



# Energy Security and Security Policy

**NATO and the Role of  
International Security  
Actors in Achieving  
Energy Security**



**Edited by Phillip E. Cornell**



Published by the NATO School Research Department

# **Energy Security and Security Policy**

## **NATO and the Role of International Security Actors in Achieving Energy Security**

**Edited by Phillip Cornell**

**DRAFT COPY**



**November 2007  
NATO School Research**

## Contents

<b>1. Introduction</b>	Phillip Cornell <i>NATO School</i>	3
<b>2. Background: The Global Energy Environment and Impacts on Euro-Atlantic Security</b>	Phillip Cornell	4
<b>3. 'Security of Energy Security': Opening Remarks by the Chairman</b>	Phillip Cornell	18
<b>4. Determining the Security Logic of Energy</b>		
4.1. NATO and Energy Security	Adrian Kendry <i>NATO International Staff</i>	21
4.2. Energy Security: What Does it Really Mean?	Gal Luft <i>Institute for the Analysis of Global Security</i>	28
<b>5. Critical Energy Infrastructure Security</b>		
5.1. The U.S. Global Energy Infrastructure Security Strategy	Bruce Averill <i>U.S. State Department</i>	36
5.2. Energy Security and Dependence on the Sea	Rear Admiral Hubert Hass <i>NATO MCC Northwood</i>	40
5.3. Vulnerability Analysis in the Iraqi Oil and Gas Infrastructure as a Result of Pipeline Sabotage	Antonio de la Cruz <i>European Union Satellite Centre</i>	46
<b>6. Risk Assessment</b>		
6.1. Risk Assessment in the Private Sector	Alfio Rapisarda <i>Eni S.p.A.</i>	52
6.2. Managing Risks to Energy Sector Critical Infrastructure	Jack Clarke <i>George C. Marshall Center</i>	59
<b>7. The Security Politics of Energy</b>		
7.1. Energy Security: Any Role for NATO?	Cezary Lusinski <i>Ministry of Defence, Poland</i>	66
7.2. The Euro-Atlantic Area and Energy Interdependence	Andrew Monaghan <i>NATO Defence College</i>	69
7.3. Turkey and the Politics of Pipelines in the Black Sea Region	Oktay Tanrisever <i>Middle East Technical University</i>	74
<b>8. Energy and the Future Security Environment</b>		
8.1. Energy and the Future Security Environment	Khazar Ibrahim <i>Ministry of Foreign Affairs, Azerbaijan</i>	80
8.2. The Future Energy Security Environment: No Alternative to a Radical Energy Shift	Susanne Peters <i>Kent State University</i>	84
8.3. World Upstream Developments	Cyril Widdershoven <i>Cap Gemini</i>	88
<b>9. The Security Dimension of Energy Infrastructure Security</b>	Heiko Borchert and Karina Forster <i>IPA Network</i>	92
<b>10. Aligning Security Risk: The Case for Public Security Provision of Internationally Critical Energy Infrastructures</b>	Phillip Cornell	116
<b>12. Conclusions</b>	Phillip Cornell	123

## 1. Introduction

The following volume is meant to serve as an assessment of the major current issues at the nexus of security policy and energy security, particularly as NATO seeks to identify its added value toward guaranteeing the energy security of its members.

Energy security is a notoriously difficult subject to analyze because it cuts across so many different disciplines. Geological sciences and engineering, international economics and finance, regulatory policy, critical infrastructure protection, geopolitics, environmental sciences, business development, risk analysis and engineering management, and information technology only begin to scratch the surface. It also means very different things to different people – consumers, producers, transit countries, industry, the military, government, scientists, and economists may take different and often opposing views on the subject.

How then is security policy linked with energy security, how should security organisations define energy security, and how can those organisations contribute to enhancing that security?

This volume is the product of a few initiatives, and as such is something of an amalgamation – a conference report *cum* policy pamphlet.

At the NATO School Research Department I have been leading an ongoing research project into NATO and energy security since the Riga Summit, when the Heads of State and Government of the Allies formally instructed the North Atlantic Council to investigate threats to energy security and define NATO's role. This document's organization, construction, and publication are some of the primary products of that effort.

Secondly, on July 19-20 2007, the NATO School and the Institute for the Analysis of Global Security convened "The 'Security' of Energy Security", a conference designed to examine the role of the international security community in comprehensive energy security policies of the West. Delegates hailed from the academy, from government ministries, from international organisations, and from industry. **Sections 4 through 8 contain articles which have been faithfully adapted from the presentations offered in that forum.** Each section represents one of the thematic panels. Discussions were off the record, and therefore not included verbatim in this report. But the outcomes and their general thrust have been integrated into the conclusions.

Given the somewhat disparate sources of the material you will find here, these entries are intended as policy articles and adapted presentations rather than academic papers. The outstanding exception to that rule is the academic paper by Heiko Borchert and Katrina Forster in Section 9. It derives from previous work conducted by the authors within the framework of the IPA Network, and formed the basis for Dr. Borchert's presentation at the conference. I would like to extend my thanks to them for their unique efforts.

Phillip Cornell  
NATO School Senior Fellow

## 9. The Security Dimension of Energy Infrastructure Security

Heiko Borchert and Karina Forster<sup>\*</sup>  
IPA Network

The strive for energy security is likely to dominate the international policy agenda of the 21st century. This is no surprise as every industrialized or developing economy depends on energy. What is however mostly overlooked is the fact that there is no energy security without energy infrastructure security.

Energy infrastructure security can be understood as a holistic approach that looks at ends, ways and means to detect and explore natural energy resources and to refine, store, transport, and distribute the relevant products. As the world depends on global energy supply chains that range from energy resources producing countries via countries of transit to the target markets, the provision of energy infrastructure safety and security is a complex and demanding task.

The dependence on a viable energy infrastructure is likely to grow for three reasons. First, energy consumption is rising worldwide. Strong economic growth in key developing countries such as India and China will spur the demand for fossil fuels and other energy sources in the next decades. This raises the need to explore existing energy resources more efficiently, find new energy resources, and increase production, refining and transmission capacities. Second, plans to diversify imports of oil and gas in particular will lead Europe, the United States and other consumers to new countries that are further away than current suppliers. This only reinforces the dependence on infrastructure as the energy supply chain will be extended. Finally, the political demand to use more renewable energy resources might help reduce geopolitical dependence, but it will not change the need for a reliable energy infrastructure. In many places current energy infrastructures are not yet appropriately designed to manage renewable energy flows such as wind power which is hard to control. This can lead to situations where the use of renewable energy poses infrastructure risks of its own.

Therefore energy infrastructure security must receive more political attention. There are clear indications that this is the case. NATO, for instance, is stepping up dialogue with energy companies and energy production countries. The 2006 declarations of the EU-US Summit and the G8 Summit in Saint Petersburg underlined the need for cooperative approaches towards energy infrastructure security. And the European Commission has proposed the European Program on Critical Infrastructure Protection (EPCIP) that outlines the first building blocks to identify European critical infrastructure.

---

<sup>\*</sup> This paper builds on the authors' study "Energy Infrastructure Security: An Underestimated Foreign Policy Challenge" commissioned by the Swiss Ministry of Foreign Affairs and does not necessarily reflect the official position of the Swiss government.

Dealing with energy infrastructure security requires sophisticated approaches that span different policy areas and across the traditional public-private divide: Foreign policy action is needed to incorporate energy infrastructure security into external relations with energy production, transit, and consumption countries. Trade policy will have to assure a level playing field for state- and private-owned energy companies, which does not yet exist. Regulation policy has to pay more attention to the possible downside effect of market liberalization. Environmental policy has to be taken into account as demands for certain types of environmental protection measures can impose economic burdens that hamper energy infrastructure investments and thus reduce incentives for safety and security investments. Development policy can help address the broader political framework in energy-producing countries.

Finally, there is the security dimension. Despite recent declarations, the key message of our paper is that the security dimension of energy infrastructure security has so far been neglected – to the detriment of European energy security and European homeland security. We will argue that overcoming this shortfall requires a combination of hard and soft power.

Soft power refers to trust and confidence-building that are indispensable to enter into dialogue with state- and non-state actors about a very sensitive issue. Soft power also entails community building. By creating a sense of ownership local communities will have an incentive to avoid infrastructure-related incidents. Finally, standards are part of the soft power agenda as well. Defining standards can help direct public and private actions towards jointly agreed safety and security levels thereby taking into account not only the changed security landscape but also political demands for market liberalization and more eco-friendly energy consumption.

The global energy supply chain has a strong territorial footprint. Pipelines, in particular, create direct interdependencies between supplier and consumer markets. Europe, for example, imports roughly 85 % of its gas by pipeline.<sup>32</sup> Ultimately there is also a role for hard power in protecting the critical energy infrastructure. While “boots on the ground” can be useful in certain cases, there are other defense and security capabilities that are likely to be more relevant. Think, for example, of unmanned platforms that can be used for infrastructure surveillance or concept development and experimentation tools to model interdependencies between the energy sector and other critical infrastructures. Furthermore, armed forces and emergency responders also have a valuable role to play in energy-infrastructure related cross-border incidents.

The focus of this paper is on concrete actions to advance the security dimension of energy infrastructure security. Before we turn to our recommendations we briefly outline our framework of analysis that highlights the complexity of energy infrastructure security.

---

<sup>32</sup> Energy Sector Inquiry. DG Competition Report, SEC(2006) 1724, Brussels, 10 January 2007, p. 25, <[http://ec.europa.eu/comm/competition/antitrust/others/sector\\_inquiries/energy/fr\\_part1.pdf](http://ec.europa.eu/comm/competition/antitrust/others/sector_inquiries/energy/fr_part1.pdf)> (access 13 July 2007).

## 9.1. Energy infrastructure security: What is it all about

Figure 1 illustrates the complexity of the tasks that must be taken into account when guaranteeing energy infrastructure security. Our model rests on three analytical dimensions:

### ■ 9.1.1. Energy supply chain

The energy supply chain at the center of Figure 1 illustrates the relevant steps to bring energy resources to consumer markets. Most importantly, the supply chain highlights the interconnectedness of all stakeholders involved: individual firms or nations depend not only on their own choices to guarantee infrastructure security, but also on those of others.<sup>33</sup>

However, despite mutual dependence between the stakeholders, the global energy supply chain is characterized by power asymmetry. It is estimated that around 85-90 % of the world's oil reserves fall under direct government control. Governments receive at least 45-90 % of the net value of crude oil over the lifetime of around 40 years of an oil field. State players also account for about 78 % of world oil and 74 % of world gas production, leaving the rest to corporate actors such as Exxon Mobil, Royal Dutch Shell, BP or Total.<sup>34</sup>

This means that a competition-based regulatory approach to energy security, which is followed by the European Union (EU) in particular, is seriously limited. In fact, competition only works on the European home market, and even there serious problems exist. As all other stages of the supply chain are dominated by power and monopolies, there are serious power asymmetries: Europe's market focus collides with the desire for upstream control of leading energy resource consumers such as China and India and the strive for downstream control followed by leading producers.

### ■ 9.1.2. Production, transit, and consumption countries

Energy infrastructures cross various countries and are thus subject to regulatory differences. This distinction makes it clear that there is a regulatory asymmetry.<sup>35</sup>

On the one hand there are safety and security provisions defined locally by a single producing nation or the parties of an infrastructure project. On the other hand, there is a regional or even global dependence on the steady provision of energy resources that is directly affected by these local provisions.

<sup>33</sup> Jeffrey Heal et. al., "Interdependent security in interconnected networks," in Philip E. Auerswald et. al. (eds.), *Seeds of Disaster, Roots of Response. How Private Action Can Reduce Public Vulnerability* (Cambridge: Cambridge University Press, 2006), pp. 258-275, here p. 258.

<sup>34</sup> GAO, *International Energy: International Forums Contribute to Energy Cooperation with Constraints* (Washington, DC: GAO, 2006), p. 20; Xavier Harel, "La pétro-politique rebat les cartes," *La Tribune*, 12 June 2006, p. 36; Jill Shankelman, *Oil, Profits, and Peace. Does Business Have a Role in Peacemaking?* (Washington, DC: United States Institute of Peace Press, 2006), p. 40.

<sup>35</sup> For a similar analysis, see also: *The paradigm change in international natural gas markets and the impact on regulation* (The Hague: The Clingendael Institute, 2006), pp. 17-26.

Today, important production and transit countries lack energy infrastructure security concepts or strategies. If safety and security standards exist at all, they are not delineated from an overall concept. Given the logic of the supply chain, this directly weakens the security of supply of consuming countries. There is thus a serious need for an international regime that sets standards for energy infrastructure security commensurate with the security assessment across all stages of the global energy supply chain.

Furthermore there is the crucial role of chokepoints, i.e. narrow geographic bottlenecks through which energy supplies are channeled. For example, 88 % of all Persian Gulf oil exports need to pass the Strait of Hormuz.<sup>36</sup> If the Strait is blocked, there are alternative routes, but delivery takes longer which increases supply costs.

■ 9.1.3. *Risks*

There are manifold risks to the critical energy infrastructure. Physical infrastructure risks describe vulnerabilities of assets such as pipelines or pumping stations. Protecting and hardening these elements can improve physical security. Information and communication technology (ICT) refers to the dependence of energy infrastructure on networks and control systems. Electronic control systems, for instance, have been called an “inroad to critical infrastructure disaster” as information security for these elements lags behind general information security.<sup>37</sup> This makes energy infrastructure security even more complex as risks that can endanger the proper functioning of ICT can also affect energy infrastructures.

Human factors illustrate that human activity can pose security risks either by deliberate attacks (e.g. in case of terrorists) or occasional malfunctions. Finally, organizational aspects need to be taken into account in order to address interfaces between the various actors along the energy supply chain. In particular in Europe these interfaces become even more important as deregulation and competition in the energy sector have led to the outsourcing of various functions that have hitherto been integrated into single companies.

---

<sup>36</sup> Jean-Paul Rodrigue, “Straits, Passages and Chokepoints. Maritime Geostrategy of Petroleum Distribution,” *Cahier de Géographie du Québec*, 48:135 (December 2004), pp. 357-374, here p. 367.

<sup>37</sup> Eric A. M. Luijck, “SCADA: An Inroad to Critical Infrastructure Disaster,” Presentation to the 4th EAPC/PfP Workshop on Critical Infrastructure Protection and Civil Emergency Planning, Zurich, 24-26 August 2006.



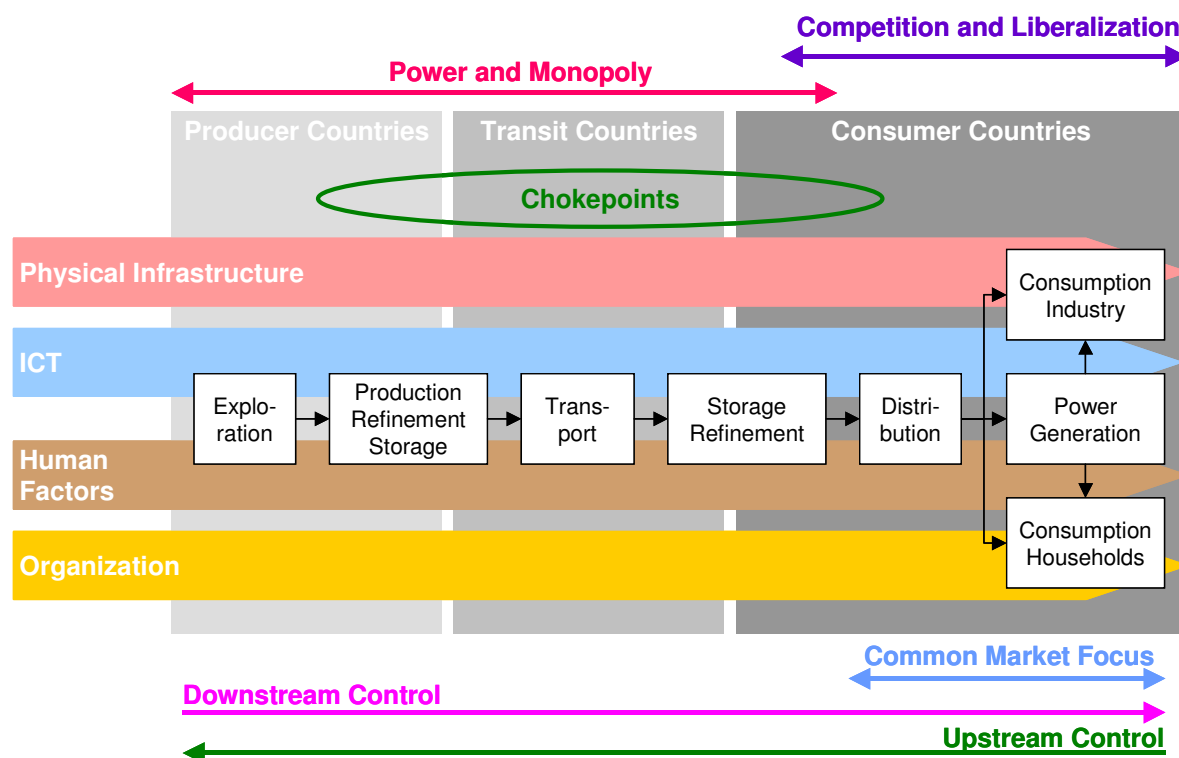


Figure 1: Energy Infrastructure Security – Model of Analysis

## 9.2. How to strengthen the security of energy infrastructure security

Against the background of our model of analysis in Figure 1 we see seven areas that should receive more attention in order to strengthen the security dimension of energy infrastructure security. First of all there is a need for an appropriate international setting to debate all aspects relevant to energy infrastructure security. The International Energy Forum (IEF) could present such a forum as all major production, transit, and consumption countries belong to it. In addition, EU member states should consider the appointment of a European Energy Infrastructure Security Coordinator to deal with all the inter-agency aspects of the issue. Second, given the different risk dimensions outlined above the adequacy of current energy infrastructure safety and security standards should be scrutinized.

Furthermore it is necessary to adapt current security paradigms with regard to the role of defense and security forces in several respects. Our third recommendation thus advocates to bring the Security Sector Reform (SSR) agenda in line with energy infrastructure security requirements. Fourth, EU member states in particular need to acknowledge that also hard power plays an important role to protect the global energy supply chain. So far, however, Europe's ambitious external energy relations agenda is not linked with the EU's security and defense policy. Fifth, private security contractors (PSC) are a matter of fact in the energy sector. Despite the risks of engaging PSC, they can also play useful roles that should be addressed more closely. Sixth, engagement efforts with local communities should be stepped up. By creating local ownership local communities have a stake in the longevity of energy infrastructures and will thus have an incentive to guarantee their security.

Finally, there is a need for cross-border emergency and consequence management along the global energy supply chain, which needs more attention. So far, mutual support for infrastructure related cross-border incidents is insufficient. This is not only an economic problem, as it hinders the free flow of energy as a basis for economic cooperation. It is also a serious problem for European homeland security.

*9.2.1. Recommendation: Get the institutional setting right to address energy infrastructure security*

Energy infrastructure security is in need of an adequate institutional environment. This is paradoxical, because there is no lack of international institutions dealing with different aspects of the issue. Overall, however, there is hardly a forum that provides the necessary comprehensiveness in particular with regard to representing the most important production, transit and consumption countries. The only organization that comes close to fulfilling this requirement is the International Energy Forum (IEF). In addition to a global platform there is also a need to advance interagency cooperation with regard to energy infrastructure security at the European level. This task could be assigned to a new European coordinator for energy infrastructure security.

9.2.1.1. USE THE INTERNATIONAL ENERGY FORUM AS A GLOBAL PLATFORM TO ADDRESS ENERGY INFRASTRUCTURE SECURITY

The IEF “provides the largest recurring global gathering of Energy Ministers”.<sup>38</sup> In addition to more than 60 states<sup>39</sup> almost all important international organizations have joined the IEF: the European Communities, the Gulf Cooperation Council, the International Energy Agency, the Organization of Arab Petroleum Exporting Countries, the Organization of Petroleum Exporting Countries, the United Nations and the World Trade Organization. Only NATO and the OSCE<sup>40</sup> are missing. Dialogue between Ministers and the industry is facilitated through the International Energy Business Forum (IEBF). The IEBF Joint Committee includes representatives from 30 national and international oil and gas companies.

The fact that the IEF is neither a negotiating nor a decision-making forum is a weakness that could turn out to be a strength in the initial phase of approaching energy infrastructure security. Like in the early days of the Conference for Security and Cooperation in Europe (CSCE), the IEF could provide an overall umbrella to discuss the matter. Concrete actions that require decision-making and specific programs could then be dealt with by the different international organizations participating in the IEF.

<sup>38</sup> GAO, *International Energy*, p. 13. For more on the forum, see: <<http://www.iefs.org.sa>> (access 13 July 2007).

<sup>39</sup> Algeria, Angola, Argentina, Australia, Austria, Bahrain, Bangladesh, Belgium, Brazil, Brunei, Canada, China, Czech Republic, Denmark, Ecuador, Egypt, Finland, France, Gabon, Germany, Greece, Hungary, India, Indonesia, Iran, Iraq, Ireland, Italy, Japan, Jordan, Kazakhstan, Kuwait, Lebanon, Libya, Malaysia, Mexico, Morocco, Netherlands, New Zealand, Nigeria, Norway, Oman, Pakistan, Philippines, Poland, Portugal, Qatar, Romania, Russia, Saudi Arabia, Slovakia, South Africa, South Korea, Spain, Sri Lanka, Sudan, Sweden, Switzerland, Syria, Thailand, Trinidad and Tobago, Tunisia, Turkey, UAE, United Kingdom, United States of America, Venezuela, Vietnam, and Yemen.

<sup>40</sup> Involving the OSCE could be of use in addressing energy security issues in the Caucasus and in Central Asia where the organization has established field missions.

There can be no doubt that energy infrastructure security is a very sensitive issue. States will thus be reluctant to provide detailed information. However, there is a momentum in favor of a sustained international dialogue about energy infrastructure security that should be seized. Information gathering and exchange about basic questions could be a starting point for the IEF. Among other things, the following topics should be addressed:

- Definition of and approach to energy infrastructure security (IEF dialogue between all relevant partners along the supply chain could highlight important differences in understanding and conceptualizing energy infrastructure security)
- Responsibilities of state and private actors with regard to setting up the necessary regulatory environment and providing infrastructure security
- Comparison of existing energy infrastructure safety and security standards and processes launched to define, review and update these standards
- Exchange of experience with regard to energy infrastructure vulnerability assessments (the comprehensive gathering of all relevant stakeholders in the IEF would also provide a unique opportunity to launch vulnerability assessments covering all stages of the energy supply chain)
- Comparison of best practice methods to identify, classify, and assess vulnerabilities, threats, and risks as well as protection and counter-measures commensurate to deal with these challenges
- Discussion of joint approaches to identify and protect critical infrastructure with cross-border importance (i.e. infrastructure residing in one country that is important for other countries)<sup>41</sup>
- Identification of lessons learned from different national protection strategies (To this purpose it would be important to include NATO because of the different roles national armed forces could play)
- Identification of international need for action, for instance with regard to providing regulatory incentives to stimulate investments, improve protection and modes of interaction to smoothen public-private cooperation.

#### 9.2.1.2. APPOINT A EUROPEAN ENERGY INFRASTRUCTURE SECURITY COORDINATOR

The global IEF-based approach should be complemented by regional initiatives. To this purpose the EU should build on the idea of European coordinators for key European infrastructure projects<sup>42</sup> and appoint a European energy infrastructure security coordinator.<sup>43</sup> In particular the new coordinator should raise awareness for the central importance of energy infrastructure safety and security, create a trustworthy environment for information exchange between public and private actors, and stimulate dialogue on risk and vulnerability assessments with all European and external partners involved in the energy supply chain.<sup>44</sup>

---

<sup>41</sup> The European Program for Critical Infrastructure Protection (EPCIP) provides a method to identify critical infrastructure. But protection strategies for European critical infrastructure have been left out. See: European Program for Critical Infrastructure Protection, COM(2006) 786, Brussels, 12 December 2006, <[http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005\\_0576en01.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf)> (access 31 July 2007).

<sup>42</sup> Priority Interconnection Plan, COM(2006) 846, Brussels, 10 January 2007, p. 10, <[http://ec.europa.eu/energy/energy\\_policy/doc/11\\_priority\\_interconnection\\_plan\\_en.pdf](http://ec.europa.eu/energy/energy_policy/doc/11_priority_interconnection_plan_en.pdf)> (access 31 July 2007).

<sup>43</sup> This idea resulted from talks with government officials, 22 January 2007.

<sup>44</sup> See also: "Russia-EU Energy Dialogue Report of the Energy Infrastructure Theme Group," October 2006, p. 8,

The new coordinator would also play a key role in coordinating the different inter-agency aspects of energy infrastructure security. As such he would coordinate energy infrastructure safety and security activities between the relevant European institutions. Furthermore he would make sure that energy infrastructure security receives the necessary attention in the conduct of Europe's external energy relations, at national and European levels and in other international fora dealing with regulatory issues to stimulate energy infrastructure investment (e.g. OECD, WTO).

As a first priority, the new coordinator should focus on European critical energy infrastructure that is currently being identified under the European Program for Critical Infrastructure Protection.<sup>45</sup> In doing so, the coordinator could establish an Energy Infrastructure Security Platform involving all relevant public and private stakeholders in Europe. The work of the platform should be coordinated with other international institutions such as the International Energy Forum. By bringing together all relevant stakeholders the new platform could, for instance, assess the adequacy of existing energy infrastructure safety and security standards and propose policy action to deal with existing shortfalls. In addition, public-public, public-private, and private-private interaction to guarantee energy infrastructure security could be analyzed in particular with regard to the division of tasks and responsibilities at European and national levels.

#### *9.2.2. Recommendation: Take stock of existing energy infrastructure safety and security standards*

The lack of common energy infrastructure safety and security standards in Europe and beyond is a problem for the cross-border management of energy flows. Among other actions the new European Program for Critical Infrastructure Protection (EPCIP) also includes methodological work to identify critical infrastructure and to assess their vulnerability. This provides Europe with a window of opportunity to address safety and security standards as well.

##### **9.2.2.1. ASSESS EXISTING SAFETY AND SECURITY STANDARDS**

An overview of existing national and international safety and security standards for the various components outlined in our model of analysis should be compiled. This should be done to assess the appropriateness of existing standards in light of future performance requirements such as the creation of a single European gas and electricity market, the increase of energy demand and the injection of increased levels of "green energy resources." In doing so, the following aspects will be important:

- At first, safety and security standards for those priority infrastructure projects that guarantee the supply of energy resources from production and transit countries to Europe should be scrutinized.<sup>46</sup> Performance requirements will need to be

---

<[http://ec.europa.eu/energy/russia/reference\\_texts/doc/2006\\_10\\_infrastructure\\_en.pdf](http://ec.europa.eu/energy/russia/reference_texts/doc/2006_10_infrastructure_en.pdf)> (access 31 July 2007).

<sup>45</sup> The European Program for Critical Infrastructure Protection.

<sup>46</sup> Priority Interconnection Plan. Commission Staff Working Document Accompanying the Communication from the Commission Inquiry pursuant to Article 17 of Regulation (EC) No 1/2003 into the European gas and electricity sectors (Final Report), SEC(2006) 1715, Brussels, 10

discussed with the respective production and transit countries. If they cannot be met, European financial or technical assistance may be required.

- Mutual interdependencies between the energy sector and other critical infrastructure sectors such as information and communication and transportation need to be addressed. Following the assessment of these critical interdependencies it will be important to identify what should be done at European and national levels and how responsibilities and tasks should be shared between public and private actors.
- There is a need to deal with ICT safety and security standards in the energy sector and other critical infrastructure sectors. As every infrastructure sector will come up with specific ICT requests, there will be a need for horizontal coordination, especially when approaching the ICT industry that delivers the relevant products. SCADA safety and security should be looked at in particular. Again, there is a need for identifying and documenting best practice and for standardizing safety and security norms. In the United Kingdom, for instance, the National Infrastructure Security Coordination Center has organized different SCADA conferences and published a good practice guide for process control and SCADA security.<sup>47</sup> This could serve as a model for pan-European initiatives and for cooperation with energy-relevant partner countries.

#### 9.2.2.2. THINK OF STANDARD SAFETY AND SECURITY AUDITS FOR ENERGY INFRASTRUCTURE PROJECTS

It could be argued that the need for energy infrastructure safety and security audits depends on the risks to be faced in each country. In many cases, social and environmental impact assessment of energy infrastructure projects could be enough to address security issues as well. However, this approach tends to overlook the fact that safety and security along the energy supply chain will be only as strong as its weakest link. Therefore we see a need for standard safety and security audits in particular for projects that are key for Europe's energy supply.

Among the different issues to be addressed by these audits, the following stand out as most important:

- The nature of a new infrastructure project (upstream, midstream, downstream) will define interfaces with existing infrastructure. These interfaces must be analyzed in particular because there is a need to address the interplay between new and ageing infrastructure in order to optimize safety and security. Furthermore, there is also a need for standards dealing with life extension of infrastructure components.<sup>48</sup>
- ICT-related risks should be analyzed as a risk category of its own, as outlined above.
- Finally a life-cycle approach should be adopted in order to make sure that safety and security measures evolve commensurate with the aging of the infrastructure and the development of the relevant risk environment. If not yet the case, life-cycle

---

January 2007,  
<[http://ec.europa.eu/energy/energy\\_policy/doc/12\\_priority\\_interconnection\\_plan\\_annexe\\_en.pdf](http://ec.europa.eu/energy/energy_policy/doc/12_priority_interconnection_plan_annexe_en.pdf)>  
(access 31 July 2007).

<sup>47</sup> <<http://www.niscc.gov.uk/niscc/scada-en.html>> (access 13 July 2007).

<sup>48</sup> Joint Research Center, "Safety and Security of Energy Infrastructures in a Comparative View", Conference Report, Brussels, 14-16 November 2005, p. 3  
<<http://www.energyrisks.jrc.nl/workshops/SEIF-CV/SummaryReport-SEIF-CV-Nov2005-final.pdf>> (access 13 July 2007).

costs should be added to investment costs in order to determine overall costs of infrastructure projects.

Requesting safety and security audits for energy infrastructure projects should become common practice for international financial institutions (IFI) that help finance these projects. This could also help advance risk-informed design by integrating safety and security issues in the design phase of an infrastructure project.<sup>49</sup> If IFIs want to exert this kind of influence, they will be required to adopt a common understanding of energy infrastructure security, the most important assessment criteria and the key measures to guarantee safety and security. Such a common understanding will be important in order to avoid diverging approaches between different IFIs that could be detrimental to the overall goal of secure energy supplies.

### 9.2.3. *Recommendation: Make energy infrastructure security part of the security sector reform agenda*

Within a relatively short time span the security sector reform (SSR) agenda has influenced the international development policy, foreign policy and military diplomacy community. By putting the main emphasis on how the security sector is governed SSR stipulates a clear link between security and development in the sense that “a responsible, accountable and effective security sector will engender conditions conducive to development, power reduction and democracy.”<sup>50</sup>

Like every other paradigm, SSR defines a set of key principles.<sup>51</sup> With regard to the need to improve energy infrastructure security, three aspects of the current SSR agenda should be reviewed: limiting security spending, the strict separation of different security forces, and the scope of capacity-building programs.

#### 9.2.3.1. POSITIVE ASSESSMENT OF ENERGY INFRASTRUCTURE SECURITY SPENDING NEEDED

As a starting point it can be argued that the more a nation depends on revenues gained from extracting energy resources the more important is the steady flow of these revenues in order to fund state activities. In guaranteeing stable flows of energy, a secure energy infrastructure is key. Most energy producing countries interpret oil and gas as strategic goods and thus foresee state ownership and control. Depending on the security situation of the respective country, the physical protection of the energy infrastructure may be a premier task for the nation's armed forces and/or its police forces. These forces must be trained and equipped to accomplish their tasks, which in turn requires adequate spending.

The SSR agenda, however, is still predominantly characterized by the focus on spending levels and spending processes with the aim of limiting or cutting back defense and security spending. Against the background of former war-torn societies where armed forces and the police were used to suppress the population, this is understandable. Given the new security landscape that might require armed forces and

<sup>49</sup> *ibid.*, p. 4.

<sup>50</sup> Mark Sedra, “European Approaches to Security Sector Reform: Examining Trends through the Lens of Afghanistan,” *European Security*, 15:3 (2006), pp. 323-338, here p. 325.

<sup>51</sup> For a comprehensive overview, see: OECD, *Security System Reform and Governance* (Paris: OECD, 2005), <<http://www.oecd.org/dataoecd/8/39/31785288.pdf>> (access 13 July 2007).

the police to accomplish energy infrastructure security, this view is no longer enough. Rather the SSR agenda should be modified in order to take into account the important role of infrastructure security spending. In order to avoid false impressions, transparency building with regard to security spending, which is part of the SSR agenda, should address infrastructure security spending in particular. This could advance trust among neighboring countries and would help provide the international community with a better understanding of existing shortcomings that need to be tackled.<sup>52</sup>

#### 9.2.3.2. FOCUS ON INTEGRATED CAPABILITIES RATHER THAN INSTITUTIONAL SEPARATION

Furthermore, energy infrastructure protection requires specific capabilities. The SSR focus on the proper delineation of powers and the respective division of responsibilities and organizations<sup>53</sup> tends to overemphasize institutional separation of armed forces and police forces rather than focusing on the provision of integrated capabilities and smooth interagency interaction. Intelligence gathering for surveillance, for instance, could include the use of Unmanned Aerial Vehicles (UAV) maintained by the country's armed forces. Information from UAV-based sensors should be distributed to all relevant actors in order to improve situational awareness and situational understanding. Similarly, crowd and riot control is a task for the police, but it could also include the armed forces in order to guarantee the availability of an instrument of power commensurate with the escalation spectrum of regional incidents. That's why building up integrated capabilities that are useful for defense, security, and infrastructure protection tasks should receive more attention in SSR activities.

#### 9.2.3.3. ADDRESS SPECIFIC CAPACITY BUILDING REQUIREMENTS OF THE HYDROCARBON SECTOR

Our plea for more jointness goes hand in hand with the demand for capacity building programs that take into account the specifics of the energy sector. Judicial and administrative reforms are most important.

In Nigeria, for instance, the justice department is in charge of all aspects of the hydrocarbon sector. In light of ongoing turmoil in particular in the Niger Delta, which is the heartland of Nigeria's oil reserves, the department's limits are becoming apparent.<sup>54</sup> There is no specialized unit within the judicial branch trained and equipped to tackle the highly complex and politically sensitive questions arising within the hydrocarbon sector. Reforming the judicial branch with a view on the

<sup>52</sup> One could object that the provision of spending figures for energy infrastructure security is illusionary. This argument, however, can be countered with reference to the history of the Conference on Security and Cooperation in Europe (CSCE) which helped overcome cold world animosity between East and West at least in parts thanks to the provision of transparency with regard to military spending.

<sup>53</sup> Thomas Debiel and Ulf Terlinden, *Promoting good governance in post-conflict societies* (Eschborn/Berlin: Deutsche Gesellschaft für Technische Zusammenarbeit and Federal Ministry for Economic Cooperation and Development, 2004), p. 11, <<http://www.oecd.org/dataoecd/47/26/34481761.pdf>> (access 13 July 2007).

<sup>54</sup> For more on this, see in particular: International Crisis Group, *The Swamps of Insurgencies: Nigeria's Delta Unrest* (Brussels: ICG, 2006), <[http://www.crisisgroup.org/library/documents/africa/west\\_africa/115\\_the\\_swamps\\_of\\_insurgency\\_nigeria\\_s\\_delta\\_unrest.pdf](http://www.crisisgroup.org/library/documents/africa/west_africa/115_the_swamps_of_insurgency_nigeria_s_delta_unrest.pdf)> (access 31 July 2007).

specific requirements of the hydrocarbon sector should thus become a key priority of future SSR activities.

International initiatives that increase transparency in the energy sector are important. However, collecting the necessary information to comply for example with the requirements of the Extractive Industries Transparency Initiative (EITI) requirements is tough. It requires seasoned personnel familiar with statistical work, a robust financial system that can track and trace the relevant money streams, budget planning and independent auditing.<sup>55</sup> As a consequence, there is a need to bring in line EITI requirements with international programs to strengthen local government institutions such as SSR.

#### *9.2.4. Recommendation: Come to terms with the military dimension of energy infrastructure security*

Ultimately energy infrastructure security also has a military dimension. Coming to terms with the role of armed forces is important for Europe's long-term energy security. Up to now, Europe has largely been free riding on the United States for the provision of hard power to guarantee energy supply security. Estimates assume that the United States spend around \$50 billion per year to defend the sea lanes of communication and to provide military assistance to oil supplying partner nations.<sup>56</sup> As a consequence, the military dimension of energy security is absent from Europe's most recent energy diplomacy agenda. At least so far, there is no direct link between this agenda and the necessary security and defense capabilities needed to underpin energy ambitions in particular vis-à-vis possible zones of turmoil that are important for Europe's energy resource supply. On Europe's homeland security front there is also no common approach to the role of armed forces and other security actors in energy infrastructure security.<sup>57</sup>

In the following we will provide food for thought for the discussion about the possible role of armed forces in energy infrastructure security. To this purpose we will address possible military tasks and the potential roles of NATO and the ESDP.

##### 9.2.4.1. IDENTIFY POSSIBLE MILITARY TASKS

The spectrum of possible energy infrastructure security tasks to be accomplished by armed forces is broad and could include:

- Confidence- and security building measures (CSBM)  
CSBM in the field of energy infrastructure security comes with two distinct specifications. First, CSBM in energy-rich zones of turmoil can create transparency with regard to the purpose of existing military and security capabilities. As suggested in recommendation 3, it will be important to avoid the impression that

<sup>55</sup> Jürgen W. Cuno, "Stellungnahme für die Anhörung des Ausschusses für wirtschaftliche Zusammenarbeit zum Thema 'Rohstoffökonomien – Auswirkungen auf Entwicklungsländer'," Berlin, 20 September 2006 (mimeo), p. 6. The same also holds true for social and environmental impact assessments. See: Shankleman, *Oil, Profits, and Peace*, pp. 158-160.

<sup>56</sup> Jos van Gennip, "Energy Security," *NATO Parliamentary Assembly Report 170 ESC 06* (Brussels: NATO Parliamentary Assembly, 2006), para. 51  
<<http://natopa.ibicenter.net/default.asp?SHORTCUT=1000>> (access 13 July 2007).

<sup>57</sup> For more on this, see: John L. Clarke (ed.), *Armies in Homeland Security: American and European Perspectives* (Washington, DC: NDU Press, 2006).



investment in military and security capabilities used for energy infrastructure security are used in an offensive manner or directed against anybody. Second, building up community relations has become an integrated aspect of infrastructure projects in turbulent regions. Given the importance of this issue it will be addressed separately below (recommendation 6).

- **Training and equipping armed forces, the police and emergency responders**  
This is an important aspect in order to guarantee that the forces are mission ready and able to cooperate across existing organizational boundaries. Joint armaments export to adequately equip energy producing countries for energy infrastructure security tasks is far from being an area where European nations have similar interests. This, however, is detrimental to joint approaches for the growing need of upstream energy infrastructure security that is in Europe's strategic interest.
- **Intelligence gathering**  
This is most important for risk and vulnerability assessments. While the categories to be analyzed can be deducted from the four risk dimensions outlined in our model of analysis in Figure 1 (tangible property, ICT, human factors, organization), intelligence fusion is more challenging. Infrastructure security depends on the provision of a comprehensive picture identifying domestic and international risks across the energy supply chain. So far, intelligence cooperation is not directed to the level of cooperation that is needed to achieve this. In particular there is a need for more and advanced intelligence sharing and cooperation between civil and military intelligence services (at national and international levels) and between the state's intelligence services, the energy sector, and private security contractors.
- **Surveillance**  
Surveillance in all relevant dimensions of operations – i.e. land, sea, air, space, and cyberspace – is a traditional military task. Together with protection this task can have structural consequences<sup>58</sup> for the armed forces and thus needs to be treated with great care. A balance will have to be established between duties that require “boots on the ground” and the use of technology. At the technology front Europe's security research program and other activities aimed at the provision of dual use capabilities can be very valuable (see below).
- **Protection**  
The task entails direct and indirect components. Direct components refer to proper infrastructure protection in the physical sense – either onshore or offshore.<sup>59</sup> This could also include military support in the cyber dimension where active and passive capabilities for electronic warfare could be used. Indirect components deal with the broader environment in which the infrastructure is located. Tasks to be fulfilled in this dimension could include perimeter control, the establishment of

---

<sup>58</sup> The key question is whether there will be dedicated units for energy infrastructure tasks (differentiated force model) or if the task will have to be accomplished by regular forces (unitary force model).

<sup>59</sup> According to NATO MC401 the defense and protection of offshore infrastructure in the north-western European and eastern Atlantic regions is a task for NATO's naval forces. Rear Admiral Hubert Hass, “Energy Security and Dependence on the Sea,” Presentation at the conference “The ‘Security’ of Energy Security,” NATO School, Oberammergau, 19-20 July 2007.

checkpoints or even challenging operations conducted against groups that sabotage the energy infrastructure. In some cases, this could also lead to counter-terrorist operations. Three protection tasks deserve special mentioning:

- Armed forces could be used in *interdiction operations* to secure the supply of energy resource flows.<sup>60</sup>
- Furthermore, the reliance on oil transport by sea makes *maritime transportation security* a specific task. The importance of this task is underlined by ongoing operations aimed at suppressing piracy or cutting off life lines for the support of terrorist groups. In addition, reliance on maritime security will increase with the raising demand of LNG, which is shipped.
- Finally, *ecological security* should be addressed as well. Basically, the use of military or any other environmental modification techniques is prohibited by international environmental law. International regulations also foresee the protection of critical infrastructure containing dangerous material/goods (e.g. nuclear plants). Against this background the protection of energy infrastructure should be interpreted as a task for the armed forces. Given growing instabilities in major regions of supply, this task requires close cooperation between local armed forces and armed forces of international alliances.<sup>61</sup>

#### ■ Continuity of services

Energy infrastructure operators must be able to guarantee continuity of services. Depending on the severity of an incident they might need security or military support to do so. This could be the case, for instance, in order to provide command and control to run control centers or to guarantee the functioning of the critical ICT infrastructure.

#### ■ Emergency and consequence management

This entails all tasks to recover from an energy infrastructure incident. Most generally this could cover support for infrastructure rebuilding (e.g. heavy engineering material), logistics, medical aid or the use of military fuel storage capacity. In case an infrastructure incident results from an attack with weapons of mass destruction, CBRNE<sup>62</sup> capabilities could be needed as well to clean the site and handle casualties.

<sup>60</sup> Jamie Shea, "Energy security: NATO's potential role," *NATO Review* (Autumn 2006), <<http://www.nato.int/docu/review/2006/issue3/english/special1.html>> (access 13 July 2007); Paul Gallis, "NATO and Energy," *CRS Report RS22409* (Washington, DC: Congressional Research Service, 2006).

<sup>61</sup> We thank Kurt-Dieter Grill, former member of the German Bundestag, for bringing this to our attention. The 1977 Convention on the prohibition of military or any other hostile use of environmental modification techniques can be found at <<http://www.fas.org/nuke/control/enmod/text/enviro2.htm>> (access 13 July 2007). See also: Susana Pimiento Chamorro and Edward Hammond, *Addressing Environmental Modification in Post-Cold War Conflict. The Convention on the Prohibition of Military or Any other Hostile Use of Environmental Modification Techniques (ENMOD) and Related Agreements* (Austin: The Sunshine Project, 2001), <<http://www.edmonds-institute.org/pimiento.html>> (access 13 July 2007); Hans Günter Brauch, "Auswirkungen der Kriege auf die Umwelt im Mittelmeerraum und die Weiterentwicklung des Völkerrechts. Aufgaben für die Europäische Union", in Erich Reiter (Hrsg.), *Jahrbuch für internationale Sicherheitspolitik 2003* (Hamburg: Mittler & Sohn, 2003), pp. 695-720.

<sup>62</sup> Chemical, Biological, Radiological, Nuclear, and Explosive.

■ Concept development and experimentation (CDE)

CDE has become a key instrument to support defense transformation. Based on modeling and simulation CDE enables armed forces to test new thinking on concepts, capabilities, structures and processes before implementing them into practice. Methodological know-how gained through CDE is also useful for energy infrastructure security. As argued above there are interdependencies between the energy sector and other critical infrastructure sectors that need to be identified and assessed in order to prepare adequate response. This can help establish cause and effect relationships. Furthermore CDE can be used to simulate interaction between armed forces, emergency responders, security forces of energy companies and other relevant stakeholders. Findings resulting from these and other simulations can be used to determine optimal capability packages to address energy infrastructure tasks.

#### 9.2.4.2. ADVANCE NATO-EU COOPERATION

In principle the EU would provide the necessary instruments to address the military dimension of energy infrastructure security. However, apart from a very general reference to ESDP in the June 2006 Presidency Conclusions, the role of the armed forces in energy security seems to be an non issue in the most recent EU capstone documents. The EPCIP only refers to methodologies, standards and the role of operators. The EDA long-term vision, which outlines future capability requirements within the ESDP context, makes no reference to energy security or energy infrastructure protection tasks. The 2006 Solana paper on an external policy to serve Europe's energy interests and the most recent Commission outline for a European energy policy only focus on energy diplomacy and "soft power" instruments.<sup>63</sup>

Within NATO there is not yet a clear consensus about the future role of the Alliance in energy security.<sup>64</sup> But at least there is a politically agreed basis for addressing this issue. The 2006 Riga summit declaration tasks the NATO Council to "consult on the most immediate risks in the field of energy security, in order to define those areas where NATO may add value." Furthermore, NATO's Comprehensive Political Guidance, which sets out capability requirements for the next 10 to 15 years, highlights the need to protect the "Alliance's populations, territory, critical infrastructure and forces, and to support consequence management."<sup>65</sup>

In light of this, NATO Secretary-General Jaap de Hoop Scheffer and Policy Planning Director Jamie Shea argued that NATO's role in energy security could include monitoring and assessing the energy security situation, security assistance to allies,

<sup>63</sup> Presidency Conclusions, Brussels European Council, 15/16 June 2006, 10633/06, CONCL2, para. 24; A European Program for Critical Infrastructure Protection; An Initial Long-Term Vision for European Defense Capability and Capacity Needs, Brussels, 3 October 2006, pp. 16-19; An External policy to serve Europe's energy interest, Council of the European Union, 9971/06, Brussels, 30 May 2006.

<sup>64</sup> Background telephone interview with NATO official, 30 November 2006.

<sup>65</sup> Riga Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council, Press Release (2006)150, Riga, 29 November 2006, para. 45, <<http://www.nato.int/docu/pr/2006/p06-150e.htm>> (access 13 July 2007); Comprehensive Political Guidance endorsed by the NATO Heads of State and Government, Riga, 29 November 2006, para. 16(c) <<http://www.nato.int/docu/basic/b061129e.htm>> (access 13 July 2007), para. 16(c).

maritime surveillance and threat-based response and interdiction operations.<sup>66</sup> In addition, Shea confirmed that NATO has entered into dialogue with oil companies and energy-exporting countries on how to best secure energy infrastructure.<sup>67</sup>

For sustained operations to the benefit of energy security or energy infrastructure security there is probably a lack of capabilities in EU and NATO. The NATO Response Force (NRF) and the EU Battle Groups are land forces with naval and air components. Some NRF naval assets could be used as entry forces to deter aggressors, for example, to protect offshore infrastructure. However, enduring operations would have to take recourse to standing naval capabilities.<sup>68</sup> Naval support for energy security thus seems to fit perfectly into the most recent US ideas for the “1,000-ship Navy”<sup>69</sup> and could therefore revitalize transatlantic cooperation in a vital area.

These preliminary observations underline the need for further military planning. In particular energy infrastructure security-related tasks would need to enter force requirement catalogues in order to influence capability planning of the member states. Given the complexity of energy infrastructure security, close cooperation between all stakeholders involved along the supply chain will be needed. To this purpose the following additional issues should be addressed:

- Initiate regional military cooperation on energy infrastructure security  
Military cooperation could be deepened via existing NATO initiatives such as the Mediterranean Dialogue and the Istanbul Cooperation Initiative. However, NATO lacks institutional ties with important producers such as Libya or Saudi Arabia, but has recently concluded an information security agreement with Kuwait. The Alliance also talks with Qatar about possible help to protect LNG facilities.<sup>70</sup>

The EU would have to add a fully fledged military diplomacy dimension to the ESDP and bring it in line with the new neighborhood policy. Furthermore the military/security dimension should be added to Europe’s external energy relations. So far, reference to the means used for energy infrastructure security is absent from the recent energy cooperation agreements with Kazakhstan and the Caucasus.<sup>71</sup>

<sup>66</sup> Shea, “Energy security: NATO’s potential role;” “Keynote address by NATO Secretary-General Jaap the Hoop Scheffer at the EAPC Security Forum,” Ohrid, 29 June 2007, <<http://www.nato.int/docu/speech/2007/s070629b.html>> (access 13 July 2007).

<sup>67</sup> Tom Bergin, “NATO eyes naval patrols to secure oil facilities,” *Reuters*, 14 May 2007, <<http://uk.reuters.com/article/topNews/idUKL141495820070514>> (access 13 July 2007).

<sup>68</sup> Background telephone interview with NATO official, 30 November 2006.

<sup>69</sup> This is a metaphorical term coined by the US Navy to describe the need for international naval cooperation to halt and reduce threats on the high seas. See: Christopher P. Cavalas, “Spanning the Globe. US Floats Fleet Cooperation Concept to Allies,” *Defense News*, 8 January 2007, pp. 11-12.

<sup>70</sup> Background telephone interview with NATO official, 30 November 2006; Nicholas Fiorenza, “Kuwait, NATO sign on information security agreement,” *Jane’s Defence Weekly*, 20 December 2006, p. 6; Bergin, “NATO eyes naval patrols to secure oil facilities.”

<sup>71</sup> Ministerial Declaration on Enhanced energy co-operation between the EU, the Littoral States of the Black and Caspian Seas and their neighboring countries, Astana, 30 November 2006, pp. 2, 6, 8-10, <[http://ec.europa.eu/dgs/energy\\_transport/international/regional/caucasus\\_central\\_asia/memorandum/doc/mou\\_azerbaijan\\_en.pdf](http://ec.europa.eu/dgs/energy_transport/international/regional/caucasus_central_asia/memorandum/doc/mou_azerbaijan_en.pdf)> (access 13 July 2007); Memorandum of Understanding on co-operation in the field of energy between the European Union and the Republic of Kazakhstan, Draft Version, 14 November 2006, pp. 2-3,

An obvious region where both organizations could join forces to combine their respective strengths is Africa.<sup>72</sup> Africa is a high priority for Europe not least since the adoption of the EU-Africa Partnership on Infrastructure and the proposal for a comprehensive Africa-Europe Energy Partnership.<sup>73</sup> NATO has provided support for operations in Darfur, and the African Union (AU) is interested in a memorandum of understanding on peacekeeping issues.<sup>74</sup> NATO and the EU could thus think about how to bolster existing and establish new local security and military capabilities and capacities to address energy infrastructure security. Strengthening local forces is mutually beneficial as it helps guarantee local and international security of supply. A dialogue on this issue could be launched in the trilateral AU-NATO-EU format thereby including the IEF. Given the interests of Russia and China in African energy resources, these two important outside actors could be included as well.

- Stimulate mutual learning  
Exchange of lessons learned and best practice are powerful instruments to advance security/military capabilities in the field of infrastructure protection. Web-based information clearing houses could be established as a first step to exchange information. To this specific workshops and joint exercises could be added.
- Use security/Defense science and technology (S&T) programs for energy infrastructure security  
NATO and the EU maintain dedicated S&T institutions (NATO Research and Technology Organization, EU Joint Research Centers) and programs (NATO Security through Science Program, 7th Framework Research Program). Some of the existing activities directly address infrastructure security. Beyond specific programs, S&T in the fields of ICT security, situational awareness, command and control, human factors, detection and protection technologies, material science, and modeling and stimulation, to name but a few examples, can provide valuable insights. Therefore it should be analyzed how energy-relevant production and transit countries could be included in respective S&T projects. The EU in particular should analyze how research activities from the 7th framework research program – outside the “security” domain and beyond the focus on energy efficiency – could be used to advance energy infrastructure security in relation with Europe’s energy-rich neighbors.<sup>75</sup>

---

[http://ec.europa.eu/dgs/energy\\_transport/international/regional/caucasus\\_central\\_asia/memorandum/doc/mou\\_kazakshtan\\_en.pdf](http://ec.europa.eu/dgs/energy_transport/international/regional/caucasus_central_asia/memorandum/doc/mou_kazakshtan_en.pdf) (access 13 July 2007).

<sup>72</sup> A similar approach for Central Asia could be possible, thereby using the EAPC and the OSCE as “antennas” to reach into the region.

<sup>73</sup> Interconnecting Africa: the EU-Africa Partnership on Infrastructure, COM(2006) 376, Brussels, 13 July 2006, p. 19, [http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006\\_0376en01.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0376en01.pdf) (access 13 July 2007).

<sup>74</sup> Background telephone interview with NATO official, 30 November 2006.

<sup>75</sup> Seventh Framework Program of the European Community for research, technological development and demonstration activities (2007-2013), Decision No 1982/2006/EC of the European Parliament and of the Council, 18 December 2006, OJ L 412, 30. December 2006, pp. 1-41, [http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l\\_412/l\\_41220061230en00010041.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_412/l_41220061230en00010041.pdf) (access 17 January 2007). The security and defense technology dimension is missing in the European strategic energy technology plan, which is part of the new energy policy for Europe. An Energy Policy for Europe, COM(2007) 1, Brussels, 10 January 2007, pp. 15-16,

One of the most obvious candidates is the European Galileo program, which can be used to provide real-time surveillance of energy networks.<sup>76</sup> Given Europe's dependence on energy resource imports, Galileo services should be expanded to cover the most important production and transit countries as well. An agreement with Norway, Europe's no. 2 gas supplier, is being drawn up and discussions with Saudi Arabia are underway.<sup>77</sup> To this list Russia and Algeria should be added as soon as possible, and cooperation with other African and Central Asian countries could follow in the future.

#### *9.2.5. Recommendation: Look more closely at beneficial contributions of private security contractors*

The debate about the role of private security contractors in international politics has intensified. The risks involved with contracting private security services and therefore the need to oversee and regulate this business is at the heart of the debate. By contrast positive contributions by private security contractors tend to be overlooked.

Private security contractors also provide services in the energy sector.<sup>78</sup> The main focus is on liaison between international oil and gas companies and national security agencies in order to harmonize security plans and arrange support.<sup>79</sup> In addition, they also engage with local communities, in particular to prevent conflicts from escalating. Private security contractors help train local forces and thus support the establishment of local security capacities. Furthermore private security contractors provide technical advice and consulting for company security plans (e.g. physical security concepts, installation of surveillance tools, engineering advice), help set up plans and procedures for different security contingencies (e.g. evacuation plans) and provide travel security. In some cases private security contractors are also involved in managing local companies that offer local guards. Finally, private security firms also offer assistance to international organizations. International financial lenders, for instance, contract private security consultants for security audits of infrastructure projects.

This illustrative list of tasks illustrates that private security contractors can offer beneficial services that should be taken into account more properly. To this purpose, the following recommendations could be helpful:

---

<[http://ec.europa.eu/energy/energy\\_policy/doc/01\\_energy\\_policy\\_for\\_europe\\_en.pdf](http://ec.europa.eu/energy/energy_policy/doc/01_energy_policy_for_europe_en.pdf)> (access 31 July 2007).

<sup>76</sup> Priority Interconnection Plan, p. 12.

<sup>77</sup> Taking stock of the Galileo program, COM(2006) 272, Brussels, 7 June 2006, p. 9

<[http://ec.europa.eu/dgs/energy\\_transport/galileo/documents/doc/comm\\_pdf\\_com\\_2006\\_0272\\_en.pdf](http://ec.europa.eu/dgs/energy_transport/galileo/documents/doc/comm_pdf_com_2006_0272_en.pdf)> (access 13 July 2007).

<sup>78</sup> This paragraph builds on background interviews with PSC experts, 10 November 2006 and 13 December 2006.

<sup>79</sup> Private security contractors hardly work for national oil and gas companies with Saudi Arabia being one of the most notable exceptions. Hiring private contractors would raise sensitive questions with regard to the performance of public armed and security forces in the respective countries. In those cases where national oil and gas companies hire private security contractors, they work with the security forces of these companies, rather than with uniformed military of the respective country.

- Regulate division of tasks in security agreements

The division of tasks between private security actors working for international gas and oil companies as well as local security and armed forces should be properly defined in security agreements. To this purpose the field guidelines for joint security measures within the work area of the Tangguh LNG project in Indonesia, where BP is involved,<sup>80</sup> could serve as a role model. These guidelines outline precisely who is doing what in case of demonstrations inside and outside the work area, withdrawal of the security assistance unit, evacuation, dealing with criminal acts and request for other security partners, in particular the armed forces. Furthermore the field guidelines also foresee that intelligence is provided by the police.<sup>81</sup>

- Think about registration of private security contractors

Private security contractors working in energy resource extracting countries could be registered in order to monitor contractor behavior. Oversight could be provided by the regulatory body in charge of the security sector. Information should be shared with the home governments of the private security contractors. Countries of origin could take further legal action against these companies if needed. In addition, private security contractor work should be regularly audited by the contracting companies.<sup>82</sup> Whether contracting companies do this, could in turn be verified by the external auditors of the contracting companies and by international human rights organizations.

- Oversee adherence to standards and promote “name and shame”

Private security contractors willing to work for international oil and gas companies should demonstrate high standards with regard to respect for human rights and security services. To this purpose, adherence to the voluntary principles on security and human rights and demonstrating satisfactory levels of training could be basic requirements to be fulfilled by contracting companies.<sup>83</sup> As “name and shame” is a perfect approach to exert peer pressure, experience from oil and gas companies in hiring private contractors could be added to the public register for private security contractors.

- Incorporate private security training for local security forces in SSR

The contribution of private security contractors to train local security forces should be incorporated in SSR projects. To this purpose it could make sense to advance joint training courses for local state security forces, local private security personnel, security guards from companies and private contractors in order to advance a common understanding of the tasks to be met, the ways to accomplish these tasks and the capabilities and capacities needed to accomplish these tasks.

---

<sup>80</sup> Field Guidelines for Joint Security Measures within the Work Area of the Tangguh LNG Project. Letter of Joint Decree between Chief of the Regional Police of Papua and Executive VP Tangguh LNG, 16 April 2004, <[http://www.bp.com/liveassets/bp\\_internet/globalbp/STAGING/global\\_assets/downloads/T/Tangguh\\_Field\\_Guidelines\\_BP\\_Papaun\\_Police.pdf](http://www.bp.com/liveassets/bp_internet/globalbp/STAGING/global_assets/downloads/T/Tangguh_Field_Guidelines_BP_Papaun_Police.pdf)> (access 13 July 2007).

<sup>81</sup> Field guidelines for joint security measures within the work area of the Tangguh LNG project, pp. 15-19, 22.

<sup>82</sup> Voluntary Principles, “Five Year Overview and Company Efforts to Implement Specific Components of the Principles,” <<http://www.voluntaryprinciples.org/reports/2005/company-efforts-specific.php>> (access 13 July 2007).

<sup>83</sup> Ibid.

Such an integrated approach is at the heart of the Tangguh LNG security agreement.<sup>84</sup> A joint approach could also help harmonize and streamline SSR programs aimed at local capacity building through international organizations such as the EU, the United Nations, the OSCE or individual donor countries.<sup>85</sup>

■ Create a level playing field between local forces and PSC

There is a need to create a level playing field between private and public security forces. Therefore local armed forces and police forces should also comply with codes such as the voluntary principles on security and human rights and other standards deemed necessary for private security contractors. The international community should monitor government adherence to these principles and should make international aid contingent upon conformity with them.

Payment is an important issue to create the necessary transparency as the first step towards the level playing field. As in the case of the Tangguh LNG project it should be clearly stated when local security forces will get reimbursed from international oil and gas companies. These payments should be approved by the companies and the respective regulatory bodies of the local government. Furthermore, payments should be published.<sup>86</sup> In addition, it must be clear who employs the state's security forces and who pays their salaries. By considering salary rises and ensuring timely payment illicit bribery and side payments by companies for members of the local security forces could be contained.<sup>87</sup>

#### 9.2.6. Recommendation: Advance community relationship management

“Hard power” needs to be complemented by “soft power” approaches. These build on community relationship management in particular. The logic behind this approach, which has been implemented for the Tangguh LNG project and the Baku-Tbilisi-Ceyhan (BTC)<sup>88</sup> pipeline, is straightforward: by involving local communities in decision-making and guaranteeing security, local ownership is created. This in turn provides an incentive to create a resilient environment in order to ensure the longevity of infrastructure projects. In a certain sense, local communities can serve as the “first line of defense”, inter alia, by identifying potential sources of conflict and devising measures for non-violent conflict resolution. Furthermore, the engagement of local

<sup>84</sup> Field guidelines for joint security measures within the work area of the Tangguh LNG project, p. 26.

<sup>85</sup> This is also underlined by the audit report of the Tangguh security arrangement. See: Tony Ling and Gare A. Smith, *Human Rights and Security Monitoring Assessment and Peer Review of the Tangguh LNG Project* (Boston/Washington, DC: Foley Hoag, 2005), pp. 6, 20, 33-34

<[http://www.bp.com/liveassets/bp\\_internet/indonesia/STAGING/home\\_assets/downloads/t/tangguh\\_human\\_rights\\_security\\_assmnt\\_2005\\_Aug\\_05th.pdf](http://www.bp.com/liveassets/bp_internet/indonesia/STAGING/home_assets/downloads/t/tangguh_human_rights_security_assmnt_2005_Aug_05th.pdf)> (access 16 January 2007).

<sup>86</sup> <<http://www.bp.com/sectiongenericarticle.do?categoryId=9004771&contentId=7009147>> (access 13 July 2007).

<sup>87</sup> International Crisis Group, *The Swamps of Insurgencies: Nigeria's Delta Unrest* (Brussels: ICG, 2006), pp. 7-11; <[http://www.crisisgroup.org/library/documents/africa/west\\_africa/115\\_the\\_swamps\\_of\\_insurgency\\_nigeria\\_s\\_delta\\_unrest.pdf](http://www.crisisgroup.org/library/documents/africa/west_africa/115_the_swamps_of_insurgency_nigeria_s_delta_unrest.pdf)> (access 13 July 2007).

<sup>88</sup> BTC Security Concept, <<http://subsites.bp.com/caspian/BTC/Eng/Misc/Security%20Concept.doc>> (access 13 July 2007).



security forces also creates economic off-springs that can benefit communities in the immediate environment of infrastructure projects.<sup>89</sup>

In advancing community relationship management to the benefit of democratization and improved energy infrastructure security the following recommendations could be helpful:

- Use integrated community-based security as a role model  
The Tangguh LNG project has advanced the idea of integrated community-based security (ICBS), which has been lauded as “mold-breaking” by independent assessors.<sup>90</sup> ICBS rests on the principle of shared responsibilities to maintain security. Local communities, government bodies, security forces, and the company involved are all given a role in providing security and resolving conflicts. Integration also foresees a joint security assistance team consisting of the local police forces, company security personnel and even armed forces, in case they are needed. Operational command and control rests with the regional unit commander of the police. The military will take over only in case martial law has been declared.<sup>91</sup>
- Use “security committees” to advance interaction with local population  
It has been suggested to take integration one step further by establishing so called “security committees” consisting of local community leaders, representatives of the company security teams, private security contractors and local security forces. A security committee could “provide oversight for the community and local ‘eyes and ears’ for the project. It could also serve as a forum for emergency consultation and coordination, early warning, and crisis response.”<sup>92</sup>
- Think about harmonizing programs for local community capacity-building  
Capacity building for local communities is also at the heart of many international programs offered by the UN, the EU or the OSCE. These programs aim at netting the fabrics of civil societies in crises-prone and war-torn societies. Therefore it should be analyzed whether there is room for harmonization and cooperation between international community-building projects and programs launched for the specific purpose of energy-related projects. Activities aimed at providing forums for local population to make their voices heard or training programs to advance literacy and negotiation techniques could serve both goals and could thus be more closely coordinated.
- Advance best practice for the use of non-lethal weapons  
Finally, there is a need to address the equipment of local security forces. Non-lethal weapons play a key role as they serve the goal of deterring potential aggressors without some of the effects of lethal weapons. In addition, non-lethal

---

<sup>89</sup> See also: Voluntary Principles, “Five Year Overview and Company Efforts to Implement Specific Components of the Principles,” <<http://www.voluntaryprinciples.org/reports/2005/company-efforts-specific.php>> (access 31 July 2007).

<sup>90</sup> Ling/Smith, *Human Rights and Security Monitoring Assessment and Peer Review of the Tangguh LNG Project*, p. 15.

<sup>91</sup> Field guidelines for joint security measures within the work area of the Tangguh LNG project, pp. 7-9, 18.

<sup>92</sup> Ling/Smith, *Human Rights and Security Monitoring Assessment and Peer Review of the Tangguh LNG Project*, p. 6, 24.

weapons also play an increasing role in crowd and riot control and other tasks to be fulfilled in international stabilization operations. This could open the door for a fruitful exchange of information with NATO and EU countries. Some of the related questions are under study by the NATO Research and Technology Organization.<sup>93</sup>

#### 9.2.7. *Recommendation: Strengthen cross-border crises and consequence management*

Physical protection of energy infrastructure with public security forces is also a challenge within Europe. While EU member states have more or less clear national regulations, cross-border cooperation is a problem. This seems to have two reasons.

First, European approaches to civil protection did not evolve by design but followed a more incremental way. The Commission has established mechanisms to facilitate cooperation and has suggested legislative action that would help pool transportation capacities, provide more money for emergency reaction and improve early warning as well as coordination of intervention in third countries. Nevertheless member states are still reluctant to share sovereignty with the Commission in this area.<sup>94</sup>

In addition, cross-border cooperation to protect critical infrastructure poses significant challenges that remain to be addressed. Preliminary findings of the Vital Infrastructure Threats and Assurance project (VITA), sponsored within the EU preparatory action for security research, showed that that there is

- a lack of mutual understanding of each others crisis management systems and responsibilities,
- a lack of mutual understanding between private and public crisis management centers,
- not enough information about existing capabilities,
- not enough training on joint operations,
- long international and public-private consultation and reaction cycles, and
- a lack of permit for power line maintenance workers to work in other nations.<sup>95</sup>

This makes it clear that Europe's single market for gas and electricity misses adequate cross-border emergency management procedures. This leads us to suggest the following recommendations:

- Advance situational awareness through Common Operational Pictures (COP)  
Emergency management depends on situational awareness and situational understanding. To this purpose COPs provided by situation centers are key. Given

---

<sup>93</sup> <<http://www.rta.nato.int/Pubs/RDP.asp?RDP=RTO-TR-SAS-040>> (access 17 January 2007).

<sup>94</sup> Magnus Ekengren, Nina Matzen, Mark Rhinard and Monica Svantesson, "Solidarity or Sovereignty? EU Cooperation in Civil Protection", *European Integration*, 28:5 (December 2006), pp. 457-476, here pp. 468-473; Establishing a Community civil protection mechanism (recast). Proposal for a Council Decision, COM(2006) 29, Brussels, 26 January 2006, pp. 7-11, <[http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006\\_0029en01.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0029en01.pdf)> (access 13 July 2007).

<sup>95</sup> Eric A.M. Luijff, "The VITA Project: Results and Recommendations," Paper prepared for the 4th EAPC/PfP Workshop on Critical Infrastructure Protection and Civil Emergency Planning, Zurich, 24-26 August 2006, pp. 5-7.

the complexity of the energy sector, there is a need for COPs integrating information from private energy companies and network operators as well as public information from police forces and other emergency responders, armed forces and intelligence services. The establishment of an overall public-private energy sector COP will be challenging. As a first step towards this goal an “operational COP” between public and private situation/operation centers should be created within and between countries. The 7th EU framework research program<sup>96</sup> and NATO activities, in particular within the Allied Command Transformation, could be used to establish these COPs.

- **Adopt bi-/multilateral prearrangements for cross-border emergency support**  
As long as an overall European framework for cross-border infrastructure protection support is lacking, there is a need for bilateral or multilateral prearrangements.<sup>97</sup> As a minimum requirement these prearrangements should be commensurate with Europe’s Priority Interconnection Plan in order to make sure that cross-border emergency management for these projects is adequate.
- **Promote joint exercises**  
Cross-border public-public, public-private, and private-private interaction in the field of energy infrastructure security should be advanced by joint exercises. In some countries there are regular civil protection/homeland security exercises that also involve the energy sector. Building on these and other experiences bi-national and multinational exercises should be launched. In doing so, the Euro-Atlantic Disaster Response Coordination Cell (EADRCC) should be involved as well in order to train interaction with NATO’s civil emergency mechanisms.
- **Include emergency assistance for infrastructure security into EU external energy relations**  
External energy relations between the EU and neighboring countries should also include provisions for cross-border emergency assistance in the field of energy infrastructure security. These provisions should also include an assessment of local capabilities available for emergency management in these countries. NATO could support this endeavor. Recently, the Alliance has adopted a memorandum of understanding within the EAPC framework that shall provide faster and more efficient assistance for the provision of humanitarian assistance in response to disasters.<sup>98</sup>
- **Address reimbursement for private companies**  
While current civil protection mechanisms within the EU foresee compensation for government support, reimbursement for private actors providing cross-border support seems to be lacking. Given the increasing trend towards cross-border joint

---

<sup>96</sup> The security section of the 7th framework program addresses the security of infrastructures and utilities and security systems integration, interconnectivity, and interoperability. Seventh Framework Program of the European Community for research, technological development and demonstration activities (2007-2013), p. 27.

<sup>97</sup> Luijff, “The VITA Project: Results and Recommendations,” p. 5.

<sup>98</sup> Press Release (2006)109, 13 September 2006, <<http://www.nato.int/docu/pr/2006/p06-109e.htm>> (access 31 July 2007)

ventures and mergers in the energy sector, there seems to be a need to “override normal competitive business models in case of an emergency.”<sup>99</sup>

#### Authors

Heiko Borchert ([hb@borchert.ch](mailto:hb@borchert.ch)) directs a business and political consultancy in Switzerland and is member of the advisory board of IPA Network International Public Affairs. He has worked with different military and national security organizations in Switzerland, Austria, and Germany on issues like scenario-based security policy planning, security sector evaluation, homeland security, defense science and technology, and energy security. Heiko studied international relations at the University of St. Gallen, Switzerland, where he also received his Ph.D.

Karina Forster ([contact@ipa-international.org](mailto:contact@ipa-international.org)) directs IPA Network International Public Affairs Network, a Berlin-based consultancy focusing among other things on defence and security, energy, and trade. Prior to joining IPA, Karina worked for US consultancies, the European Parliament, the European Commission and the German Bundestag. She studied international relations at the London School of Economics, Columbia University and the University of Maryland.

---

<sup>99</sup> Luijff, “The VITA Project: Results and Recommendations,” p. 7.