

FIVE DIMENSIONS OF HOMELAND AND INTERNATIONAL SECURITY

ESTHER BRIMMER, EDITOR

The book considers the intersections between homeland and international security and the implications of these connections for preparedness. After the terrorist attacks of September 11, 2001, many analysts abandoned traditional strategic tools, such as deterrence and dissuasion, arguing that a new era had begun in which such mechanisms were no longer relevant. Yet policymakers need to consider a range of effective actions to enhance preparedness. The possibility of catastrophic, high consequence events demands that policymakers go beyond piecemeal extensions of current policies or stovepiped approaches to specific challenges and devise comprehensive defense-in-depth. They could develop policy in "5D" – by integrating new approaches to five dimensions of policy: deterrence, dissuasion, denial, diplomacy and defense. The 5Ds could contribute to a more resilient society by giving policymakers ways to work with others to influence the international context to support homeland security. Each of the 5Ds suggests ways to "project resilience" with others abroad as we build resilience at home. The book addresses these themes with chapters by:

Heiko Borchert
Esther Brimmer
M. Elaine Bunn
Bruce Davis
Sean E. Duggan
Karina Forster
Daniel Hamilton
Lawrence J. Korb
James H. Lebovic

Charles D. Lutes
Jennifer Machado
Tamara Makarenko
Sir David Omand
Chantal de Jonge Oudraat
Robert Quartel
Amy Sands
Jonathan Stevenson

The Center for Transatlantic Relations engages international scholars, students, government officials, parliamentarians, journalists, business executives and other opinion leaders on contemporary challenges facing Europe and North America. The goal of the Center is to strengthen and reorient transatlantic relations to the dynamics of a globalizing world. It is an integral part of the Paul H. Nitze School of Advanced International Studies (SAIS), one of America's leading graduate schools devoted to the study of international relations. Center activities include seminars,

policy study groups and research projects, media programs and web-based educational and policy efforts. The Center also serves as the coordinator for the American Consortium on European Union Studies (ACES), which is a partnership among five national-capital area universities—American, George Mason, George Washington, Georgetown and Johns Hopkins—to improve understanding of the European Union and U.S.-EU relations. The Consortium has been recognized by the European Commission as the EU Center of Excellence in Washington, D.C.



JOHNS HOPKINS
UNIVERSITY



Mixed Sources
Product group from well-managed
forests, controlled sources and
recycled wood or fiber
Cert no. SW-COC-2062
www.fsc.org
© 1996 Forest Stewardship Council

ISBN: 978-0-9801871-0-6

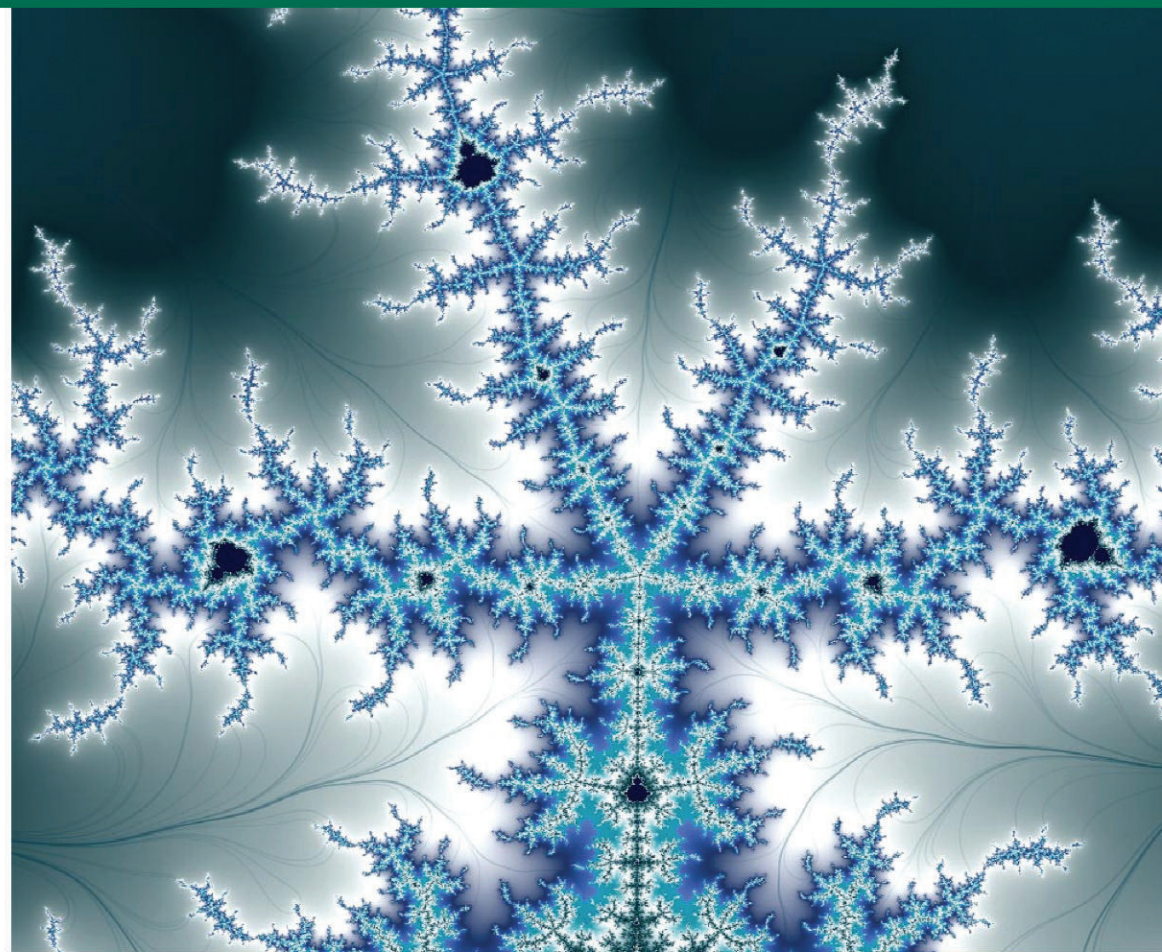


CENTER FOR TRANSATLANTIC RELATIONS

FIVE DIMENSIONS OF HOMELAND AND INTERNATIONAL SECURITY

ESTHER BRIMMER, EDITOR

C-T-R



FIVE DIMENSIONS OF HOMELAND & INTERNATIONAL SECURITY

ESTHER BRIMMER, EDITOR

**Five Dimensions of Homeland
and International Security**

Edited by

Esther Brimmer

Brimmer, Esther, ed., *Five Dimensions of Homeland and International Security* (Washington, D.C.: Center for Transatlantic Relations, 2008).

© Center for Transatlantic Relations, The Johns Hopkins University 2008

Center for Transatlantic Relations
The Paul H. Nitze School of Advanced International Studies
The Johns Hopkins University
1717 Massachusetts Ave., NW, Suite 525
Washington, D.C. 20036
Tel. (202) 663-5880
Fax (202) 663-5879
Email: transatlantic@jhu.edu
<http://transatlantic.sais-jhu.edu>

ISBN 10: 0-9801871-0-9

ISBN 13: 978-0-9801871-0-6

This publication is supported in part by the U.S. Department of Homeland Security through a grant (N00014-06-1-0991) awarded to the National Center for Study of Preparedness and Critical Event Response (PACER) at the Johns Hopkins University. Any opinions, findings, conclusions or recommendations expressed in this publication are those of the author(s) and do not represent the policy or position of the U.S. Department of Homeland Security.

Cover Image: In mathematical fractals, images display the same characteristics at different scales. Similarly, there may be connections among security issues although they occur at different levels of “magnification” (local, national, international). Image used with permission of Dave Massey, available at www.free-background-wallpaper.com.

Table of Contents

Acknowledgements	v
Introduction: Five Dimensions of Homeland and International Security	1
<i>Esther Brimmer and Daniel S. Hamilton</i>	
Chapter 1	
The International Aspects of Societal Resilience: Framing the Issues	15
<i>Sir David Omand</i>	
Chapter 2	
Chemical Weapons Terrorism: Need for More Than the 5Ds	29
<i>Amy Sands and Jennifer Machado</i>	
Chapter 3	
Reviving Deterrence	43
<i>Jonathan Stevenson</i>	
Chapter 4	
Criminal and Terrorist Networks: Gauging Interaction and the Resultant Impact on Counter-Terrorism	57
<i>Tamara Makarenko</i>	
Chapter 5	
Dissuasion and the War on Terror: What is Meant by Dissuasion, and How Might It Apply to the War on Terror?	73
<i>Charles D. Lutes and M. Elaine Bunn</i>	
Chapter 6	
Trade Security: Stovepipes in Motion	85
<i>Robert Quartel</i>	

Chapter 7
**Deterrence and Homeland Security: A Defensive-Denial
Strategy Against Terrorists** 97
James H. Lebovic

Chapter 8
Creating a National Homeland Security Plan 109
Bruce Davis

Chapter 9
The Case for a New Guard Operational Model 119
Lawrence J. Korb and Sean E. Duggan

Chapter 10
**Homeland Security and the Protection of Critical Energy
Infrastructures: A European Perspective** 133
Heiko Borchert and Karina Forster

Chapter 11
**The Use of Economic Sanctions to Maintain
International Peace and Security and Combat
International Terrorism** 149
Chantal de Jonge Oudraat

About the Authors 175

About PACER 181

Chapter 10

Homeland Security and the Protection of Critical Energy Infrastructures: A European Perspective¹

Heiko Borchert and Karina Forster

Homeland security is about the nexus between new national and international security risks, the way our states prepare themselves to deal with these risks and the resulting political leeway. States that remain vulnerable at home cannot assume a global leadership role.

The European Union (EU) assumes to be a global player. Despite ongoing efforts to improve the national security of EU member states, the region remains vulnerable. There is no better issue to illustrate Europe's vulnerability than energy security in general and energy infrastructure security in particular.

EU member states are energy-import dependent and rely on the stability of those countries, that harbor energy resources and critical energy infrastructures. Extracting energy resources, refining and transporting them to consumer markets and distributing energy products depends on a functioning energy infrastructure. For example Europe transports 85 percent of its gas imports by pipeline.² This energy infrastructure becomes even more important as the EU tries to diversify its energy resource imports and turns to suppliers that are further away. Finally, the EU aims at establishing a common European market for gas and electricity. In this context the creation of a cross-border emergency management framework to deal with infrastructure-related incidents becomes indispensable but remains to be established.

¹ This paper was extracted from the authors' study on energy infrastructure protection commissioned by the Swiss Ministry of Foreign Affairs and does not necessarily reflect the official position of the Swiss government.

² Energy Sector Inquiry. DG Competition Report, SEC(2006) 1724, Brussels, January 10, 2007, p. 25.

There is thus a clear link between energy infrastructure security and European homeland security. So far, however, energy issues are a matter of competition and environmental policy, rather than security policy. This is a serious problem for Europe.

This paper argues that Europe's current competition-based approach is insufficient to address the homeland security tasks posed by energy infrastructure security. The EU should acknowledge that the global energy supply chain is dominated by power and monopolies that benefit producing countries rather than competition and market liberalization. Therefore the EU should engage in creating an appropriate international set up to address energy infrastructure security.

With regard to the regulatory environment, the EU should harmonize and further develop existing safety and security standards. These standards should also receive more attention when providing stimuli for energy infrastructure investments. Finally, the EU must back its soft power approach to energy security by credible hard power and improve cross-border emergency management for energy infrastructure-related incidents.

The paper starts with a brief outline of current European activities in the field of critical infrastructure protection (CIP). Then we portray energy infrastructure security as a European homeland security challenge. We conclude by submitting concrete proposals for EU action to advance energy infrastructure security.

Europe's Approach to Critical Infrastructure Protection

According to the European Commission critical infrastructures "consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States."³ The Commission has identified energy, nuclear industry, information and communication technologies, water, food, health, the financial sector, transportation, the chemical industry, space and

³ Critical Infrastructure Protection in the fight against terrorism, COM (2004) 702, Brussels, October 20, 2004, p. 3.

research facilities as critical infrastructure sectors.⁴ To advance their protection the Commission has proposed the European Program for Critical Infrastructure Protection, a directive for identifying European critical infrastructure, the creation of a new information network, funding alternatives, and new research opportunities.

- *European Program for Critical Infrastructure Protection (EPCIP)*
The Commission presented the EPCIP in December 2006 after two years of preparatory work. The EPCIP provides a methodology to identify European critical infrastructures. These are infrastructures “which are of highest importance for the Community and which if disrupted or destroyed would affect two or more Member States or a single Member State if the critical infrastructure is located in another Member State.”⁵ The EPCIP also includes an action plan and addresses the role of contingency planning and CIP cooperation with third countries.
- *Directive for European Critical Infrastructure*
The directive sets out criteria to identify European critical infrastructure. It is up to the member states to identify critical infrastructure on their own territory and outside their territory. Based on their compilation, the Commission will propose a list of European critical infrastructures.⁶ In addition, the directive asks member states to make sure that owners and operators of European critical infrastructure establish and update operator security plans.
- *Rapid Alert Information Exchange*
To complement existing networks for emergency management information exchange, the European Commission has proposed the critical infrastructure warning information network (CIWIN), “which could stimulate the development of appropriate

⁴ Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection, COM (2006) 787, Brussels, December 12, 2006, p. 21. In addition, many EU members also identify government structures and emergency responders as critical infrastructure sectors.

⁵ European Program for Critical Infrastructure Protection, COM (2006) 786, Brussels, December 12, 2006, p. 4.

⁶ It remains open, however, how genuine European aspects will be taken into account in this process.

protection measures by facilitating an exchange of best practices.” Right now, a team led by Unisys Belgium, which had won the contract,⁷ is conducting interviews in order to identify EU member states’ expectations *vis-à-vis* CIWIN.

- *Funding*

Under the program “Prevention, Preparedness and Consequence Management of Terrorism” the Commission provided €3.7 million in 2005 mainly for preparatory actions. On February 6, 2007 the Commission launched a new call worth €3 million for projects to enhance protection measures for critical infrastructure, risk mitigation strategies, the development of contingency plans or the development of common security standards.⁸

- *Research*

As part of the new 7th Research Framework Program⁹ security research has a dedicated CIP focus. In addition, other program areas such as information and communication technologies (e.g. intelligent infrastructures), energy (e.g. smart energy networks), transport (e.g. support for the European global satellite navigation system Galileo and EGNOS) or space (e.g. development of satellite-based and in-situ monitoring and early-warning systems) are relevant for CIP as well.¹⁰

Energy Security and European Homeland Security

Oil and gas are dominating Europe’s energy mix. In 2000, 38 percent of Europe’s primary energy needs were satisfied by oil and around 23 percent by gas. This is likely to change until 2030 when oil is expected to account for 34 percent and gas for 27 percent.

⁷ See: http://ec.europa.eu/justice_home/news/tenders/2006_S044_045852/invitation_tender_en.pdf <http://www.dgmarket.com/eproc/np-notice.do?noticeId=1512748>.

⁸ See: http://ec.europa.eu/justice_home/funding/epcip/funding_epcip_en.htm#.

⁹ 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, December 18, 2006, OJ L 412, December 30, 2006, pp. 14-27.

¹⁰ Before launching the 7th Research Framework Research the Commission used the Preparatory Action on Security Research to launch infrastructure relevant projects such as the VITA project (Vital Infrastructures Threats and Assurance) to analyze threats to and assurance and protection of highly networked infrastructures. See http://ec.europa.eu/enterprise/security/doc/project_flyers/766-06_vita.pdf.

More important, Europe's energy import dependence is projected to grow. In 2000 Europe imported around half its energy needs from abroad with Russia, Norway, North Africa and the Persian Gulf as the key suppliers. The spur in gas demand is very likely to increase gas import dependence from around 50 percent in 2000 to over 84 percent in 2030. By then 93 percent of Europe's oil demand will be satisfied by imports compared to about 76 percent in 2000.¹¹

The projected shift in Europe's energy mix towards increased gas demand has strategic consequences. On the one hand, it means that key gas suppliers such as Russia and Algeria, which have formed a strategic partnership in mid-2006 between Gazprom and Sonatrach, will gain in relative importance *vis-à-vis* oil suppliers and are likely to become Europe's most important gas suppliers. On the other hand, it can be speculated how the influence of these suppliers will affect the transatlantic partnership.¹²

The Complexity of Energy Infrastructure Security

Energy infrastructure security must 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 our model of analysis (Figure 1) makes clear several analytical dimensions need to be taken into account:

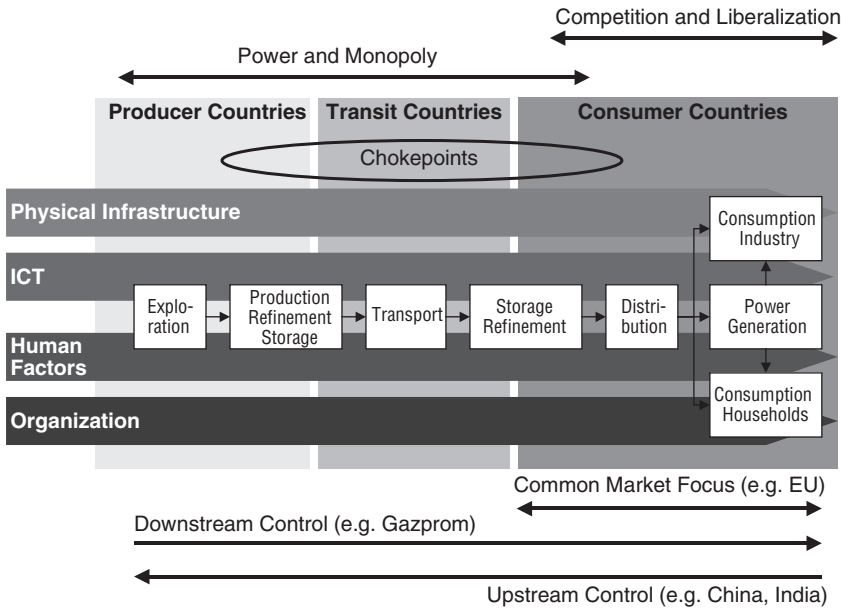
- *Energy Supply Chain*

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.¹³

¹¹ *European Energy and Transport. Trends to 2030—update 2005* (Luxembourg: Office for Official Publications of the European Communities, 2006), pp. 26-27.

¹² Belkin, Paul and Vince L. Morelli, *The European Union's Energy Security Challenges*, CRS Report RL33636 (Washington, DC: Congressional Research Service, 2007), p. 29.

¹³ Heal, Jeffrey et. al., "Interdependent Security in Interconnected Networks," in Auerswald, Philip E. 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.

Figure 1 Energy Infrastructure Security—Model of Analysis

- *Production, Transit, and Consumption Countries*

Energy infrastructures cross various countries and are thus subject to regulatory differences. 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.

Furthermore there is the crucial role of chokepoints, i.e. narrow geographic bottlenecks through which energy supplies are channeled. For example, 88 percent of all Persian Gulf oil exports need to pass the Strait of Hormuz.¹⁴ If the Strait is blocked, there are alternative routes, but delivery takes longer which increases supply costs.

¹⁴Jean-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.

- *Risks*

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. 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.

Analyzing energy infrastructure security on the basis of our model yields five distinct problems, which illustrate the complexity of this important homeland security task:

- *Power Asymmetry in the Supply Chain*

It is estimated that around 85-90 percent of the world's oil reserves fall under direct government control. Governments receive at least 45-90 percent 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 percent of world oil and 74 percent of world gas production, leaving the rest to corporate actors such as Exxon Mobil, Royal Dutch Shell, BP or Total.¹⁵

This means that the EU's competition-based regulatory approach 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

¹⁵ GAO, *International Energy: International Forums Contribute to Energy Cooperation with Constraints* (Washington, DC: GAO, 2006), p. 20; Harel, Xavier, "La pétro-politique rebat les cartes," *La Tribune*, June 12, 2006, p. 36; Shankelman, Jill, *Oil, Profits, and Peace. Does Business Have a Role in Peacemaking?* (Washington, DC: United States Institute of Peace Press, 2006), p. 40.

and India and the striving for downstream control followed by leading producers such as Gazprom.

- *Insufficient Network Management*

The European desire for “green energies” from renewable sources collides with existing network capacities. Wind power, for example, is hard to control. Overcapacity of power from wind parks can thus lead to critical power grid situations in particular in neighboring regions used to diverge surge capacities. So far investments and planning procedures are insufficient to tackle this problem, which means that inadequate network design can pose serious risks to energy infrastructures.

- *Manifold Vulnerabilities*

More attention needs to be paid to the security repercussions of deregulation. Stimulating competition can lead to cuts in reserve building, reduction of storage capacity and lower spending on training and maintenance.¹⁶ Furthermore, interdependencies between energy infrastructures and other critical infrastructures need much more attention. 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.¹⁷

- *Underinvestment*

The European Commission estimates that Europe needs to invest up to €1.8 trillion in its energy infrastructure until 2030 in order to meet the requirements of the common European market for gas and electricity. Around €310 billion are forecasted for investments in oil and gas infrastructure. Of the roughly €1.4 trillion needed for Europe’s electricity infrastructure around €900 billion alone are required for power generation.¹⁸

¹⁶ Thomas, Stephen and David Hall, *Restructuring and Outsourcing of Electricity Distribution in EU* (London: Public Services International Research Unit, 2003), p. 28; Buchan, David, “The Threat Within: Deregulation and Energy Security,” *Survival*, 44:3 (Autumn 2002), pp. 105-116, here p. 113.

¹⁷ E Luijff, Eric A. M., “SCADA: An Inroad to Critical Infrastructure Disaster,” Presentation to the 4th EAPC/PPF Workshop on Critical Infrastructure Protection and Civil Emergency Planning, Zurich, August 24-26, 2006.

¹⁸ EU Energy Policy Data, SEC(2007) 12, Brussels, January 10, 2007, p. 17.

The sums currently available are nowhere near these benchmarks. The European Investment Bank, for example, provides around €0.5-1 billion annually until 2013 for trans-European energy network projects.¹⁹ Whereas electricity transmission operators earned €334 million in 2005 from maintaining cross-border interconnectors, they have only reinvested €25 million between 2002 and 2005.²⁰

- *Regulatory Deficits*

Regulatory deficits result from the lack of a common regulatory area for energy infrastructure security and from power asymmetries. Europe, it is said, is a world-leading gas consumer and could thus influence producers. But as long as European countries prefer bilateral agreements with key suppliers it will not be possible to leverage European buying power. Furthermore, the quest for downstream control by leading producers poses the risk of interference of foreign actors into national and European critical energy infrastructures. So far there seems to be a regulatory hole for dealing with foreign companies investing in Europe's critical infrastructures. The problem needs to be solved on a national basis which opens the door for diverging approaches.

Current European Energy Regulation

Energy infrastructure-related aspects were addressed before the above mentioned directive was proposed. Based on the key directives launched in the second half of the 1990s to establish common rules for the internal market in electricity and natural gas two directives in particular addressed measures to safeguard security of natural gas supply as well as electricity supply and infrastructure investments.²¹

¹⁹ EIB, *EIB Financing of the Trans-European Networks* (Luxembourg: EIB, 2006), p. 6.

²⁰ Kopp, Gudrun, "Grenzüberschreitende Stromnetze ausbauen," FDP im Deutschen Bundestag, Presseinformation Nr. 12, 5 January 2007.

²¹ Directive 2004/67/EC of the European Parliament and of the Council of 26 April 2004 concerning measures to safeguard security of natural gas supply, OJ L 127, April 29, 2004, pp. 92-96; Directive 2005/89/EC of the European Parliament and of the Council of January 18, 2006 concerning measures to safeguard security of electricity supply and infrastructure investment, OJ L 33, February 4, 2006, pp. 22-27.

In addition European energy associations also engage in defining safety and security regulations. For example, the Union for the Coordination of Transmission of Electricity (UCTE) has set up regulations for electricity transmission to be followed by the respective national associations, and Marcogaz has developed guidelines and performance indicators for pipeline integrity management systems (PIMS).²²

Overall, however, Europe's quest for energy security is not driven by security issues. In principle Europe's energy policy rests on competitiveness, environmental issues and security of supply.²³ In practice, the European Commission's emphasis on market liberalization is strongest. As of July 1, 2007 Europe's gas and electricity markets should be fully opened for competition, but EU member states are far from achieving this goal.²⁴

Examples of Critical European Energy Infrastructures

Transportation and energy are the first sectors for which the Commission proposed criteria to identify critical infrastructures. The document is confidential²⁵ and not available publicly. However, possible candidates for this list can be identified by approximation and could include:

- Projects of high-priority identified under the Priority Interconnection Plan to realize the common European market for gas and electricity (e.g. Nabucco pipeline);
- Interconnectors which link foreign energy supply infrastructures with the European network, for example in Belgium, the Netherlands, Poland or Slovakia;
- Intra-European interconnectors which link supply lines with intra-European transmission pipelines, for example between Slovakia and Austria or Slovakia and the Czech Republic;

²² For more information, see: <http://www.ucte.org>, <http://marcogaz.org>.

²³ A European Strategy for Sustainable, Competitive and Secure Energy. Green Paper, COM (2006) 105, Brussels, March 8, 2006, pp. 5-17.

²⁴ Prospects for the internal gas and electricity market, COM(2006) 841, Brussels, January 10, 2007.

²⁵ http://ec.europa.eu/dgs/energy_transport/security/infrastructure/index_en.htm.

- Oil refineries producing oil-based products which are key for European industry sectors and are not easily offset by other refineries;
- Liquefied natural gas (LNG) receiving terminal capacity which will be mainly concentrated in Spain and Italy. A growing portion of the new LNG terminal capacity under construction will be held by non-EU producers;²⁶
- Shipping capacity to deliver LNG to Europe (already today 25 percent of the total existing shipping capacity that serves European markets with LNG is held by Bonny Gas Transport, a 100 percent subsidiary of Nigeria LNG Ltd).²⁷

Possible Next Steps

There is a need for institutional reform to address energy infrastructure security at the global and at the European level. The International Energy Forum could provide a global umbrella to start discussing the issue, and the EU could appoint a special Coordinator as a focal point for activities in different policy areas. With regard to the regulatory framework there is a need to take stock of existing safety and security standards and to advance them commensurate with ongoing threat assessments and the needs of Europe's common energy market. Safety and security standards should also receive more attention when thinking about stimuli for energy infrastructure investments. Finally, energy policy and security and defense policy need to be brought together. The EU should address the potential role of hard power in energy infrastructure security and should step up its efforts to strengthen cross-border crises and consequence management for infrastructure-related incidents.

Create an Appropriate Institutional Setting

Although discussions on energy infrastructure security take place in different formats, there is no overall umbrella to bring the different work strands together. This void could be filled by the International

²⁶ Energy Sector Inquiry, p. 269-270.

²⁷ Ibid, p. 268.

Energy Forum (IEF) which involves 60 states and almost every relevant international organization.²⁸

Given the sensitivity of the subject matter confidence- and security-building by exchanging information is key. This could be the starting point for the IEF, inter alia, by looking at different definitions of and approaches to energy infrastructure security, debating responsibilities and competencies of state and private actors, comparing existing safety and security standards, conducting joint risk assessments and discussing possible joint approaches to identify and protect critical energy infrastructures with cross-border impact.

To complement this global approach the EU should appoint a European Energy Infrastructure Security Coordinator.²⁹ The new Coordinator would have to raise awareness, create a trustworthy environment for information exchange, stimulate dialogue among public and private actors, serve as a point of contact, identify best practices, coordinate safety and security activities in the energy sector, and make sure that the issue receives the necessary attention as a cross-sector item in Europe's different policy areas.

As a first priority the new Coordinator should focus on European critical energy infrastructures identified in the EPCIP framework. 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 and should mirror IEF activities.

Take Stock of Existing Safety and Security Standards

The lack of common energy infrastructure safety and security standards along the energy supply chain is a problem for cross-border energy flows. As a first step to solve this problem, an overview of existing national and international safety and security standards should be compiled in order to identify needs for action.

²⁸ For more on this, see: Borchert, Heiko and Karina Forster, "Energy Infrastructure Security: High Time for a Networked Public-Private Governance Approach," *Middle East Economic Survey*, 50:21 (May 21, 2007), pp. 32-36.

²⁹ This builds on the idea of European coordinators for key European infrastructure projects. See: Priority Interconnection Plan, COM(2006) 846, Brussels, January 10, 2007, p. 10.

In this context safety and security standards for priority infrastructure projects that connect Europe with key supply regions or provide major intra-European interconnections should be scrutinized. Performance requirements will need to be discussed with the respective production and transit countries and companies involved. If these requirements cannot be met, European financial or technical assistance may be required.

In addition, mutual interdependencies between the energy sector and other critical infrastructure sectors such as ICT and transportation need to be addressed. Following the assessment of these critical interdependencies it will be important to identify what should be done at the international, regional, and national, and sub-national levels and how responsibilities and tasks should be shared between public and private actors.

Finally, there is a need to deal with ICT safety and security standards, in particular for Supervisory Control and Data Acquisition systems (SCADA) used in the energy sector. Given the lack of awareness of SCADA problems, there is a need to identify and document best practices and to standardize safety and security norms. This could be done, for example, by conferences and publications launched by the European Energy Infrastructure Security Coordinator.

Pay More Attention to Safety and Security in Europe's Regulatory Framework for Infrastructure Investments

A regulatory framework for energy infrastructure investments that takes into account safety and security spending requires market-based incentives for increased spending in combination with monitoring and regulatory oversight.

Market-based stimuli could include tax incentives for safety and security investments, preferential deduction of safety and security investments during the life-cycle of an infrastructure project, or tax incentives for research and development into infrastructure safety and security technologies. The level of these incentives should be commensurate with energy infrastructure risk assessments. This helps avoid that incentives are tilted away from safety and security towards other purposes when threats vanish.

Safety and security spending needs to be monitored. This could be done by the European Commission (for European critical energy infrastructure projects) or by national energy market regulators. Possible investment categories that should be tracked could include new investments, spending on operation and maintenance, recruitment, training, safety and security in general, ICT safety and security in particular, and life extension upgrades.

As safety and security matters along the supply chain, the EU should consider how these ideas could be addressed as part of Europe's external energy dialogue with production and transit countries. For example programs such as the EU-Africa Partnership on Infrastructure Initiative and overseas development aid could be targeted more directly at energy infrastructure safety and security.

Address the Role of Hard Power in Energy Infrastructure Security

So far, hard power plays no role in Europe's energy policy. NATO, by contrast, has engaged in dialogue with oil and gas producing companies and countries about how the alliance could help provide energy infrastructure security and has identified critical infrastructure protection as a future task for NATO forces.³⁰

Military capabilities relevant for homeland security can also advance energy infrastructure security. This is true for intelligence gathering and assessment or surveillance for example with unmanned aerial vehicles, networked sensor applications or radar systems. In addition, armed forces could help provide physical protection of infrastructures and support the stabilization of areas in which infrastructures are situated. Passive and active electronic warfighting capabilities could be used to assure ICT security. Finally, armed forces could provide emergency assistance in case an infrastructure-related incident involves the use of weapons of mass destruction.

First of all, the EU should bring in line its ambitious external energy policy agenda with the European Security and Defense Policy

³⁰ Bergin, Tom, "NATO Eyes Naval Patrols to Security Oil Facilities," *The Scotsman*, May 14, 2007. Available at: <http://news.scotsman.com/latest.cfm?id=748442007>; Comprehensive Political Guidance, endorsed by NATO Heads of State and Government on November 29, 2006, Para. 16(c). Available at: <http://www.nato.int/docu/basicxt/b061129e.htm>.

(ESDP). The Long-Term Vision which outlines future capability requirements for EU armed forces only makes very general references to energy security.³¹ However, as long as there are no explicit energy infrastructure related requirements, possible tasks for the armed forces will not enter national capability planning. The EU should thus address potential ESDP contributions to energy infrastructure security and adapt existing scenarios for the European Headline Goal 2010.

The EU and NATO could advance energy infrastructure security through joint science and technology projects involving key energy production and transit countries. Joint projects would be most suitable in the fields of ICT security, situational awareness, command and control, human factors, detection and protection technologies, material science, and modeling and simulation.

Regional military cooperation with key partners in the Greater Middle East, the Caucasus and in Central Asia should be envisaged as well. Both organizations have outreach programs that help advance dialogue with these regions. Together they could launch regional military training programs designed to bolster local security and military capabilities for energy infrastructure security tasks. Given the strategic interests of Russia and China in energy security, thought should be given as to how these countries could be involved as well.

Strengthen Cross-Border Crises and Consequence Management

Cross-border cooperation to protect critical infrastructures in Europe suffers from the lack of mutual understanding of each other's crisis management systems and responsibilities, information about existing capabilities, training on joint operations, and mutual understanding between private and public crisis management centers.³²

Emergency management depends on situational awareness and situational understanding. To this purpose a common energy sector operation picture (COP) could provide an information umbrella for

³¹ European Defense Agency, *An Initial Long-Term Vision for European Defense Capability and Capacity Needs*, October 3, 2006, Para. 11.

³² Luijff, Eric A. M., "The VITA Project: Results and Recommendations," Paper prepared for the 4th EAPC/PfP Workshop on Critical Infrastructure Protection and Civil Emergency Planning, Zurich, August 24-26, 2006, pp. 5-7.

private energy companies and network operators as well as police forces, other emergency responders, armed forces and intelligence services. It would make sense to start building such a COP in those European countries where cross-border exchanges of energy flows are highest and which are thus key for the common European energy market.

Furthermore there is a need for bi- and multilateral pre-arrangements for cross-border emergency support that allows for the mutual exchange of aid among public and private actors of different countries. This interaction needs to be trained in advance. To this purpose the European Commission, for example in cooperation with the Euro-Atlantic Disaster Response Coordination Cell (EADRCC), could establish a joint exercises agenda. In all of these activities key external energy partners of the EU should be included.