

Energy Infrastructure Security Time for a Networked Public-Private Governance Approach

Heiko Borchert and Karina Forster

Energy security is about guaranteeing the availability of affordable energy resource supplies. Given the energy import dependence of most consumption countries in North America, Europe and East Asia, energy security has become a strategic concern.

In 2000, Europe for example imported around half of its energy needs from abroad, with Russia, Norway, North Africa and the Persian Gulf being the most important supply regions. European import dependence is likely to grow to 80 % for gas and around 88 % for oil until 2030. Furthermore, Europe imports roughly 85 % of its gas by pipeline and thus depends on geopolitical stability in production and transit countries. Other consuming areas such as East Asia depend on the security of critical chokepoints such as the Strait of Hormuz or the Strait of Malacca.

Energy security is thus not possible without guaranteeing the security of the energy infrastructure and stabilizing the broader environment in which energy infrastructures are embedded. However, the current international institutional setting is not ready to deal with the challenge of energy infrastructure security. We argue that it is high time to bring all relevant stakeholders from production, transit and consumption countries together in a public-private network to advance energy infrastructure security. To this purpose, the International Energy Forum could be used as an umbrella organization. Production and consumption countries could capitalize on their downstream responsibility by helping to create a resilient international energy supply chain.

We develop our argument in three steps. First we briefly address the need for a holistic and networked approach to energy infrastructure security. Then we outline the possible role of the International Energy Forum as central nod of an international energy infrastructure security network. Finally, we present four areas for international cooperation to advance energy infrastructure security.

Energy infrastructure security and the need for networked governance

Energy infrastructure security requires a holistic approach that looks at ends, ways and means to detect and explore energy resources and to refine, store, transport and distribute the relevant products. In doing so, energy infrastructure security must cover the whole supply chain from production and transit countries to the target markets where energy resources are needed. Furthermore several risks that can endanger the proper functioning of the energy infrastructure need to be taken into account. The most important risk factors are

- tangible properties (i.e. physical security),
- security of information and communication technology (ICT),
- human factors (e.g. negligence, deliberate attacks against infrastructures)
- organizational aspects (e.g. interaction between public and private actors for emergency response, negative impact of outsourcing on energy infrastructure maintenance).

Energy infrastructure security thus is a perfect example of modern security challenges that defy easy solutions. Energy infrastructure security crosses not only the boundaries of a single nation or a region, it also transcends the responsibilities of national ministries and international organizations and requires close interaction with non-state actors such as national and international oil and gas companies.

In short, energy infrastructure security requires a networked governance approach. Reference to the network describes the need for close interaction between public and private actors at national and international levels throughout all states of the supply chain. Governance depends on the ability of these actors to make and implement policy regarding energy infrastructure security. This, in turn, requires a common understanding of the challenge and rules and procedures to deal with energy infrastructure security.

The International Energy Forum could play a key role

The problem is that today's institutional setting at national and international levels is hardly adequate to bring together the different strands that reach from foreign policy to competition and financial policy, science and technology as well as environmental issues to security and defense policy. Therefore a new institutional setup is needed. However, nothing is more difficult than creating new international organizations. Hence a networked approach could build on existing institutions and make sure that these institutions are properly linked in order to coordinate relevant activities. We believe that the International Energy Forum (IEF) would be ideally positioned to serve as a nod of a new energy infrastructure security network.

The IEF involves 60 states and almost every relevant international organization. Only links to NATO and the Organization for Security and Cooperation in Europe are missing. Furthermore, the IEF also reaches into the business world. With this set up the IEF could provide an umbrella to discuss the different facets of energy infrastructure security. Concrete action that might follow these debates and would require specific decision-making could then be dealt with by the different international organizations participating in the IEF.

As energy infrastructure security is a sensitive matter, confidence- and security-building by exchanging information is key. Information gathering and exchange about basic questions could thus be a starting point for the IEF. The list of issues to be addressed could include:

- Definition of and approaches to energy infrastructure security (IEF-sponsored 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 under the IEF umbrella 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)
- Identification of lessons learned from different national protection strategies
- Identification of international needs for action, for instance with regard to providing regulatory incentives to simulate investments, improve protection and modes of interaction to smoothen public-private cooperation

Suggestions for possible next steps

Against the background of this general list we believe that four areas could be identified to initiate energy infrastructure security cooperation: safety and security standards, investment incentives, the role of national oil and gas companies, and the possible role of armed forces.

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. In doing so, three aspects will be important:

- First, safety and security standards for those priority infrastructure projects that guarantee the supply of energy resources from production and transit countries to key target markets should be scrutinized. From a European perspective, some of these projects fall under the Priority Interconnection Plan. This plan identifies projects that are of European interest such as the GALSI pipeline linking Algeria and Italy or various gas connections between Central and South East Europe and the Caspian Sea countries and the Middle East. Performance requirements will need to be discussed with the respective production and transit countries. If they cannot be met, European financial or technical assistance may be required.
- Second, mutual interdependencies between the energy sector and other critical infrastructure sectors such as information and communication and transportation need to be addressed. In this regard maritime transportation security will be a key issue in particular for LNG supplies which are likely to increase in the future. Following the assessment of these critical interdependencies it will be important to identify what should be done at international, regional and 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. Reports indicate that SCADA information security lags five to ten years behind general information security since most protocols were developed for a non-hostile environment. This and other difficulties are aggravated by the lack of awareness of SCADA problems. This raises the 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. This could serve as a model for similar initiatives under the auspices of the IEF.

Investments and safety and security spending

Current underinvestment in the energy-supply infrastructure mainly results from low oil prices in the past. Low prices have led producing countries and companies to refrain from investments. Today the lack of adequate energy infrastructure has become a security risk of its own. According to the 2006 IEA World Energy Outlook the cumulative investment need in the global energy-supply infrastructure is more than \$20 trillion until 2030. Of this roughly \$4 trillion are needed in the oil sector.

At the same time there is a growing trend towards rivaling energy investments. As market prospects for LNG are said to look promising, many companies and producing countries are investing in this field. Between 2000 and 2005 around \$90 billion were invested globally, but more than \$275 billion are projected to be invested in the next five years. This will most

likely lead to crowding out effects at the expense of investment needed to beef up existing capacities in the gas sector.

When thinking about the design of regulatory frameworks to stimulate energy infrastructure investments, safety and security spending should receive more attention. How and to what extent incentives for safety and security spending will be granted has direct implications for the competitiveness of national markets and oil and gas companies. Therefore, three issues should be addressed:

- First, incentives for safety and security investments should be market-based and commensurate with risk assessments. 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 when threats vanish incentives are tilted away from safety and security towards other purposes.
- Second, there is a need to monitor safety and security spending. Building on the IEF experience with the Joint Oil Data Initiative (JODI) it should be considered whether the IEF Secretariat, for example in cooperation with the IEA, could assume the role of a clearing house. 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 upgrades (e.g. for life extension). Ultimately, investment monitoring depends on the oil and gas companies' readiness to disclose investment plans. Here the International Energy Business Forum could be used to achieve consensus on how to strike a balance between the need to protect company data for reasons of competition and assure investment transparency required to advance safety and security.
- Finally, compensation for safety and security spending in production and transit companies should also be part of the external energy relations of consumption countries. The EU, for example, should go beyond the provision of funds for energy infrastructure projects that are of direct importance to its members only. Among other things thought should be given to the use of development aid to advance energy infrastructure safety and security, science and technology cooperation and the provision of safety- and security-relevant services such as space-based infrastructure monitoring by Galileo that could help shoulder the burden with production and transit countries.

Role of national oil and gas companies

State-owned and state-sponsored oil and gas companies control access to oil and gas reserves and dominate the production. This not only gives them monopolistic power. Rather it also puts the main responsibility for safety and security of the energy supply chain into their hands. Getting these companies to jointly address safety and security issues could provide major benefits for production and transit countries. By actively engaging in the debate about energy infrastructure safety and security these countries could portray themselves as responsible suppliers that engage with consumption countries. This in turn could make it easier to find commercial partners that provide know-how, technology and funds.

Most importantly, national oil and gas companies could play a crucial role in advancing energy infrastructure safety and security in other production and transit companies. As Valerie Marcel has observed in her study *Oil Titans* the engagement of national oil and gas companies is more palatable in certain regions than engagement of commercial companies. This could provide a window of opportunity to advance the exchange of best practice among na-

tional oil and gas companies via the IEF. In doing so, information exchange could be complemented by lessons learned from commercial players and from other companies. ICT companies could provide insights in how to protect the cyber dimension of the energy infrastructure, and defense companies could offer insights about physical protection and infrastructure surveillance.

Furthermore closer dialogue with national oil and gas companies is also needed when it comes to public-private task and revenue sharing with regard to energy infrastructure safety and security. It is no secret that revenue models that ask for more than 80 % of the earnings to be transferred from international to national oil and gas companies question the economic rationality of energy infrastructure projects. These revenue models also inhibit private investments to the detriment of energy infrastructure security.

Therefore alternative revenue models that allow for revenue sharing commensurate with task sharing should be considered. It could be argued that when national oil and gas companies shoulder the main burden of energy infrastructure security they should also get the lion's share of the revenues. If international oil and gas companies are prepared to invest in infrastructure safety and security, they should benefit from respective incentives. In these cases, for example, it might be feasible to set up flexible revenue sharing models that increase the private companies' share in relation to their infrastructure investments.

Hard power security provision

Finally, it should be recognized that energy infrastructure security also has a hard power dimension. Military capabilities can be used to protect energy infrastructure and to stabilize the broader environment. Right now the issue is somewhat controversial. On the one hand policymakers do not want to "militarize" the discussion about energy security. On the other hand the fact that certain countries, that are militarily engaged in the Greater Middle East, are also members of NATO could make it difficult for states in the region to cooperation with the Alliance.

However, it should be acknowledged that military capabilities that help bolster energy infrastructure security are also useful to provide regional stability for instance on the African continent or in the Greater Middle East. This is especially true for intelligence gathering and assessment to improve energy infrastructure risk assessments; surveillance of energy infrastructure by unmanned aerial vehicles, networked sensors or radar system and protection of energy infrastructure which could benefit, inter alia, from air defense or ground-based defense systems. Therefore closer military dialogue between countries of energy production, transit and consumption could serve the dual purpose of advancing energy infrastructure security and bolstering local capabilities for crisis management in contested production and transit regions.

Initial military contacts with energy-relevant production and transit countries have been established via the NATO and EU Mediterranean Dialogue and the NATO Istanbul Cooperation Initiative. This network, however, is not enough. By engaging NATO, the EU and the IEF a more comprehensive platform could be created. Therefore the IEF and its participating states and organizations should think about establishing liaison with NATO, as the EU already takes part.

To start with the military dialogue could include the exchange of lessons learned and best practice about military assistance in the field of energy infrastructure security. This could include discussions about doctrines and training for the respective tasks. Furthermore NATO and the EU could open their defense and security science and technology programs to include energy-relevant production and transit countries. Science and technology cooperation in 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 –

could provide valuable insights. Finally, joint exercises could help engage in real-life activities and identify interoperability problems.

Dr Heiko Borchert is a member of the advisory board of Berlin-based IPA Network International Public Affairs, and Karina Forster is the organization's Managing Director. This article was extracted from their study on energy infrastructure security commissioned by the Swiss Ministry of Foreign Affairs and does not necessarily reflect the official position of the Swiss government. The authors can be reached at contact@ipa-international.org.