EU transferability;
- ◆ A procedure for the identification and designation of European Critical Infrastructures (ECI), and a common approach to the assessment of the need to improve the protection of such infrastructures. This is to be implemented by way of the aforementioned Directive, which was formally adopted on 8 December 2008.



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

Legal framework

Directive 2008/114/EC of 8 December 2008 "on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection", is the cornerstone of the current EU policy on CIP. Its most relevant features are listed below.

Definition of "European Critical Infrastructure" or "ECI": *means critical infrastructure located in Member States, the disruption or destruction of which would have a significant impact on at least two Member States of the EU. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure;*

The scope of the Directive is limited to the Transport and Energy sectors. The following sub-sectors are mentioned:

Energy

1. Electricity: Infrastructures and facilities for generation and transmission of electricity in respect of supplying electricity
 2. Oil: Oil production, refining, treatment, storage and transmission by pipelines
 3. Gas: Gas production, refining, treatment, storage and transmission by pipelines. LNG terminals
- Nuclear cycle facilities are exempted from the scope.

Transport

4. Road transport
5. Rail transport
6. Air transport
7. Inland waterways transport
8. Ocean and short sea shipping and ports

The Directive explains the criteria for assessing the criticality of an infrastructure in terms of the severity of the impact that its disruption or destruction would cause. The following general or cross-cutting criteria are to be considered:

- ♦ Casualties criterion (assessed in terms of the potential number of fatalities or injuries);
- ♦ Economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects);
- ♦ Public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services).

The precise thresholds applicable to the cross-cutting criteria shall be determined on a case-by-case basis by the Member States concerned by a particular critical infrastructure.

The trans-national dimension of the impact, inherent in the definition of ECI, is highlighted through the so-called sectoral criteria, which identify those infrastructures with cross-border implications. The process of identifying and designating ECIs, as explained in the Directive, is to be undertaken by the Member States within the two-year period following the adoption of the Directive.

Following such designation, the implications in the actual ECI are immediate:

I) Establish an Operator Security Plan (OSP).

The OSP will have the following contents:

1. Identification of important assets;
2. A risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact shall be conducted;
3. Identification, selection and prioritization of counter-measures and procedures with a distinction between:
 - Permanent security measures, which identify indispensable security investments and means which are relevant to be employed at all times.



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

II) Establish a Security Liaison officer (SLO)

The SLO shall function as the point of contact for security related issues between the owner/operator of the ECI and the relevant Member State authority.

The Directive also includes some obligations towards the MS in which an ECI is designated. These refer to the conducting of threat assessments in relation to ECI sub-sectors where an ECI has been designated and where there is a need to report the results to the Commission. Based on these reports, the Commission and the Member States shall assess on a sectoral basis whether further protection measures at Community level should be considered for ECI.

Complementary activities

While the process of implementation of the Directive by the Member States is well underway, there are a number of complementary activities within the different remits of EPCIP:

Projects funded by the Programme on Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks;

- ◆ Studies funded by thematic Commission services on CIP issues;
- ◆ Seventh Framework Programme for Research (FP7) 2007-2013, under which the European Commission has made an amount of EUR 1.4 billion available specifically for Security Research [5] (CIP and more).

Amongst other topics, the priorities for projects addressed by these instruments include assessment of threats and vulnerabilities, dependencies, cyber-security, risk management, contingency planning, exchange of knowledge and training.

Summary

Protection of critical infrastructure is a relatively new area of work at the institutional level in the European Union, given that it has traditionally been the sole responsibility of the Member States.

The European Programme for Critical Infrastructure Protection represents the mainstay of this policy effort, while the first steps towards establishing a specific legal framework have already been taken through Directive 2008/114/EC.

The measures put forward by the European Commission and those that the Member States apply on their own initiative represent genuine progress in ensuring the highest level of protection of critical infrastructures in the territory of the European Union.

NOTES:

[1] COM(2004) 702 final, 20.10.2004

[2] COM(2006) 786 final, 12.12.2006

[3] Council Directive 2008/114/EC of 08.12.2008

[4] COM(2007) SEC(2006)1697, 02.02.2007

[5] Info on FPVII funding at http://cordis.europa.eu/fp7/security/home_en.html

DISCLAIMER: *The views expressed are purely those of the writer and may not in any circumstances be regarded as stating an official position of the European*

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

Protection of Critical Energy Infrastructure against Terrorist Attacks in the Commonwealth of Independent States (CIS)

Police Colonel-General Andrey Novikov, Head of the CIS Anti-Terrorist Center

Global terrorism is currently undergoing a process of modification. First and foremost, terrorist activities have evolved into a remodeled guerilla war, which led national law-enforcement agencies to switch from army tactics to localized counterterrorism operations. Secondly, modern terrorism has become a significant feature of today's global geo-economic map, notably with respect to energy interests - there is a sustained linkage between scaled up terrorist activities and regional distribution of hydrocarbon production and other energy generation.

According to the United Nations University 2020 Global Energy Scenarios, the world has entered the age of resource-driven conflicts; the ultimate goal of multiple terrorist and extremist groups is no longer to overthrow the central government and gain civil rights which were denied to their social, ethnic or religious group, but to establish and retain control over resources. It is also worth while mentioning that the authors of the 2007 World Economic Forum Report, that discussed global risks, argued that the terrorist activity region-wide and the hydrocarbons price growth were interrelated. A reputable analytical centre, Crisisgroup, offers in its Asia Report 133 (May 2007) similar explicit assessments of destabilization in Central Asia underpinned by the 'commodity curse'.

The state participants of the Commonwealth of Independent States (CIS) have now been pulled into the orbit of "energy terrorism". The CIS region's oil and gas pipelines clearly constitute a target for sabotage and terrorist attacks. A context analysis reveals that the geography of energy security and, accordingly, of terrorist threats encompasses the Caspian region and Central Asia. Energy transportation infrastructure, by and large, are potential targets for sabotage and terrorist attacks. For instance, the economic and political interests of Kazakhstan are affected by the security of oil supply. Just the 1,200 km long oil pipeline going from Kazakhstan to China has a throughput annual capacity of 10-20mln tons of oil, and Kazakhstan and China have joined their efforts to bring down terrorist risks. In the case of Turkmenistan, which is developing its network of gas pipelines, UN assessments found that some of the planned pipelines will run through areas that are not safe from the perspective of terrorist threats. It is obvious that such large-scale projects as export oil and gas pipelines, which essentially represent transport corridors, will draw the attention of not only economic competitors but also terrorists. Reducing terrorist risks at these facilities constitute an immediate objective of national intelligence services and law-enforcement agencies.

Undoubtedly, the antiterrorist security interests of the CIS state participants overlap with their economic interests. I believe that boosting business and restoring large-scale economic ties among the CIS state participants in the area of energy resources and energy supply, particularly with regard to Central Asia, forces us to employ a more pragmatic and legally considered approach to address terrorist threats, as part of a transport security strategy. From my professional experience, I think that one should take into account regional specifics when addressing the issues of critical infrastructure protection from sabotage and terrorist attacks.

According to the CIS Antiterrorist Centre, priority measures to prevent terrorist attacks against oil and gas pipelines should include the following actions:

- ◆ Dissemination of the common Transport Security Concept CIS-wide;
- ◆ Incorporation of the CIS Transport Security Model Law in national regulatory frameworks of the CIS state participants;
- ◆ Upgrade of the CIS Pipeline Transport Model Law to reflect urgent issues of countering terrorism at oil and gas pipelines and its subsequent integration in national legal frameworks of the CIS state participants;
- ◆ CIS-wide monitoring of oil and gas pipeline facilities (or sections) that face a potential hazard of being targets for sabotage and terrorist attacks (cutting-edge forecasting and risk assessment technologies are expected to be drawn upon in this regard);
- ◆ Continued joint antiterrorist exercises at hazardous industrial facilities and extension such practice at transport corridor facilities of the CIS state participants.



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

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.

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

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



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

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



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

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.

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

Global Platforms and Big Returns: Energy infrastructure targeting in the 21st Century

Ms. Jennifer Giroux, Center for Security Studies (CSS), Swiss Federal Institute of Technology (ETH) Zurich

From the 1970s to 1990s, terrorist attacks aimed at energy infrastructure (EI) in the oil and natural gas (ONG) occurred sporadically and had limited effects. For example, the bombing of Pacific Gas and Electric Company pipelines in California during the mid-1970s was sponsored by the New World Liberation Front and were largely inconsequential outside of the symbolic nature of the attacks. However, over the years EI targeting has proliferated; spanning the globe from Canada onwards through Mexico, Colombia, Nigeria, Algeria, Sudan, Yemen, Ethiopia, Pakistan, Iraq, Saudi Arabia, Russia, and Eurasia. A closer look exposes that attacks are not only occurring more frequently and causing broader effects, but are also no longer confined to acts of terrorism or other manifestations of political violence. Rather, violent non-state actors (VNSA) are increasingly motivated by a range of objectives where the distinction between political and criminal motivations is blurred. This development is fueled by the advent of globalization, where world markets and economies have become interdependent and major advances in information communication technology have accelerated the ability to produce, share, and exchange information cheaply over vast geographic distances. This has encouraged the spread of ideology, networks, and techniques and has empowered groups with new access, global visibility, and profitable, illicit ventures. Structurally, VNSA have replaced hierarchical structures with small, dispersed, and highly adaptable networks that are increasingly driven by the desire for business rather than state sovereignty.

Political Platforms

EI targeting is a form of economic targeting that allows VNSA to air political grievances in a graded, differentiated manner and to delegitimize the state by challenging its ability to protect a critical sector. Successful attacks can cause financial losses for the state, damage infrastructure and disrupt production, and can trigger ONG market reactions and public fear (especially among multinational and national oil companies). Attacks typically include the use of explosive devices and/or swarm-based attacks using light weapons. Furthermore, recent trends have highlighted the issue of infrastructure *criticality*. While a sector – such as the energy industry – may be considered critical, there is also a sub-layer of criticality that is linked to the importance of specific nodes within a sector's infrastructure chain whose disruption would have a sudden and serious impact throughout the system. Though this nexus is important, it may cause an exaggerated tendency to focus on low-probability, high-consequence attacks that take aim at critical components. Nevertheless, notable campaigns in Colombia, Iraq, and Nigeria have shown that frequent, small EI attacks can result in sustainable disruptions that aggregate into substantial failures and costs.

To illustrate, in the mid-1980s the Revolutionary Armed Forces of Colombia (FARC) and the National Liberation Army (ELN) began targeting the 100'000-bpd, 480-mile Cano Limon-Covenas pipeline in Colombia. In 1996, attacks began to increase – peaking in 2001 with a reported 170 perforations from small, frequent attacks that left the pipeline largely inoperable and cost the Colombian government an estimated US\$500 million in lost revenues. In 2003, insurgents in Iraq launched an EI targeting campaign that was part of a mission to create large-scale disruption. To date, over 500 EI attacks have been reported, many of which were small, repeated pipeline bombings while others targeted critical nodes and equipment that resulted in significant damages and lengthy repairs. Until 2008, insurgents were able to thwart the EI protection efforts of occupation forces, creating a constant state of disruption that dramatically reduced oil exports and revenues. This resulted in what analysts defined as a security premium – ranging from as low as US\$4 to as high as US\$25 per barrel – being placed on crude oil prices. Such market sensitivity fed into broader regional uncertainty. Other ONG producers, such as Saudi Arabia and Yemen, were not immune from attacks, either, as seen in the multiple attempts to destroy or damage domestic pipelines coupled with the growing calls within Salafi Jihadi groups to target oil pipelines, tankers, and other assets. Offshore assets in this region have also been vulnerable. The 2002 terrorist attack on the *Limburg*, a French oil tanker carrying approximately 400'000 barrels of oil from Iran to Malaysia, increased insurance premiums by 300 per cent for vessels docking at Yemeni ports. This led to a temporary decrease in shipping activity that cost Yemen nearly US\$4

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

million in losses per month. More recently, in July 2009, 25 individuals connected to al-Qaida were arrested by Egyptian security forces for conspiring to attack tankers passing through the Suez Canal. Subsequently, Kuwaiti officials reported the arrest of al-Qaida affiliated members who had allegedly used Google Earth to plan an attack on the Shuaiba oil refinery.

Likewise, militants in the Niger Delta, Nigeria's oil-producing region, have carried out continued attacks aimed at on- and offshore EI. After the formation of the Movement for the Emancipation for the Niger Delta in late 2005, more aggressive attacks were reported that cut daily oil production by 25 per cent (equivalent to between 500'000 and 700'000 barrels per day). During this escalation, many foreign ONG workers were evacuated, and some oil companies suspended operations in the region. In 2008, MEND claimed responsibility for the offshore attack on Shell's Bonga field, its main offshore facility, which pumps 225'000 barrels of oil per day when operating at full capacity. Demanding the removal of expatriate workers from Nigeria, the statement emphasized that the "location for today's attack was deliberately chosen to remove any notion that offshore oil exploration is far from our reach." Currently, EI attacks have declined due to a government-sponsored amnesty program for militants. However, a similar program was launched in 2005, and it was partly due to its failure that the new wave of attacks between 2006 and 2009 was set off.

Examples of smaller campaigns include the ongoing conflicts in India and Pakistan; in the former, the United Liberation Front of Asom has carried out numerous attacks aimed at the natural gas and crude oil sector, whereas in Pakistan, militants in Balochistan regularly bombed gas pipelines and electricity infrastructure. In 2007, the Popular Revolutionary Army (PRA) of Mexico claimed responsibility for a brief, yet intense bombing campaign aimed at natural gas pipelines, causing damage and a spike in gas prices. The PRA justified its actions as a "national campaign of harassment against the interests of the oligarchy and of this illegitimate government that has been put in motion." Nevertheless, these cases are examples of simple, relatively low-cost campaigns aimed at accessible targets that provide substantial leverage in a changing operational environment. Of more concern to the ONG industry is that from 2002/3 to 2008, EI attacks played a part in rising global crude oil prices that reached a historic high of US\$147 per barrel in July 2008.

Profitable Ventures

A more recent development is the emergence of EI attacks driven by criminal ambitions. In this case, perpetrators can reap financial gains from tapping and sabotaging pipelines to support oil theft operations to hijacking tankers carrying energy products and kidnapping ONG sector employees for considerable ransoms. For instance, piracy in the Gulf of Aden has risen dramatically; with over 150 reported attacks in 2008 and 2009, respectively. Tankers carrying energy products have accounted for around 25 per cent of attacks. The November 2008 hijacking of a Saudi supertanker traveling 450 miles off the coast of Somalia carrying 2 million barrels of oil worth more than US\$100 million captured international headlines and resulted in a brief spike in crude oil prices. One year later, undeterred by the presence of international naval and air forces, pirates managed to hijack another supertanker traveling nearly 1,000 miles offshore and carrying US\$20 million worth of crude oil. Armed with grenades and assault rifles, and endowed with technology, access, and the desire for sizable ransoms, the groups have developed a lucrative business in hijacking vessels that can bring anywhere from US\$500'000 to US\$3 million per ship. According to a Chatham House report, pirates garnered somewhere between US\$18 to US\$30 million in ransoms during 2008. Compounding the issue, the Somali pirates have also been linked to "Al-Shabab Al-Mujahideen", a Somali jihadi organization that provides a permissive environment for the pirates to carry out their operations in exchange for money and various services such as smuggling and other illicit activities. The Gulf of Guinea, in West Africa, has also been a zone of increasing criminal attacks aimed at energy tankers.

In addition to the politically motivated attacks aimed at the Iraqi energy sector, VNSA have also engaged in oil theft – via pipeline sabotage – that generates sizeable returns for the perpetrators while also costing the state a reported US\$12 billion in losses per year, according to government estimates. Naturally, this figure shifts in accordance with crude oil market prices. Correspondingly, oil theft in Nigeria has become a major business, with the United Nations Office for Drug and Crime reporting a loss of roughly 10 per cent of total production to illicit activities. In fact, though politically motivated attacks are currently down, oil theft attacks have risen. Whether by attaching unauthorized secondary pipelines to a company mainline or by



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

sabotaging a pipeline to create a spare pipeline, stolen oil is fed into the regional and international energy market, and profits go to an interconnected nexus of militants, complicit private companies, corrupt government officials, and criminals.

In another example of the criminal-political symbiosis, the Russian-Chechen conflict during the 1990s brought to light a massive oil theft operation where Chechen insurgents tapped the Baku-Grozny-Novorossiysk pipeline more than 100 times. Stolen oil was sent to secret refineries for processing into cheap gasoline, creating steady income in support of continued operations and for criminal gain. In 2009, reports surfaced that Mexican organized criminal groups had expanded their operations from the illicit drug to the illicit oil trade. They have also tapped oil pipelines and built tunnels and independent pipelines to support growing theft of oil that is sold on the domestic market as well as the US market.

A Dangerous Brew

Taken together, the cases discussed above provide a glimpse of a much broader phenomenon where the attacks of VNSA are having broader effects. Through their ability to disrupt supply and production capacity, influence crude oil pricing, garner broad media attention, and secure attractive ransom payments, VNSA targeting EI are a showcase example of the modern-day globalization paradigm, where events rarely occur in isolation, but rather ripple across the globe. Indeed, such trends bring to light the role that energy infrastructure security plays in present-day and future energy security concerns. The energy infrastructure in the last decade has undergone a great deal of volatility, complete with extreme swings in crude oil prices, growing global demand for ONG resources, resource nationalism, and increased reliance on ONG resources produced in, or transiting through, troubled on- and/or offshore pathways where EI targeting has flourished. As major ONG producers such as Venezuela, Iran, Saudi Arabia, Russia, and Nigeria – along with the many other smaller, yet significant suppliers – continue to grapple with instability, the issue of energy infrastructure security will become even more challenging, require greater resources, and ultimately, demand collective action to enhance understanding of EI targeting and address the considerable weaknesses that exist throughout the EI chain due to inconsistent security and protection standards.

NOTE: Ms. Jennifer Giroux is a researcher at the Center for Security Studies (CSS), ETH Zurich where she heads the targeting energy infrastructure (TEI) project.

Characteristics and Vulnerabilities of Critical Energy Infrastructure

Prof. Wolfgang Kröger, Swiss Federal Institute of Technology (ETH) of Zurich

Energy infrastructure aim at securing adequate, affordable supply of energy, thus comprising the whole supply chain - from producing to consuming areas including transport and transmission. Focusing on the electric power supply and the high voltage transmission grid, respectively, this should -inter alia- be capable of coping with "variations", absorbing impact/attack and getting back to initial conditions - and by this avoid major disruption of service.

The electric power grid, e.g. in continental Europe, is a large-scale, spatially distributed, synchronized system which is basically open, evolved unsystematically, has been subject to rapid developments (e.g. integration of intermittent energy sources such as wind and solar) and organizational changes (e.g. from monopoly to deregulated markets and unbundled structure).

Electricity is regarded as common good and the infrastructure behind fulfils all characteristics of complexity including non-linear, emergent behavior difficult to anticipate. It is subject to a multi-faceted set of technical and human failures, natural hazards and various threats including malicious acts. The ubiquitous use of modern information and communications technology (ICT) has enabled beneficial system integration but has also introduced new risks, e.g. of common cause failures and cyber attacks.

CTN Newsletter Special Bulletin

Protecting Critical Energy Infrastructure from Terrorist Attacks

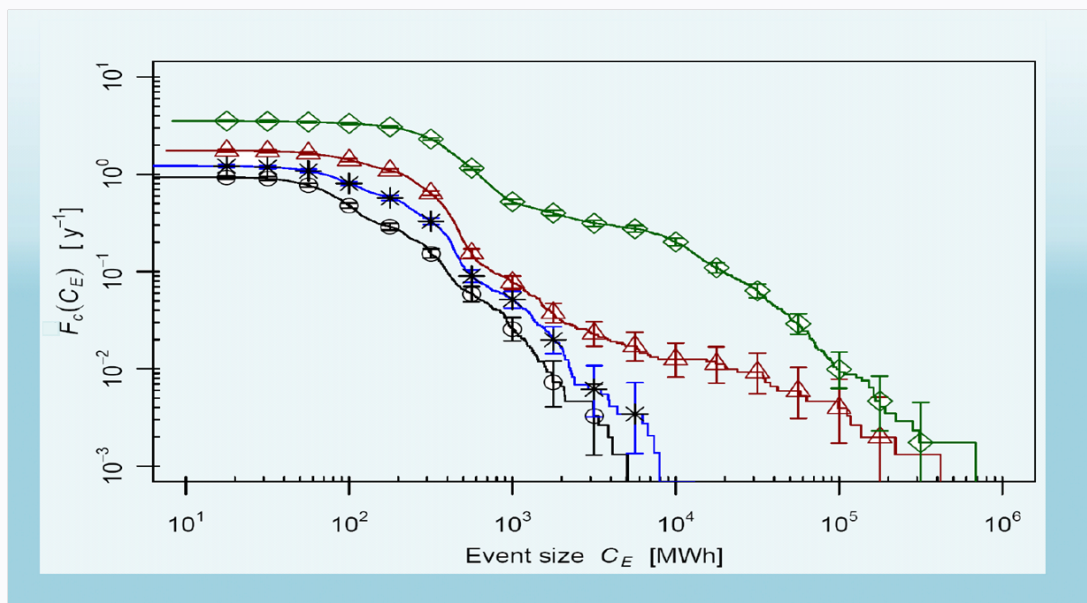
January 2010

"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

Recent major blackouts in industrialized countries have revealed certain vulnerabilities which followed common patterns such as:

- ◆ Operation of the systems beyond the original design parameters (market liberalization, integration of wind power, etc.)
- ◆ Malfunction of critical equipment and adverse behavior of protective devices; insufficient system automation in some cases
- ◆ Lack of situational awareness and short-term emergency preparedness
- ◆ Poor timely coordination in case of contingencies across control areas
- ◆ Inadequacy of N-1 security criterion, of its implementation/evaluation

Besides experience theoretical investigations are necessary to provide insights which can be used to identify, reduce and/or better manage vulnerabilities. These call for a combination of methods within an analytical framework and finally for a new systems approach [1].



Complementary cumulative blackout frequencies F_c versus event size C_E for different grid load levels: 100% (circles), 110% (stars), 120% (triangles) and 137% (diamonds)

A two layers, object-oriented modeling approach and Monte Carlo simulation turned out to be a promising tool to understand the response behavior of the electric power grids to "disturbances". The following figure shows the blackout frequency versus event size and confirms its sensitivity to increased grid loads. Other results illustrate the importance of adequate (i.e. within first 15 minutes) operator response times [2]. Structural investigations by applying graph theory help to understand the topology of a given system and its sensitivity to "attacks": Most of the electric power transmission systems tend to be rather of "random type" and by this being susceptible to random failures and robust against targeted attacks while "scale free systems" (with hubs) show the opposite but counteract cascading of failures (support "islanding").

Besides dependencies within the infrastructure interdependencies among infrastructures, either physical, geospatial, informational and logical, or coupling characteristics are of great practical relevance. Many critical infrastructures depend on available electricity; the electric power supply system is closely connected to information and communication systems for supervisory control and data acquisition (SCADA). The use of open access internet for data and command transfer varies from country to country which is essential for the degree of cyber security. The use of non- dedicated commercial soft and hardware may aggravate the risk of common cause failures.



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

It is known from dynamic analyses that loss of single elements including substations due to technical failure, targeted attack or even large-area events (e.g. earthquake) may lead to local/regional power losses but will not inevitably cascade to the national or trans-national (UCTE) level, a sign of high robustness.

One of the greatest challenges to combat vulnerability of critical energy infrastructure is a bundle of adequate awareness, willingness to take (and pay for) de-stressing actions and being prepared for disruption of main supply.

NOTE: This article is partially based on insights gained from a respective project commissioned by the Swiss Federal Office for Civil Protection.

REFERENCES:

- [1] W. Kröger, Critical Infrastructures at Risk: A Need for a New Conceptual Approach and Extended Analytical Tools, in Reliability Engineering & System Safety, Vol. 93, No. 12, 12/08
- [2] M. Schlöpfer, T. Kessler, W. Kröger, Reliability Analysis of Electric Power Systems Using an Object-oriented Hybrid Modeling Approach, in Proc. of the 16th Power Systems Computation Conference, Glasgow,

How the OSCE Can Really Contribute to Energy Security

Dr. Kevin Rosner, Senior Fellow, Institute for the Analysis of Global Security, Washington D.C.

Little is known and even less is understood about the role of the Organization for Security and Co-operation in Europe (OSCE) in the field of energy security. Probably best known for its election monitoring activities, the OSCE has a mandate to promote dialogue on energy security, including at the expert level, involving producing, transit and consuming countries. This mandate is both instructive and important. Among the organization's 56 member states, the OSCE is the only European multinational organization that includes both European and North American net energy producers and exporters such as Canada, Kazakhstan, Norway, the Russian Federation, and Turkmenistan along with some of the world's largest energy consuming states such as the United States, Russia, and Germany. It also includes among its members key transit states for European energy supply including Belarus, Ukraine, Poland, Azerbaijan, Georgia, and Turkey. The OSCE is therefore unique in that it provides a unique platform for dialogue certainly within a European context between energy producers, consumers and transit states that are counted as full-members of the organization.

Over recent months there has been accelerating activity on energy security within the OSCE. In July, 2009 the Slovak government sponsored an OSCE conference entitled "Strengthening Energy Security in the OSCE area." During deliberations the Slovak Minister of Foreign Affairs H.E. Miroslav Lajcak pointed out that, "The issue of energy security encompasses a broad array of technical, technological, economic and security aspects, which are covered by a political umbrella. The role of the OSCE is not to duplicate, but rather to complement the activities of international energy organizations. It takes a declaration of political will and a quest for consensus for the necessary changes in the area of external energy security to materialize. The OSCE can become a forum which spells out such political support to the steps taken by other initiatives and organizations. By the same token, the outcome of discussions within the OSCE can serve as an example of the existing common approaches and joint interests of OSCE members."

The challenge is for the OSCE to identify where it can add value to the activities of other organizations within the energy sphere and in doing so support the political dialogue within other organizations leading to better coordination between producers, consumers, and transit states on issues critical to energy supply security and the security of the infrastructure that delivers it.

Where Can the OSCE Add-Value?

One key area where the OSCE can add net value where other institutional initiatives have been lacking is in the area of tracking and detailing disruptions to critical energy infrastructure (CEI) in the OSCE's area of responsibility (AOR). The OSCE was mandated to engage on the issue of terrorist attacks against CEI at



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

an OSCE Conference in Madrid in November 2007. To have lasting and enduring value however the tracking of incidents which disrupt, debilitate or destruct critical energy infrastructure should be cover inter alia the following types of incidents:

- ♦ Attacks of a deliberate nature;
- ♦ Breakdowns of a technical nature or those caused by accidental human activity;
- ♦ The debilitation or destruction of critical infrastructure from natural causes;
- ♦ Disruptions of a commercial or political nature.

Recent History

Critical infrastructure protection is key to energy supply security and to global price stability. Energy prices in a time of scarcity [present lower energy prices due to the effects of the global recession are but a deviation from a future upturn in energy prices] are particularly vulnerable to even small attacks on global energy supply vis-a-vis the infrastructure that transits it. According to researchers at the Centre for Security Studies in Zurich, "The main factors driving high crude oil prices from the 2004 to mid-2008 period can largely be attributed to record demand from a global economic boom, price inelasticity, and tightened supply. However, political instability in producer regions further compounded this challenging Environment. Such turbulence resulted in what analysts defined as a security or "risk premium" – ranging from as low as US \$4 to as high as \$25 dollars per barrel – being placed on crude oil prices within this timeframe. In fact, during this period one can find a direct correlation between EI attacks and increasing global energy prices driven by traders and speculators who viewed EI targeting as a threat to supply and, perhaps, an exploitable opportunity to inflate prices." In short, the select targeting of CEI by terrorists, criminal gangs or groups vying to exercise leverage over national governments to achieve political, economic or social objectives through the targeting of energy infrastructure not only significantly contributed to pre-recessionary high energy prices (2004-2008) but price volatility (for both consumers as well as producers) in recent years.

OSCE Energy Security Policy Framework

OSCE involvement in energy security is based on the 2003 Maastricht Strategy Document agreed in December 2003 at the Maastricht Ministerial Council. This document states that a high level of energy security requires a predictable, reliable, economically acceptable, commercially sound and environmentally friendly energy supply. It also underlines the need to ensure the safety of energy routes.

In 2006, the Ministerial Council adopted in Brussels a more focused approach to the issue highlighting the importance of an energy dialogue it could facilitate with partner organizations such as the Energy Charter and the IEA. The Council pointed out that the OSCE concept of energy security goes beyond security of supply to include security of demand and security of transit, as well as energy efficiency. Under the 2006 Belgian Chairmanship, the Chairman-in-Office (CIO) also requested the OSCE Secretariat to conduct a technical fact-finding mission to gather and analyze information on energy security within the OSCE area, and to make suggestions on renewed international dialogue.

This mandate was reaffirmed in Athens on 2 December 2009 when it called for intensified dialogue and cooperation on energy security without however spelling out any specific provision(s) where pragmatic mechanisms should be developed that move the dialogue process beyond the talking phase. The development of a database to detail and track events which impact on critical energy infrastructure, within the OSCE's AOR and beyond, would ground OSCE aspirations in the form of a tangible deliverable

Why the OSCE?

Supplier, transit and net energy consuming countries all have clear national interest in the integrity of downstream cross-border energy flows. Tracking and detailing disruptions to European energy supply networks is key to safeguarding those interests. The development of a discrete and well defined analytical tool, under the auspices of the OSCE, to help better understand, measure and to prevent future events with a negative impact on CEI, would be to the benefit of all OSCE participating States.

Several other international structures have undertaken or are contemplating initiatives to prevent disruptions. In 2007 APEC states had considered a regionally based initiative to develop a rapid response network



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

for CEI protection. The North Atlantic Treaty Organization has also been mandated to protect critical infrastructure in its AOR. However, the perception of NATO's role in the protection of critical energy infrastructure differs from member state to member state and therefore has impeded consensus on the issue.

The OSCE, as noted, is an organization that features very extensive membership. Whereas some NATO member states may view the development and utility of such a database as primarily the responsibility of international oil companies (IOCs), this is not an issue for many OSCE members where energy supply is in the hands of state owned companies. This incidentally reflects the ownership pattern of the vast majority of oil and gas assets and their reserves around the world (i.e. publically owned versus privately owned and managed) and quid pro quo holds true for the ownership structure of the majority of oil and gas assets in the OSCE's AOR. The OSCE offers a different set of perspectives and priorities, allowing for a great degree of influence to be exercised within its comprehensive framework. Therefore the choice of the OSCE as a place to park the development of a CEIID.

Unlike the United Nations Economic Commission for Europe which also facilitates energy dialogue, the OSCE has a security mandate and as such can embrace more robust acts, such as the development of an actual mechanism in this case in the form of a CEIID, to prevent, mitigate or to help respond to challenges faced by energy producers, transit states, and end users where infrastructure is concerned. Several energy supplying states are OSCE members and as such may welcome a concrete and collective step forward to ensure their own endogenous energy resources and the infrastructure that transits them.

What is an Infrastructure Database and Why is it Important?

A critical energy infrastructure database is essentially a knowledge-based intellectual tool. It contains information culled from non-proprietary information resources that track, and detail as much as possible, global attacks carried out against critical energy assets are they up-mid-or downstream. This database will result in the ability to run time-series analyses on attacks against CEI on a global scale. In short, while one cannot predict a specific attack against a specific installation one can assess the probability of the type of attack based on analytical tools that are empirically based.

In culling and importing data into a database non-proprietary data is sufficient as it covers approximately %95 of all incidents carried out against this infrastructure. Some may argue that it is the remaining %5 of incidents that is most important. These incidents are typically detailed by national intelligence and defense organizations but the database's objective is trend analysis not specific incident analysis in the first instance. There is a good precedent for this.

While a CEIID could be newly constructed it could also be adapted from an existent software platform. The SIPRI (Stockholm International Peace Research Institute's) Arms Transfer Model database could be applied to tracking and detailing energy infrastructure incidents. SIPRI's database is well respected by military establishments around the world and its inputs are from non-proprietary sources as well.

Second, OSCE member states may object to culling and inputting data on incidents involving energy infrastructure on a global basis versus focusing exclusively on incidents which occur in the OSCE's AOR. This would be a mistake. Where terrorist activities occur against individuals or infrastructure the migratory nature of the modalities used to carry out attacks is well documented. For example, the use of IEDs in Iraq is now the overwhelming weapon of choice in Afghanistan. So too do the modalities of attacks against energy assets and infrastructure migrate from theatre to theatre or even within specific theatres. For states and energy companies it is as important to know what to protect against (tactically) as much it is to pinpoint what will be attacked (target fields). Together, a CEIID would assist in satisfying both of these objectives by detailing them on an empirical basis.

Third, the contentious issue of 'disruption' cannot be avoided. Downstream consuming states have an interest in availing themselves with as much data as possible when a disruption of a commercial nature cascades in significant energy supply failure. Commercial disruptions can have the same supply magnitude of impact as do technical failures, accidents or terrorist attacks. The database, as an empirically-based mechanism, does not foresee as a deliverable the identification of political determinants that lead to fault determination in the



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

case of a commercial dispute. Individual users can derive their own conclusions. The CEIID will simply record the energy supply failure impact on producing, transit, and consuming states in empirical terms.

Fourth, the issue of cyber-war and attacks carried out against IT infrastructures which control energy and power networks must be addressed and included in the incident database. Frank Umbach and his colleagues at the Center for European Security Strategies in Munich have extensively researched the cyber side of the energy security challenge. Frank writes, "In both Western governments and industries, security concerns about increasing cyber warfare attacks by individuals, crime organizations and governments regarding espionage or malicious software programs that damage and disrupt processes of critical infrastructure assets and processes have grown considerably in the last several last years. These cyber attacks have risen to an unprecedented level of sophistication. As a result, the vulnerabilities of digital systems and networks have grown exponentially. However, public awareness has not kept up with these new threats, and vulnerabilities in cyberspace, which have the potential to affect all sectors of private and public life, national and international businesses, and even the defense policies of states, multinational organizations like the EU" and by implication the OSCE. One can only conclude that a CEIID without the inclusion of cyber-related attack data would be an anathema to a full analysis of risks which challenge CEI within the framework of the current threat environment.

If energy security is a topic salient to the security concerns of states, commercial enterprise, and policy makers charged with assessing the cascading effects of critical energy and power failures on civil society then both enhanced dialogue and informed actions need to occur to address identified threats. Dialogue alone will not do the trick. Better data can inform all stakeholders on their individual role and contribution to enhancing this security environment for the collective benefit of all concerned. The OSCE Secretariat as mandated may want to take this recommendation under consideration.

NOTE: Dr Kevin Rosner is a Senior Fellow with the Institute for the Analysis of Global Security in Washington D.C. and is the Managing Editor of the on-line Journal of Energy Security

Critical Energy Infrastructure Protection in the Electricity and Gas Industries: Coping with Cyber Threats to Energy Control Centres

*Dr. Frank Umbach, Senior Associate for International Energy Security
Centre for European Security Strategies (CESS) Munich-Berlin*

The 21st Century Threat Environment for Companies and Governments

Although the worldwide energy industry and many governments have extensive experience with ensuring operational safety, managing natural catastrophes and prevention of damaging and disrupting energy flows, the increasing sophistication of global terrorism and the growing cyber warfare capabilities of private hackers, organized crime and terrorist groups represent new challenges of a rapidly changing global security environment. While the traditional security measures of "guns, gates and guard" are still needed, they are insufficient to cope with the new risks and threats stemming from a new and rapidly changing security environment.

During the last years, the vulnerabilities of digital systems and networks have grown exponentially, while the public awareness has not kept up with those new threats and vulnerabilities in cyberspace. But these threats have the potential to affect all sectors of private and public life, national and international businesses and even security policies of national states or multinational organizations like the OSCE. In the age-old struggle between attacker and defender, the attacker more than ever appear to have the advantages by being better armed, freely choosing the intensity of the attack as well as the target and being no longer constraint by any geographical distances and frontiers. Those threats are challenging traditional assumptions and thinking of national as well as collective security. The emergence of botnets in particular - by implementing dormant virus, unnoticed by Internet users, which the attacker can activate at any time (trojans) and at any place in the world - allow criminal or terrorist attackers to launch massive hostile operations for data espionage, falsifying,



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

destroying or altering confidential data with extraordinary harmful effects in the industry as well as critical national infrastructures by the border between cyber crime, cyber terrorism, and private cyber attacks, new “unholy alliances” of crime syndicates, terrorists or nationalist movements and individuals have increased the threat of a “digital Pearl Harbour” by conducting a new form of “asymmetric warfare” in the 21st century.

The EU Efforts since 2004

Since 2001 the EU has increasingly recognized the need for protection of critical infrastructure as an important and rising national as well as international security risk that needs to be addressed by its member states and collectively within the EU. But the progress has been hindered by the fact that the single member states have traditionally developed their own individual approaches, institutions and programmes to cope with these new security challenge to protect critical infrastructures, including critical information infrastructure (CII), despite the perceived common risks, threat, vulnerabilities and strategies for securing critical (information) infrastructure. Furthermore, the EU has only limited early warning and incident response capabilities – even on a national base of its member states. Equally European-wide governance and public-private partnerships (PPPs) are lacking.

Despite these shortcomings, a first step to address those common risks and vulnerabilities as well as to cope with the cross-border effects of damaged infrastructure or its disrupted processes has been made by establishing the “European Network and Information Security Agency (ENISA)” in 2004 to enhance European coordination on information security. A broader initiative has been made by the Commission of the European Communities at the end of 2005 by adopting a “Green Paper on a European Program for Critical Infrastructure Protection”. In December 2006, the European Council adopted a “European Program for Critical Infrastructure Protection (EPCIP)” that has defined principles, processes and instruments for its implementation. The EPCIP has been the nucleus for the EPCIP Action Plan, the Critical Infrastructure Warning Information Network (CIWIN), the use of CIP expert groups at EU level, CIP information sharing processes, a procedure for a common approach to the assessments of the needs to improve the protection of such infrastructures and the identification and analysis of interdependencies between very different critical infrastructures.

Against this background, the Commission has tendered a series of studies since the second half of 2007 under the EU’s 7th Framework Program for the Commission’s General Directorate for Justice, Liberty and Security (JLS) that includes studies on specific sectoral infrastructures and assets. The Octavio-Project, in which CESS was involved, had three major objectives: (1) to focus on structures, functionalities and security of critical assets (i.e. Control Centers) in electricity and gas supply systems; (2) to provide an accurate (risk) assessment regarding energy sector control centers in the natural gas and electricity sectors and their cyber structure requirements; and (3) to develop a comprehensive approach to improve the security of energy control centers based on establishing criteria and methodologies to assess, audit and mitigate risks for the EU’s electricity and natural gas control centers and their interdependent ICT infrastructures.

In regard to critical energy infrastructure, the EU has recognized two major challenges:

The spread of ICT highlights numerous new security implications of our dependencies on them in all areas of our daily life. Market liberalization and privatization of state-owned infrastructure operators as well as new regulations have made the private industry and government agencies increasingly dependent on external providers of goods and services, including commercial off the shelf (COTS)-products. At the same time, almost every single service depends directly or indirectly on the secure supply of electricity. The physical, virtual or logical networks have grown in size and complexity. As the result of those growing interdependencies between various critical infrastructures, those dependencies and impacts of supply shortages and disruptions are often not apparent until a crisis occurs and the connection breaks down. Even smaller outages, failures and disruptions can have dramatic consequences and non-anticipated cascading effects in ever more complex system between various critical infrastructures and beyond national borders (“vulnerability paradox”).

In previous times, the energy supply system was decentralized with a power plant for each region and a local distribution network, which connected the producer with the consumers. If the power plant failed, the whole region was without energy. When the regional networks were interconnected by transmission networks, security of supply was enhanced by the possibility to exchange energy between the regional networks.



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

It also saved financial resources particularly on the side of producers. Today those regional networks have been expanded across national states, connecting individual EU member states with the perspective of creating a common, liberalized energy market in the entire EU. Whereas this is true for both electricity and gas supplies, the European pipeline-based gas supply system, perceived as the "Achilles heel" of the EU's energy supply security, is covering a much wider geographical area by long distance gas pipelines, connecting producer, transit and consumer countries.

The Functionalities of Energy Control Centers and its Vulnerabilities

The operational processes of the electricity and natural gas supply chains as well as its security and control are highly dependent on the ICT infrastructure. Energy Control Centers control the operation of power plants as well as of networks. The operation of huge border crossing electricity and gas networks require a network management and a control center hierarchy (Main, Regional and District Control Centers) to ensure security of electricity and gas supplies. The efficiency of control centers by applying methods of data handling and processing is closely linked with the development and application of ICT. Their task is:

Measurement and information gathering by sensors – incl. satellite based surveillance and control of pipeline systems, power plants, pump stations, storage sites and networks;

Acquisition: transmission of necessary information from the network to the Control Center transmission of commands from Command Centers to "operational" components like substations;

Processing, display and archiving of information from the network, generation of control information.

In contrast to the former auxiliary function for the control of operations of plants and networks, meanwhile it has been transferred into a centralized complex instrument with the central function in energy supply. Without this central function, any operation within the energy and gas supply chains ranging from production to distribution and supply would be impossible. The efficiency and reliability of those Control Centers, in particular the System or Central Command and Network Control Centers, is essential and the biggest threat in case of physical and electronic attacks. They could have extensive consequences on other critical infrastructures and could also lead to heavy losses of companies at the stock exchange and ten thousands of consumers.

Acquisition and processing tasks are elements of SCADA (Supervisory Control and Data Acquisition) System. With SCADA, control centers are able to identify and repair interferences, to take the necessary measures of repair centrally and to acquire data relevant for planning and further action. Originally, each power plant had its own Control Center linked with others a part of a hierarchy of networks. The development of ICT enhanced the capabilities to combine not only the different tasks of command structure for the hierarchy of networks, but also for different media, such as electricity, gas, water or district heating in a Central Command Center. The latter have extended their capabilities by using Geographical Information Systems (GIS) to provide geo-referencing information of facilities, networks, vehicles and geographical or political details. Modern SCADA systems use standard interfaces and standard components (of computers operating under UNIX or Windows). It has improved system interconnection and efficiency, but has also increased significantly the system vulnerability to outside electronic attacks.

Perspectives

In addition to the new forms of terrorist attacks, private hackers and (transnational) criminal organizations, the vulnerability of the different sectoral infrastructures have also increased because they are much more linked with each other in some way due to the rapid spread of information technologies. ICT infrastructures in the energy, transport, banking and financing sectors have become the nervous system of our modern information societies. Disruptions of ICT can multiply in other locations, branches or sectors, with an impact that extends far beyond the original area of damage as well as across the state-border of an EU-member state. Their security and resilience cannot be ensured and enhanced by purely national and uncoordinated strategies. Furthermore, market forces do not provide sufficient incentives to private operators for investing to protect critical infrastructures. The fundamental and still underestimated problem is that the low level of protection in some member states can increase the vulnerability of others, whereas, in parallel, the insufficient systematic interstate cooperation in Europe substantially reduces the effectiveness of preventive and timely countermeasures. While the Octavio project had primarily to identify the physical and cyber threats to and vulnerabilities of the



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

energy control centers as well as other infrastructures in the electricity and gas supply chains, the presently conducted INSPIRE-project of the EU goes a step further: it aims to mitigate the threats and to improve robustness as well as resiliency of energy control centers and other Large Complex Critical Infrastructures (LCCI) by increasing safety and security of the LCCI's control systems.

When the financial and personnel resources available to operators protect their infrastructure systems are limited, both the energy industry and their governments need to use all available resources efficiently by assessing risks and setting priorities for an adequate risk management. While it is impossible to protect a utility 100% from a physical or cyber attack on a utility's facilities and infrastructure, those threats can be minimized without compromising their productivity and day-to-day operations. A professional security and risk assessment needs in a systemic perspective to address physical and cyber security, SCADA and distributed control systems (DCS), communications security, grid security, distribution security, generation security, and biological/chemical issues in new holistically integrated security concepts.

International Energy Infrastructure Security

Dr. Bruce Averill, Founder and Senior Partner of Strategic Energy Security Solutions LLC

One of the primary responsibilities of senior managers of private energy companies is ensuring continuity of production. In many countries, one of the most significant risks is that of a terrorist attack, which could severely decrease or even interrupt production for prolonged periods of time. Recent experience in countries such as Saudi Arabia, Yemen, and the Gulf of Guinea has demonstrated that energy facilities remain attractive targets for terrorists. Unfortunately, these facilities are often highly vulnerable to terrorist attack due to a disconnect between the industrial security function provided by the private sector and the external security function provided by the governments of the host countries. Because a significant and prolonged interruption of production and export income due to a terrorist attack is clearly not in the best interest of neither the energy company nor the host nation, the situation described above is far from optimal.

What is the real risk of supply interruption due to a terrorist attack?

There is no generally agreed upon answer to this question. Rather, the answer depends upon the perspective of the respondent, as well as the geographic region in which a particular facility is located. At one end of the spectrum is the view represented in Ernst & Young's 2009 report on strategic business risks for the oil and gas industry, in which "Supply Shock" ranks number nine on their list of the top ten risks. The events postulated as potential triggers for a supply shock, however, were primarily geopolitical, including regional insecurity and instability and/or deliberate disruptions by energy exporters for political purposes. But in contrast to the 2008 report, the possibility of attacks on pipelines, offshore installations, and tankers were specifically mentioned, and it was noted that "oil installations [are] an attractive target for the disaffected." In the 2008 report, only one from the panel of experts assembled by Ernst & Young suggested that it might be wise to consider the risk of terrorist attacks on oil facilities in the Middle East as part of "a move from symbolic targets to economic targets." Although there is a slightly increased recognition of the risks of terrorist attacks, the clear message is that corporate management need not spend a great deal of time and resources to address this risk.

In contrast to this rather sanguine view, most knowledgeable observers believe that the risk of a successful terrorist attack is high, especially for energy facilities located in certain geographic regions. This view is supported by the trend in postings on jihadi websites and by recent events.

Over the past dozen years, on-line postings and statements have shown a remarkable turnaround in the jihadi view of energy facilities as suitable targets. Thus, in August 1996 Osama bin Laden released a statement that clearly indicated that energy facilities in the Islamic world were not a target: "I would like here to alert my brothers, the Mujahideen, the sons of the nation, to protect this (oil) wealth and not to include it in the battle as it is a great Islamic wealth and a large economical power essential for the soon to be established Islamic state." Targeting foreign personnel ("crusaders" and "infidels") was permissible, but not the energy infrastructure itself. In contrast, in December 2006 Osama bin Laden called on his followers to focus on

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

stopping oil production by any means possible: "One of the main causes for our enemies' gaining hegemony over our country is their stealing our oil; therefore, you should make every effort in your power to stop the greatest theft in history of the natural resources of both present and future generations...Focus your operations on it [oil production], especially in Iraq and the Gulf area, since this [lack of oil] will cause them to die off."

This escalation of rhetoric regarding the need to attack energy facilities is reflected in fatwas and other writings from a variety of sources. For example, in June 2004 Shaykh Abdullah bin Nasser al-Rashid issued a fatwa entitled "The Laws of Targeting Petroleum-Related Interests and a Review of the Laws Pertaining to the Economic Jihad". Unfortunately, this went unnoticed in the West until al-Qaeda drew attention to it as justification for the abortive attack on Abqaiq in February 2006. Also published in 2006 was a "Decree on Targeting Oil Installations", which gave comprehensive religious and political arguments in favor of attacks on energy facilities. In 2007, an article entitled "Bin Laden and the Oil Weapon" was published, calling for attacks worldwide on oil facilities supplying the U.S. Finally, just last year the "Decree on Targeting Oil Installations" was reposted on several jihadi websites, and a new article, "Al-Qaeda and the Battle for Oil", was posted, claiming that al-Qaeda must use energy attacks to cause an increase in oil prices that would damage the U.S. economy.

Over the same period of time, a string of terrorist attacks indicates that the escalating rhetoric has not been falling on deaf ears. Attacks on energy facilities that actually reached the execution phase (albeit with varying degrees of success) include: the use of an explosive-laden dinghy to attack the French tanker, M/V Limburg, off the coast of Yemen in October 2002, which did significant damage to vessel; the attack on the Oasis Compound in Al-Khobar, Saudi Arabia, in May 2004, in which 19 foreign employees of oil companies were killed; the narrowly averted double vehicle bomb attack on the world's largest petroleum facility, Abqaiq, in Saudi Arabia, in February 2006; and the unsuccessful attack on a Yemeni oil refinery in September 2006. In addition, a number of other potential attacks were uncovered and disrupted in the planning stage, including: a plot to attack the Australian electrical grid in April 2004; surveillance of oil storage facilities in Australia and the U.S. in 2005 and 2006, respectively; and a threat to Ras Tanura in Saudi Arabia and Bahraini refineries in October 2006. It seems likely that a number of other such threats have been disrupted but not publicized, for obvious reasons.

Of course, energy infrastructure constitutes a potentially attractive target for a variety of terrorist groups in addition to those motivated by jihadist rhetoric. As has been pointed out by others, the relatively low cost of such an attack in both materiel and personnel presents an opportunity for a small group to exert an impact out of all proportion to the size of their organization. For example, "One small attack on an oil pipeline in southeast Iraq, conducted for an estimated \$2,000, cost the Iraqi government more than \$500 million in lost oil revenues. That is a return on investment of 25,000,000%." In addition, the extended nature of energy infrastructure such as pipelines makes them virtually impossible to defend effectively, a point neatly summarized by the term "the ten-thousand mile target". Illustrative examples are numerous; they include: the ongoing attacks by the Movement for the Emancipation of the Niger Delta (MEND) on oil infrastructure and personnel in the Gulf of Guinea; hundreds of attacks by the National Liberation Army (ELN) on the Caño Limón-Coveñas pipeline in Colombia over the last two decades; and the coordinated attacks on Mexican pipelines, supposedly by the Popular Liberation Army (EPR) in 2007. In addition, the Kurdistan Workers Party (PKK) claimed responsibility for the explosion and resulting fire on the Turkish portion of the BTC pipeline in November 2008, although Turkish officials maintained that the incident was due to a mechanical malfunction.

Because the nature of terrorist organizations, as well as their motivations, resources, and capabilities, varies widely from one geographic region to another, it is not possible to make general statements about the risks of a terrorist attack on a generic energy facility. Instead, it is necessary to focus on the specific risks to energy infrastructure in a given region, such as Canada, Eurasia, Indonesia, Latin America, and North Africa. Of these, only the Canadian analysis reflected the sentiment of the Ernst & Young reports, concluding that the risks of a successful terrorist attack on Canadian energy infrastructure were rather low.

The U.S. government apparently agrees with the conclusion that major energy facilities in certain regions face a substantial risk of damage due to terrorist attack. In 2006, it approved a Global Critical Energy Infrastructure Protection (GCEIP) Strategy. The stated objective of the GCEIP Strategy was to work with the

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

governments of selected countries to improve security at energy facilities that were both critical to the global energy market and likely targets for terrorist attack. Although details of the program and the identities of the partner nations remain classified, it is clear that protecting major energy facilities overseas was a high priority for the Bush administration.

The gap between the private industrial security function and the public external security function

While major energy facilities generally have very effective industrial security programs, in most cases private sector security forces are unlikely to be able to repel a determined attack by well-armed terrorists. Indeed, in most countries private security forces are generally not allowed to carry weapons (other than sidearms, and then only in a few cases), and some companies have firm "no weapons" policies at all their locations. In reality, the private security forces focus on industrial safety, accident prevention and mitigation, ensuring that only authorized personnel have access to critical facilities, and preventing pilferage or theft of products. Consequently, it is not surprising that in most of the major energy companies the heads of security report to the board through the Health, Safety, and Environment (HSE) line, with several levels of management between them and the board. Under these circumstances, security is only one of a number of competing priorities for a senior manager.

As a result, in almost all countries real security against terrorist threats is provided by armed personnel belonging to a host government ministry or agency, such as the Ministry of the Interior. The gates. These forces are responsible for security outside the facility perimeter and usually control both vehicle and personnel access at the gates. Typically, they also work closely with the nation's intelligence professionals to identify and defeat threats before they can approach the perimeter. In principle, the government forces at the perimeter should have the personnel, weaponry, and training to repel an attack by a determined and well-armed group of terrorists using car or truck bombs, automatic weapons, and high explosives. In practice, however, experience to date indicates that the government forces are seldom up to the task, even in countries that have taken the risk of terrorist attacks very seriously.

Armed government forces may not provide adequate security for several reasons. First, most governments of hydrocarbon-rich countries have not yet designated a single ministry or office that has both the responsibility for security at energy facilities and the authority needed to implement effective security measures. Second, "stove-piping" and competition between ministries inhibits cooperation and information sharing between all of the parties involved in security issues. Third, the authority to make decisions regarding a response to an attack is usually restricted to relatively high-ranking officers rather than delegated to the junior or non-commissioned officers who would bear the brunt of an attack. As a result, no one can or will make a decision in real time to counter an attack, effectively paralyzing the defense. Fourth and finally, prevailing attitudes that "it can't happen here", or that "if it does, it is God's will and nothing can be done" (in some Muslim countries), need to be overcome.

Consequently, the senior managers of energy companies that own or operate overseas facilities with a significant risk of a terrorist attack are faced with a dilemma: they are unable to take effective action inside the facility perimeter, yet they are aware that the forces outside the perimeter are unlikely to be effective. Until these circumstances can be changed, management must rely upon good fortune. Should a successful terrorist attack occur, however, the managers could be hard-pressed to demonstrate to their board and shareholders that they exhibited due diligence and adequately discharged their fiduciary responsibility.

If it is generally recognized that the security status at many energy facilities is unsatisfactory, why does the current unsatisfactory state of affairs persist? What is preventing or delaying significant improvements in security? In most cases, a number of factors can be identified. First, in many countries the private sector operator is a partner with the national oil company, and the relationship between the two is often delicate and complex. Suggesting that the host government is not able to provide the level of security that it claims could be perceived as undiplomatic and possibly causing more problems than it solves. Second, the private sector security chiefs usually feel that they are "doing everything they can," and that they are severely limited by budgetary constraints. As indicated above, in many companies security competes with safety and environmental issues for a single pool of resources, and an HSE director may well give a higher priority



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

to other concerns. Third, security professionals tend to rely upon familiar approaches and tried and true solutions, and they are often intrinsically distrustful of the new and the unfamiliar. This can lead to the unfortunate situation of "doing the same thing, over and over again, but expecting different results" (Albert Einstein's pithy definition of insanity).

Using public-private partnerships to bridge the gap

The U.S. GCEIP Strategy offers a potential model for developing public-private partnerships to close the gap between the private and public security forces and improve energy facility security in many countries. This strategy was based on government-to-government outreach efforts that encouraged nations that host critical energy facilities to improve both government- and operator-provided security, with USG technical advice and assistance to ensure that expenditures actually result in improved security. The basic argument was that it was neither in the best interests of the host country nor for the US that a major energy facility be taken off-line for a prolonged period of time, and that investing a small portion of the host government's fossil fuel revenues in improved security constituted an effective insurance policy to minimize the risk of losing that revenue. This approach proved to be exceptionally effective, and virtually all countries that were approached agreed to make major expenditures to improve security at energy facilities, either in cooperation with the USG or a private sector security firm. Typically, the host government mandated that the facility operator be responsible for physical improvements to perimeter security and to security within the perimeter, while the host government was responsible for security outside the perimeter, including the armed forces that provide perimeter protection.

The model discussed above for the division of responsibility between facility operators and host government seems appropriate for many other countries, with minor modifications, depending on the magnitude of the revenue revenues from hydrocarbon exports. In the case of major exporters like Qatar, Angola, and Kazakhstan, current or projected revenues from LNG and petroleum exports are such that there is no question that these countries can afford to improve perimeter security at major energy sites which in many cases are currently and essentially unprotected.

In contrast, a country such as Oman, with net oil exports of about 700,000 b/d, is not generally regarded as a major exporter. Although Oman's income from hydrocarbon exports is substantially lower than those of the countries mentioned above, they nonetheless account for 75% of the Sultanate's revenues. This situation constitutes a two-edged sword: on the one hand, the government of Oman has less disposable income to invest in security improvements, but on the other hand it is especially vulnerable to the loss of that income, which would be considerable. For example, at current prices, disruption of the approximately 550,000 b/d that Shell produces in Oman would cost Oman and Shell about \$24 million and \$14 million per day, respectively, in addition to the costs of reconstruction, environmental remediation, and (for Shell) potential stock losses. Although Shell would continue to make money due to its operations elsewhere, Oman would not, and a prolonged disruption of exports could prove catastrophic for the Sultanate. In a case like Oman, one cannot assume that the host nation would automatically bear all the costs of improved security at and outside the facility perimeter. However, given Oman's relatively open borders and society, and its proximity to potential sources of terrorists such as Yemen, Saudi Arabia, and Iran, a very strong argument could be made for developing a public-private partnership to improve energy facility security in cooperation with operators such as Shell. The details of cost sharing would have to be negotiated.

The key requirement for this approach is the presence of a functional central government that is able to enter into such an arrangement and keep any commitments it makes with regard to energy infrastructure security improvements. Unfortunately, not all energy producers meet this criterion. One such example that comes to mind is the situation in Nigeria, where the oil-producing regions are largely ungoverned and where the rule of law is questionable. If the current efforts of the Nigerian government to bring many of the MEND rebels into the fold via an amnesty program are successful, and if it is also able to get the culture of corruption under control and bring effective government to the region, then one might well be able to extend the public-private partnership concept to attack even this previously intractable problem.

NOTE: Dr. Bruce Averill is former Senior Coordinator for Critical Energy Infrastructure Protection Policy at the U.S. Department of State. This article was first published in the *Journal of Energy Security* in October 2009



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

Paving the Way to a Secure Smart Grid

Mr. David Baker, Director of Services at IOActive

With the implementation of the Smart Grid, energy distribution is becoming rapidly more advanced. The Smart Grid is designed to save money and resources while providing better accounting of energy usage; however, like any new technology, it is critical to examine the implications of the Smart Grid and all of its components. If history has taught us anything, it's that early-to-market technologies are likely to exhibit security vulnerabilities, making them a prime target for attack.

The Smart Grid connects local power distribution with the national infrastructure; its delivery network is characterized by a two-way flow of electricity and information, capable of monitoring everything from power plants to customers' individual appliances. The grid leverages the benefits of distributed computing and fault-tolerant communications to deliver real-time information and enable the near-instantaneous balance of supply and demand at the device level.

An essential component of the Smart Grid is the Advanced Metering Infrastructure (AMI), or smart meter network, which acts as both a distribution and endpoint for communication and sensor nodes. Smart meters include a wireless network interface and mesh networking software, which allow utility companies to automatically update the software running the devices and allows them to shut off a customer's electricity over the network, known in the industry as *remote disconnect*.

Smart meters promise to deliver utilities and consumers better control over electricity distribution, generation, and usage in addition to greater savings and more reliable, efficient services. This sounds great in theory, but how reliable are these meters?

Smart meters are fundamentally miniature computers; however, many lack the protection and security features that have become standard on modern computers and networks. Like computers and software developed in earlier years, these devices were not designed with security in mind and IOActive's research on a series of smart meter devices confirmed this fact.

In addition to being vulnerable to common attack vectors, IOActive researchers achieved proof-of-concept, *worm-able* code execution on standard smart meters. Since the smart meter's radio communication chipset is publicly sourced and the communication protocols lacked authentication and authorization, IOActive researchers were able to leverage these weaknesses, among others, to produce a proof-of-concept worm. If an attacker were to install a malicious program on one meter, the internal firmware could be made to issue commands that would flash adjacent meters until all devices within an area were infected with the malicious firmware.

Theoretically, once the worm spreads to meters, the attacker gains several abilities including:

- ◆ Connecting and disconnecting customers at predetermined times.
- ◆ Changing metering data and calibration constants.
- ◆ Changing the meter's communication frequency.
- ◆ Rendering the meter non-functional.

If a truly malicious worm were to infect meters in a particular area, there would be a best- and a worst-case scenario. Under the best-case scenario, the utility would send a firmware update across the standard wireless network to all the affected meters, overwrite the worm, and return the meters to normal operation.

In a worst-case scenario, the normal wireless update mechanisms would no longer be intact or the calibration of the meters would have been altered. If meters supported remote disconnect capability they could be instructed to simultaneously or individually disconnect service to customers' homes. To return power to effected homes, the utility would need to take time to understand the vulnerability and develop a patch, and then physically repair or replace each meter. Restoring power to homes would likely be an expensive and long process—detrimental to the utility and frustrating to the consumers.



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

On a large scale, terrorists could exploit weaknesses in the Smart Grid to shut off power to large areas in demand for ransom from the utility or even to make a political statement. On a smaller scale, petty criminals could leverage these vulnerabilities to sever power to individual homes and break into the residence, or simply to be a nuisance.

Despite these vulnerabilities, the reality is that the Advanced Metering Infrastructure is here to stay. So, how do we move past these inherent security vulnerabilities to realize the benefits of *smart* power distribution?

Utilities play a critical role in securing the Smart Grid; they have the power to drive competition in the smart meter market, ensuring that only well-made and secure meters are deployed. By continuing to test the security, quality, and reliability of smart meter devices for the duration of the product lifecycle, utilities can help ensure that meter vendors continually maintain and improve the security of their product.

To help vendors develop more secure meters that are better able to withstand attacks, IOActive encourages vendors to implement a formal Security Development Lifecycle (SDL). The SDL takes a proactive stance to security by employing security and privacy measures during each stage of development, and conducting a final review before software is released.

By implementing and adhering to a SDL, meter vendors will be better equipped to resolve many of the design flaws present in smart meter devices and employ the most basic rule of security: layer your defenses. Multiple layers of defense provide the best security, using the theory that if one mechanism fails you have several others in place to help prevent a breach. It is especially important for meters to have layered defenses because they reside on the outside of homes with very little physical protection. Without a layered defense, someone with a basic understanding of electronics and enough curiosity could easily steal a meter, reverse engineer it, and uncover exploitable vulnerabilities.

Strong encryption, authentication, and authorization are additional security basics that seem to be poorly implemented in many smart meter devices. IOActive found that many devices do not use encryption or implement any authentication before carrying out sensitive functions like executing software updates or performing disconnect operations. For meters that had encryption algorithms in place, IOActive researchers found that functionality was unmanageable; the keys were often exposed, extremely weak, or could be recovered through simple hardware hacking techniques.

The Smart Grid brings the concept of the Internet to the electric grid, promising to revolutionize and improve energy distribution. Like the Internet, the Smart Grid promises significant benefits, but it also introduces new security challenges. Fortunately, due to ongoing research, the effort to secure the Smart Grid infrastructure is taking place already. With the support of the government—as well as leading security and privacy experts—utility companies are holding meter vendors responsible for security by implementing a formalized SDL and mandating third-party auditing. By following leading security and privacy best practices, utilities can prosper from the benefits of the Smart Grid, while still maintaining the safety of this critical infrastructure.

NOTE: Mr. David Baker is a subject matter expert on information security, CIPS compliance work, and Smart Grid architectures. Baker specializes in developing security requirements and identifying best practices for critical infrastructure and utility system management, having debriefed the Department of Homeland Security on AMI research. Established in 1998, IOActive is an industry leader that offers comprehensive computer security services with specializations in smart grid technologies, software assurance, and compliance. IOActive works with a majority of Global 500 companies (www.ioactive.com).

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

Oil Infrastructure Protection

Mr. Umberto Saccone, Corporate Security Manager, ENI Spa

Nowadays, the threat of terrorist attacks versus the critical infrastructures has brought to the attention the strategic issue of the energy sector security, highlighting the potential vulnerabilities of this sector. Critical Infrastructure Protection (CIP) is by now a key component of the national security in several countries, and after the 11 September 2001 the issue has become the centre of the debate on terrorism and internal security in the USA.

The energy resources are strategic assets both from the political and economic point of view for the oil producing countries, as well as for their clients. Talking about pipelines, the countries where these assets are located (transit countries) are considered of primary strategic importance at international level. Since the end of the Cold War, the regions rich in oil like the Persian Gulf, the Caspian basin and the southern Chinese sea, became more and more important from the strategic point of view. As consequence of this mutating geostrategic order, the protection of the key resources, notably oil and natural gas, has been empathized. The international terrorism has always looked with interest at the oil and gas resources in order to meet its political and economic targets.

The "oil world", with its corporations, the related infrastructures and managers, is one of the declared targets of al-Qaeda and its leader Osama Bin Laden. In fact, since the 1997 Bin Laden has outlined his strategy in an interview with the Pakistani journalist Hamid Mir: *"the oil price growth is not significant if compared to the growth of other commodities. From the 1973 the price of the crude oil has grown only 8\$ a barrel, while the price of some other commodities has grown three times more. The wheat of the United States, for instance, has become three times more expensive, unlike the Arab oil. The Muslim world is suffering a loss of 115\$ per barrel. Every day 10 millions of barrels are produced in Saudi Arabia only. Therefore the daily loss is more than one million \$, while the total one (including other Arab countries), is two millions \$. The Muslims are dying in privation all over the world because the U.S. are stealing our oil."*

Taking into account these assumptions, however, the strategy of al-Qaeda faced the dilemma of how to attack the interests of the oil corporations, while minimizing the impact on the interests of the Muslim world. In his "Declaration of War Against Americans" in 1996, Bin Laden invited clearly the Mujahideen to avoid the involvement in the guerrilla of the key energy resources of the forthcoming Islamic State.

Attacking the productions sites (upon which the western economies rely) in the Muslim countries is therefore a fundamental component of the terrorist strategy that, however, contrasts with the consideration that a permanent damage to the oil fields would heavily impact the economy of the entire Muslim community.

Facing this dilemma al-Qaeda has thus developed a strategic plan that avoids attacks to the oil wells, while encourages attacks to the refining facilities, to the pipelines, tankers, oil terminals, as well as managers and employees of the non Muslim oil corporations.

It is likely that the al-Qaeda attack to the refinery Abqaiq in Saudi Arabia on the 24th of February 2006 represents the beginning of a new and more structured terrorist strategy versus the oil infrastructures. In fact, two days after the attack, Sheik Abd-al-Aziz bin Rachid al-Anazi, a religious man affiliated to al-Qaeda, has published on the Internet the doctrine and the religious justification on attacks to oil facilities, with a treatise titled "The religious Rule on Targeting Oil Interests". The purpose of the argument was to legitimize the attacks from a religious point of view, provided that the energy stocks of the Muslim world would not be affected as a consequence of those attacks. The sabotage is a good weapon, while the attacks to oil wells are forbidden, as Bin Laden said. Three targets are allowed:

- ♦ **Pipelines:** indicated as an "easy target". The benefits deriving from the destruction of a pipeline outdo largely the costs suffered by the Islamic population.
- ♦ **Oil refineries and related facilities (port facilities, tankers, oil terminals):** only the facilities owned by Muslims (and not by the joint ventures) are to be spared.

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

The favourite targets are non Muslims, but also Muslims can be targeted if their dispatching is seen as necessary and beneficial.

Here below some of the most vulnerable facilities related to the oil industry

- ♦ **Exploration and development sites:** are often located in remote areas with inadequate routes and communication difficulties with the authorities and the security related structures. When national security forces are committed to the protection of the site, their number is definitely lower than the terrorists, which often are also part of the surrounding local communities. Therefore, these sites represent an appealing target for the terrorists.
- ♦ **Vessels:** also the watercrafts are running the risk of becoming a favourite target for the terrorist due to a variety of reasons:
 - The security measures on board are often limited to high pressure water cannons or to high power horns to beat off possible attacks.
 - The crew committed to the security is usually small
 - The transported materials are generally highly flammable and hazardous for the environment.
 - In the event of attack, an external support would be available only after a long lapse of time.
 As a consequence, the tankers are considered as relatively easy targets.
- ♦ **Pipelines:** the distribution of oil and gas at long distance is performed through pipelines. The latter are built on the land surface and therefore are highly visible, or in the subsoil but also in this case are easily detectable. Moreover the related supporting equipments (for example the compression stations), are usually left unprotected. Being those equipments located in remote areas, the vulnerability to terrorist attacks is increased.
- ♦ **Oil refineries:** an oil refinery represents the most important asset in the entire oil and gas cycle. Only the continuity of its operations assures the national energy supply. The big extent of a refinery, the complexity of the operations, the large number of individuals, as well as the kind of products represent an incentive to challenge the security measures.

It can be certainly affirmed, that the international terrorist groups are in a position to satisfy the logistic requirements to successfully attack the entire retail and distribution system of the oil and gas industry. Although the potential damage to a single site would be limited, a coordinated attack to several sites could provoke a meaningful damage to the national economy with further socio-political consequences.

All the sub sectors of the oil and gas industry are vulnerable at various levels to the terrorist menace, as the international terrorism has already proven its ability to successfully attack exploration sites, pipelines, oil refineries and the retail end product distribution system.

The Need for Private Sector Involvement in Protecting Critical National Infrastructure

Mr. David Taylor-Smith, CEO G4S Secure Solutions (UK & Ireland)

As global security threats continue to grow the protection of critical national infrastructure (CNI) has become an important area in which the public and private sectors need to work more closely together. This is becoming ever more important as governments are increasingly unable to provide the necessary wide ranging and rapid support they once may have been able to provide. There is no credible choice but to involve the private sector, which already funds, builds and operates critical infrastructure, more fully in its protection.

The former U.S. President, Bill Clinton, summed up CNI's importance when he said it was "critical infrastructures that are so vital that their incapacity or destruction would have a debilitating impact on the defence or economic security of the Nation." In the UK, the Government's Centre for the Protection of the



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

National Infrastructure sets out nine CNI sectors: communications; emergency services; energy; finance; food; government services; health; transport; and water. Without these services, any state could suffer serious consequences, including economic damage, social disruption or even the large-scale loss of life.

In each sector, particularly in countries where private finance initiatives have been successful, many elements of CNI are now the responsibility (and even property) of the private sector. Such a dramatic shift in operational control and ownership demonstrates the value of private sector involvement in the construction and operation of critical infrastructure. It also obliges Governments to rethink their approach to protecting the CNI and industry to wake up to the realisation that securing their facilities is crucial.

Terrorist attacks and insurgency remain the key threats and the issues which dominate the headlines, particularly following the recent outrages in Mumbai and Lahore. The difficulty on countering these threats is driven by their dependence on disparate social networks across international boundaries and the difficulty of identification of those involved.

However, there is a huge risk if our efforts and expenditure decisions are dominated by terrorism alone. Companies need to consider a wider range of risks they may face, from natural disasters to the growth in more malicious activism. The devastation caused by Hurricane Katrina, the 2004 tsunami or even the more recent floods across the UK, threatened the viability of communities and the infrastructure upon which they depend. Companies need to start preparing now to effectively combat this growing spread of national and international threats.

When a disaster strikes, we assume that it should be governments and their agencies which will spring into action to provide essential services and infrastructure recovery, restoring social and economic normality. We also tend to pin the blame on government if there is chaos and disruption following any event we judge to have been foreseeable, avoidable or easily controlled. However, whilst governments do prepare for such events, providing in many cases an excellent response, emergency services and armed forces are often stretched to their limits due to operational or budgetary constraints.

There is also the complicating factor that national governments and agencies are also not always able to deal with international incidents, for a wide range of reasons from political to a lack of capability. So where can they find additional resources that can not only protect assets but also help them assess the threats to which they're exposed?

The obvious response is the international security industry which has deployable resources across the globe and a major vested interest in helping to prevent and minimize the effects of CNI disruptions.

Companies within this industry already have the expertise to handle these tasks, both domestically and when necessary overseas. We protect airports, power stations, water treatment centres and banks in many countries and, in some of them, we also build and operate critical infrastructure such as prisons, youth offender facilities and cash centres. As both CNI operator and protector, this puts us in a strong position to deliver real support to governments seeking to improve national resilience.

So what should Governments do? To kick start the process they need to force all relevant parts of the private sector to take protection of CNI more seriously by creating explicit obligations on owners and managers to protect their infrastructure, as the UK Government already does for those in the aviation or water industries. These obligations can be created either through legislation or through regulation: but whilst they remain discretionary and voluntary, some businesses will continue to ignore the problem for financial or operational reasons.

Governments can also take a more pragmatic approach to using the private sector to operate, protect and provide surge capacity in the protection of CNI both at home and abroad. In many circumstances, the private sector's flexible, national and international resources are equal to or superior to those owned by individual governments and as such should be trusted to perform as required.

Take G4S for example. In North America, we are already relied on to secure around 50 per cent of commercial nuclear power stations and to help protect high sensitivity sites such as the Pentagon and NASA.

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

In Europe, we protect the European Parliament, NATO headquarters, a number of secure UK Government facilities and a growing list of major international ports and airports such as Amsterdam's Schipol airport and Heathrow International. We also protect Embassies and diplomats for the UK, US and other sovereign governments in a wide range of complex environments around the world as well as providing timely, emergency cross-border services which far outstripped the efforts of individual government agencies.

Furthermore, with the pressure on Government agencies to produce ever more accurate and pre-emptive intelligence, private sector organisations with their myriad international networks offer new avenues for providing appropriate intelligence, often much more quickly than individual nations can achieve. After all, the private sector has been using security consultancies to provide business intelligence for many years. Making such intelligence networks available to the public sector is simply common sense.

Therefore the private sector has already proved the very real benefits of using it to provide CNI-related services previously thought of as the exclusive domain of the public sector. In reality there is no alternative but for the public and private sector to work together to protect and build critical infrastructures. Governments that choose to maintain the status quo rather than involve the private sector in CNI protection are taking unnecessary risks and ultimately over stretching their resources and exposing their CNI to potential attacks.

NOTE: This article was first published in the *GIT Security+Management* magazine Vol. 5 (April 2009)