CRN REPORT

Focal Report 1

Critical Infrastructure Protection

Zurich, October 2008

Crisis and Risk Network (CRN)
Center for Security Studies (CSS), ETH Zürich

Commissioned by the Federal Office for Civil Protection (FOCP)

CRN
Supported by ISN

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Purpose: As part of a larger mandate, the Swiss Federal Office for Civil Protection (FOCP) has tasked the Center for Security Studies (CSS) at ETH Zurich to compile "focal reports" (Fokusberichte) on critical infrastructure protection and on risk analysis to promote discussion and inform about new trends and insights.

Contact:
Center for Security Studies
Seilergraben 45-49
ETH Zürich
CH-8092 Zurich
Switzerland
Tel.: +41-44-632 40 25

crn@sipo.gess.ethz.ch
www.crn.ethz.ch

Contracting entity: Federal Office for Civil Protection (FOCP)
Project supervision FOCP: Stefan Brem, Head Risk Analysis and Research Coordination
Contractor: Center for Security Studies (CSS), ETH Zurich
Project supervision ETH-CSS: Myriam Dunn, Head New Risks Research Unit

Table of Contents

Introduction

Critical infrastructure protection (CIP) is currently seen as an essential part of national security in numerous countries around the world, and a broad range of political and administrative initiatives and efforts to improve the security of critical infrastructures are underway in the US, in Europe, and in other parts of the world. The coordination of Switzerland's CIP efforts and the creation of a CIP strategy are also key tasks of the Swiss Federal Office for Civil Protection (FOCP). As part of a larger mandate, the FOCP has tasked the Center for Security Studies (CSS) at ETH Zurich to produce two annual "focal reports" (Fokusberichte) on critical infrastructure protection.

These focal reports are compiled using the following method: First, a 'scan' of the environment is performed with the aim of searching actively for information that helps to expand and deepen the knowledge and understanding of the issue under scrutiny. This is a continuous process that uses the following sources:

- *Internet Monitoring*: New publications and documents with a) a general CIP focus and b) a focus on scenarios with specific importance for the FOCP (i.e., earthquakes, pandemics, power outages, ICT failures) are identified and collected.
- *Science Monitoring*: Relevant journals are identified and regularly evaluated (with the same two focal points as specified above).
- *Government Monitoring*: The focus is on policy developments in the US, Canada, Sweden, Norway, Denmark, Germany, the Netherlands, and the UK as well as other states in the European vicinity that are relevant to Switzerland.

Second, the material thus collected is filtered, analyzed, and summarized in the focal reports.

Structure of first focal report

This report is structured as follows:

1. First, it identifies three trends in CIP based on the review of governmental protection policies and the science monitoring.[1] This is followed by an extensive annotated bibliography, which covers texts and resources for critical infrastructure protection in three sections: policy documents, academic texts, and internet resources.
2. Second, this report focuses on a topic that has gained increased attention in the last couple of years: attacks on the energy infrastructure. This topic is still largely under-researched and is usually not discussed under the larger heading of CIP, despite its link to the issue. It is particularly interesting because it deals with physical attacks rather than cyber-attacks, which still dominate the general CIP literature. The second section is also followed by an annotated bibliography that provides some recently produced resources on threats to the energy infrastructure.

[1] To the best of our knowledge, nothing of relevance has been published specifically on CIP in relation to earthquakes, pandemics, power outages, or ICT failures in the last 6 months.

1) Critical Infrastructure Protection Policies

Over the last decade, the protection of critical infrastructures has been firmly established as a topic of high interest in many countries. While practically all states show a high consistency in the direction of their protection policies since approximately 2002, some changes and new developments can be identified nonetheless. For this focal report, recent CIP policy documents from 25 countries[2] were systematically sifted through to identify key changes and trends.

Three Trends

This broad monitoring activity let to the identification of three main trends. While trend one and three could seem almost contradictory at first sight, they concern communities that often have little to no overlap:

- First, many countries pay increasing attention to the concepts of resilience and all-hazard approaches.
- Second, this has direct implications for how CIP is organized: A move towards the centralization of responsibility in this policy domain can be observed.
- Third, there is continued or even growing attention to the cyber-dimension of the issue, linked to the growing awareness that the globally connected information and communication technologies have become a particularly vulnerable part of every country's national infrastructures (often also discussed under the heading of "cyberwar").

The first two trends can best be exemplified by pointing to recent changes that have taken place in Canada (1), Sweden (2), and the United Kingdom (3), all three of which can be called forerunners not only with regard to the overall approach to CIP policies, but also with regard to the implications of this for organizational change. The third trend is exemplified by developments in the United States (5) and France (6), and NATO (7) and its member countries.

Below, all three trends are briefly summarized, and the potential implications of these trends for Switzerland and its CIP policy are discussed.

[2] Including Australia, Austria, Brazil, Canada, Estonia, Finland, France, Germany, Hungary, India, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Poland, Russia, Singapore, Spain, Sweden, United Kingdom, and United States. The range of countries was deliberately expanded beyond the ones mentioned in the introduction to this report to have a broader base to choose from.

Trend 1: Resilience and all-hazard approach

In the monitored countries, an increasing focus on the concept of resilience can be observed. The reason for this is the following: Comprehensive protection of all critical infrastructures – once they have been identified – against all threats and risks is impossible, not only for technical and practical reasons, but also because of costs. Priorities can be established, for example, by distinguishing between critical infrastructures that deserve a greater level of attention, or by identifying vital points within a critical infrastructure. Criteria used for prioritization can focus on the relative likelihood of the threat, on the criticality of one asset compared to another one, or on the relative cost of protection, to name just a few approaches.

However, as long as there is no reliable data on the likelihood of threats (which is often the case), another (more pragmatic) approach promises better results. This approach focuses more on the likely *effects* of a failure of a specific infrastructure or asset and seeks to mitigate them. Often, risk management is approached with the help of scenarios. The reasoning for this approach is quite simple: From the perspective of maintaining reliable services, it does not matter whether the events that triggered the disruption originated from within or from outside the infrastructure. It is also often difficult to determine whether a particular detrimental event is the result of a malicious attack, of a component failure, or of an accident. In practice, the first and most important question is not what exactly caused the incident, but rather what the possible results and complications of the unavailability of a certain service may be.

What this shows is that it is beneficial to follow an "all-hazards" approach, designed for comprehensive protection irrespective of the nature of the threat, with a focus on the capability to respond to a whole spectrum of unanticipated events. The key is to create greater resilience, commonly defined as the ability of a system to recover from adversity, restoring it either to its original state or to a modified state based on new requirements. Resilience is commonly embedded in processes rather than individual physical assets or protection measures. Such an approach makes it easier to focus on synergies instead of trade-offs between the various stakeholders involved. Furthermore, the concept of resilience is a move away from a focus on national security understood narrowly as defense and is often a very pragmatic solution in light of the overwhelming task of protecting all the assets that a country defines as critical, especially in the light of having to win the support of the private sector for protection policies. Heightening the resilience of critical infrastructures is in everyone's interest – whether they aim at ensuring business continuity or, ultimately, guaranteeing the safety and well-being of all citizens.

It must be said, however, that even though the concept seems to be moving to the center of most protection efforts worldwide, concrete implementations of the resilience concept in CIP policies that could be used as best practice models do not (yet) exist. In fact, a variety of key issues remain unresolved, among them the following:

- For example, even when thinking in terms of 'resilience' and 'all-hazards', governments still need to identify the assets most critical to the functioning of their societies because these assets will require specific attention. This leads straight back to the question of how 'criticality' of infrastructures and their functions can be measured (as a basis for prioritization).
- In addition, especially in cases of high criticality, the question of what policy tools governments should and can use to ensure that private actors make their systems more resilient moves to the

forefront. This discussion is very similar if not identical to the one in the field of public-private partnerships more generally.

Thus, while resilience as a guiding concept seems a good solution, it is too early to say whether it will be of a real problem-solving nature.

Examples

Recent examples for an increasing focus on the concept of resilience from the monitored countries are the following:

- *Canada*: The Canadian Public Safety department (Public Safety Canada) addresses the need for coordinated action to enhance the resilience of Canada's critical infrastructure with its project "Working Towards a National Strategy and Action Plan for Critical Infrastructure"[3]. This document, drafted in coordination with the federal, provincial, and territorial governments, considers the strengthening of the resilience of critical infrastructures against current and emerging threats the core of the new policy. Public Safety Canada strives to achieve this by building 'trusted and sustainable partnerships', by implementing an all-hazards risk management approach, and by advancing the timely sharing and protection of information among partners.
- *Sweden*: The purpose of creating the new Swedish Civil Contingencies Agency (SCCA), taking effect in January 2009[4], is to solidify a comprehensive approach to societal security, a term thought to better reflect the reality that fluid risks and threats and the challenges of the 21st century are not so much directed against the integrity of the territory, but jeopardize critical functions in society.[5] As in the Canadian case, this represents an all-hazards risk management approach and will be geared towards increasing the overall resilience of critical infrastructures.

Implications for Switzerland

The Swiss approach to CIP embraces the concept of resilience and all-hazards by integrating a very broad number of stakeholders from all different departments, including the networks of the responsible lead agencies such as the Federal Office of Energy, of Transport, or Communication and by focusing on a very broad number of potential threats to the national infrastructure. It might be useful, however, to embrace the concept of resilience even more explicitly and move it to the center of the future CIP policy. This is likely to facilitate discussion with a larger set of stakeholders not only from different branches of the federal government, but also from the private sector. However, the caveats mentioned above also apply to the Swiss case: prioritization and measures of criticality remain key issues that require specific attention and additional research. In Switzerland, criticality criteria have been developed and recently tested and the criteria to identify individual critical assets are currently underway.

[3] For the document details see the annotated bibliography.

[4] For more information on this organizational transformation of the Swedish protection policies see centralization of responsibility below.

[5] George Mason University. The CIP Report Vol. 6 N° 12. A New Leader of Societal Security Efforts in Sweden.

Trend 2: Centralization of responsibility

The second discernible tendency is a trend towards the centralization of responsibility with regard to the protection of critical infrastructures on the federal level, which is a direct consequence of the focus on resilience and all hazards. Whether CIP is understood as an issue of Public Safety (CA), of Civil Contingencies (SUE), or of National Infrastructure (UK) is becoming less important than the fact that the approach guiding the current policy developments is informed by an understanding of security that identifies society as a whole, and in particular its undisturbed and smooth functioning, as the core referent object of security rather than single sectors of infrastructures. This societal core is understood as being subjected to a vast and varied spectrum of potential threats. Protection from these threats is increasingly subsumed under centralized state agencies holding overall responsibility for their identification, but delegating operational matters for effective provision of protection.

Examples

Recent examples for this trend are the following:

- *Canada*: In light of increasing interdependency also acknowledged in the above mentioned project "Working Towards a National Strategy and Action Plan for Critical Infrastructure", Public Safety Canada has taken a leadership role not only in promoting a national partnership among private and public-sector infrastructure stakeholders but also in Canada's general CI protection policy.
- *Sweden:* A major organizational transformation concerning CIP is currently underway in Sweden. The functions and responsibilities of a number of governmental agencies are under review. In January 2009, the merger of three current agencies, namely the Swedish Emergency Management Agency (SEMA), the Swedish Rescue Services Agency (SRSA), and the Board of Psychological Defence (SPF), will take effect. The new agency, called the Swedish Civil Contingencies Agency (SCCA) will have an all-encompassing task with regard to civil contingencies; that is to say, its work will cover the whole spectrum of contingencies from everyday road traffic accidents, fires, chemical emergencies, power cuts, and other technical failures to even more serious emergencies such as bomb threats and other hostile attacks, epidemics, natural disasters, and war. It will be involved in planning, education and training, research, and coordination of emergency management activities. Also, the new agency will be given the authority to issue binding regulations.
- *United Kingdom*: The UK Centre for the Protection of National Infrastructure (CPNI) has, since its formation from the merger of the National Infrastructure Security Co-ordination Centre (NISCC) and the National Security Advice Centre (NSAC) in 2007, been involved in updating the system for identifying critical national infrastructure and is charged with protecting the UK's CNI from both physical and electronic attacks. As in the two other countries cited above, this move was also aimed towards increased centralization of CIP responsibilities.

Implications for Switzerland

The current efforts in Switzerland by the interdepartmental working group under the lead of the Federal Office for Civil Protection are consistent with this centralizing tendency insofar as they acknowledge the need for a single entity that defines strategic criteria for the identification of critical elements and parts of Swiss infrastructure. It could become necessary, however, not only to define such criteria clearly, but also to draw consistent consequences and act accordingly. While the interdepartmental approach of Swiss CIP policy, which is mainly geared towards coordination, is a sensible approach for the Swiss context, the question is at what point in the policy process coordination alone might become insufficient. In comparison to other countries, the FOCP has far less power, responsibility, and resources than other actors that are in charge of CIP. This could lead to problems in the future when it comes to enforcing certain decisions in the CIP domain.

Trend 3: Increased focus on the cyber-dimension

The third trend identified is the increased focus on cyber-related threats and vulnerabilities. Recent initiatives undertaken not only by the US and France, but also by NATO, are guided by the concern that the information and communication infrastructures are increasingly vulnerable not only due to their extremely dense connectivity, but also due to both the state's and society's dependency on them. While this is not a new development, it is noteworthy that this topic continues to be one of the driving factors of the whole CIP debate. The main governmental efforts to protect information and communication infrastructures discussed here concentrate on the state's use of these technologies; their aim is to better secure networks against intrusion and, in the case of NATO, to do so collectively.

Not surprisingly, in this domain, military concerns and a more broadly conceptualized CIP debate begin to merge as the same tools necessary for protection of civil infrastructures are also needed to protect military infrastructures. What is more, military infrastructures and civil infrastructures can often not be clearly separated to the point where they have to be considered one and the same. In addition, it has become clear over the last couple of years that militaries all around the world mainly focus on "their" networks when it comes to CIP or CIIP and that CIP is an inherently civil domain that requires non-military solutions.

Examples

Recent examples for the (increased and continued) focus on cyber-related threats and vulnerabilities can be found in the following countries:

- *United States*: The National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 established a multi-agency, multi-year plan to secure the federal government's cyber-networks called the *Comprehensive National Cyber Security Initiative* (CNCI) in January 2008.[6] Moreover, the White House has published a *National Strategy for Information Sharing*[7] that builds upon the existing efforts and provides guidelines for sharing information to protect critical infrastructures. More than ten years after having identified information-sharing between all relevant actors in the field of CIP as "the most immediate need" for the protection of critical infrastructures,[8] the US is still trying to improve its policies and approaches in this domain, and many of the problems with regard to trust and confidentiality remain unsolved. The experience in the US is also of great interest to other countries in terms of lessons learned and mistakes to avoid.
- *France:* In France, particular attention has recently been devoted to cyberwar, with direct implications for CIP. In June 2008, the French president announced the most wide-ranging

[6] The Department of Homeland Security has the lead in the initiative, but is reluctant to share details with either Congress or the public: The hearings of the Congressional Committee that is in charge have been classified or are available only in a censored version. Senate Committee on Homeland Security and Governmental Affairs. Lieberman, Collins Release Detail on the National Cyber Security Initiative. 31 July 2008. <http://www.fas.org/sgp/news/2008/07/cybersec.html>.

[7] For more information on this document see annotated bibliography.

[8] President's Commission on Critical Infrastructure Protection. Critical Foundations. Protecting America's Infrastructures, Washington, 1997: pp. 21, 27.

reform of the French armed forces since 1994. *The Defense and National Security White Paper* (Défense et Sécurité nationale: Le Livre Blanc) states that global terrorism poses the most virulent threat to the security of France and its citizens. The substantial increase in funding in order to confront this challenge is intended to be used to strengthen satellite surveillance and information and communication technology in general in order to prevent cyber-attacks. Moreover, France plans to develop offensive means to prevent cyber-attacks.[9] With this step, France has joined the range of countries that have integrated conceptions of offensive and defensive cyberwar into their national security planning.

- *NATO* as a defense alliance is, not surprisingly, focusing on the conflict-related aspects of CI. In May 2008, Estonia and six other nations including Germany, Italy, Latvia, Lithuania, Slovakia, and Spain signed a memorandum of understanding concerning the establishment, administration, and operation of the *Cooperative Cyber Defence Centre of Excellence*. The center established in May by the top military commanders of the seven NATO countries mentioned above is hosted by the city of Tallinn. The cyber-attacks on Estonia in 2007[10] highlighted the potential vulnerability of NATO countries, their institutions and societies, and even NATO itself to disruption by penetration of their information and communication systems. The center is intended to develop concepts and doctrines in the field of cyber-defense, to elaborate methodologies and capabilities to eliminate cyber-threats, and to analyze and simulate a variety of threats.[11]

Implications for Switzerland

Compared internationally, Switzerland's Information Assurance Policy (as the center piece of Switzerland's critical information infrastructure protection (CIIP) policy), based on the four pillars of prevention, early recognition, crisis management, and technical problem solution, is a qualitatively high-ranking approach that has yielded some results in the last couple of years. However, there seems to be a tendency in the Swiss case to consider CIIP and CIP as separate issues, partly due to historical reasons and partly due to the early success with the Information Assurance Policy and the Reporting and Analysis Centre for Information Assurance MELANI. While a renewed focus on the entirety of CIP was necessary and useful, it is of key importance to conceive of CIP and CIIP as a whole. Neither turf battles nor the fact that some policy areas are further advanced than others should lead to an undue differentiation of the two in the CIP policy process.

[9] Défense et Sécurité nationale. LE LIVRE BLANC. Odile Jacob. La Documentation Française: Paris (June 2008). <http://www.rpfrance-otan.org/article.php3?id_article=590>.

[10] For more information on these attacks see annotated bibliography, SEMA study 2008 on large scale internet attacks.

[11] This goes back to the Bucharest Summit declaration of early April 2008 which states in paragraph 47 that: "NATO remains committed to strengthening key Alliance information systems against cyber attacks. We have recently adopted a Policy on Cyber Defence". Bucharest Summit Declaration, issued by the heads of state and government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008. <http://www.summitbucharest.ro/en/doc_201.html>.

Annotated Bibliography

The literature on critical infrastructure protection is mostly produced by states that publish their national strategies and action plans to address the challenge of protecting their critical infrastructure. There are very few scientifically inspired and theoretically driven analyses of state strategies and policies. Most scientific analysis focuses on the purely technical aspects of securing the critical infrastructures and vital systems. The following annotated bibliography presents the most recent (from the last two years) key governmental documents, scientific analyses, and internet sources.

Policy documents/reports

Public Safety Canada. 2008. Working Towards a National Strategy and Action Plan for Critical Infrastructure, Draft for Consultation. Available at: <http://www.publicsafety.gc.ca/prg/em/cip/_fl/nat-strat-critical-infrastructure-eng.pdf>.

This document sets out the collective national approach to enhancing the resilience of Canada's critical infrastructure. Its aim is to reduce risks and vulnerabilities, and provide swift and effective responses to disruption when they occur. Primary responsibility for protecting critical infrastructures rests with both private and public-sector owners and operators. Due to the interconnected nature of CI, an integrated approach across all levels of government and the private sector is seen to be necessary on the strategic level. Therefore, the strategic part of this document is based on principles built around partnerships, risk management, information-sharing, and protection. The document's action plan is considered a blueprint for implementing the strategy. It shall guide the identification of risks, the implementation of protective measures, and effective responses to disruptions of CI. Moroever, the public-private partnership model is described by the National Strategy and Action Plan as providing the basis for effective critical infrastructure protection.

United States Department of Homeland Security. 2006. National Infrastructure Protection Plan. Available at: <http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf>.

Since the US has historically been and continues to dominate agenda-setting in the issue of Critical Infrastructure Protection, this plan can be considered one of the important documents in the field and a source of inspiration for other countries. It aims to provide a coordinated approach to critical infrastructure, and specifies key resource protection roles and responsibilities for both state actors and private-sector security partners. It sets priorities, goals, and requirements for distribution of funding and resources in order to ensure continuity in the event of terrorist attacks or other disasters.

United States Department of Homeland Security. 2007. Critical Infrastructure and Key Resources Sector-Specific Plans. Available at: <http://www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm#2>.

These sector-specific protection plans support the National Infrastructure Protection Plan (NIPP) by providing the means for its implementation across all sectors. Plans related to the following sectors are publicly available: Agriculture and Food, Banking and Finance, Communications, Defense Industrial Base, Energy (Redacted), Information Technology, National Monuments and Icons, Transportation Systems, and Water. Plans concerning the following sectors are classified: Chemical, Commercial Facilities, Dams, Emergency Services, Government Facilities, Nuclear Reactors, Materials and Waste, Postal and Shipping, and Public Health and Healthcare.

United States White House. 2007. National Strategy for Information Sharing. Available at: <http://www.whitehouse.gov/nsc/infosharing/NSIS_book.pdf>

With a focus on the prevention of further terrorist attacks, this document sets forth the US plan to build upon progress and establish an integrated information-sharing capability. It aims to improve information-sharing at the federal level, while also facilitating information-sharing between the federal government and non-federal partners. The strategy clearly highlights the need to share information with those who need it, rather than to conceal information. It states that "the exchange of information should be the rule, not the exception."

NATO Parliamentary Assembly, Lord Jopling (UK) Special Rapporteur. 2007. 162 CDS 07 E rev 1 – The Protection of Critical Infrastructures. Available at: <http://www.nato-pa.int/default.asp?SHORTCUT=1165>.

This document is a special report given to the NATO Parliamentary Assembly by Lord Jopling (UK) on critical infrastructure protection, national stakeholders, the role of EU and NATO, and sectoral policies, with a special focus on energy security, civil aviation security, port security, and critical information infrastructure protection.

Swedish Emergency Management Agency. 2008. Large scale Internet attacks. The Internet attacks on Estonia. Sweden's emergency preparedness for Internet attacks. Available at: <http://www.krisberedskapsmyndigheten.se/upload/3040/Large%20scale%20Internet%20attacks_utb-ser_2008-2.pdf>.

The extensive attacks on the Estonian branch of the internet in spring 2007 have triggered a heightened awareness of the so-called cyber-defense component of critical infrastructure protection. A sound analysis of these events, this SEMA study constitutes a good contribution to the field of 'cyber-defense'. Moreover, as an attempt to analyze the possible consequences of experiences of the Estonian internet attacks regarding the protection of societal functions in Sweden, it represents a good comparative starting point for other countries.

Commission of the European Communities. 2006. Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection. Available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0787:FIN:EN:PDF>.

This latest European document strives to lay the baseline for appropriate action to strengthen critical infrastructure protection as a central aspect of preventing and fighting terrorism at the European level. It presents the measures proposed by the EC to this end.

Furthermore, the European Commission plans to launch a policy initiative on Critical Communication and Information Infrastructure Protection in 2008. The aim is to ensure an adequate and consistent level of protective security and the resilience of critical information infrastructure throughout the EU. This initiative will be part of the broader framework of the European Program for Critical Infrastructure Protection and will be managed independently by the Information and Media Directorate-General. Moreover, in the Framework Program 7 (FP7), critical infrastructures (often in connection with information and communication technologies) are a new focal point.[12] The European case is of interest in so far as that the lessons learned from the efforts to coordinate CIP policy across a large number of countries will be of great interest to any other country involved in coordination activities of all sorts (be it on the federal or cantonal level). Its focus on the information and

[12] <http://ec.europa.eu/research/future/themes/index_en.cfm>.

communication technology aspect is also noteworthy. Furthermore, any development on the European level will be of direct consequence for Switzerland, which should be as closely involved as possible.

Academic literature

Dunn Cavelty, M. and Kristensen, K.S. (eds). 2008. Securing 'the Homeland'. Critical infrastructure, risk and (in)security. Routledge: London and New York.

This edited volume with contributors from across Europe and the US adopts an academic and theory-inspired approach to the various aspects of critical infrastructure protection. The book ultimately engages the question of what is defended by security policy in this day and age. It aims at disclosing the continuities and discontinuities of contemporary CIP protection policies. Therefore, it is divided in two parts: The first examines the origins, conception, and the public-private rationale underpinning CIP policies, while the second considers terrorism as a trigger for the 'new' politics of protecting the homeland. The book is guided by so-called critical security studies and is a contribution towards "academization" of the CIP debate.

Lipschutz, Ronnie D. (2008). Imperial Warfare in the Naked City – Sociality as Critical Infrastructure. In: International Political Sociology, 2, 204–18.

Critical Infrastructure Protection is still rarely a subject of theory-inspired scientific research. The few contributions focusing on CIP from this angle mostly do so due to some concurrence with developments related to recent terrorist incidents. One example is the article by Lipschutz, which understands the so-called 'Global War on Terror (GWOT)', framed as conflict with groups and individuals determined to disrupt and destroy 'critical infrastructures', as being heavily dependent on technological and psychological discourses and practices to identify terrorists and their plots. These methods seek to protect the material 'backbone' of contemporary society and to detect potentially violent actors whose capabilities might progress to action. However, the social nature of all action suggests that 'critical infrastructure is people,' and that surveillance alone is not sufficient to determine who will act and who will not. The ultimate purpose and effect of the GWOT is better understood as involving the transformation of individual mentalities, so that 'heretical' thoughts and practices become impossible. This article, though interesting from a critical security studies angle, has little relevance for practical purposes.

International Journal of Critical Infrastructures (IJCIS). Available at:
<http://www.inderscience.com/browse/index.php?journalID=58&year=2008&vol=4&issue=4>.

This scientific journal, published in 4 issues per year by Inderscience Publishers, possesses a pronouncedly technical focus and aims to provide a professional and scholarly forum for cross-learning between different scientific and technological disciplines, and between societal and managerial disciplines in the area of critical infrastructures. The goal is to provide an authoritative source of information in the field of risk and vulnerability assessment and management of vital societal systems exposed to anthropogenetic and natural threats.

Since 2007, three special issues have been published on Critical Electricity Infrastructures (vol. 3, no. 1/2 2007), on Transportation Disaster and Degradation Management (vol. 3, no. 3/4 2007), and on Complex Network and Infrastructure Protection (vol. 4, no. 1/2 2008). Among the articles published as part of the regular issues, we consider the following to be of particular relevance:

- *Ghorbani, Ali A. and Bagheri, Ebrahim. The state of the art in critical infrastructure protection: a framework for convergence. In: IJCIS, vol. 4, no. 3 (2008): 215–44.* The protection of critical infrastructure systems has recently become a major concern for many countries. The investigations of researchers have encompassed

issues of national security, policymaking, infrastructure system organization, and behavior analysis and modeling. In this paper, the authors look into the latter subject and explore the attempts that have been made. Based on the available schemes and the requirements of this area, the authors propose a five-dimensional framework that introduces the major research gaps in this field. Among the various available schemes, they study ten of the most recently developed and/or influential systems. A comparison of these schemes is made based on the features of the proposed framework. The comparison allows the authors to conclude the examination with the identification of current research strengths and guidelines for future work.

- *Zhang, W.J., Liu, X., Chai, Choon-Lee, Deters, Ralph, Liu, D., Dyachuk, Dmytro, Tu, Y.L., and Baber, Zaheer. Social network analysis of the vulnerabilities of interdependent critical infrastructures. In: IJCIS, vol. 4, no. 3 (2008): 256–73.* Interdependency among critical infrastructures contributes to vulnerabilities of those infrastructures. In this paper, the vulnerabilities of critical infrastructures are identified and analyzed using social network analysis. In the analysis of network centrality, the importance of each critical infrastructure is ranked in terms of its contribution to infrastructure interdependency. The findings show that electricity and telecommunication are the two most important critical infrastructures that contribute to infrastructure interdependency, which further render the infrastructure network vulnerable to cascading damage. An example system is given to illustrate the ideas and results presented in this paper.

- *Robert, Benoit, De Calan, Renaud, and Morabito, Luciano. Modeling interdependencies among critical infrastructures. In: IJCIS, vol. 4, no. 4 (2008): 392–408.* Over the years, critical infrastructures have become increasingly automated and interlinked. This linkage between CI elements results in a very complex and dynamic system that increases their vulnerability to failures. In fact, interdependencies between parts of the CI are a true means of propagation of hazards from one network to another. Thus, when an infrastructure is experiencing difficulties and failures, it can rapidly generate a cascading effect affecting the other infrastructures. Identifying, understanding, and modeling these interdependencies is thus necessary to prevent these cascading effects. This paper presents a model developed to understand the interdependencies between CI elements and to prevent cascading effects from happening. Based on the resources exchanged by various parts of the CI, this model facilitates visualization and anticipation of domino effects in time and space, allowing CI managers to set up convenient preventive and protective measures in order to avoid their propagation.

Journal of Contingencies and Crisis Management. Available at: <http://www3.interscience.wiley.com/journal/118535940/home>.

This scientific journal, published 4 times a year by Blackwell Publishing, focuses on all aspects of contingency planning, scenario analysis, and crisis management in both corporate and public sectors and strives to provide analysis of the opportunities and threats facing organizations. It presents case studies of crisis prevention, crisis planning, recovery, and turnaround management. For the period since 2007, the special issue published on Critical Infrastructures (vol. 15, no. 1, 2007) is of particular relevance. Its authors share the conviction that the effective functioning of CI is crucially important to citizens, businesses, the public administration, and political leaders. But there are varying degrees of criticality. This special issue, which devotes special attention to internal threats, strives to provide both a state-of-the-art assessment and a point of departure for future research. It includes the following articles:

- Boin, Arjen and McConnell, Allan. 'Editorial: Unravelling the Puzzles of Critical Infrastructures', pp. 1–3.

- Egan, Matthew Jude. 'Anticipating Future Vulnerability: Defining Characteristics of Increasingly Critical Infrastructure-like systems', pp. 4–17.
- De Bruijne, Mark and van Eeten, Michel. 'Systems that Should have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment', pp. 18–29.
- Fritzon, Åsa, Ljungkvist, Kristin, Boin, Arjen, and Rhinard, Mark. ‚Protecting Europe's Critical Infrastructures: Problems and Prospects', pp. 30–41.
- Schulman, Paul R. and Roe, Emery. 'Designing Infrastructures: Dilemmas of Design and the Reliability of Critical Infrastructures', pp. 42–9.
- Boin, Arjen and McConnell, Allan. 'Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience', pp. 50–59.
- LaPorte, Todd R. 'Critical Infrastructure in the Face of a Predatory Future: Preparing for Untoward Surprise', pp. 60–4.
- Stark, Alastair. 'Book review: Policymaking for Critical Infrastructures: A Case Study on Strategic Interventions in Public Safety Telecommunications, by Gordon A. Gow', pp. 65f.

Internet resources

George Mason University (GMU), Critical Infrastructure Protection (CIP) Program. Available at: <http://cipp.gmu.edu/index.html>.

The GMU CIP program and its frequently updated website is a valuable source of information for both US and international CIP-related issues and developments. Maintained in partnership with James Madison University and the National Institute of Standards and Technology, the program seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting critical infrastructures. Moreover, it maintains an extensive outreach effort to highlight and advance current topical issues relevant to the US national agenda. Also, it provides a valuable electronically accessible library with bibliographies, summaries of projects, a CIP digital archive, selective government reports on infrastructure protection and critical infrastructure recovery and restoration, reports on natural disaster, selective international reports, and other documents.

Furthermore, the program publishes the monthly CIP Report newsletter, which provides an overview of the latest related developments within the US. Once a year, it provides an international issue giving a concise summary of what are identified as the most significant CIP-related developments at the state level world-wide. All issues are electronically available at: <http://cipp.gmu.edu/report/>.

The Critical Infrastructure Protection Blog. Available at: <http://criticalinfrastructure.blogspot.com/>

Highly accurate and daily updated information on Critical Infrastructure Protection and Critical National Infrastructure programs at the state level is provided by the Critical Infrastructure Protection Blog. It provides news, documents, papers, events, and research results from Europe and the US on critical infrastructure protection and critical national infrastructure issues.

The Design of an Interoperable European Federated Simulation network for critical infrastructures, DIESIS-project. Available at: <http://www.diesis-eu.org/>.

This project proposes to establish a basis for a European modeling and simulation e-Infrastructure based on open standards to foster and support research on all aspects of critical infrastructures, with a focus on their protection. Specifically, it strives to address the difficulties involved with the availability of models and data for

single infrastructures, with the interoperability simulation of multiple infrastructures, and with test beds and benchmarks for protection solutions.

CIIP Matters – The Meridian Newsletter. Available at: <http://www.meridian2006.org/index.php?page=8>
The so-called Meridian Process – a high-level initiative launched by the UK in 2005 that also focuses on the information dimension – is open to all countries and aimed at senior government policy-makers. It strives to provide governments worldwide with a platform for discussing how to work together at the policy level on critical information infrastructure protection. It claims to enable governments to explore the benefits and opportunities of cooperation with the private sector, and to exchange information and good practices between governments internationally, paying tribute to the call for truly international approaches to CIP. The process began to be formalized after its first conference in 2005 launched by UK's CPNI. Subsequent conferences were held in Budapest and Stockholm, and the next conference will be in Singapore (2008). A quarterly newsletter called CIIP Matters issued by the Editorial Committee of the Meridian Process gives an excellent overview of recent developments.It is likely that other initiatives will be started in the future with a focus on international exchange of best practices, as this is a need identified by all countries involved in CIP activities. The quarterly newsletter issued by the editorial committee of the Meridian Process since the 2006 Meridian conference provides excellent coverage of international CIIP issues and developments.

ECN – European CIIP Newsletter. Available at: <http://www.irriis.org/?lang=en&nav=289>
This newsletter provides coverage of CIIP issues with a particular European focus.

2) Security Threats to the Energy Infrastructure

Since the 1980s, the energy infrastructure (EI)[13] has been used as a strategic weapon and symbolic economic target by various non-state armed groups operating in many, largely, fragile countries.[14] But while targeting EI is not an entirely new phenomenon, the 21st century has opened the door to a world where local events have global consequences, communication and information move rapidly through a variety of media, financial systems are intertwined, and developing nations that once struggled now compete for vital natural resources to feed their burgeoning economies. Prior to 1999, EI attacks went largely unnoticed outside of the locale in which they occurred. Today, however, these events not only generate broad media attention but they can also create broad economic turbulence – translated into higher global energy costs in a world accustomed to low-cost petroleum – due to the energy market's interconnected nature, growing demand, and short-term supply shortages.

With oil accounting for nearly "40% of the world's energy and 96% of its transportation", the protection of EI from both attacks and natural disasters has become a top priority for most industrialized nations.[15] As efforts have been made to enhance the protection of EI throughout North America and the EU, the most significant sites of oil and gas exploration and production are located in locations that are increasingly politically unstable, marred by poor economic and social conditions.[16] While the likelihood of attacks on Switzerland's domestic EI is low, in the unstable oil- and gas-producing regions of the world marked by violence and insurgency, EI attacks are not only becoming more prevalent in some countries, but are also creating supply uncertainty that have financial markets reacting to any threats to the energy sector.

To illustrate this point, following a January 2008 attack on oil facilities in Nigeria, crude oil futures increased as analysts speculated that Nigerian supply would face further disruptions.[17] Shortly after this attack, Olivier Jakob of Petromatrix in Switzerland noted: "With the military and the militant warlords engaged in a violent tit-for-tat, the risk for oil disruptions in Nigeria remains higher than in the past few month."[18] In light of this development, this section will discuss ways in which energy supply and demand has changed in the 21st century, factors relating to market sensitivity, and will briefly highlight cases where energy resources have been threatened. Concluding remarks will identify public and private

[13] 'Energy infrastructure' in this report refers to oil, gas, and electricity (produced by wind, water, coal, nuclear power, or oil and gas) infrastructure.

[14] The following are examples of attacks prior to 2000: In El Salvador during the 1980s, the Farabundo-Marti National Liberation Front carried out attacks that interrupted electricity services in up to 90 per cent of the country. Since 1986, in Colombia, the National Liberation Army (ELN) and FARC have repeatedly attacked the Caño Limón-Coveñas oil pipeline, causing severe damage and disruptions. Since 1980, the United Liberation Front of Asom has attacked oil infrastructure and pipelines in Assam, India. Peru's Sendero Luminoso attacked ElectroPeru's facilities in the 1980s and sabotaged several electrical transmission towers in Lima, causing a citywide blackout.

[15] Luft, G., 2005. Pipeline sabotage is terrorist's weapon of choice. Institute for Analysis of Global Security (IAGS) Energy Security. 25 March. Available at: <http://www.iags.org/n0328051.htm>.

[16] The world's most significant sites of oil and gas exploration and production are located in increasingly politically unstable locations, such as Algeria, Indonesia, Iran, Iraq, Libya, Nigeria, Russia, Sudan, and Venezuela.

[17] Heath, N., 2008. DJ Update: Oil Futures: Crude Up $2 on Nigerian Attacks, US Data. Dow Jones Commodities News, [internet]. 2 January. Available Online: <http://www.zibb.com/article/2432485/DJ+UPDATE+OIL+FUTURES+Crude+Up+2+On+Nigerian+Attacks+US+Data>.

[18] BBC News. 2008. What is driving oil prices so high? BBC News Online. 2 January. Available at: http://news.bbc.co.uk/2/hi/business/7048600.stm

strategies that are used to mitigate threats posed to EI in countries where the state is unable to secure such assets.

A changing scenario

Concerns about the threat posed by transnational terrorists and armed non-state actors seeking to cause local and global disruptions to energy supplies are warranted. According to the US State Department, between 1996 and 2004, there were at least 80 terrorist attacks against oil companies worldwide that resulted in kidnappings, casualties, damages, and large monetary losses.[21] However, since 2004, there have been 442 attacks on oil pipeline in Iraq alone – with a similar picture in Nigeria since 2006, when militant groups began carrying out monthly and at times weekly attacks on the EI.[22]

Not only are such resources being targeted both inside and outside of conflict zones,[23] but the energy sector is increasingly sensitive to any disruptions, whether perceived or real, due to a number of factors that relate to the 'peaking' of supply. Such factors include increased demand by growing developing economies as well as continued robust demand from

Key Energy Facts[19]

- Characteristics of modern energy systems include increased use of fossil (non-renewable) fuels (mainly oil, coal and natural gas), centralized & large scale structures throughout supply chains, 24/7 supply and growing demand.
- New oil discoveries have been in decline since peaking in 1960
- World demand for oil had risen to some 85 million barrels a day and is projected to grow by 50 per cent between 2005 and 2030 (Asia, Latin America, Africa, the Middle East, and India accounting for increase in demand); natural gas will climb by over 120 per cent; coal by nearly 60 per cent (by 2020, electricity demand could be 70 per cent higher than today).
- In 2008, Angola and Nigeria accounted for nearly half of all growth in OPEC output.[20]
- The global economy depends on cheap oil for about 40 per cent of its energy needs.
- The US, with less than 5 per cent of the world's population, uses almost 25 per cent of the world's total energy.
- Russia has 27 per cent of the world's gas reserves and 6 per cent of proven oil reserves; the remaining G-7 has only 4 per cent of gas reserves and 9 per cent of the oil.
- Since 2003, average world oil prices have risen steadily – reaching US$147 per barrel in July 2008, but falling back to US$60 by November 2008.
- The energy sector is worth an estimated US$10 trillion – this includes oil wells, pipelines, tankers, refineries, power plants, transmission lines, and other related infrastructure.
- 56 per cent of the world's proved oil reserves are located in the Middle East, with Saudi Arabia harboring the most reserves (265 billion barrels).

[19] Energy Information Administration. 2008. International Energy Outlook 2008. Available at: <http://www.eia.doe.gov/oiaf/ieo/index.html>; Roberts, P. 2005. The end of oil. The decline of the petroleum economy and the rise of the new energy order. London: Bloomsbury Publishing, pp. 7–15.

[20] Organization of the Petroleum Exporting Countries (OPEC): Algeria, Angola, Ecuador, Indonesia, Iran, Iraq, Kuwait, Libya, Nigeria, Qatar, Saudi Arabia, the United Arab Emirates, and Venezuela.

[21] Lindsay, M., 2005. The Security Threat to Oil Companies in and out of Conflict Zones, Business Briefing: Exploration and Production: The Oil & Gas Review, 2.

[22] Iraqi Pipeline Watch <http://www.iags.org/iraqpipelinewatch.htm>; Nigeria: oil infrastructure, delta militants and increased attacks. Stratfor. 30 July 2008. Available at: <http://www.stratfor.com/analysis/nigeria_oil_infrastructure_delta_militants_and_increased_attacks>.

[23] Attacks by Kataeb Jund al-Yemen (Soldiers of Yemen Brigades – an affiliate of AQ) against oil facilities in Yemen and attempted attacks on Saudi facilities, both non-conflict zones, are indications that non-state armed groups can achieve global energy disruptions by targeting installations in their home territory where they can take advantage of security deficits and more local support. Zambelis, C. 2006. Attacks in Yemen reflect al-Qaeda's global oil strategy. Terrorism Monitor 6(17).

developed countries, short-term supply shortages, tight production characteristics (little spare capacity for oil production) and lack of growth in OPEC production between 2005 and 2007, accelerated speculation, higher costs for oil exploration and development (much of which is being conducted in deepwater, offshore locations), a weaker US dollar, and increased commodity prices. In short, higher energy costs have been result of market fears that rising demand will eventually outgrow available supply. These concerns are reinforced by threats to energy supplies. In regards to the current climate where oil has dropped down to nearly US$60 per barrel due to slowed demand, thus providing cushioning on the supply side, it is important to note that this price is still 300 per cent higher than it was in 2000 and once the global economy improves – which it will – energy prices will continue to make their ascent as demand grows.[24] Hence in the long-term markets will continue to be characteristically sensitive to disruptions.

While market-related factors, such as tighter supply chains and changes in demand, are the primary areas that dictate global energy costs, other events such as geopolitical turbulence and threats of any kind to the oil infrastructure create uncertainty and also weigh into pricing.[25] Such uncertainty results in a security premium being placed on oil prices. According to international energy consultant Dr. Gal Luft, "whether perpetuated for political or criminal reasons, assaults on oil infrastructure have added a 'fear premium' of roughly $10 per barrel of oil." Thus a single energy 'event' can create "shockwaves through the world energy order, pushes prices up or down, and sets off tectonic shifts in global wealth and power."[26] Thus, while the EI has been targeted for many years in various countries, the effects of attacks have only recently generated more attention.

Grasping the trends

Elements of the EI, such as oil pipelines and electrical pylons, are oftentimes easily accessible and present the perfect "soft" target that can result in economic damage and losses if attacked.[27] In February 2003, members of a violent Muslim extremist group who had realized the value of attacking the EI published an online call to the "mujahideen of all Arab and Muslim countries in which the West has military bases or are involved in the energy industry, to rise against these interests in the name of the Muslim Ummah." Al-Qaida (AQ), which had previously opposed targeting oil in the Middle East, followed suit and announced a major shift in the group's strategy by calling on members to "do everything you can to stop the biggest plundering operation in history – the plundering of the resources of the present and future generations in collusion with the agents and the aliens [...] Be active and prevent them from reaching the

[24] IEA 2005: Oil Market Report. International Energy Agency. 12 April. According to the IEA, between the1980s to 2003/04 oil demand rose consistently and thus pushed oil inventories to lower levels. This tight supply coupled with the geopolitical uncertainties and the increased market speculation related to these uncertainties that have characterized the last decade have been the chief reason why prices have increased so dramatically.

[25] For example, a war in an oil-producing country, poor weather conditions (such as tropical storms) in oil-producing region, or direct attacks on the EI all create uncertainty in the market that can result in price volatility.

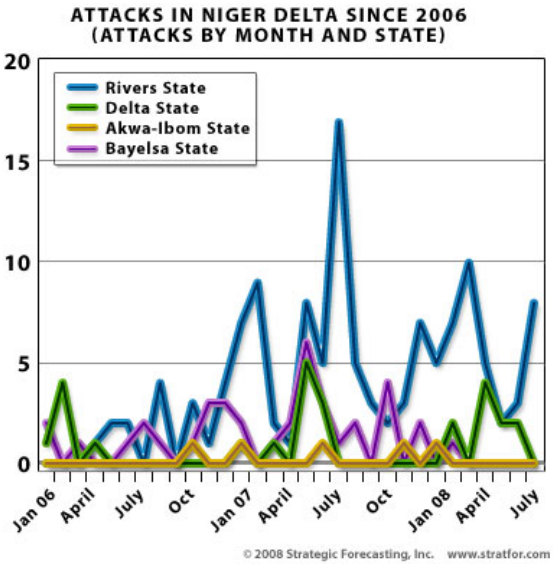
[26] Roberts p. 93.

[27] Nuclear facilities, which are typically located in relatively stable and developed nations, have not been targeted. In addition, these facilities are 'hard' targets that are operationally challenging to attack. Hydroelectric facilities, on the other hand, were targeted by Sendero Luminoso (The Shining Path) in Peru and caused a city-wide blackout in 1983. The vast networks of interrelated facilities in the petroleum and natural gas industries, however, are more accessible targets and require less investment.

oil, and mount your operations accordingly, particularly in Iraq and the Gulf."[28] This call for attacks against the EI, along with the increased volatility in the Middle East and elsewhere, resulted in a jump in security premiums from US$2 to $15 per barrel depending on the event.[29] For example, following an April 2008 attack on a Japanese oil tanker off the coast of Yemen, sweet crude rose to a record US$117.40 per barrel.[30] Shortly afterwards, another attack in May 2008 on an oil refinery in Aden, Yemen resulted in prices increasing to US$122.80 per barrel.

Middle East

Since 2003, Iraqi oil pipelines have been attacked by insurgents nearly 500 times, resulting in lost revenue amounting to US$11 billion between June 2003 and May 2005 alone.[31] Furthermore, attacks have not been isolated, but rather dispersed throughout the northern and southern region, causing minor to severe damages to infrastructure. But while the situation in Iraq has somewhat stabilized recently, the EI is still considered vulnerable and a highly desired target by AQ and its affiliates who seek to focus operations on hard economic targets, especially energy resources. Furthermore, and perhaps more significantly, Iraq has been an excellent training opportunity for armed groups to export EI attack techniques learned in Iraq to other countries.



AQ has also extended its efforts to harm the EI in Saudi Arabia and Yemen. In February 2006, AQ in the Arabian Peninsula attacked the Abqaiq oil facility, the world's largest oil complex. While this attack was unsuccessful, the event drove oil prices up by US$2 per barrel.[32] It should be noted that such attacks have little chance for success with Saudi Arabia spending between US$1.2 to 1.5 billion annually to protect its oil and gas industry; however in this case we see that even the threat to supplies resulted in a jump in prices.[33] More recently, AQ has carried out attacks on oil installations in Yemen, including a June 2008 attack on the Safir oil refinery and a subsequent video of

[28] Website Posts Full Version of New Audiotape Attributed to Bin Ladin, FBIS Report - FEA20041227000762, December 27, 2004.

[29] Zambelis, 2008.

[30] Fackler, M. 2008. Oil market rattled by attack on Japanese tanker. International Herald Tribune. 21 April. Available at: http://www.iht.com/articles/2008/04/21/asia/22tanker.php

[31] Iraqi Pipeline Watch. Available at: <http://www.iags.org/iraqpipelinewatch.htm>.

[32] Saudis foil oil facility attack. BBC News. 24 February 2006. Available at: <http://news.bbc.co.uk/2/hi/middle_east/4747488.stm>.

[33] Gasandoil.2005.Newsletter (10)19. Also see http://www.eia.doe.gov/emeu/cabs/Saudi_Arabia/Oil.html Saudi Arabia's oil and gas industry is well equipped to manage attacks or disruptions. Security forces have also been increased around facilities for additional protection.

the attack posted online.[34] The recently released online essay "Al Qaeda and the Battle for Oil" has stated that "al-Qa`ida's strategy to defeat the United States rests on bankrupting America by driving up oil prices by any means necessary" and furthermore goes on to mention the significance of recent attacks against EI in Yemen, Iraq, and Saudi Arabia.[35]

Africa

Nigeria, the world's eighth-largest oil exporter, has also been heavily assaulted by militants of, or affiliated with, the Movement for the Emancipation of the Niger Delta (MEND), which has carried out repeated attacks (an estimated 60 to 70 annually) on EI since 2006 - causing production to be cut by 20 to 25 percent (around 4-600,000 barrels per day).[36] MEND, a Niger Delta-based group that has introduced a new level of militancy and insurgency in this region by carrying out significant, large-scale attacks on the oil industry, has sought to severely, if not completely, destabilize Nigeria's oil production while also using various media outlets to communicate grievances involving ownership oil resources to the global community.[37] Due to the abysmal security in the Delta, the chief oil-producing region, oil installations have been an easy target for militants and criminal actors. MEND has also proven to be a formidable group with the ability to carry out destabilizing attacks, one of the most notable being the attack on the Shell Bonga deepwater offshore oil installation which, alone, cut Nigerian production by 10 per cent in June 2008 and set oil prices climbing.[38] The more recent six-day 'oil war' launched by MEND in mid-September 2008 resulted in damaged flow stations and oil pipelines, along with multiple casualties.[39] The Nigerian government reported that between 1999 and 2005 oil losses amounted to $6.8 billion, however, the more recent attacks carried out by MEND have pushed losses up to nearly US$61 million per day.[40]

Many other African oil-producing countries have also experienced such attacks, although none as severe as the deteriorating situation in Nigeria. From 1999 to 2004, the People's Liberation Army (SPLA), the main rebel group based in the south that fought the Sudanese government until 2005, attacked the oil

---

[34] "Saudis 'foil oil facility attack'". BBC News. 24 February 2006. Available at: <http://news.bbc.co.uk/2/hi/middle_east/4747488.stm>. Video available at: <http://clearinghouse.infovlad.net/showthread.php?t=15362>.

[35] See http://www.jamestown.org/terrorism/news/article.php?articleid=2374393 referring to At-Taqwa, Z., Al Qaeda and the Battle for Oil. Available at: <http://www.alqimmah.net/showthread.php?t=1226>.

[36] Nigeria is Africa's top oil producer; however, due to attacks by militants, Angola has been able to exceed Nigeria in terms of daily output. A million barrels of Nigerian oil are delivered to the US each day. Polgreen, L. 2008. Oil field operation suspended after attack by Nigerian rebels. The New York Times. 20 June. Available at: <http://www.nytimes.com/2008/06/20/world/africa/20nigeria.html?fta=y>.

[37] Giroux, J. 2008. Turmoil in the delta: trends and implications. Perspectives on Terrorism 2(8). MEND militants are the largest of several armed groups operating in the Delta region. They frequently kidnap foreign oil workers and sabotage oil installations and pipelines.

[38] The shutdown of this installation was significant as Bonga has a nameplate capacity of 220,000 barrels per day. It should also be noted that oil prices climbed to an all-time high of US$147 per barrel during this period. BBC News. 2008. Nigerian militants call ceasefire. 22 June. Available at: <http://news.bbc.co.uk/2/hi/africa/7468449.stm>.

[39] It is worth noting that during the month of September, demand for oil began to show a serious decline due to a weakened global economy; thus, the 'oil war' had only a minimal impact on global oil prices, since demand has sharply declined.

[40] Watts, M. 2007. 'Petro-Insurgency or Criminal Syndicate? Conflict & Violence in the Niger Delta." Review of African Political Economy,34:114.

industry multiple times. In one incident, the SPLA stated that "we chose the oil fields because this is the wealth of Sudan, which this government is not sharing with all of its people."[41] In addition, in 2007, the Chinese Zhongyuan Petroleum Exploration Bureau (ZPEB) facility in Ethiopia was attacked by militants believed to be with the Ogaden National Liberation Front (ONLF). This event resulted in multiple casualties and physical damage and represents the worst attack so far on Chinese interests in Africa.[42] On the other hand, geographical factors and security measures have limited EI attacks in Algeria, despite a resurgence of terrorist activity by al-Qaida of the Islamic Maghreb (AQIM). Algeria's energy sector has excellent security and is located in the unpopulated south; by contrast, in Nigeria, Angola, and other politically unstable emerging oil-producing African countries, production sites are in closer proximity to populated areas.[43] However, given AQ's global oil strategy and the adaptability and innovative nature of armed groups, the possibility of attacks against Algeria's EI should not be dismissed in the future.

Miscellaneous cases around the globe

Other recent campaigns targeting the EI have been launched in Pakistan, Turkey, Russia, India, and Mexico. During the last 25 years, the Kurdistan Workers' Party (PKK) has threatened and carried out attacks on pipelines – the most recent of which was the bombing of the Baku-Tbilisi-Ceyhan (BTC) pipeline in August 2008, forcing it to temporarily shut down.[44] Similar efforts to sabotage pipelines have been carried out by Chechen terrorists who bombed several pipelines during 2004 near Moscow, Volgograd, and Stavropol.[45] The United Liberation Front of Asom (ULFA) in India has also claimed credit for a series of pipeline attacks in 2006, while in neighboring Pakistan, Baloch militias have carried out numerous attacks against power transmission lines and gas installations; the sabotage of a gas pipeline in 2003 cut off supply to the Punjab and resulted in increased investment in security of the infrastructure.[46] In 2007, a string of oil and gas pipeline attacks carried out by militants of the Popular Revolutionary Army EPR in Mexico resulted in supply shortages, economic losses, and damages, while news of the attacks caused natural gas futures to increase.[47]

Additionally, groups targeting such resources appreciate the significance of EI and the global implications of energy disturbances caused by targeting such resources. Following the Bonga platform

[41] Luft. 2005.

[42] China, Ethiopia: facing the price of engaging in Africa. Stratfor. 24 April 2007. Available at: <http://www.stratfor.com/china_ethiopia_facing_price_engaging_africa>.

[43] While Angola's oil sector was rarely threatened during the 27-year long civil war (due to pressure from the US and France, who provided support to UNITA, to avoid hitting oil interests), separatist rebels in the oil-rich region of Cabinda pose threats to the industry.

[44] The BTC pipeline, recently built in 2005, transports 1 million barrels of oil a day from the Caspian Sea to Western markets through the Turkish port of Ceyhan. This was the first attack on this pipeline. <http://www.nzz.ch/nachrichten/international/pkk_meldet_anschlag_auf_oelpipeline_1.801051.html>.

[45] Luft. 2005. Russia is one of the world's top oil producers and receives 40 per cent of its state revenue from oil.

[46] Pakistan's population is growing rapidly. Thus its demand for gas will expand significantly. India's gas demand is expected to double by 2015, and the country will diversify its energy source to include more gas. Poor economic development has resulted local resistance where the Balochistan tribes oppose any energy projects in this resource-rich region.

[47] Hernandez, M. 2007. Mexican rebels claim pipeline attacks. Associated Press. 11 September. Available at: http://www.washingtonpost.com/wp-dyn/content/article/2007/09/10/AR2007091000596_pf.html.

attack, Jomo Gbomo, a spokesperson for MEND, stated: "The location for [today's] attack was deliberately chosen to remove any notion that offshore oil exploration is far from our reach."[48] MEND has also referred to the volatility of market prices in its statements. Following a 2006 attack, Gbomo noted that "the fact that we have influenced the price of world oil, no matter how little, and caught the attention of the foreign media indicates we are on the right track."[49] Such a statement was strikingly similar to statement issued by AQ following the 2002 attack on the *Limburg*, a French oil tanker off the coast of Yemen carrying 397,000 barrels of crude. AQ made sure to point out that the incident "was not an incidental strike at a passing tanker but [...] on the international oil-carrying line in the full sense of the word."[50]

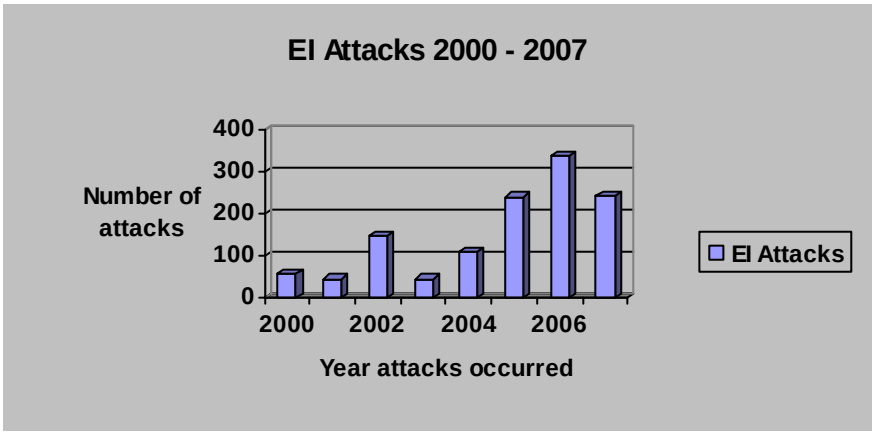


Figure 2 [51]

Conclusion

A snapshot of this brief empirical picture reveals that EI attacks are widespread geographically and are becoming not less, but more frequent. In the 21st century, the reality of tighter energy supplies and competition for global notoriety has made EI a more attractive target for non-state actors seeking to carry out attacks with maximum impact.[52] In this way, armed groups not only obtain success by causing state disruptions, but they also generate global economic turbulence that can translate into higher

[48] Luft. 2005.

[49] Cummins, C., 2005. As oil supplies are stretched, rebels, terrorists get new clout: Media-savvy guerrillas roil global oil prices in fight with Nigerian government. The Wall Street Journal, [internet]. 12 April. Available at: <http://online.wsj.com/article/SB114463092157621421.html?mod=todays_us_page_one>.

[50] Daly, J.C.K. 2006. Saudi Oil Facilities: Al-Qaeda's Next Target? Terrorism Monitor vol. 4, no. 4. 23 February 2006.

[51] This data was compiled using data gathered from the Global Terrorism Database. Additional monitoring was performed to capture attacks that may have not been included in the GTD. The data for 2007 is still being gathered and thus 2007 attacks may be slightly higher than currently listed. Between June 2003 and March 2008 there have been 469 attack aimed at Iraqi energy infrastructure (2003 = 37; 2004 = 148; 2005 = 100; 2006 = 101; 2007=59; 2008 = 4). At this point the number of attacks for 2008 is approaching 200 however data is still being collected in this area.

[52] A few simple attacks could disrupt the supply chain and inflict significant economic damage. Fedorowicz, J.K. 2007. The ten thousand mile target: energy infrastructure and terrorism today. CCISS, Critical Energy Infrastructure Protection Policy Research Series, 2.

energy prices for a world that depends on low-cost petroleum and a reliable, constant supply.[53] In another example, Somali pirates attack oil tankers, and other commercial and non-commercial ships, traversing through the Gulf of Aden for sheer profit.[54] In addition, due to accessible and affordable technology, EI attacks by militants now receive the desired global attention.

Implications for EU energy policy

North Africa, specifically Algeria, is an important source of energy – mainly gas - for Europe. However, in line with the trend described herein, resources in this region are threatened by ongoing conflict and politically motivated violent groups, such as Al-Qa`ida of the Islamic Maghreb (AQIM), who have begun to threaten and/or attack the energy sector, although not as significantly as in groups in Sudan or Nigeria. Given AQ's global oil strategy, which seeks to target EI, more attacks aimed at Algeria's energy sector may emerge in the years ahead. However, unique to the 21st century energy picture EI attacks, or the threat of, can lead to uncertainty amongst market players and overall insecurity that raises global energy costs – thus placing additional budgetary pressures on states and consumers. The worst case scenario being that attacks can affect supply along key routes. In addition, the natural gas found within the Maghreb is of particular importance to its European neighbors as gas is a regional commodity – thus disruptions that originate in the Maghreb can affect the regional supply chain.

To counter this trend and the inflexibility of the current energy environment, states need to adopt a multifaceted approach. In the long-term, the EU needs to make a concerted effort to diversify its energy portfolio, develop domestic energy sources and invest in alternative energies so not to rely so heavily on oil and gas from unstable neighborhoods. In the short-term, however, not only should states address the issue of disruption to energy flows by assisting in the fortification of facilities, but they must also work with the media and financial markets that react – and overreact - to such threats.[55] Energy security can also be improved by increasing global strategic stockpiles in consumer countries and hence the international community – lead by North America and the EU – must press for capacity increases to mitigate the consequences of disruptions.[56]

In addition, oil and gas importing countries, such as Switzerland and EU countries, can allocate much-needed aid to producing countries – such as Sudan and Algeria – who struggle with securing energy resources. As mentioned, the EU needs to look beyond simply securing its domestic energy infrastructure, but also assist those key producing countries where governments are unable – or unwilling – to secure resources. European countries, for instance, could provide funding for costly technology to enhance the security of pipelines, facilities and ports. Other assistance can come in the

[53] In the US, for example, oil prices rose to nearly US$40 billion in 2004 due to threats and/or attacks to the EI.

[54] Piracy off of the Somali cost has reached record highs in 2008 with over 80 attacks. In each case the perpetrators demanded hefty ransoms. The recent attack on the Saudi oil tanker carrying over 2 million barrels of oil was captured 450 nautical miles offshore and lead to a jump in oil costs to more than US $58 a barrel. Prior to this attack oil was approaching US$55 per barrel. http://network.nationalpost.com/np/blogs/posted/archive/2008/11/17/today-in-piracy-pirates-hijack-saudi-owned-oil-tanker-with-25-crew-aboard.aspx

[55] Schmid, A.P. 2007. Targeting oil and other energy resources and infrastructure. MIPT.

[56] Ibid. Capacity increases can help cushion market sensitivity. For example, despite continued turmoil in Nigeria's oil-producing region, the price of oil has been declining steadily since August 2008 due to decreased demand from a slowing global economy.

form of military training, funding police and community patrols, and strengthening capacity and facilities.[57]

In Iraq, the US helped fund 14,000 security guards that were placed in critical locations along major pipelines and at facilities. Similar efforts are underway in the Gulf of Guinea and off Somalia's coast where NATO, the EU and the US Navy, respectively, have provided assistance in maritime security. Southern Europe, who relies on gas supplies from Northern Africa, may also require the assistance of NATO to help protect key installations in the Maghreb.

Although security measures are necessary, they do not address the factors that drive violence. In order to deter attacks effectively, external state actors can work with central and local governments to allocate more resources to addressing the abysmal socio-economic realities that are oftentimes the crux of hostilities aimed at EI.[58] Such an approach takes into account the need to protect resources (security) while also meeting community needs to decrease poverty (development). For example, in 2003, Swissaid requested that the World Bank and Exxon Mobile, who shared in the cost of building Chad's oil pipeline to Cameroon, ensure that civil society benefited from this new source of state income.[59]

Broader private sector engagement

Multinational oil companies and community organizations (NGOs) also have a unique role to play, as they can reach out directly to the community to assess needs and implement bottom-up solutions. Shell in Nigeria, for example, has hired "community liaison officers" to initiate direct dialogs with the Niger Delta communities. These consultations have resulted in the provision of storage tanks and generators to 21 towns and villages. But they need to go a step further. Multinational oil companies have the resources to broaden and deepen the scope and reach of their corporate social responsibility (CSR) initiatives so to increase community support of energy production initiatives. Currently many of the communities in these unstable yet energy-wealthy environments do not see the benefits derived from the oil and/or gas extraction and thus there is little to deter them from carrying out attacks, whether criminally or politically motivated. Such an approach would require working directly with local governments, NGOs, external state actors, and international organizations to implement basic development programs that would include the building of roads, homes, schools, hospitals, etc. Essentially, this would employ a bottom-up approach to counter-balance the security measures employed from the top down. Such a multifaceted approach has the potential to enhance security, address community needs, and deter attacks.

---

[57] Such security measures can involve: burying pipelines, hardening the pipeline against corrosion, increasing patrols and security forces for facilities, security cameras, etc. Technology is another important investment that can provide better protection. Developments using seismic sensing of underground vibrations can identify whether unauthorized personnel are near a pipeline – thus preventing sabotage.

[58] The US has recently initiated a number of measures to address the multitude of security issues in sub-Saharan Africa, with particular focus on the Gulf of Guinea (GoG) region. In late 2007, the US Navy began training government officials from the GoG region to improve maritime security and have since worked specifically with the Nigerian Navy to enhance their ability to counter the threats posed by MEND and other militants. In addition, in September 2008, the US was also looking to launch the US Africa Command (AFRICOM), which seeks to encourage US military cooperation with African governments. Such initiatives, which are clearly connected to protecting US interests, offer some promise; however they do not address the abysmal socio-economic realities that have fueled militancy and insurgency where terrorism is increasingly the tactic of choice.

[59] http://www.globalpolicy.org/security/natres/oil/2003/0204af.htm.

Annotated Bibliography

The available literature on energy security is fairly extensive, since the availability of low-cost energy and the security of such resources are a significant element of modern, developed economies. Energy security concerns the vulnerability of energy supplies created by political instability, state competition over energy resources, concerns over the viability of long-term oil production (i.e., the debate on peak oil), and the uncertainty of resource availability due to accidents, natural disasters, and attacks on the infrastructure. Within this literature, the topic of threats to EI is the least developed field, and thus there is a need within the scientific community to further study the effects of EI attacks in the 21st century. As this body of literature is rather small, the select resources highlighted in this section have all been published in the last eight years.

Policy documents/reports

Åshild, K. and Brynjar, L. 2001. Terrorism and oil – an explosive mixture? A survey of terrorist and rebel attacks on petroleum infrastructure 1968–1999. FFI Rapport. Norwegian Defense Research Establishment.

This report presents an overview of terrorist and rebel attacks against the petroleum production infrastructure during the past three decades and provides an empirical basis for the development of scenarios for long-term defense and crisis management planning.

Parfomak, P.W. and Frittelli, J. 2007. Maritime Security: Potential Terrorist Attacks and Protection Priorities. United States CRS Report for Congress.

This report examines the terrorist threat to maritime activities. Because oil tankers are constantly shipping exports from unstable locations where piracy and attacks are of concern, the report presents potential attack scenarios based on actual past attacks or potential attacks developed for maritime security exercises. It also notes the challenge to maritime security planners and implications for homeland security policy.

Tørhaug, M. 2006. Petroleum supply vulnerability due to terrorism at North Sea oil and gas infrastructures. In: Protection of Civilian Infrastructure from Acts of Terrorism, NATO Security through Science Series. Springer Netherlands.

This article discusses the management of risks related to terrorism and focuses on North Sea oil and gas production and transportation systems and the European oil and gas markets. The author notes how threats to oil and gas markets have added to a perception of uncertainty regarding supplies, which may already have caused a higher market price for crude oil.

Academic literature

Baev, P.K. 2006. Reevaluating the risks of terrorist attacks against energy infrastructure in Asia. China and Eurasia Forum Quarterly, vol. 4, no.2: 33–8.

The author asks why there have not been more devastating attacks on energy infrastructure, despite the relative ease in carrying out EI attacks. He points out that the biggest recent interruptions in energy supplies (i.e., Hurricane Katrina and the Moscow blackout of May 2005, which was due to a short circuit) were not caused by breaches to security due to intentional human agency. He notes the availability of softer tourist targets and the recent "hardening" of numerous energy targets, which has made it more difficult for terrorists to hit them successfully. He also notes some other interesting strategic considerations that factor into the targeting of EI.

Forest, J.J. and Sousa, M.V. 2006. Oil and terrorism in the New Gulf: Framing US energy and security policy in the Gulf of Guinea. Lexington Books.

This book focuses on US national security interests and the nexus between energy wealth and good governance in the Gulf of Guinea (West Africa). It does a good job at covering the growing energy security interests in Africa from a policy perspective. The authors make the case that the US has a unique opportunity in Africa to harmonize its efforts to secure energy resources while also assisting governments in addressing poverty and development needs. US policy in the Gulf of Guinea, according to the authors, should develop a long-term, integrated approach that takes both security and development needs into account.

Fedorowicz, J.K. 2007. The ten thousand mile target: energy infrastructure and terrorism today. The Canadian Center of Intelligence and Security Studies, at Carleton University, Policy Research Series, 2. Available at: www.carleton.ca/cciss/res_docs/ceip/fedorowicz.pdf

This study was part of the CCISS Critical Energy Infrastructure Protection Policy Research Project in Canada. It examines terrorist attacks on critical infrastructure in several countries. The author also reviews state responses to EI attacks in an effort to provide policy advice for Canada. This is a basic study that succeeds in briefly covering the history of EI attacks and putting the threat into context for a developed economy like Canada.

Lindsay, M., 2005. The Security Threat to Oil Companies in and out of Conflict Zones, Business Briefing: Exploration and Production: The Oil & Gas Review, 2. Available at: <http://www.touchoilandgas.com/security-threat-companies-conflict-a688-1.html>

The author discusses how the most powerful industrialized nations are becoming increasingly reliant on oil supplies from political unstable zones in the Middle East, Venezuela, Libya, Kazakhstan, Nigeria, and other poor countries with significant reserves. He notes that attacks are occurring both within and outside of conflict zones and discusses some key trends. This notable paper discusses the broader trend of more oil and gas being produced in less developed countries with little security.

Luft, G. & Korin, A. 2003. Terror's next target. The Journal of International Security Affairs. Available at: <http://www.iags.org/n053004a.htm>

The authors argue that political violence movements – especially transnational ones – have identified the world's energy system as a major vulnerability. Thus, such groups have sought to target these resources in an effort to cause economic disruption. While some of this article delves into hypotheticals, the authors do a fair job of describing the threat and the potential implications for the global economy. One of the authors, Gal Luft, is among the world's foremost experts on this topic.

Roberts, P. 2005. The end of oil. The decline of the petroleum economy and the rise of the new energy order. London: Bloomsbury Publishing

The author provides a great introduction to the changing global supply of oil, which is decreasing while demand is increasing, creating greater vulnerability. The author aptly describes changes to energy security and puts the threat and uncertainty in the market into perspective. Roberts also covers the development of alternative energy sources, which may stem economic turbulence.

Schmid, A.P. 2007. Targeting oil and other energy resources and infrastructure. MIPT.

The author examines threats to world oil supplies from al-Qaida and other militant groups. This is a good background study that puts the threat into context. While the author does not go into any great detail and while his conclusion could have provided more concrete recommendations on how to counter such threats, he

does make one appropriate recommendation by calling for states to reach out to media and financial institutions that react – or rather overreact – to attacks on the EI.

Williams, J.F. 2008. Al-Qaida Threats and Strategies: The religious justification for targeting the international energy economy. The Canadian Center of Intelligence and Security Studies, at Carleton University, Policy Research Series, 3. Available at:
<http://www.carleton.ca/cciss/ceipprs_publications/williams_03_2008.pdf>

This article describes methods that can be used for threat analysis in the international energy economy. The author looks specifically at al-Qaida's interest in attacking the EI and petroleum interests by examining the religious justification offered by Salafi-Jihadi religious scholars for attacking petroleum-related interests throughout the world.

Internet resources

IAGS Journal of Energy Security. Available at: <http://www.ensec.org/>

Provides various articles relating to energy security.

Institute for the Analysis of Global Security (IAGS). Available at: <http://iags.org>

The Institute for the Analysis of Global Security is an organization that focuses on energy security and provides a number of resources such as the Iraq Pipeline Watch and energy security articles.

BP. Statistical Review of World Energy. Available at:
<http://www.bp.com/productlanding.do?categoryId=6929&contentId=7044622>

Provides an annual review of world energy consumption, sources, etc.

The Oil Drum: Blog. Available at: <http://www.theoildrum.com/>

A blog that provides a number of resources and analysis on energy security.

United States Energy Information Administration. International Energy Outlook. Available at:
<http://www.eia.doe.gov/>

The EIA provides annual reports on global energy supplies. Such a resource is a critical component to any study on energy security, as it puts market uncertainty into context.

CSS
An ETH Center

The Center for Security Studies of the ETH Zurich (Swiss Federal Institute of Technology) was founded in 1986 and specializes in the fields of international relations and security policy. The Center for Security Studies is a member of the Center for Comparative and International Studies (CIS), which is a joint initiative between the ETH Zurich and the University of Zurich that specializes in the fields of comparative politics and international relations.

The Crisis and Risk Network (CRN) is an Internet and workshop initiative for international dialog on national-level security risks and vulnerabilities, critical infrastructure protection (CIP) and emergency preparedness.

As a complementary service to the International Relations and Security Network (ISN), the CRN is coordinated and developed by the Center for Security Studies at the Swiss Federal Institute of Technology (ETH) Zurich, Switzerland. (www.crn.ethz.ch)

Focal Report 1 CRITICAL INFRASTRUCTURE PROTECTION. Zurich, October 2008 Crisis and Risk Network (CRN) Center for Security Studies (CSS), ETH Zurich Commissioned by the Federal Office for Civil Protection (FOCP). Purpose: As part of a larger mandate, the Swiss Federal Office for Civil Protection (FOCP) has tasked the Center for Security Studies (CSS) at ETH Zurich