18. Critical energy system infrastructure protection in Europe and the legitimate economy

Kevin Rosner

I. Introduction

On 14 August 2003 there was a catastrophic breakdown in the transmission of electricity in North America, affecting at least 50 million consumers and spanning an area as far west as the US automobile capital of Detroit, Michigan, as far north as Canada's largest city, Toronto, and as far east as the US financial centre of New York.[1] In late August and early September, several other incidents throughout the world involved interruptions in energy systems: power outages in the south of London, stranding hundreds of thousands of rail passengers; a terrorist attack on a vital Iraqi pipeline; attempts to kidnap Western oil executives in the South Caucasus region; and further guerrilla attacks on Colombia's power supply and delivery network. The lesson to be learned from these events is clear. At a minimum, the replication of debilitative events with an impact on critical energy system infrastructure (CESI) integrity in Europe is an established reality. At the other extreme, a repetition of similar events designed by sinister actors is at least a distinct possibility.

New integrated energy enterprises, power developers, regulated transmission and distribution companies, unregulated enterprises, municipal power authorities, oil and gas exploration and production companies, gas transmission companies, pipeline developers, local distribution companies, industry associations, investors, financial institutions and above all the 450 million people in an enlarged European Union (EU) of 25 states are all exposed to the primary or cascading effects of the debilitation or destruction of CESI. On the low-intensity, asymmetric side of the equation are low-probability but high-risk attacks, for example on congested transmission lines in densely populated areas, to cyber attacks on the information systems that regulate electric power and pipeline throughput. The only certainty regarding these threats from human factors is that they are changing in a way that could allow such attacks to be carried out without a high risk of detection or interdiction.

Javier Solana, the EU High Representative for Common Foreign and Security Policy, has pointed out that 'the European Union is, like it or not, a global

[1] On this event see, e.g., the Internet site of the Office of Electric Transmission and Distribution of the US Department of Energy at URL <http://www.electricity.doe.gov/2003_blackout.htm>.

actor; it should be ready to share in the responsibility for global security'.[2] A major disruption in the supply of vital natural resources, and the debilitation or destruction of CESI for the generation, refinement, storage, transport and distribution of these resources, would cause severe, cascading economic and human hardships for not only for the directly affected national infrastructures and populations but also for regional or even global security. Recent emphasis on the threats to energy supply and CESI have focused on up- and mid-stream infrastructures in the Gulf region, the Caspian Sea Basin and the South China Sea. However, attention must also be drawn to terrorist threats to mid- and downstream CESI in the European theatre. These hazards should be incorporated into the process of building comprehensive and transnational strategies for dealing with the security challenges of the 21st century.[3]

Observations made by Paul Ionescu, State Secretary of Romania, help to put in context several important considerations regarding threats to energy system infrastructure in an enlarged European theatre. With respect to conflict prevention and threat assessment, Ionescu made the following statement.

> The twentieth century has left us with what some experts have called 'a symptom of conceptual uncertainties'. We must recognize that globalization has presented us with a new state of affairs which compels us to rethink our security strategies. Our core problem is that we knew well the world we left behind, but we are still unclear on how to manage the security of the world we are now entering. In a globalizing world it is not only prudent but necessary to try and identify the global consequences of threats, irrespective of their 'national' or 'local' character. We have already learned that transnational threats cannot be fought successfully with national means alone. In this regard, it is sufficient to remind ourselves of the tremendous change in the character of threats since the Cold War—from traditional to non-traditional, from national to transnational—and the required change in our manner of dealing with them. Accepting the changed nature of the terrain in which we operate, we must now concentrate our attention on the accurate and thorough identification of developing threats and emerging crises.[4]

II. Implications of the new European security framework

Several observations on the evolving new European security framework are worth particular consideration in the context of energy infrastructure.

1. An enlarged European Union implies increased responsibilities for the European Security and Defence Policy (ESDP), with a corresponding increase

[2] Javier Solana, EU High Representative for the Common Foreign and Security Policy, 'A secure Europe in a better world', European Council, Thessaloniki, 20 June 2003, URL <http://www.statewatch.org/news/2003/sep/solanasec.pdf>, p. 3.

[3] In this context the terms up-, mid- and downstream refer to the entire energy cycle, from exploration and extraction through transport, storage and distribution.

[4] Ionescu, P., 'Procedural interoperability', Paper presented at the NATO Advanced Research Workshop (ARW) on Future NATO Security: Addressing the Challenges of Evolving Security and Information Systems and Architectures, 8–10 Mar. 2003, Prague, Czech Republic (on the NATO ARWs see URL <http://152.152.96.1/science/calendar/2003/arw-srcs-2003.htm#Mar>).

in threats from non-traditional, transnational actors to CESI integrity in an enlarged European theatre.[5]

2. An enlarged European Union will worsen the already bleak state of EU dependence on the import of energy. On a national basis, European import dependence is an established fact: 9 out of 33 European countries are more than 95 per cent dependent on imports, and only 5 are either self-sufficient or net exporters.[6] Fossil fuels account for four-fifths of total EU energy consumption, and almost two-thirds of these fuels are imported. Natural gas from Russia alone represents 20 per cent of EU consumption and made up one-third of the EU's gas imports in 2000. By the EU's estimate, this figure is expected to double by 2020. The EU's own energy supply covers barely half of what it needs, and it is estimated that, in the absence of effective mitigating actions on the part of EU member states, European energy imports will be much higher in 30 years' time, amounting to 70 per cent of total consumption. Ninety per cent of oil is likely to be imported.

The associated vulnerabilities of a continuous EU energy flow, which depends directly on CESI integrity, have been addressed in a number of EU policies that rely heavily on demand management, the introduction of renewable energy-generating capacity, and the creation of an integrated, flexible internal market for power. However, EU hydrocarbon supplies must often transit numerous highly volatile regions with individuals, cells, groups and movements that constitute threats of a non-traditional nature. These regions are external to and still largely beyond the reach of the EU itself. The Azerbaijan–Georgia–Turkey (AGT) corridor[7] for the delivery of both oil and gas from the Caspian Sea to Ceyhan, Turkey, is but one in a long list of ongoing energy supply development projects that could provide additional hydrocarbon supply for Europe. Yet the political risk profile of the states involved is largely high, given their historic legacy of internal separatist and terrorist movements.

Enhancing energy supply and the networks that deliver it is but one aspect of an overall CESI protection plan. In short, a Common Security and Defence Policy for the EU should comprehensively assess and develop response mechanisms to these fluid, external physical threats to CESI integrity and not rely simply on 'market mechanisms' to provide a comprehensive matrix of solutions to CESI protection, debilitation or destruction.

3. Globalization itself presents extreme challenges for CESI integrity, particularly for new EU member states in economic transition. The CESI in many of these states dates largely from the Soviet era, with a poor level of safety and monitoring equipment, coupled with an often complete lack of comprehensive planning, control and response policies on the part of CESI transition partners against attacks on CESI from 'rogue', human-incited causal factors. Global-

[5] See also chapter 7 in this volume.

[6] Stern, J., *Security of European Natural Gas Supplies: The Impact of Import Dependence and Liberalization* (Royal Institute of International Affairs: London, July 2002), available at URL <http://www.riia.org/pdf/research/sdp/Sec_of_Euro_Gas_Jul02.pdf>.

[7] See 'Azerbaijan, Georgia, Turkey Pipelines Project: Azerbaijan section, International Fact Finding Mission: Preliminary Report', Sep. 2002, URL <http://www.bicusa.org/eca/AzerbaijanFFMreport.htm>.

ization, and the competition policies it promotes, is partly responsible for this situation because it prioritizes debt reduction and high asset valuations (against the backdrop of the privatization of public utilities), both of which could be put at risk if the need for investment in safety and security technologies was recognized and met.

4. To the extent that threats to CESI emanate from non-traditional, non-state actors, why is there no comprehensive database which could serve to model, track and assess the impacts, both in human and non-human terms, of known or potential attacks on CESI, for which information could be drawn from global, open sources?[8]

5. To the extent that European CESI is an interdependent, transnational network of power grids, pipeline networks, and distribution routes and facilities, it is by definition beyond the protective capacity of any single national security, defence, regulatory or coordinating institution to oversee and control. Hence, methodologies, vulnerability assessment criteria and counter-terrorism measures should be driven by international collaboration reflecting the transnational character of CESI.

Before taking steps to assess the threats to CESI and develop counter-terrorism strategies for its protection, an inclusive definition of what CESI constitutes is required. CESI could be defined as encompassing the entire cycle, from energy production to consumption. While energy supply is a critical element of CESI, it is but one element in a much broader system. A RAND Corporation paper defined critical infrastructure (CI) as 'transportation and energy systems, defense installations, banking and financial assets, water supplies, chemical plants, food and agricultural resources, police and fire departments, hospitals and public health systems, government systems'.[9] However, this is no more than a list of hard- and soft-target assets, and it does not prioritize them. CESI could also be defined as the 'core value' on which all other CI assets largely depend, regardless of any given national CESI configuration. It is both gratifying and paradoxical that much national and international research, planning and emergency response work has been carried out on critical information infrastructure protection (CIIP),[10] while the main determinant for continuous operation of critical information infrastructure systems (excluding cyber terrorism) is continuous energy flow—a core CESI value.

[8] For a proposal for such a database see chapter 2 in this volume.

[9] Don, B. and Mussington, D., 'Protecting critical infrastructure', *RAND Review*, vol. 26, no. 2 (summer 2002), available at URL <http://www.rand.org/publications/randreview/issues/rr.08.02/infrastructure.html>.

[10] See, e.g., Wenger, A., Metzger, J. and Dunn, M. (eds), *International CIIP Handbook: An Inventory of Protection Policies in Eight Countries* (Swiss Federal Institute of Technology, Center for Security Studies: Zurich, 2002), available at URL <http://www.isn.ethz.ch/onlinepubli/publihouse/misc/ciip>.

III. Developing CESI protection models and strategies

Many of the country-specific efforts to analyse and evaluate various aspects of CIIP, and the methods developed for CIIP vulnerability assessment, are extremely valuable for considering evaluative, vulnerability and prevention/protection strategies for CESI. One pragmatic first step towards developing transnational CESI protection models and strategies might thus be to launch an effort, based on the exemplary collaboration of the Swiss Federal Institute of Technology and the Swedish Emergency Management Agency, for CIIP evaluation and analysis. The desired output in this case would be a series of national studies on CESI protection, and threat assessment measures that would lead to the elaboration of a better understanding of the entire issue. Policy planners could begin by identifying high-risk critical energy infrastructure assets on a national basis. National energy resources (from natural endowments), the types of generating facilities, and resource import dependencies will obviously vary from country to country, but the overall objective of establishing a baseline for a better understanding of CESI issues on a nation-by-nation basis should hold good.

A second step would be to detail the interdependencies of national CESI assets on a transnational basis. This data-gathering activity would allow individual states, regions and the EU as a whole to assess CESI along the up-, mid- and downstream supply continuum referred to above. These two steps would then form the bedrock for further steps in overall CESI protection in an effort to deny 'rogue', non-state actors the ability to generate crises in CESI networks.

Even when extensive analyses of transnational interdependencies of CESI are undertaken, there may be financial or even geographic barriers to the effective introduction of sufficient redundancy systems for energy supply and delivery. One example is drawn from the Central European Pipeline System (CEPS) managed by the Central Europe Pipeline Management Agency (CEPMA) of the North Atlantic Treaty Organization (NATO).[11] CEPS is a vintage cold-war energy supply and distribution system which begins approximately 100 kilometres east of Munich, running south along the Mediterranean coast, north as far as Hamburg, and west to Rotterdam, Le Havre and Dunkerque. It is a comprehensive, 10 000-km system on which both military and civilian aircraft and their respective airports depend for jet fuel delivery. The Brussels National and Luxembourg airports, for example, depend on CEPS for 100 per cent of jet fuel deliveries. The Frankfurt International Airport, a key hub for both military and civilian aviation, depends on this system for 50 per cent of its jet fuel. However, despite extensive scenario building and contingency planning, including redundancy systems for fuel deliveries by

[11] On the CEPS and the CEPMA see, e.g., NATO, *NATO Logistics Handbook,* Oct. 1997, chapter 15, 'Fuels, oils, lubricants and petroleum handling equipment', URL <http://www.nato.int/docu/logi-en/1997/lo-1506.htm>.

pipeline, land-based transport and barge along the Rhine River, incidents have occurred which highlight the vulnerabilities in this system. During the extensive heat wave in the summer of 2003, fuel barge deliveries were severely hampered on the Rhine owing to the reduction of the river's depth. Further vulnerabilities or challenges are created by NATO enlargement. For example, the Czech Republic, which like most other Central and East European states has a well-founded historic aversion to increasing its fuel dependency on Russia, is not yet connected to the CEPS grid. Extending the CEPS network to supply the Czech Republic's needs is at the present time considered financially untenable.

In general, the defining task for CESI protection in the legitimate economy is to develop and refine a comprehensive strategy for anticipating and preempting, intervening and reacting, and ultimately for ensuring prompt recovery after interruptions to supply and delivery.

A rigorous planning system must: (*a*) catalogue and define high-risk CESI; (*b*) analyse the costs and effects of proposed solutions; (*c*) construct pragmatic modalities for prevention and response mechanisms, particularly on a transnational basis; (*d*) adapt solutions and investments as necessary, based on peer dialogue; and (e) identify best practices related to CESI that have already been implemented in Europe and elsewhere.

The formulation and implementation of a strategy must be long-term in vision and holistic in approach. Cooperation with organizations focused on energy transport security, such as GUUAM (Georgia–Ukraine–Uzbekistan–Azerbaijan–Moldova)[12] and the Shanghai Cooperation Organization (SCO),[13] while positive, is insufficient. The key to success in protecting CESI is the development of a continuous planning system (CPS) that will remain relevant in the face of constantly changing circumstances. Benign cooperation must be augmented with active, constant collaboration against new threats. The use of computational techniques and models for the process of prioritizing infrastructure vulnerabilities can improve resource allocation and enable better analysis of interdependencies among critical systems.

A second strand for formulating strategies for the protection of CESI should include an analysis of the activities undertaken by those states outside the European community to protect their energy assets. An assessment of the security measures taken by a number of states in the Persian Gulf region may point to energy transport and distribution protection strategies that have not been properly considered by other nations.

CESI is a fundamental building block of all modern societies because its assets, systems and functions are vital to national security. By definition, all CESI faces some level of risk, but the question must be asked: What risks are

[12] See the GUUAM Internet site at URL <http://www.guuam.org>.

[13] On the SCO see, e.g., the Internet site of the Ministry for Foreign Affairs of Kazakhstan at URL <http://missions.itu.int/~kazaks/eng/sco/sco01.htm>; and Bailes, A. J. K. *et al., Armament and Disarmament in the Caucasus and Central Asia*, SIPRI Policy Paper no. 3 (SIPRI: Stockholm, July 2003), especially chapter 4, available at URL <http://editors.sipri.se/recpubs.html>.

unacceptable, and to whom? The answer must be based on a variety of assessment criteria.

However, physical asset protection is but one aspect of a comprehensive CESI plan. In a sense, just as the revolution in information technology has transformed global markets and those who control these markets—financial intermediaries which evaluate, administer and execute currency trade, commodity purchases, and financial asset management over loan and portfolio investment—so, too, has control over energy protection been ceded to cyberspace. Advanced, post-industrial societies and economies are critically dependent on the linked computer information and communication systems which serve as the foundation for economic activities in all modern, market-based economies. Control over these networks is far from secure, however. Cyber-attack strategies directed against CESI can be a highly effective 'asymmetrical' technique for small states and non-state actors, not least because of the relatively modest cost of waging cyber war.[14]

IV. Conclusions

The potential weaknesses in CESI in Europe and the problems of its protection are numerous and complex. These problems are vastly greater than the existing architectures for ensuring the continuous flow of energy to states in this region. A number of recommendations are therefore proposed below.

A small combined joint task force of technical, scientific, economic and political officers, perhaps within the framework of the EU–NATO dialogue process or within a broader framework incorporating the Organization for Security and Co-operation in Europe, the EU, NATO and the research community, should work to: (*a*) collaborate with European states, allies and partners in cataloguing high-priority CESI; (*b*) identify critical weaknesses leading to system vulnerabilities and suggest best practices for protecting CESI based on peer-to-peer dialogue; (*c*) focus on the downstream impact of breaches in energy supply and of CESI debilitation and disruption on critical defence, industrial and financial infrastructures; (*d*) measure the economic and human costs of CESI debilitation and destruction; (*e*) estimate the time required for real-life CESI recovery; and (*f*) launch a continuous planning system based on active collaboration with EU member states and with NATO members, partners and allies.

[14] Shimeall, T., Williams, P. and Dunlevy, C., 'Countering cyber war', *NATO Review*, vol. 49, no. 4 (winter 2001), pp. 16–18, available at URL <http://www.nato.int/docu/review/2001/0104-04.htm>.