Myriam Dunn and Victor Mauer (eds.)

INTERNATIONAL **CIIP HANDBOOK** 2006

VOL. II

ANALYZING ISSUES, CHALLENGES, AND PROSPECTS

Series Editors
Andreas Wenger and Victor Mauer

Center for Security Studies, ETH Zurich

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

CSS
An ETH Center

Myriam Dunn and Victor Mauer (eds.)

INTERNATIONAL **CIIP HANDBOOK** 2006

VOL. II

ANALYZING ISSUES, CHALLENGES, AND PROSPECTS

Series Editors
Andreas Wenger and Victor Mauer

Center for Security Studies, ETH Zurich

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

The CIIP Handbook is also available on the Internet in full text: www.crn.ethz.ch
All comments on the CIIP Handbook are most welcome.

Eds. Myriam Dunn, Victor Mauer
Center for Security Studies at ETH Zurich (Swiss Federal Institute of Technology)

Contact:
Center for Security Studies
Seilergraben 45–49
ETH Zentrum / SEI
CH-8092 Zurich
Switzerland

The Handbook represents the views and interpretations of the authors, unless otherwise stated.

Layout and Graphics: Fabian Furter

ISBN 3-905696-08-8
ISSN 1660-3222

Contents

Introduction

By Myriam Dunn and Victor Mauer

Certain forms of infrastructure, or infrastructure sectors, are of special importance for modern society. Among these so-called critical infrastructures (CI), which are interrelated and interdependent, are electricity production and distribution, transport, telecommunications, and water supplies. If any of these infrastructures should cease to function for a prolonged period, society will be hard pressed to maintain its functioning as a whole.[1] In general, one of the remarkable features of modern, computer-based society is that a seemingly endless series of small details must function correctly and in co-operation in order to maintain the numerous processes that we take for granted. A single "bug", the smallest aberration, so subtle as to be virtually impossible to foresee, can theoretically initiate a complex chain of events, the effects of which can become manifest at a national or even global level.[2] This particular feature distinguishes data communication and computers in the broad sense of the word, as well as networks, from other critical infrastructure elements: The term information infrastructure is usually used to describe the totality of such interconnected computers and networks, as well as the essential information flowing through them. The distinguishing characteristic of the information infrastructure is that it is all-embracing, because it links other infrastructure systems together.

Protecting these critical information infrastructures (CII) against disruption of any kind is increasingly crucial in maintaining both domestic stability and national security. In accordance, the security of cyberspace has become an important consideration in most countries, and governments worldwide are already putting a fair amount of effort into cyber-security. In Volume I of the 2006 International CIIP Handbook, we have compiled 20 country surveys and six surveys on international efforts for the protection of cyberspace, and have

1 Cf. the definition used in President's Commission on Critical Infrastructure Protection (PCCIP). Critical Foundations: Protecting America's Infrastructures (Washington, October 1997). See also the definitions of CI and CIP of various countries in Volume I of the International CIIP Handbook 2006.

2 Westrin, Peter. "Critical Information Infrastructure Protection". In: Wenger, Andreas (ed.): The Internet and the Changing Face of International Relations and Security. Information & Security: An International Journal, Vol. 7 (2001), pp. 67–79.

pointed out the issues of highest importance. As an extension of Volume I, we offer the following in-depth analysis of key issues and major future challenges for the CIIP community. Specifically, we focus on those issues that demand the integration of a variety of viewpoints. At present, CIIP is in the capable hands of engineers, consultants, practitioners, and IT-security experts. All of these communities address important aspects, but often miss crucial key features of the complex systems at hand — namely their socio-political aspects. In bringing a socio-political perspective to the debate, we hope to stimulate a much-needed dialog between the different disciplines and to provoke a discussion of specific issues in a new and fruitful manner.

The volume has three parts, covering a broad range of topics: Part I deals with conceptual issues. Because the problem complex that CIIP deals with represents a highly dynamic social phenomenon, the workings of critical systems and their exact role and criticality for society are still very elusive. This might change once this area of research gains a more stable scientific and methodological base. In the meantime, basic issues need to be addressed: What exactly is CIP? What is CIIP? How do the two concepts differ? What approaches are in use to analyze these systems? What do we seek to protect? These and similar questions are addressed in Part I.

Part II deals with aspects of the threat to the information infrastructure, in order to deepen the understanding of issues raised in Part I. In specific, we look at what it is that actually threatens the information infrastructure. The outline of possible actors includes hostile states, terrorist groups, fanatical religious movements, criminal organizations, and extremist political parties, as well as individuals such as discontented insiders and irresponsible hackers or crackers. In addition, complexity itself brings about the risk of a truly major, society-threatening chain reaction of IT-related events. At the same time, the nature and diversity of the threat makes it difficult for nation-states to act in a timely manner.

In Part III, we address two persistent policy issues identified in Volume I in some more detail: public-private partnerships and the need for international cooperation. We will see that these issues are interrelated and that ultimately, first-rate solutions for cyber-security demand a global culture of cyber-security that starts at the national level. But how does the national become global or, to put it differently, how can we move from these national approaches to a global culture? Is there some common denominator to aim for? Or does a

global culture of cyber-security already exist, at least in a rudimentary form? With these questions in mind, Part III helps to identify common themes, best practices, but especially problems and pitfalls for a future global culture of cyber-security.

Part I CIIP Conceptual Issues

Infrastructure owners, regulators, decision-makers, and researchers currently face difficulties in understanding the complex behavior of interdependent critical infrastructures, because infrastructure networks present numerous theoretical and practical challenges. In general, networks are inherently difficult to understand and to manage. There are several reasons: the structural and dynamical complexity of the networks, their large-scale and time-dependent behavior, their dynamic evolution, the diversity of possible connections between nodes, and node diversity.[3]

Additionally, many of the challenges and problems posed by the infrastructures are only just emerging. The inherent system characteristics of new information infrastructures differ radically from those of traditional infrastructures in terms of scale, connectivity, and dependencies. Moreover, there are several "drivers" that will likely aggravate the problem of critical information infrastructures in the future. Among these drivers are the interlinked aspects of market forces, technological evolutions, and newly emerging risks. This situation forces analysts to constantly look ahead and to develop new analytical techniques, methodologies, and mindsets to keep up with the rapid developments in the technological sphere.[4]

Assessment of Methods and Models

In general, an assessment of approaches for analyzing various aspects of the CII is very enlightening. In effect, the methodological toolbox can serve as an indicator of the current understanding of key CIIP issues. In her chapter,

3 Strogatz, Steven H. "Exploring Complex Networks". Nature, 410 (8 March 2001), pp. 268–276. http://tam.cornell.edu/SS_exploring_complex_networks.pdf.

4 Parsons, T.J. "Protecting Critical Information Infrastructures. The Co-ordination and Development of Cross-Sectoral Research in the UK". Plenary address at the Future of European Crisis Management Conference (Uppsala, March 2001).

Myriam Dunn compares methods, models, and approaches used in a variety of countries to analyze and evaluate aspects of critical information infrastructures. Such methods and models are considered to be of particular relevance for the field of CIIP, because it is important to understand CI/CII behavior under normal circumstances and under stress, as well as their role and criticality for government and society. Such an understanding is ultimately necessary in order to cost-effectively prioritize means of preparing for, mitigating, and responding to possible threats.

Dunn points out that current methodologies for analyzing CII are insufficient in a number of ways: One of the major shortcomings is that the majority of them do not pass the "interdependency test". In other words, they fail to address, let alone understand, the issue of interdependencies and possible cascading effects. Besides, the available methods are either too sector-specific or too focused on single infrastructures and do not take into account the strategic, security-related, and economic importance of CII. Dunn also addresses the extensive problem of "conceptual sloppiness" that the community is culpable of. This conceptual negligence often leads to analytical negligence — with negative consequences for approaches to the issue in general and for the design of protection measures in particular.

Viewpoints and Protection Measures

Apart from a basic understanding of what to protect and how to protect it, different conceptions and viewpoints logically also have an impact on protection measures: Depending on their influence or on the resources at hand, various key players shape the issue in accordance with their view of the problem. Different groups, whether they be private, public, or a mixture of both, do not usually agree on the exact nature of the problem or on what assets need to be protected with which measures. In the second chapter of this volume, Isabelle Abele-Wigert elaborates on the various actors involved in CIIP such as governments, businesses, individuals, or the academia. Abele-Wigert identifies four typologies for cyber-security: an IT-security perspective, an economic perspective, a law enforcement perspective, and a national-security perspective. While all typologies can be found in all countries, the emphasis given to one or more of them varies to a considerable degree. Ultimately, the dominance of one or several typologies has implications for the shape of the protection

policies and, subsequently, for determining appropriate protection efforts, goals, strategies, and instruments for solving problems.

In the end, the distribution of resources and the technical and social means for countering the risk are important for the outcome. We can observe that the different actors involved — ranging from government agencies and the technology community to insurance companies — have divergent interests and compete with one another by means of scenarios describing how they believe the threat will manifest itself in the future.[5] Furthermore, the selection of policies seems to largely depend upon two factors: One is the varying degree to which resources are available to the different groups. The other factor is the impact of cultural and legal norms, because they restrict the number of potential strategies available for selection.[6] In general, we can identify two influential discourses: On the one hand, law enforcement agencies emphasize their view of the risk as "computer crime", while on the other hand, the private sector running the infrastructures perceives the risk mainly as a local, technical problem or in terms of economic costs.[7] Because the technology generating the risk makes it very difficult to fight potential attackers in advance, protective measures focus on preventive strategies and on trying to minimize the impact of an attack when it occurs. Here, the infrastructure providers are in a strong position, because they alone are in the position to install technical safeguards for IT security at the level of individual infrastructures.

Norms are also important in selecting the strategies. Most importantly, the general aversion of the new economy to government regulation as well as legal restrictions limit the choice of strategies.[8] Besides these cultural differences with regard to strategy, the nature of cyber-attacks naturally positions law enforcement at the forefront: It is often impossible to determine at the outset whether an intrusion is an act of vandalism, computer crime, terrorism,

5 Bendrath, Ralf. "The American Cyber-Angst and the Real World – Any Link?" In: Robert Latham (ed.), Bombs and Bandwidth: The Emerging Relationship between IT and Security (New York, The New Press, 2003), pp. 49–73; id. "The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection". In: Wenger, Andreas (ed.). The Internet and the Changing Face of International Relations and Security, Information & Security: An International Journal, Vol. 7 (2001), pp. 80–103.

6 Dunn, Myriam. "Cyber-Threats and Countermeasures: Towards an Analytical Framework for Explaining Threat Politics in the Information Age". Conference paper, SGIR Fifth Pan-European IR Conference, The Hague, 10 September 2004.

7 Bendrath, "The Cyberwar Debate", p. 97.

8 Ibid., p. 98.

foreign intelligence activity, or some form of strategic attack. The only way to determine the source, nature, and scope of the incident is to investigate. The authority to investigate such matters and to obtain the necessary court orders or subpoenas clearly resides with law enforcement. As a consequence of the nature of cyber-threats, the cyber-crime/law enforcement paradigm is emerging as the strongest viewpoint in most countries.

Part II CIIP Threat Issues

The infrastructure of modern societies has always been, and still is, vulnerable to all kinds of threats. The information infrastructure can be employed as a means to bring about the disruption of critical infrastructure – including the information infrastructure itself. Information can be stolen or manipulated. Computers can be infected with malicious programs, which can disrupt not only software and directly linked hardware, but also adjoining, or bordering technical systems – besides eroding trust and confidence in society as a whole. But what exactly is it that threatens us?

The Threat Spectrum

Statistically, some of the most dangerous threats stem from attacks committed by "insiders" – individuals who are, or previously had been, authorized to use the information systems that they eventually employ to spread harm.[9] However, most stakeholders are far more concerned with external attacks. In fact, long before 11 September 2001, it was understood that more and more state actors, as well as non-state actors, are willing to contravene national legal frameworks and hide in the relative anonymity of cyberspace.[10] If these actors carry out their attacks using "cyber-"weapons and strategies, one label often bestowed upon them is "hacker". This term has two major connotations, one positive

9 US Secret Service and Carnegie Mellon University Software Engineering Institute. Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors (2005). http://www.secretservice.gov/ntac_its.shtml (last accessed on 10 June 2005).

10 President's Commission on Critical Infrastructure Protection (PCCIP). Critical Foundations: Protecting America's Infrastructures (Washington, DC, October 1997); National Academy of Sciences, Computer Science and Telecommunications Board (1991). Computers at Risk: Safe Computing in the Information Age (Washington, DC, National Academy Press: 1991).

and one pejorative: In the computing community, it describes a member of a distinct social group, a particularly brilliant programmer or technical expert who knows a set of programming interfaces well enough to write novel and useful software. In popular usage and in the media, however, it generally describes computer intruders or criminals.[11]

Currently, the most frequently discussed topic in connection with cyberspace is cyber-crime. Most of these crimes are becoming more sophisticated by the day. Incidents of "phishing", which involves sending false e-mails purportedly from banks or other institutions to their customers to trick them into giving out their account details, have increased significantly during the past couple of years. Issues of identity theft and authentication on the internet are impeding e-commerce across the globe, and regular attempts of distributed denial-of-service (DDOS) attacks cause high losses to business establishments.

Nonetheless general, cyber-crime is often considered to be an unstructured threat, because it is random and relatively limited.[12] It consists of adversaries with limited funds and organization and short-term goals. The resources, tools, skills, and funding available to the actors are too limited to accomplish a sophisticated attack, and they also lack the motivation to do so. In contrast, structured threats are considerably more methodical and better supported. Adversaries from this group have all-source intelligence support, extensive funding, organized professional support, and long-term goals. Foreign intelligence services, criminal elements, and professional hackers involved in information warfare, criminal activities, or industrial espionage also fall into this threat category.[13]

Unstructured threats are not a danger to national security and would not normally concern the national-security community. Nonetheless, such attacks can cause considerable damage mainly in the economic realm. Furthermore, there are no clear boundaries between the two categories: Even though an unstructured threat is not of direct concern, there is the danger that a structured threat actor could masquerade as an unstructured threat actor, or that structured

11 Levy, Steven. Hackers: Heroes of the Computer Revolution (New York: Anchor Press, 1984). Erickson, Jon. Hacking: The Art of Exploitation (San Francisco: No Starch Press, 2003); OCIPEP, Threat Analysis.

12 National Academy of Sciences, Computer Science and Telecommunications Board. Computers at Risk: Safe Computing in the Information Age (Washington, DC: National Academy Press, 1991).

13 Minihan, Kenneth A. Prepared statement by Lt. Gen. Kenneth A. Minihan, Director, National Security Agency, before the Senate Governmental Affairs Committee, 24 June 1998.

actors could seek the help of technologically skilled individuals from the other group. In fact, state-sponsored hacking has long been of concern to Western governments and businesses. Even though an ordinary "hacker" generally lacks the motivation to cause violence or severe economic or social harm,[14] it is feared that a human actor with the capability to cause serious damage but lacking motivation could be swayed by sufficiently large sums of money to provide their knowledge to a "malicious" group of actors. "Cyber-terrorism" in particular has become a catchphrase in the debate, and experts and government officials like to warn of cyber-terrorism as a looming threat to national security.

Cyber-terrorism

However, the discussion surrounding cyber-terrorism has overwhelmingly taken place not within the confines of academe, but in the mass media. In other words, the majority of the "literature" on this topic is not literature at all, but journalism. The hallmark of the sparse academic literature is that most of it is unsatisfactory in terms of intellectual substance: Too many arguments on the nature and scale of cyber-terrorism are uncritically adopted from official statements or from media coverage.[15] This is epitomized in the tendency of many authors to "hype" the issue with rhetorical dramatization and alarmist warnings.[16] However, if we define cyber-terror as an attack or series of attacks that is carried out by terrorists, that instills fear by effects that are destructive or disruptive, and that has a political, religious, or ideological motivation, then none of the disruptive "cyber-" incidents of the last years qualify as examples of cyber-terrorism. So why has this fear been so persistent?

14 Denning, Dorothy. "Is Cyber Terror Next?" In: Calhoun, Craig; Paul Price; and Ashley Timmer (eds.). Understanding September 11 (New York: W. W. Norton, 2002). http://www.ssrc.org/sept11/essays/denning.htm (last accessed on 10 June 2005).

15 The media loves to use the "cyber-" prefix in connection with disaster, and routinely features sensationalist headlines that cannot serve as a measure of the problem's scope. Examples for such articles are: Christensen, John. "Bracing for guerrilla warfare in cyberspace", CNN Interactive, 6 April 1999; Kelley, Jack. "Terror groups hide behind Web encryption". In: USA Today, 6 February 2001; McWilliams, Brian. "Suspect Claims Al Qaeda Hacked Microsoft – Expert". In: Newsbytes, 17 December 2001; CNN. "FBI: Al Qaeda may have probed government sites", 17 January 2002; Newsweek. "Islamic Cyberterror. Not a Matter of If But of When", 20 May 2002.

16 Arquilla, John. "The Great Cyberwar of 2002. A WIRED Scenario" In: WIRED, 6 February 1998, pp. 122–7, 160–70; Schwartau, Winn. Information Warfare. Cyberterrorism: Protecting Your Personal Security in the Electronic Age. 2nd ed. (New York: Thundermouth Press, 1994).

In his article, Clay Wilson addresses the issue of cyber-terrorism and argues that continual internet and computer security vulnerabilities, which have been widely publicized, may gradually encourage such actors to develop new computer skills, either through education or through alliances with criminal organizations, and to consider attempting a cyber-attack against critical infrastructure. Reports show that terrorists and extremists in the Middle East and South Asia may be increasingly collaborating with cyber-criminals to illegally transfer money, arms, and drugs. These links with cyber-criminals may be adding to the computer skills of such groups, and may also provide them with access to highly skilled computer programmers.

But even though most terrorist groups have seized on the opportunity accorded by the information revolution by establishing a multiple web presence, making available uncensored propaganda, and by using the web as an auxiliary recruitment and fundraising tool,[17] cyber-space has so far mainly served as a force multiplier in intelligence gathering and target-acquisition for terrorist groups and not as an offensive weapon. Therefore, at least until now, cyber-terror, as defined above, remains fiction. To answer the question of how likely a cyber-terror attack is in the future, we would need concrete intelligence data of which non-state actor is likely to employ cyber-tools as an offensive weapon at what point in time.[18] This, in turn, is not a solution, but represents another problem, since the difficulties of the intelligence and law enforcement communities in obtaining relevant information on the scope and degree of the threat are well known.

It seems that we cannot afford to shrug off the threat altogether, due to uncertainty about the rapid progress of technological development as well as dynamic change of the capabilities of terrorism groups themselves.[19] The main problem with the concept of cyber-terror seems to be the "terror" suffix: The notion of "terrorism" has been abused and overstretched, especially in the wake

17 Thomas, Timothy L.. "Al Qaeda and the Internet: The Danger of 'Cyberplanning'". In: Parameters Spring (2003), pp. 112–123; Weimann, Gabriel, www.terror.net. How Modern Terrorism Uses the Internet. United States Institute of Peace, Special Report 116, March 2004; id. "Cyberterrorism - How Real Is the Threat?". United States Institute of Peace, Special Report 119, May 2004.

18 Nicander, Lars and Magnus Ranstorp (eds.). Terrorism in the Information Age – New Frontiers? (Stockholm: Swedish National Defence College, 2004), pp. 12–13.

19 Technical Analysis Group (TAG), Institute for Security Technology Studies. Examining the Cyber Capabilities of Islamic Terrorist Groups (Dartmouth College, 2003). https://www.ists.dartmouth.edu/TAG/ITB/ITB_032004.pdf; Denning, Dorothy , op. cit.

of 9/11. Many of the (perceived) characteristics of cyber-terror create maximum fear, which is then often turned into a powerful profit engine. But since the fuzzy notions of cyber-threats and cyber-terror will most certainly remain on the national security agenda, decision-makers should be careful not to foment "cyber-angst" to an unnecessary degree, even if the threat cannot be completely dismissed. In seeking a prudent policy, decision-makers must navigate the rocky shoals between hysterical doomsday scenarios and uninformed complacency. If action really is required, the focus should move away from malicious attacks towards the far broader range of potentially dangerous occurrences involving virtual tools and targets, including failure due to human error or technical problems. This not only does justice to the complexity of the problem, but also prevents us from carelessly invoking the specter of terrorism.

Complexity and System Vulnerability

As Michel van Eeten and his colleagues point out, the infrastructures themselves are their own worst enemy in many ways because of their complexity. When systems – including infrastructure systems – begin to blend into one another due to increasing use of IT and increasing functional demands, it is useless to try to maintain a fictitious separation of systems, each with an internally demarcated mode of responsibility. The distinction between inside and outside the system, and even the concept of systems boundaries as such, becomes blurred. The fact that planned maintenance, even after careful assessment and approval procedures, can cause disruptions is a prime example of surprise arising out of complexity.

Moreover, from the perspective of maintaining reliable services, it is not so important whether the events that triggered the surprise originated from within or from outside the infrastructure. In practice, 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,[20] which means that from the practitioner's point of view, the distinction between a failure, an accident, or an attack is often less important than the impact of the event. Technically speaking, information is a string of bits and bytes traveling from a sender to a receiver. If this string arrives in the intended order, the transfer has been successful. If the

20 Ellison, R. J., D. A. Fisher, R. C. Linger, H. F. Lipson, T. Longstaff, and N. R. Mead. Survivable Network Systems: An Emerging Discipline (technical report, November 1997). CMU/SEI-97-TR-013. ESC-TR-97-013, p. 3. http://www.cert.org/research/97tr013.pdf.

information is altered, intercepted, or diverted, however, problems are likely to arise. In practice, this means that the first and most important question is not what exactly caused the loss of information integrity, but rather what the possible result and complications may be. A power grid might fail because of a simple operating error without any kind of external influences, or because of a sophisticated hacker attack. In both cases, the result is the same: A possible blackout that may set off a domino effect of successive failures in systems that are linked through interdependencies. Analyzing whether a failure was caused by a terrorist, a criminal, a simple human error, or a spontaneous collapse will not help to stop or reduce the domino effect.

Early Warning

In the context of national security, however, the possibility of human agency is of special interest. In this context, early-warning systems have, at least since the start of the Cold War, constituted an indispensable element of efforts to maintain the sovereignty and security of nation states against looming attacks. Although early warning has become less important since the end of the Cold War, it took on new significance in the mid-1990s in the context of critical infrastructure protection. The ability of governments to gauge threats to critical infrastructures has traditionally been contingent upon their ability to evaluate a malicious actor's intent and ability to carry out a deliberate action. This was significantly easier during the Cold War, when the authorities were merely concerned with the security of physical structures. Due to the global nature of information networks, attacks can be launched from anywhere in the world, and discovering the origin of attacks remains a major difficulty, if, indeed, they are detected at all. Compared to traditional security threat analysis, which consists of analyses of actors, their intentions, and their capabilities, cyber-threats have various features that make such attacks difficult to monitor, analyze, and counteract:[21]

- Anonymity of actors: The problem of identifying actors is particularly difficult in a domain where maintaining anonymity is easy and where

21 Dunn, Myriam. "Threat Frames in the US Cyber-Terror Discourse". Paper presentation at the 2004 British International Studies Association (BISA) Conference, Warwick, 21 December 2004.

there are time lapses between the action that an intruder takes, the intrusion itself, and the effects of the intrusion. In addition, the continuing proliferation of sophisticated computer technologies among the mainstream population makes the identification of actors increasingly difficult.

- Lack of boundaries: Malicious computer-based attacks are not restricted by political or geographical boundaries. Attacks can originate from anywhere in the world and from multiple locations simultaneously. Investigations that follow a string of deliberately constructed false leads can be time-consuming and resource-intensive.
- Speed of development: Technology develops extremely quickly. The time span between the discovery of a new vulnerability and the emergence of a new tool or technique, which exploits that vulnerability, is getting shorter.
- Low cost of tools: The technology employed in such attacks is simple to use, inexpensive, and widely available. Tools and techniques for invading computers are available on computer bulletin boards and various websites, as are encryption and anonymity tools.
- Automated methods: Increasingly, the methods of attack have become automated and more sophisticated, resulting in greater damage from a single attack.

These characteristics considerably hamper the ability to predict certain adverse future scenarios. Various types of uncertainties make it difficult for the intelligence community to analyze the changing nature of the threat and the degree of risk involved effectively.

Thomas Holderegger discusses how an early-warning system can be realized in the area of critical information infrastructure protection (CIIP). He examines the players in the CIIP sector, discusses the respective CIIP approach of each, and specifies their tasks and responsibilities. In conclusion, this chapter discusses the role of the nation-state: how can it integrate the different approaches and guarantee communication flows between the players? How can such a dialog be internationalized? With these questions in mind, a concept is presented for integrating different players, including the public, into a national CIIP strategy. Furthermore, the article examines services that the state can offer to operators of critical infrastructures, in order to receive reports and informa-

tion from private players in return, thereby improving its ability to realize an early-warning capability.

Part III CIIP Public Policy Issues

We have aimed to shed some light on the issue of CIIP by investigating national and international CIIP initiatives in Volume I. On the one hand, we have found a great many approaches at the national level, as well as a great degree of diversity. It is obvious from the findings of Volume I that governmental cyber-security policies are at various stages of implementation – some are already being enforced, while others are just a set of suggestions – and come in various shapes and forms, ranging from a regulatory policy focus concerned with the smooth and routine operation of infrastructures and questions such as privacy or standards, to the inclusion of cyber-security into more general counter-terrorism efforts. On the other hand, we have identified some common themes that are of central importance in all countries: The most important of these are public-private partnerships, legal issues, and the need for international cooperation, which is the focus of our third section.

Public-Private Partnerships

Public-Private Partnerships are considered by many to be a panacea for all governance problems in a deregulated economy, and not only for CIP/CIIP-related issues. Driven by poor performance and inspired by neo-liberal economics, public monopolies have undergone dramatic transformation. In many countries, the provision of energy, communication, transport, financial services, and health care have all been, or are being, privatized as previously protected markets are deregulated.[22] However, while liberalization has in many cases improved efficiency and productivity, it has also led to concerns regarding the accessibility, equality, reliability, and affordability of services. Moreover, the privatization of public monopolies and infrastructure networks and the deregulation of service provision have important implications for national and

22 Héretier, Adrienne. "Market integration and social cohesion: The politics of public services in European integration". In: Journal of European Public Policy Vol. 8, No. 5 (2001), pp. 825–52; idem. "Public-interest services revisited". In: Journal of European Public Policy Vol. 9, No. 6 (2002), pp. 995–1019.

international security. In a non-liberalized economy, the state assumes both the responsibility as well as the costs of guaranteeing functioning systems and services. However, assigning responsibility for securing such systems and services is more problematic in a liberalized global economy. Who should implement and pay for protective measures undertaken in the name of national security? These and similar issues are addressed in Jan-Joel Andersson's and Andreas Malm's article. The authors look at measures that should be the responsibility of national and local governments and of the private sector. Furthermore, they discuss how national solutions to these problems fit with the internationalization of markets for goods and services and the emergence of transnational information and communications networks. They argue that by refraining from imposing regulation and engaging in Public-Private Partnerships, the government pushes the responsibility for implementation and costs on to industry. Industry, in turn, is reluctant to accept the responsibility and to incur costs without clear guidance and economic compensation, so that there is a distinct possibility that private actors simply participate in PPP as a means to deflect attention from insufficient emergency preparedness measures and to avert outright regulation.

Legal Issues

Apart from regulatory issues, the need to harmonize national legal provisions and to enhance judicial and police cooperation has been a key issue for a number of years. However, so far, the international legal framework has remained rather confused and is actually an obstacle to joint action by the actors involved.

The most important legislative instrument in this area is the Council of Europe Cybercrime Convention (CoC), which was signed on 23 November 2001 by 26 members and four non-members of the Council. This convention is the first international treaty on crimes committed via the internet and other computer networks. Its main objective is to pursue a common law enforcement policy aimed at the protection of society against cyber-crime, especially by adopting appropriate legislation and fostering international cooperation.[23] An additional protocol to the CoC outlaws racist and xenophobic acts committed through computer systems.

23 Council of Europe Convention on Cybercrime. Available at: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

While other politically powerful entities such as the G8 also try to foster collaboration and a more efficient exchange of information when it comes to cyber-crime and terrorism, the CoC goes one step further. It lays out a framework for future collaboration between the signature state's prosecution services. It achieves this mainly by harmonizing the penal codes of the CoC signatory states. As a result, crimes such as hacking, data theft, and distribution of pedophile and xenophobic material etc. will be regarded as illegal actions per se, thus resolving the problem of legal disparities between nations that was mentioned above. This also allows the authorities to speed up the process of international prosecution. Since certain activities are defined as illegal by all CoC member-states, the sometimes long and painful task of crosschecking supposed criminal charges committed in a foreign country becomes obsolete if the offence is already included in the national penal code. Consequently, reaction times will be shortened and the parties to the CoC will establish a round-the-clock network within their countries to handle aid requests that demand swift intervention.[24] While the implementation of the CoC will most likely be a slow and sometimes thorny process, the idea of finding a common denominator and harmonizing the response to at least some of the most crucial problems is certainly a step in the right direction.

The Need for International Cooperation

From the discussion of legal issues, it becomes obvious that like other security issues, the vulnerability of modern societies — caused by dependency on a spectrum of highly interdependent information systems — has global origins and implications. To begin with, the information infrastructure transcends territorial boundaries, so that information assets that are vital to the national security and the essential functioning of the economy of one state may reside outside of its sphere of influence on the territory of other nation-states. Additionally, "cyberspace" — a huge, tangled, diverse, and universal blanket of electronic interchange — is present wherever there are telephone wires, cables, computers, or electromagnetic waves, a fact that severely curtails the ability of individual states to regulate or control it alone. Any adequate protection policy

24 Taylor, Greg (no date). "The Council of Europe Cybercrime Convention. A civil liberties perspective". http://www.crime-research.org/library/CoE_Cybercrime.html.

that extends to strategically important information infrastructures will thus ultimately require transnational solutions.

There are four possible categories of initiatives that may be launched by multilateral actors: deterrence, prevention, detection, and reaction.

- Deterrence – or the focus on the use of multilateral cyber-crime legislation: Multilateral initiatives to deter the malicious use of cyberspace include initiatives a) to harmonize cyber-crime legislation and to promote tougher criminal penalties (e.g. the Council of Europe Convention on Cybercrime),[25] and b) to improve e-commerce legislation (e.g., the efforts of the United Nations Commission on International Trade Law (UNCITRAL) for electronic commerce).[26]
- Prevention — or the design and use of more secure systems and better security management, and the promotion of more security mechanisms: Multilateral initiatives to prevent the malicious use of cyberspace center around a) promoting the design and use of more secure information systems (e.g., the Common Criteria Project);[27] b) improving information security management in both public and private sectors (e.g., the ISO and OECD standards and guidelines initiatives);[28] c) legal and technological initiatives, such as the promotion of security mechanisms (e.g., electronic signature legislation in Europe).
- Detection — or cooperative policing mechanisms and early warning of attacks: Multilateral initiatives to detect the malicious use of cyberspace include a) the creation of enhanced cooperative policing mechanisms (e.g., the G-8 national points of contact for cyber-crime); and b) early warning through information exchange with the aim of providing early warning of cyber-attacks by exchanging information between the public and private sectors (e.g., US Information Sharing & Analy-

25 Convention on Cybercrime, op. cit.
26 http://www.uncitral.org/english/workinggroups/wg_ec/index.htm.
27 http://www.commoncriteriaportal.org.
28 The International Organization for Standardization ISO has developed a code of practice for information security management (ISO/IEC 17799:2000). http://www.iso.org/iso/en/prodsservices/popstds/informationsecurity.html (last accessed on 10 June 2005); the Organisation for Economic Co-operation and Development (OECD) promotes a "culture of security" for information systems and networks. http://www.oecd.org/document/42/0,2340,en_2649_33703_15582250_1_1_1_1,00.html.

sis Centers, the European Early Warning & Information System, and the European Network and Information Security Agency (ENISA)).

- Reaction — or the design of stronger information infrastructures, crisis management programs, and policing and justice efforts: Multilateral initiatives to react to the malicious use of cyberspace include a) efforts to design robust and survivable information infrastructures; b) the development of crisis management systems; and c) improvement in the coordination of policing and criminal justice efforts.

Subimal Bhattacharjee provides an overview of the huge variety of issues that are of importance in these international organizations. Based on their activities over the past few years, he summarizes the main roles of these organizations and states their shared view that national laws need to be harmonized to ensure a common understanding of the need for all global cyber-security concerns to be addressed.

Indeed, regulatory regimes[29] are the result of the mediation of disparate interests of various stakeholders within arenas of political interaction. These interactions usually result in new rules that constrain actors' choices and prescribe who can act when, and which affect behavior both directly and indirectly. Divergences between national CIIP policies are a major obstruction to the development of an international regime, for international regimes are based on at least a minimal convergence of expectations and interests of (national) key actors. However, in the light of economic and security interests, industrialized states are working to overcome these temporary obstacles in order to move resolutely towards robust international conventions and mechanisms that protect the global information environment.

29 A regime can be defined as "sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a given area of international relations". See: Krasner, Stephen D. (ed.). International Regimes (Ithaca: Cornell University Press, 1984), p. 2.

Part I
CIIP Conceptual Issues

Understanding Critical Information Infrastructures: An Elusive Quest

By Myriam Dunn

Introduction

Today, it is becoming increasingly important to enhance the security of communication networks and information systems, some of which are more essential than others and are therefore called critical information infrastructures (CII). This urgency is due to their invaluable and growing role in the economic sector, their interlinking position between various infrastructure sectors, and their essential role for the functioning of many of the critical services that are essential to the well-being of developed societies.

In order to plan adequate and cost-effective protection measures, the working of these systems and their role for society should be sufficiently understood. But in reality, such an understanding is still lacking, mainly because the complex behavior of infrastructure networks and their environment presents numerous theoretical and practical challenges for the various stakeholders that are involved: Apart from the interlinking of the computer networks that now underpin most productive activity, the privatization process that gathered strength in the 1990s in many parts of the world has caused a wide range of economic activities that had previously been under state control to be transferred to the private sector, leading to fragmentation and a dire need for coordination. Furthermore, the globalization process, which extends beyond frontiers and creates increasing overlap and dependency, means that critical infrastructure in a given country may be controlled by companies in a neighboring country. Strategic supply chains may also become highly dependent on external markets.[1] The tasks of managing and protecting the infrastructure are thus becoming increasingly difficult, and the "threshold of insecurity" has risen significantly in our developed societies over recent years.

1 Narich, Richard. "Critical Infrastructure Protection: Importance, Complexity, Results". In: Défense Nationale et Sécurité Collective, No. 11 (November 2005). http://www.defnat.com/naviref/aff_numresume.asp?cid_article=20051133&ctypenecours=0&ccodeoper=1&cidr=200511.

In this chapter, we analyze how states approach the issue of CIIP analytically and what these approaches teach us about the general understanding of the CIIP problem complex. We believe that an assessment of approaches for analyzing various aspects of the CII and a glimpse into the methodological toolbox can serve as an indicator of the current comprehension of key CIIP issues and point us towards key issues in this matter.[2] In addition, by critically assessing these approaches, we point out the major current shortcomings both in practical evaluation and in the general understanding of the issue.[3]

Below, we first address questions that are mainly of a conceptual nature. We believe that a clear and stringent distinction between the two key terms "CIP" and "CIIP" is desirable, but not easily achieved. In official publications, both terms are used inconsistently, with the term CIP frequently used even if the document is only referring to CIIP. This has concrete implications for the evaluation of these systems. The majority of methods and models are designed and used for the larger concept of CI, and not for CII in particular – due partly to conceptual sloppiness, partly to the use of old tools that were developed for completely different applications, and partly to the fact that the CII is often treated as one special part of the overall CI.

Approaches exist for all of the four hierarchies of CI systems, namely the system of systems, individual infrastructures, individual systems or enterprises, and technical components. This means that most of the approaches can only be applied to certain limited aspects of the problem. However, we can group approaches into two broad categories: They either attempt to define critical sectors and assets and seek to understand the working of CI(I) systems in greater or lesser detail – methods that we address in our second chapter –, or to understand the level of risk to these systems, taking into consideration outside influence and the planning of countermeasures, issues that are addressed in the third section.

2 Dunn, Myriam. "The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP)". In: International Journal for Critical Infrastructure Protection, Vol. 1, No. 2/3 (2005), pp. 58–68.

3 The analysis is based on the detailed description of approaches as described in Part II of the 2002 and 2004 editions of the CIIP Handbook: Dunn, Myriam and Isabelle Wigert (eds.). The International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries (Zurich: Center for Security Studies, 2004); Wenger, Andreas, Jan Metzger, and Myriam Dunn (eds.). The International CIIP Handbook: An Inventory of Protection Policies in Eight Countries (Zurich: Center for Security Studies, 2002).

From Conceptual Sloppiness Towards Conceptual and Analytical Clarity

A self-imposed focus on CIIP creates immediate difficulties for any researcher, since the basis for distinguishing between CIP and CIIP is far from clear. That the two concepts are closely interrelated is apparent from the current debate on protection requirements: The debate keeps jumping from a discussion on defending critical physical infrastructure – telecommunications trunk lines, power grids, and gas pipelines – to talk of protecting data and software residing on computer systems that operate these physical infrastructures.[4] This indicates that the two cannot and should not be discussed as completely separate concepts. Rather, CIIP seems an essential part of CIP: While CIP comprises all critical sectors of a nation's infrastructure, CIIP is only a subset of a comprehensive protection effort, as it focuses on the critical information infrastructure. The lesson from this seems to be that an exclusive focus on cyber-threats that ignores important traditional physical threats is just as dangerous as the neglect of the virtual aspect of the problem.

One could therefore be tempted to argue that the distinction between CIP/CIIP is overly artificial or simply an academic fad. However, not only would more reflection on terminology bring about a much-needed sharpening of the conceptual apparatus, there are also a number of persuasive indicators that the main future challenges lie with the emerging CII, so that the CIP community would benefit significantly from a clear conceptual distinction between CI/CII that permits a better understanding of these challenges:

- The protection of the CII has generally become more important due to the invaluable and growing role of the infrastructure elements in the economic sector, their interlinking position between various infrastructure sectors, and their essential role for the functioning of other infrastructures at all times;
- On the threat side, cyber-threats are evolving rapidly both in terms of their nature and of their capability to cause harm, so that protec-

4 Porteous, Holly. "Some Thoughts on Critical Information Infrastructure Protection". In: Canadian IO Bulletin, Vol. 2, No. 4 (October 1999). http://www.ewa-canada.com/Papers/IOV2N4.htm.

tive measures require continual technological improvements and new approaches, which means giving constant attention to the CII;

- The system characteristics of the emerging information infrastructure differ radically from traditional structures in terms of scale, connectivity, and dependencies.[5] Additionally, the interlinked aspects of market forces and technological evolution will likely aggravate the problem of CII in the future:
- Market forces: security has never been a design driver. Since pressure to reduce time-to-market is intense, a further surge of computer and network vulnerabilities is to be expected.[6] We are therefore faced with the potential emergence of infrastructures with inherent instability, critical points of failure, and extensive interdependencies;
- Technological evolution: On the other hand, we are facing an ongoing dynamic globalization of information services, which in connection with technological innovation (e.g., localized wireless communication) will result in a dramatic increase of connectivity and lead to ill-understood behavior of systems, as well as barely understood vulnerabilities.

This prospect clearly indicates a need to distinguish conceptually between CIP and CIIP, without treating them as completely separate concepts. Moreover, the careless use of terms points to deficiencies in understanding important differences between the two concepts and is a direct consequence of substantial flaws in the existing terminology. This can be illustrated using the components of the term "CIP", which are either quite carelessly introduced into the political agenda from a technical-scientific or system-theoretical expert level without adaptation to the socio-political context, as is the case for "critical", or are borrowed, as in the case of "infrastructure", from man-made technical infrastructures, such as railways, roads, or airports,[7] as a label for far more elusive complex, interdependent, open systems.

5 Parsons, T.J. "Protecting Critical Information Infrastructures. The Co-ordination and Development of Cross-Sectoral Research in the UK". Plenary address at the Future of European Crisis Management conference (Uppsala 2001).

6 Näf, Michael. "Ubiquitous Insecurity? How to 'Hack' IT Systems". In: Wenger, Andreas (ed.). The Internet and the Changing Face of International Relations and Security, Information & Security: An International Journal, Vol. 7 (2001), pp. 104–118.

7 Moteff, John, Claudia Copeland, and John Fischer. Critical Infrastructures: What Makes an Infrastructure Critical? CRS Report for Congress RL31556 (Updated 29 January 2003).

But even though the need for conceptual precision is obvious, it is still very difficult to understand what exactly the (national or global) information infrastructure is. This is due to the fact that technologies have not only a physical component that is fairly easily grasped – such as high-speed, interactive, narrow-band, and broadband networks; satellite, terrestrial, and wireless communications systems; and the computers, televisions, telephones, radios, and other products that people employ to access the infrastructure – but they also have an equally important immaterial, sometimes very elusive component, namely the information and content that flows through the infrastructure, the knowledge that is created from this, and the services that are provided. As a result, we are caught in the tangled web of inadequate terminology, which will likely have an impact on how we perceive and ultimately approach the issue.

More often than not, the actual objects of protection interests are not static infrastructures, but rather the services, the physical and electronic (information) flows, their role and function for society, and especially the core values that are delivered by the infrastructures. This is a far more abstract level of understanding essential assets, with a substantial impact on how we should aim to protect them. This fact is widely acknowledged, but it remains to be seen in the following two chapters how these observations are reflected in current approaches to analyzing CI/CII systems.

Sectors and Beyond: Analyzing what is Critical

Approaches discussed in this chapter mainly deal with the questions of "what is critical" and "how do we establish what is critical". In designating a list of "sectors" as critical units,[8] many countries have followed the example of the Presidential Commission on Critical Infrastructure Protection (PCCIP), which was the first official publication to equate critical infrastructures with business sectors or industries.[9] The choice of the sector as a unit of analysis is a pragmatic approach that roughly follows the boundaries of existing business/industry

8 See Abele-Wigert, Isabelle and Myriam Dunn. International CIIP Handbook 2006, Vol. I.: An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies (Zurich: Center for Security Studies, 2006).

9 President's Commission on Critical Infrastructure Protection (PCCIP). Critical Foundations: Protecting America's Infrastructures (Washington, DC, October 1997). This publication is quoted in the following as PCCIP.

sectors, a division that mirrors the fact that the majority of infrastructures is owned and operated by private actors. In general, though the exact definitions vary from country to country, sectors are deemed critical when their incapacitation or destruction would have a debilitating impact on the national security and on the economic and social well-being of a nation.[10]

There are many aspects that might be analyzed in connection with individual sectors, such as how and why they are critical, or which of their components are particularly vulnerable. In general, sector analysis adds to an understanding of the functioning of single sectors by highlighting various important aspects such as underlying processes, stakeholders, or resources needed for crucial functions. Approaches that examine the vertical structure of sectors (sectors, sub-sectors, processes, functions, etc.) are discussed in our first subchapter.

To determine how critical sectors function, what the influencing parameters are in particular sectors, and how important specific sectors are to the economy, including the identification of core functions, value chains, and dependency on information and communication technology in each critical sector, is a prerequisite for subsequent interdependency analysis. In our second subchapter, we will investigate approaches that focus on the horizontal structure, especially on interdependencies between sectors.

Sectors and Subsectors – the Vertical Dimension

A sector is deemed "critical" if a breakdown or serious disruption of that sector could lead to damage on a national scale, or in other words, if the impact of a disruption would be sufficiently severe. Usually, a component or a whole infrastructure is defined as "critical" due to its strategic position within the whole system of infrastructures, and especially due to interdependencies between the component or the infrastructure and other infrastructures. In a broader view, some infrastructures or components of infrastructures have come to be seen as critical due to their inherent symbolic meaning.[11]

It is broadly acknowledged, however, that the focus on sectors is far too restricted to represent the realities of complex infrastructure systems. For a

10 See differing definitions in CIIP Handbook 2006, Vol. I.

11 For more details, see Metzger, Jan. "The Concept of Critical Infrastructure Protection (CIP)". In: A.J.K. Bailes/I. Frommelt (eds.). Business and Security: Public-Private Sector Relationships in a New Security Environment (Oxford, 2004).

more meaningful analysis, it is therefore deemed necessary to evolve beyond the conventional sector-based focus and to look at the services, the physical and electronic (information) flows, their role and function for society, and especially the core values that are delivered by the infrastructures. Therefore, experts groups often focus on four steps in the identification of what is critical: 1) critical sectors, 2) sub-sectors for each sector on the basis of organizational criteria, 3) core functions of the sub-sectors, and 4) resources necessary for the functioning of the sub-sectors.[12] The CII plays important roles in all four areas.

To identify sectors, products, and services comprising the national critical infrastructure requires input from private-sector experts as well as experts and officials at various levels of government. In the view of many countries, an effective way of getting information on various aspects of CI/CII is to circulate a questionnaire among key persons and experts, or to interview them. A questionnaire may contain multiple-choice answers that can be assessed with the help of an evaluation key, or questions can be phrased to leave more latitude for semi-structured answers. The information thus collected will need to be augmented and refined in workshops with representatives of vital public and private sectors.[13]

Since such a process always involves different people from different communities, a common understanding and definition of the term "critical" is crucial. First of all, the classification of what is "critical" lies mainly in the eye of the beholder, and such an assessment is shaped to a large degree by subjective viewpoints and organizational backgrounds. Therefore, unless a minimum agreement can be reached on the precise topic of the discussion and on standardization of the assets to be considered prior to any attempted assessment, owners and operators of potentially critical assets might not all agree on a common language nor a common level of granularity.[14] In addition,

12 Dunn, Myriam. "Part II: Overview of Methods and Models to Assess Critical Information Infrastructures". In: Dunn and Wigert, op. cit., p. 227f.

13 Luiijf, Eric A.M., Helen H. Burger, and Marieke H.A. Klaver. "Critical Infrastructure Protection in The Netherlands: A Quick-scan". In: Gattiker, Urs E., Pia Pedersen, and Karsten Petersen (eds.). EICAR Conference Best Paper Proceedings 2003. http://www.tno.nl/instit/fel/refs/pub2003/BPP-13-CIP-Luiijf&Burger&Klaver.pdf.

14 For example, a representative of the electric power generation business might identify generating stations or dams as critical, while others might extend that assessment to the level of turbines or bearings. Cf. Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP). Tool to Assist Owners and Operators to Identify Critical Infrastructure Assets (19 December 2002), p. 2.

most critical sectors have different structures and requirements, so that the appropriate level of detail might vary considerably from sector to sector.[15]

The potential damage impact of loss or disruption of vital products and services is measured with the help of indicators derived from definitions of national security and national interest. Generally, all societies are said to have three fundamental core values: (1) the protection of citizens and territory; (2) the protection of political independence and autonomy; and (3) the protection of national economic safety.[16] National security is often defined as the absence of threats to these core values.[17] In accordance, a product or a service is defined as vital if it provides an essential contribution to one of these core values. For example, it is "vital" if it is necessary for maintaining a defined minimum quality level of (1) national and international law and order, (2) public safety, (3) economic activity, (4) public health, (5) the ecological environment, or (6) if the loss or disruption of the product of service would affect citizens or the government administration at a national scale.[18] Depending on national particularities, these indicators might vary. In general, however, in defining "vital" sectors, all countries take the potential loss of life as well as economic, social, and political consequences into consideration.

From a national-security perspective, it is the government that must determine the level of damage impact that is acceptable to society. In addition, it is necessary to distinguish between products and services that are vital to the nation and those that are merely very important. A relatively high threshold is needed when one attempts to identify something as truly critical: For instance, many important systems are self-repairing or self healing, such as the

15 Reinermann, Dirk and Joachim Weber. "Analysis of Critical Infrastructures: The ACIS Methodology (Analysis of Critical Infrastructural Sectors)". Paper presented at the Critical Infrastructure Protection (CIP) Workshop (Frankfurt, 29–30 September 2003).

16 Berkowitz, Bruce D. American Security (Yale: Yale University Press, 1986).

17 Wolfers, Arnold. "National Security as an Ambiguous Symbol". In: Id. Discord And Collaboration: Essays on International Politics (Baltimore: Johns Hopkins, 1962), pp. 147–165

18 Examples are: National Contingency Planning Group. Canadian Infrastructures and their Dependencies (March 2000), Preface; Charters, David. "The Future of Canada's Security and Defence Policy: Critical Infrastructure Protection and DND Policy and Strategy". Research paper of the Council for Canadian Security in the 21st Century. http://www.ccs21.org/ccspapers/papers/charters-CSDP.htm. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Critical Infrastructure Protection in the Netherlands: Quick Scan on Critical Product and Services (April 2003).

internet, which redirects traffic to avoid damaged infrastructure elements.[19] Thus, despite the fact that breakdowns in banking and payment systems can have nation-wide consequences, or that disruptions in a subway system can affect millions, such disruptions are, essentially, local occurrences. That is, the disruptions are contained within a given, restricted system. In such cases, a certain delimited, more or less well defined function or service is affected, and there are usually more or less acceptable reserve procedures or backup-functions. In short, there are ways to get around such problems, and one can hardly maintain that they constitute a serious threat to society, let alone threaten society's very existence.[20]

This points to the fact that it is very difficult to establish the criticality of an asset without taking into account its extended environment and various other factors such as threats, impact, control mechanisms, etc. In addition, the question of criticality in the socio-political context is always inextricably linked to the question of how damage or disruption of an infrastructure would be perceived and exploited politically. Actual loss (monetary loss or loss of lives) would be compounded by political damage or loss in basic public trust in the mechanisms of government, and erosion of confidence in inherent government stability.21 From this perspective, the criticality of an infrastructure can never be identified preventively based on empirical data alone, but only ex post facto, after a crisis has occurred, and as the result of a normative process.

Interdependencies — the Horizontal Structure

Critical infrastructures are frequently connected at multiple points through a wide variety of mechanisms, so that the conditions for any given pair of infrastructures are mutually reinforcing. This means that CI are highly interdependent, both physically and in their greater reliance on the information infrastructure, resulting in a dramatic increase of the overall complexity and posing significant challenges to the modeling, prediction, simulation, and analysis of CI. The information infrastructure plays a crucial role, as most of

19 Cukier, Kenneth Neil, Viktor Mayer-Schoenberger, and Lewis Branscomb. "Ensuring (and Insuring?) Critical Information Infrastructure Protection". KSG Working Paper No. RWP05-055 (October 2005). Available at: http://ssrn.com/abstract=832628.

20 Westrin, Peter. "Critical Information Infrastructure Protection". In: Wenger, Andreas (ed.): The Internet and the Changing Face of International Relations and Security. Information & Security: An International Journal, Vol. 7 (2001), pp. 67–79.

the critical infrastructures are either built upon or monitored and controlled by ICT systems, a trend that has been accelerating in recent years with the explosive growth of information technology.[22]

Due to the explosive growth of information technology, the study of interdependencies and possible cascading effects in case of failures has become the focal point in CIIP discussion. At an initial stage, most countries have opted for qualitative, expert-based approaches to mapping interdependencies. Expert opinions are collected by means of working groups, roundtables, workshops, or questionnaires.[23] The identification of nodes and linkages between sectors helps to establish the degree of interdependency: Interdependencies can exist between components, but also between functions or resources; they can have different characteristics (i.e., physical, virtual, related to geographic location, or logical in nature) and may differ in degree. Other important factors to be considered include the impact of the effect caused by the dependency, time lags, redundancy, etc. The extent of direct dependency between infrastructure elements is described using values such as "high", "medium", "low", and "none".[24] While experts are usually able to evaluate direct dependency relationships, calculating the potential cascading impact of degradation to any level of depth in the maze of dependency relationships is a more difficult matter and requires the help of software.[25]

It is generally recognized, however, that it is necessary to move beyond mere qualitative understanding of interdependencies and towards sophisticated

21 Ibid.

22 "Interdependency" can be understood as a "bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other." "Dependency", on the other hand, denotes a unidirectional relationship. Rinaldi, Steven M., James P. Peerenboom, and Terrence K. Kelly. "Complex Networks. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies". IEEE Control Systems Magazine, Vol. 21 (6 December 2001), p. 14.

23 Dunn, Myriam. „Part II: Overview of Methods and Models to Assess Critical Information Infrastructures". In: Dunn, Myriam and Isabelle Wigert. International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries (Zurich: Center for Security Studies, 2004), pp. 229–42.

24 Ibid.

25 An application known as Relational Analysis For Linked Systems (RAFLS) has been developed in Canada for measuring and modeling the cascading effects of these direct dependencies. RAFLS, which is based on an algorithm, uses scored interdependencies and iteratively determines dependencies and impacts. It shows high and medium degrees of dependencies and can reveal second-, third-, fourth-, and fifth-level dependencies. It also helps to trace linkages and potentially to interdict a path in time of crisis.

modeling of cause-and-effect relationships and possible cascading failures. A comprehensive analysis of interdependencies is a daunting challenge, though, mainly because the science of infrastructure interdependencies is relatively immature. Many models and computer simulations have been developed in the past for specific aspects of isolated infrastructures. However, these efforts are not sufficient for modeling cascading failure in complex networks. Simulation frameworks that allow the coupling of multiple interdependent infrastructures to address infrastructure protection, mitigation, response, and recovery issues are only beginning to emerge.

The problem of interdependencies is complex and difficult to analyze, not least because the nature of interdependencies is still very little understood. Besides technical aspects, the larger environment also needs to be taken into account, especially the interrelated factors and system conditions that complicate the challenge of identifying, understanding, and analyzing interdependencies. According to a much-cited article, at least six aspects can be distinguished:[26]

- Environment: Examples for parameters related to the environment are: Economic and business opportunities and concerns, public policy, government investment decisions, legal and regulatory concerns, and social and political concerns. The environment influences normal system operations, emergency operations during disruptions and periods of high stress, and repair and recovery operations.
- Coupling/Response Behavior: The degree to which the infrastructures are coupled, or linked, strongly influences their operational characteristics. Some linkages are loose and thus relatively flexible, whereas others are tight, leaving little or no flexibility for the system to respond to changing conditions or failures that can exacerbate problems or cascade from one infrastructure to another.
- Infrastructure Characteristics: Infrastructures have key characteristics that figure in interdependency analyses. Principal characteristics include spatial (geographic) scales, temporal scales, operational factors, and organizational characteristics.
- Types of Interdependencies: These linkages can be physical, virtual, related to geographic location, or logical in nature.

26 Rinaldi and Peerenboom, op. cit.

- State of Operation: The state of operation of an infrastructure can be thought of as a continuum that exhibits different kinds of behavior during normal operating conditions (which can vary between peak and off-peak conditions), during times of severe stress or disruption, or during times when repair and restoration activities are under way. At any point in the continuum, the state of operation is a function of the interrelated factors and system conditions.
- Type of Failure: Infrastructure disruptions or outages can be classified as cascading, escalating, or common-cause failures.[27]

Developing a comprehensive architecture or framework for interdependency modeling and simulation requires the coupling of multiple interdependent infrastructures. Furthermore, a comprehensive architecture or framework should be able to address all aspects of CIP/CIIP, including mitigation, response, and recovery issues. Generally speaking, simply "hooking together" existing infrastructure models is not feasible, as the differences between the models would be too large. Furthermore, such models generally do not capture emergent behavior, a key element of interdependency analysis.[28] The idea behind emergent behavior is that from simple interactions and/or rules, complex behavior can emerge at the group level that would not occur at the individual level. An emergent property is one that appears as the unpredictable result of the complex interactions of parts that themselves obey simple rules or laws.[29]

Today, many experts believe that CI interdependencies can be investigated most efficiently by comparing infrastructures to Complex Adaptive Systems (CAS), which are populations of interacting agents where an agent is an entity with a location, capabilities, and memory. CAS are real-world systems that are characterized by apparently complex behavior, which emerges as a result of often nonlinear spatial-temporal interactions among a large number of component systems at different levels of organization. With this perspective, each

27 Ibid.

28 Ibid., p. 23.

29 Crutchfield, James P. "Is Anything Ever New? Considering Emergence". In: Cowan, G., D. Pines, and D. Melzner (eds). Complexity: Metaphors, Models, and Reality, SFI Series in the Sciences of Complexity XIX (Addison-Wesley: Redwood City, 1994), pp. 479–497; Mihata, Kevin. "The Persistence of 'Emergence'". In: Eve, Raymond A., Sara Horsfall, and Mary E. Lee (eds.). Chaos, Complexity, and Sociology: Myths, Models, and Theories (Thousand Oaks (etc.): Sage Publications, 1997), p. 33.

component of an infrastructure constitutes a small part of the intricate web that forms the overall infrastructure. This approach offers benefits for modeling and simulation, such as agent-based modeling and simulation (ABMS), and is able to explain emergent behavior.[30]

Modern simulation technology capitalizes on recent technological advances in evolutionary learning algorithms and massive parallel computing. Agent-based models are computer-driven tools to study the intricate dynamics of CAS. The primary assumption is that system behavior can be explained by individual traits, as the agents interact and adapt to each other and their environment. In agent-based models, complex interactions are emergent, whereas in other models, the types of interactions must be anticipated and written into the model.31 In situations with sparse or non-existent macro-scale information, as is the case for infrastructure interdependencies, agent-based models may utilize rich sources of micro-level data to develop interaction forecasts. The big disadvantage of these simulation models is that the complexity of the computer programs tends to obscure the underlying assumptions and inevitable subjective input, so that faulty assumptions can distort results significantly.

In addition, there are severe limits to the system paradigm, the main problem being one of system ontology: calculation and modeling inherently rely on our ability to define the variables of the system. This is dependent on our ability to describe the system, or more specifically, on our ability to describe the system boundaries by distinguishing between factors external to a system that may affect it (exogenous) and those internal to the system (endogenous).[32] An object, and in particular a system, can only be defined by its cohesion in a broad sense, that is, in terms of the interactions of the component elements.[33] However, it is one of the hallmarks of critical infrastructures that we may not know how to define these systems, not least because we cannot know whether a variable is part of a system, unless we already know all the variables it interrelates with, which we do not.

30 Rinaldi and Peerenboom, op. cit.

31 http://www.cas.anl.gov.

32 Bertalanffy, Ludwig von. General Systems Theory: Foundations, Development, Applications (New York: George Braziller Publishing, 1968), p .141.

33 Id. Perspectives on General System Theory: Scientific-Philosophical Studies (New York: George Braziller Publishing, 1975), pp. 165f.

Risk Analysis: Analyzing What is Threatened and How to Counter the Threats

As we have mentioned above, understanding how systems work is not sufficient for estimating what exactly to protect. In this chapter, we will focus on approaches that take into account the broader environment surrounding these infrastructures, including possible threats. These approaches are subsumed under the label of "risk analysis": Risk is a function of the likelihood of a given threat source displaying a particular potential vulnerability, and the resulting impact of that adverse event.[34] Risk analysis refers to the processes used to evaluate those probabilities and consequences, and also to the study of how to incorporate the resulting estimates into the decision-making process. The risk assessment process also serves as a decision-making tool, in that its outcomes are used to provide guidance on the areas of highest risk, and to devise policies and plans to ensure that systems are appropriately protected.[35]

The risk estimate is produced mainly from the combination of threat and vulnerability assessments. It analyzes the probability of destruction or incapacitation resulting from a threat's exploitation of the vulnerabilities in a critical infrastructure. At the very least, risk analysis encompasses risk identification, risk quantification, and risk measurement, according to the three classic questions:

34 Stoneburner, Gary, Alice Goguen, and Alexis Feringa. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-30 (Washington, January 2002), p. 8, available at: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

35 Commonwealth of Australia, Information Security Group. Australian Communications-Electronic Security Instruction 33 (ACSI 33) Handbook 3, Risk Management (draft version). http://www.dsd.gov.au/_lib/pdf_doc/acsi33/HB3p.pdf. The Australian government is currently developing a new manual: http://www.dsd.gov.au/library/acsi33/acsi33.html; Methods to Achieve Information Systems Security. Expression of Needs and Identification of Security Objectives (EBIOS). Memo - Version 1.4. http://www.ssi.gouv.fr/en/confidence/documents/memo-gb.html; Gran, Bjørn Axel. The CORAS Methodology for Model-Based Risk Assessment, version 1.0, WP2, Deliverable 2.4. (29 August 2003); New South Wales Office of Information and Communications Technology's (OICT), Information Security Guideline for NSW Government Part 1 — Information Security Risk Management. no. 3.2, first published in September 1997, current version: June 2003. http://www.oit.nsw.gov.au/pages/4.3.16-Security-Pt1.htm; Alberts, Christopher and Audrey Dorofee, OCTAVESM Method Implementation Guide, version 2.0, vols. 1–18 (Carnegie Mellon University, June 2001). http://www.cert.org/octave/pubs.html. See also: Alberts, Christopher and Audrey Dorofee. An Introduction to the OCTAVESM Method. http://www.cert.org/octave/methodintro.html.

a) What can go wrong?
b) What is the likelihood of it going wrong?
c) What consequences would arise?[36]

Often, this is followed by risk evaluation, risk acceptance and avoidance, and risk management, according to the following questions:

a) What can be done?
b) What options are available, and what are their associated trade-offs in terms of cost, benefits, and risks?
c) What impact do current management decisions have on future options?[37]

As can be easily seen, risk assessment methodologies are step-by-step approaches. The number of steps may vary and can also be adjusted to the specific needs. In the following, we show a possible nine-step approach, which is an amalgamation of various approaches currently in use.[38] Systems-based approaches often include standard security safeguards, implementation advice, and aids for numerous IT configurations typically found in IT systems today. In the context of CIP/CIIP, risk analysis could theoretically address any degree of complexity or size of system. However, when the boundaries of the evaluated system are set too wide, the lack of available data makes accurate assessment difficult or even impossible. In most cases, measures are applied locally with a focus that is confined to a business, agency, or organizational context. These approaches are based on the supposition that sufficient protection at the technical system level nullifies threats to the larger system of CI.

36 Haimes, Yacov Y. Risk Modeling, Assessment, and Management (New York, 1998).
37 Ibid., pp. 54–55.
38 Stoneburner et al., op. cit.

Step 1: System Characterization

Step 1 is to define the scope of the effort and the boundaries of the system assessed. The term "system" can be defined in many different ways: It often refers to a combination of related elements organized into a complex whole, or to any collection of component elements that work together to perform a task. In the engineering disciplines, the term is often applied to an assembly of mechanical or electronic components that function together as a unit. In computing, it describes a set of computer components – an assembly of computer hardware, software, and peripherals functioning together. In the context of CIP/CIIP, a system can be seen as a compound of several CI, a single infrastructure, an infrastructure-dependent enterprise, or a particular system within a given infrastructure, according four hierarchy levels: 1) System of systems; 2) Individual infrastructures; 3) Individual system or enterprise; and 4) Technical components.[39] Once again, the larger the system we want to address, the less sure we can be of our ability to define system boundaries in any meaningful way.

Step 1 further includes the identification of all kinds of resources, assets, and information that constitute the system. An "asset" can be a tangible item (such as hardware), or a grade or level of service, staff, or information. The strategic, organizational, and risk management contexts in which the rest of the process will take place are also established in this first step. Furthermore, criteria for evaluating risk should be established , and the structure of the analysis has to be defined.[40]

39 Schmitz, Walter. ACIP D6.4 Comprehensive Roadmap - Analysis and Assessment for CIP. Work Package 6, Deliverable D6.4, Version 1 (European Commission Information Society Technology Program, May 2003), p. 52.

40 Emergency Management Australia. Critical Infrastructure Emergency Risk Management and Assurance Handbook (Mt. Macedon, 2003). http://www.disaster.qld.gov.au/publications/pdf/Critical_Infrastructure_handbook.pdf.

Step 2: Threat Identification

Step 2 includes the determination of (1) the nature of external and internal threats, (2) their source, and (3) the probability of their occurrence.[41] Threats can originate from a variety of sources:[42]

Natural Threats: Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events.

Environmental Threats: Long-term power failure, pollution, chemicals, liquid leakage.

Human Threats: Humans may be threat-sources through intentional acts (such as deliberate attacks by malicious persons) or unintentional acts (such as negligence and errors). A deliberate attack can be either (1) a malicious attempt to gain unauthorized access to an IT system (e.g., via password guessing) in order to compromise system and data integrity, availability, or confidentiality, or (2) a benign, but nonetheless purposeful, attempt to circumvent system security.

Individuals that have the necessary motivation and resources for carrying out an attack are potentially dangerous threat-sources. Table 1 shows an overview of common human threats, their possible motivations, and the methods or threat actions by which they might carry out an attack against the CII. This information is considered useful to organizations studying their human threat environments and customizing their human threat statements:

41 Stoneburner et al., op. cit.
42 Ibid., p. 13.

Human Threat-Sources	Motivations	Methods/Threat Actions
Hacker, cracker	Challenge, ego, rebellion	Hacking Social engineering System intrusion, break-ins Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	Computer crime (e.g. cyber-stalking) Fraudulent act Information bribery Spoofing System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	Bomb/terrorism Information warfare System attack (e.g., distributed denial of service) System penetration System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic gain	Economic exploitation Information theft Intrusion on personal privacy Social engineering System penetration Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	Assault on employee; Blackmail; Browsing of proprietary information; Computer abuse; Fraud and theft; Information bribery; Input of falsified, corrupted data; Interception; Malicious code (e.g., virus, logic bomb, Trojan horse); Sale of personal information; System bugs; System intrusion; System sabotage; Unauthorized system access

Table 1: Human Threats — Threat Source, Motivation, and Threat Actions[43]

However, while there is data especially for natural and environmental threats, data for human threats is hard to come by. Quantitative information on the nature and source of external threats can be derived from police reports, computer security surveys and bulletins, reports of an audit analysis, or actuarial studies. Information on internal threats can be estimated using previous experience and data, generic statistical information, or a combination of both. But it is generally acknowledged that in order to truly know how vulnerable critical infrastructures are to cyber-attacks, we would require much more information,

43 Ibid., p. 14.

including a detailed assessment of redundancy for each target infrastructure, normal rates of failure and response, the degree to which critical functions are accessible from public networks, and the level of human control, monitoring, and intervention in critical operations.[44] However, there is no public or even readily available data on how vulnerable critical systems might be. Defense-related computers are buried under layers of secrecy and classification, and private companies are not likely to volunteer such information.[45]

Especially when dealing with actor-based threats such as terrorism, we are dealing with a "people business" that is intrinsically non-quantifiable and thus poses significant problems for a traditional risk analysis aproach.[46] But various types of uncertainties make it difficult for the intelligence community to effectively analyze the changing nature of the threat and the degree of risk involved. These uncertainties are linked to inherent characteristics of cyber-threats — characteristics that they share with a whole set of "new" threats to security.

Step 3: Vulnerability Identification

Step 3 is the development of a list of system vulnerabilities that could be exploited by the potential threat sources. Vulnerability can be defined in the context of CIP/CIIP as "a characteristic of a critical infrastructure's design, implementation, or operation that renders it susceptible to destruction or incapacitation by a threat".[47] When considering limited, technical subsystems, a vulnerability may be seen as a "flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy".[48]

44 Lewis, James A. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats (Center for Strategic and International Studies, 2002), p 10. http://www.csis.org/tech/0211_lewis.pdf. Haimes, Yacov Y. and Pu Jiang. "Leontief-Based Model of Risk in Complex Interconnected Infrastructures". In: Journal of Infrastructure Systems, 7, 1 (2001), pp. 1–12.

45 Chapman, Gary. "National Security and the Internet". Paper presented at the Annual Convention of the Internet Society, Geneva, July 1998.

46 Zimmermann, Doron. The Transformation of Terrorism. The "New Terrorism," Impact Scalability and the Dynamic of Reciprocal Threat Perception. In: Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung No. 67 (Zurich, 2003), p. 61. http://www.isn.ethz.ch/crn/extended/docs/ZB67.pdf and Metzger, op. cit.

47 PCCIP, op. cit., Appendix, B-3.

48 Stoneburner et. al., op. cit., p. 15.

Vulnerability assessment involves the systematic examination of critical infrastructure and the interconnected systems on which it relies (including information and products) to identify those critical infrastructures or related components that may be at risk from an attack.[49] Recommended methods for the identification of system vulnerabilities are the use of vulnerability sources, the performance of system security testing, and the development of a security requirements checklist. Again, it is far easier to assess the vulnerabilities of a relatively restricted IT system such as a business network than to do so at a higher system level.

There is a lot of emphasis on vulnerabilities in the current CIP/CIIP debate, resulting in a variety of vulnerability assessment methods and tools. However, these vary considerably in terms of the size and nature of the system they can evaluate. In the US in particular, there is a tendency to substitute vulnerability assessments for risk assessments, as exemplified in the CIAO Vulnerability Assessment Process/Project Matrix. However, it is easy to deceive oneself through over-confidence: when looking at relatively limited systems, many factors are known, and data may even be available. This may create a false sense of accuracy. Especially when considering human threats, for example terrorism, a sole focus on vulnerabilities, sensible though it may be with respect to cost-benefit considerations, often implicitly assumes that terrorist actors will also recognize and identify the same infrastructures as priority targets — an assumption that might backfire.[50] Wrong assumptions, and hence wrong protection measures, are therefore one possible outcome of a misled vulnerability assessment.

Step 4: Control Analysis

In step 4, planned or implemented controls are analyzed in order to minimize or eliminate the likelihood (or probability) of a threat exploiting any existing system vulnerability. Security controls encompass the use of technical and non-technical methods: Technical controls are safeguards incorporated into computer hardware, software, or firmware. Non-technical controls include management and operational controls, such as security policies; operational procedures; and personnel, physical, and environmental security.

49 PCCIP, op. cit., Appendix, B–3.
50 Zimmermann, op. cit., pp. 61–65.

Technical protection manuals recommend security measures for selected IT systems.[51] The aim of these recommendations is to achieve a reasonable security level for IT systems that is adequate to protection requirements ranging from normal to high degrees of protection. Others provide models for the design, development, or implementation of secure IT systems, taking into consideration the four IT-security objectives: availability (of system and data for intended use only); integrity of system or data; confidentiality of data and system information; accountability.[52] Most of these objectives are business-oriented and centered on organizational information systems, which precludes them from being directly applicable to larger systems.

Step 5: Likelihood Determination

In determining the likelihood of a threat, one must consider threat sources (step 2), potential vulnerabilities (step 3), and existing controls (step 4). There are several techniques for estimating probabilities in risk analysis, such as statistical inference, scenario technique, fault trees, and event trees, which we will not discuss in more detail here. Apart from quantitative measures, the likelihood that a potential vulnerability could be exploited by a given threat source can also be described in terms of different qualitative categories (e.g., high, medium, low), based on subjective expert knowledge.

Step 6: Impact or Harm Analysis

In step 6, the adverse impact resulting from a successful threat exploitation of a vulnerability is determined. An isolated vulnerability and an isolated threat are not enough to cause harm or damage to CI/CII. Rather, the convergence of a threat with a specific vulnerability, combined with the possibility of a harmful impact, produces the risk. Such impacts represent disruptive challenges of different types, durations, and levels of severity, and can be measured using different parameters such as economic loss or social and political damage. The term "impact" is also used interchangeably with the terms "harm", "effect", or "consequence".

51 Bundesamt für Sicherheit in der Informationstechnik. IT Baseline Protection Manual. Standard Security Safeguards (updated July 2001). http://www.bsi.de/gshb/english/menue.htm.

52 Stoneburner et. al., op. cit.

The impact of possible harm to an asset is best determined by a business executive, an asset owner, or an asset manager. The adverse impact of a security event in an IT system can be described in terms of loss or degradation of any, or of a combination, of the IT-security objectives. Other categories might be applied if risk analysis is conducted for more abstract systems: The impact of the loss or disruption of such assets can be assessed by the use of impact factors such as area of impact, severity of impact, and time.[53] For some events (such as electronic attacks), occurrence, detection, and remedial action may all take place within a matter of days. Others will have a much longer timeframe: for example, the impact of global warming will be felt over decades and centuries. Also, impact categories that correspond to indicators used to measure criticality can be used, such as service delivery, public, economic, political, environmental, interdependency.

Some tangible impacts can be measured in a quantitative manner in terms of lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other effects (e.g., loss of public confidence, loss of credibility, damage to an organization's interest) cannot be measured in specific units, but can at least be qualified or described in terms of high, medium, and low impact.[54] However, in interdependent systems, assessing the result of the loss of a critical asset becomes fairly complex.

Step 7: Risk Determination

The purpose of step 7 is to assess the level of risk to the system. The determination of risk is a function of the likelihood that a given threat source will attempt to exploit a given vulnerability (step 5) and the magnitude of the impact, should a threat source successfully exploit the vulnerability (step 6).

Step 8: Countermeasure Priority Rating

The countermeasure rating expresses the difference between the required risk (desired "risk level" as set by the management authority of the system) and the resultant risk (step 7). It is used to provide guidance as to the importance

53 Public Safety and Emergency Preparedness Canada (PSEPC). Assets criteria. http://www.psepc-sppcc.gc.ca/prg/em/nciap/assets_criteria-en.asp.

54 Stoneburner et. al., op. cit., p. 22.

that should be placed on security countermeasures. Again, applied values and categories may vary widely.

Table 2 is an example of a Risk Assessment Table, which helps to calculate the level of the Countermeasure Priority Rating (column 7). Column 7 is simply the difference between the resultant risk and the required risk (Columns 6 and 5 in the example) expressed as a numerical value.

Column 1 Asset Identification	C 2 Threat to the Asset	C 3 Threat Likelihood	C 4 Harm	C 5 Resultant Risk	C 6 Required Risk	C 7
Row 1: Reliability of e-commerce-related web-site	Accidental electrical power or equipment failure	Medium	Grave	Critical	Nil	4
Row 2: Accuracy of publicly available web information	Loss of confidence or goodwill due to "hacking" of web page	High	Minor	Medium	Low	1
Row 3: Secure access to internal network services by authorized staff, from external networks	Loss of crypto token or keys required to access the secure channel(s)	Very Low	Serious	Medium	Low	1

Table 2: Risk Assessment Table[55]

Step 9: Risk Mitigation

Step 9 is about risk mitigation and involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls suggested by the risk assessment process. Because the elimination of all risk is usually impractical or near-impossible in reality, the stakeholders themselves must use the least-cost approach and implement the most appropriate controls to decrease mission risk to an acceptable level.[56]

55 Commonwealth of Australia. ACSI 33. Handbook 3, Risk Management, Appendix. http://www.dsd.gov.au/_lib/pdf_doc/acsi33/HB3Ap.pdf.

56 Stoneburner et. al., op. cit.

Different kinds of security controls, or a combination of such controls, can be applied at the technical, management, and operational levels with the goal of maximizing the effectiveness of controls for IT systems and organizations.

- Technical security controls for risk mitigation can be configured to protect against given types of threats. These security controls may range from simple to complex measures. They usually involve system architectures; engineering disciplines; and security packages with a mix of hardware, software, and firmware.
- Management security controls, in conjunction with technical and operational controls, are implemented to manage and reduce the risk of loss and to protect an organization's mission. Management controls focus on the stipulation of information protection policy, guidelines, and standards.
- Operational controls, implemented in accordance with a basic set of requirements (e.g., technical controls) and good industry practices, are used to correct operational deficiencies that could be exploited by potential threat sources.

This concludes our exemplified risk analysis approach.

Analysis of Methods in Use and Conclusion

In order to cost-effectively prioritize means of preparing for, mitigating, and responding to possible risks against crucial assets, a variety of issues need to be evaluated and analyzed. A review of current methodologies for analyzing CII – both for information systems as well as for the larger set of critical infrastructures –shows that they often prove to be insufficient. In fact, it is obvious that various methodological approaches fall short in a number of substantial areas, mainly due to the ever-more complex risk environment and the dynamically changing characteristics of the systems under consideration.

Many conceptual shortcomings become apparent when the discussion moves to the systems that have become vital to modern society. The greatest of these shortcomings is the failure to understand interdependencies and possible cascading effects. Besides, the available methods are either too sector-specific or too focused on single infrastructures and do not take into account the

strategic, security-related, and economic importance of CII. At the moment, our "methodological toolbox" is filled with old tools, which have, in some cases, been hurriedly adapted to a new set of problems. However, both the systems and the risk environment have become qualitatively different in a way that demands new analytical techniques and methodologies for their evaluation:

Unbounded systems: Risk assessment originated in the technical context of limited or "closed" systems. Today, however, we are no longer dealing with closed systems in a centrally networked environment, but systems that are part of global network environment that knows no bounds, no central control, and offers only limited insight into the underlying system structure. These unbounded systems also lack well-defined geographic, political, cultural, and legal and jurisdictional boundaries.[57]

Complex, interdependent systems: Risk assessment breaks problems down into smaller parts. However, both infrastructures and information infrastructures are highly complex and interdependent systems. One of the hallmarks of complex systems is that they display emergent behavior that is a property of the system as a whole and that cannot be studied by taking it apart.[58] Due to system complexity, vulnerabilities and infrastructure disruptions are no longer traceable in any useful way to single technical subsystems and vice versa. Therefore, even if one carefully examines a relatively localized subsystem from the point of view of risks and threats, these insights can hardly be generalized and formalized for application "beyond" the subsystem itself or at a higher system level.

Interdependency: In addition, current assessment methods fail to address the crucial issue of (bi-) directional relationships between infrastructure components, subsystems, or systems (interdependencies) in any meaningful way. In this way, interdependencies serve as a benchmark for CII methods and models, because the major shortcomings of present approaches become particularly apparent in their inability to cope with the problem of interdependencies. This is true for risk analysis methodologies as well as for technical security models – in fact,

57 Ellison, R. J., D. A. Fisher, R. C. Linger, H. F. Lipson, T. Longstaff, and N. R. Mead. Survivable Network Systems: An Emerging Discipline (technical report, November 1997). CMU/SEI-97-TR-013. ESC-TR-97-013, pp. 4–6. http://www.cert.org/research/97tr013.pdf; Allen, Julia H. and Carol A. Sledge. "Information Survivability: Required Shifts in Perspective". In: CrossTalk: The Journal of Defense Software Engineering, July 2002: pp. 7–9. http://www.stsc.hill.af.mil/crosstalk/2002/07/allen.html.

58 Crutchfield, op. cit., pp. 479–97.

it applies to practically all of the approaches currently in use. What becomes abundantly clear is that it will be necessary to move beyond mere estimates of interdependencies towards sophisticated modeling of cause-and-effect relationships and possible cascading failures.

A sole focus on technical systems and subsystems is misleading: The importance of laws, regulations, policies, and other economic, social, and national-security considerations for the infrastructure environment makes it indispensable to study their impacts on interdependent infrastructures at all times.[59] In addition, the level of damage impact that is acceptable to society is determined more by political criteria than by system-technical standards: One of the crucial questions is how damage to or the disruption of an infrastructure would be perceived and exploited politically.[60] Risk assessment, however, does not offer any method for cataloguing objects, vulnerabilities, and threats at a strategic policy level, such as the economy at large, in a meaningful way. In addition, a preoccupation with technologies risks disregarding one rather central element of the information infrastructure – people. Humans are, in effect, one of the most substantial parts of the information "infrastructure", as they provide, manage, and generate new information, operate, maintain, and occasionally even subvert other elements of information infrastructure. As the cognizant agent in the game, they also play a major part on the threat side of the equation. This is especially interesting since experts consider the threat emanating from "insiders" to be far greater than that of anonymous "cyber-terrorists"[61] — meaning that an element that is part of the information infrastructure can also constitute the greatest danger to it.

Lack of data for many important threats: Even though there are various methods of conducting a risk assessment, they often entail a very similar structure under which objects, threats, vulnerabilities, and probabilities are catalogued and links between them are defined. One of the main difficulties is that there are both theoretical and practical difficulties involved in estimating the probabilities and consequences of low-probability, high-impact events — since there are no useful statistics for possible damage and failure probabilities.

59 Rinaldi and Peerenboom, op. cit.
60 Metzger, op. cit.
61 Lewis, op. cit.

Static approach: Even though a risk assessment could theoretically be carried out on a daily basis, it is a static approach aimed at evaluating current systems and vulnerabilities. Since the process is time-consuming, there is always a delay until its results can be determined and implemented. This is especially worrying in view of the continuous rapid technological developments and because many related challenges and problems are only just emerging; the system characteristics of the emerging information infrastructure will, in fact, differ radically from traditional structures in terms of scale, connectivity, and dependencies. The interlinked aspects of market forces, technological evolutions, and newly emerging risks forces analysts to constantly look ahead and to develop new analytical techniques, methodologies, and mindsets. Their development will, in turn, require great efforts in unconventional and proactive thinking.

In conclusion, effective security demands a far more profound understanding of various crucial aspects of the communication networks and information systems under consideration, such as their behavior under normal circumstances and under stress, as well as their role and criticality for the economy and society. We should therefore aim to widen the focus of our enquiry in order to understand emerging risks in their appropriate technological and socio-political context. In addition, governments could help to encourage dialog between experts from various disciplines, ranging from engineering and complexity sciences to policy research, political science, psychology, and sociology.

Challenges Governments Face in the Field of Critical Information Infrastructure Protection (CIIP): Stakeholders and Perspectives

By Isabelle Abele-Wigert

Introduction

The task assigned by the US president was daunting. After 15 months of evaluating the infrastructures, assessing their vulnerabilities, and deliberating assurance alternatives, the US Presidential Commission on Critical Infrastructure Protection presented its report in October 1997. The commission's charter included all critical infrastructures, such as power, water, communication, financial, health and so forth, and its members had access to classified information. However, the commission chose to focus on one critical infrastructure — the cyber-infrastructure: "[…] the collective dependence on the information and communication infrastructure drives us to seek new understanding about the information age. Essentially, we recognize a very real and growing cyber dimension associated with infrastructure assurance."[1] The commission further stated that the dependence of all critical infrastructures on information and communication systems was the source of rising vulnerabilities, and that it had therefore concentrated its efforts on this area.[2] As a result, CIIP became the focus of their attention.

Today, almost ten years after the US commission's report, CIIP is an even more vital issue, not only in the US, but also in most other developed states. Key sectors of modern societies are increasingly dependent on the smooth exchange and storage of information in electronic networks.[3] For instance, electricity, banking and finance, health, and emergency services cannot work properly without ICT. These critical information infrastructures underpin and connect other infrastructure systems and make them interrelated and interdependent. Any damage to or interruption of the critical (information) infrastructure

1 "Critical Foundations: Protecting America's Infrastructures". The Report of the President's Commission on Critical Infrastructure Protection (October 1997), p. vii.

2 Ibid., p. i.

3 Joint Economic Committee. United States Congress. Security in the Information Age. New Challenges, New Strategies (Washington, May 2002), p. 12. http://www.fas.org/irp/congress/2002_rpt/jec-sec.pdf.

could cause cascading effects across technical systems and throughout the fabric of society.

Because information systems offer many opportunities, they are attractive targets for malicious attacks. Following the example set by the US in the mid-1990s,[4] many developed countries have taken steps to better understand the vulnerabilities of and threats to their critical information infrastructure and have drafted necessary protection concepts. It became clear that cyber-attacks as well as network and information security pose complex problems that have unprecedented effects on various aspects of national security and public policy. The overview of governmental efforts listed in the CIIP Handbook 2006 reveals a major challenge: The fact that so many different communities and stakeholders are involved — all of whom are trying to shape the topic according to their interests and the resources at hand — makes it very difficult for governments to address the issue of CIIP comprehensively.

In all countries covered in the CIIP Handbook, multiple government agencies are involved, ranging from law-enforcement to civil defense organizations. Next to the government, private infrastructure operators have an interest in the smooth functioning of the critical (information) infrastructures. A further actor group is the academic community conducting research in different fields of CIIP. Last but not least, there are the individual users or consumers of critical infrastructure services. These actors sometimes have divergent perceptions of what CIIP is. Differing positions within governments and the private sector complicate the assignment of responsibility, and lead to discussions of whether CIIP is a matter of ordinary day-to-day politics or belongs to the realm of national or international security.[5]

4 Clinton, William J. Executive Order 13010 on Critical Infrastructure Protection (Washington, 15 July 1996). http://www.info-sec.com/pccip/web/eo13010.html; Clinton, William J. Protecting America's Critical Infrastructures: Presidential Decision Directive 63 (Washington, 22 May 1998). http://www.fas.org/irp/offdocs/pdd-63.htm.; The President's Commission on Critical Infrastructure Protection (PCCIP). Critical Foundations: Protecting America's Infrastructures (Washington, October 1997); White Paper on PDD-63. The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 (Washington, 22 May 1998). http://www.cybercrime.gov/white_pr.htm; Bendrath, Ralf. "Critical Infrastructure Protection in the United States". In: ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead (Zurich, 8–10 November 2001).

5 Metzger, Jan. The Concept of Critical Infrastructure Protection (CIP). In: A.J.K. Bailes/I. Frommelt (eds.), Business and Security: Public-Private Sector Relationships in a New Security Environment (Oxford, 2004).

This article is mainly based on information compiled in the CIIP Handbook[6] as well as on government and workshop papers. The aim of this article is to elaborate the difficulties governments face when dealing with CIIP, taking into consideration all of the different actors' perspectives. The challenge arises what governments' role should be when being confronted with the actors' disparate expectations.

Different Actors

Many of the national CIIP efforts were triggered by the Presidential Commission on Critical Infrastructure Protection set up by former US president Bill Clinton in 1996,[7] and also, to some extent, by fears of a "Y2K" computer problem. This led to the establishment of interdepartmental committees, task forces, and working groups. In the aftermath of 11 September 2001, several countries have launched further initiatives and have allocated additional resources to their CIIP efforts.

Various actor groups dealing with CIIP can be identified: The first of these is the public sector, consisting of governments and their different agencies. Governments are responsible for the country's overall security, public safety, the effective functioning of the economy, and the continuity of government services in case of an emergency or crisis. Moreover, governments have a critical role at the strategic level in providing a clear assessment of potential risks and threats, and adequate responses as well as leadership. Governments can provide emergency plans and the required resources, enact appropriate laws and legislation, support security initiatives, raise awareness, and foster dialog with the stakeholders involved.

Most of the critical (information) infrastructures are administered by the private sector, especially by private infrastructure operators. The ongoing privatization of vital infrastructure sectors such as water, energy, or transportation since the 1980s has led to a rise in private-sectors ownership and a decline

6 Dunn, Myriam and Isabelle Wigert. International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries (Zurich: Center for Security Studies, 2004); and Abele-Wigert, Isabelle and Myriam Dunn. International CIIP Handbook 2006, Vol. I. An Inventory of 20 National and 6 International Protection Policies (Zurich: Center for Security Studies, 2006). http://www.isn.ethz.ch/crn/publications/publications_crn.cfm?pubid=224.

7 Executive Order 13010 on Critical Infrastructure Protection, op. cit.

of government ownership of critical infrastructures.[8] As a result, the greater capability for dealing with critical information infrastructure risks lies not in the hands of governments, but with the private sector entities that actually manage and operate the ICT infrastructure. Whereas governments guarantee national security and facilitate information and communication processes, private businesses have detailed knowledge about their critical infrastructures, so that the implementation of effective protection policies rests mainly with the private sector.[9] Given the dynamic threat to critical (information) infrastructures and the possible consequences of a successful attack, the private sector may seek advice and additional information from governments and vice versa.[10]

With respect to critical infrastructures, the interests of the private and the public sectors are identical: The focus is on the smooth functioning and uninterrupted availability of the critical assets. The negative consequences of a major interruption would be serious for both groups of actors. The scenarios that exceed everyday business risks underscore the necessity of public-private partnerships between companies and the public sector. Therefore, at a practical level, private companies have a real interest in minimizing their business continuity risks. The effectiveness of their CIIP approaches in the context of national security depends on how comprehensively private companies take events into consideration that could affect them. The definition of an "adequate" level of information security can vary considerably.[11] The government's emergency preparedness measures, and a lack of interest on the part of private actors in providing sufficient measures for society as a whole, sometimes leave a security gap.

Especially when dealing with threats and risks that exceed ordinary business risks, cooperation and information exchange within public-private partnerships would be beneficial for both sides: governments may have (intelligence) information on threats that could be essential for private companies, whereas

8 Henriksen, Stein. "The Shift of Responsibilities within Government and Society". In: CRN-Workshop Report. Societal Security and Crisis Management in the 21st Century (Stockholm, 2004), pp. 60–63.

9 Bundesministerium des Innern. Schutz Kritischer Infrastrukturen — Basisschutzkonzept: Empfehlungen für Unternehmen (Berlin, 2005), p. 6.

10 The White House. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (Washington, February 2003). http://www.whitehouse.gov/pcipb/physical.html.

11 TNO Information and Communication Technology. TNO report 33680. International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues (30 June 2005), p. 29.

the private sector has a lot of practical experience in the field of information assurance that could be of interest for governments.[12]

A third actor group that can be identified is the academic community, doing research into different fields of CIIP, ranging from technical issues to political or economic aspects of the topic. Until now, CIIP has mainly been a topic for engineers, IT security specialists, and other experts, while the socio-political dimensions of the topic have been neglected. In the current debate over homeland security and terrorism, where CIP and CIIP are key issues, it has become obvious that an exclusive focus on technical measures is not sufficient.[13] In fact, the complexity of the issue and the challenges of CIIP demand an integration of a variety of disciplines.

Last but not least the individual users or consumers of critical infrastructure services expect all services to be constantly available without interruptions, preferably at a cheap rate. Whereas our economy is propelled by complex, imperfect ICT, the average users of this technology do not understand the threat, nor do they know how to protect themselves. Ideally, companies should respond to the demands of their customers' security needs in the field of computer and information security. On the other hand, the consumers' willingness to pay for extra security measures may be limited.

Finally, the fact that so many elements of the critical infrastructures are in the hands of the private sector or of foreign actors in other countries is an additional challenge. Also, governments have to operate in unfamiliar ways by sharing influence with experts in the IT community, with businesses, and with nonprofit organizations.

12 Wigert, Isabelle. "Der Schutz kritischer Informationsinfrastrukturen in der Schweiz: Eine Analyse von Akteuren und Herausforderungen". In: Bulletin zur schweizerischen Sicherheitspolitik 2005 (Zurich: Center for Security Studies, 2005), pp. 97–121. http://www.isn.ethz.ch/pubs/ph/details.cfm?v21=62185&lng=en&id=10720.

13 Dunn, Myriam. "The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP)". In: International Journal for Critical Infrastructure Protection, Vol. 1, No. 2/3 (2005), pp. 258–68.

Different Perspectives on CIIP

These actors consider CIIP from different angles and with varying motivations.[14] As a result, differences in positions, for instance between governments and the private sector, complicate the assignment of roles and responsibilities. When deciding upon appropriate measures for dealing with the problem, disagreement can arise. Questions such as which critical (information) infrastructures need to be protected, by whom, how, and when may be determined by the allocation of resources. Moreover, the boundaries between the different perspectives overlap. Among the most important viewpoints, we can list the following ideal-type and simplified perspectives:[15]

- The system-level, technical perspective: With this perspective, CIIP is approached as an IT-security or information assurance issue, with a strong focus on internet security. In this view, threats to the information infrastructure are to be confronted by technical means such as firewalls, anti-virus software, or intrusion and detection software. The establishment of so-called Computer Emergency Response Teams (CERTs) and similar early-warning approaches in various countries are examples of this perspective.
- The business perspective: Here, CIIP is seen as an issue of "business continuity", especially in the context of e-business. This requires not only permanent access to IT infrastructures, but also permanently available business processes to ensure satisfactory business performance. The means of achieving this coincide, by and large, with the ideas of the technical community mentioned above; however, the focus is not solely on the system level, but includes organizational and human factors. This perspective is also reflected in some countries' protection approaches that mainly aim to support the information society.
- The law-enforcement perspective: CIIP is seen as an issue of protecting society against (cyber-) crime. Cyber-crime is a very broad concept

14 Dunn/Wigert, op. cit., p. 22, and Wigert, op. cit.

15 Dunn/Wigert, op. cit., p. 22; and Myriam Dunn. "Critical Information Infrastructure Protection (CIIP). Sicherheit im Informationszeitalter als gemeinsame Herausforderung für Politik und Wirtschaft". In: digma: Zeitschrift für Datenrecht und Informationssicherheit (June 2004), pp. 66–69.

that has various meanings, ranging from technology-enabled crimes to crimes committed against individual computers, including issues such as computer fraud, child pornography, or violations of network security. The struggle against cyber-crime involves more or less traditional law-enforcement strategies, and is assisted by adopting appropriate legislation and fostering international co-operation.

- Finally, there is the national-security perspective: This is a very comprehensive view of CIIP. Usually, the whole of society is perceived as being endangered, so that action is taken at a variety of levels (e.g., at the technical, legislative, organizational, or international levels), and the actors involved in protection efforts include government officials from different agencies, as well as representatives of the private sector and of the general public.

All of these perspectives have an impact on protection policies. In which situations and areas of national security do the public and the private sector, respectively, have the responsibility for appropriate measures and provisions? This discussion leads to the central question of whether CIIP is an issue of ordinary day-to-day politics or belongs to the realm of national or international security. The answers may vary depending on the scenario, and are linked to the question of which protection efforts, goals, strategies, and instruments are appropriate for problem solution.[16]

The fact that about 85 per cent of the critical infrastructures are in the hands of the private sector or of foreign actors in other countries only aggravates the problem of demarcation.[17] Therefore, states can no longer assure security on their own. They have to establish new ways of interaction and cooperation with different national and international actors that have not traditionally been in the security arena. The internet has no political boundaries, and cyber-security policy responsibilities cannot be assigned easily across borders.

Moreover, many actors in different governmental agencies are dealing with the problem. Very often, responsibility is given to well-established organizations or agencies that appear suitable for the task. Only in a few countries, such as Canada, Germany, Sweden, the United Kingdom, or the United States, have

16 Dunn/Wigert, op. cit.

17 Remarks by US Secretary of Homeland Security Michael Chertoff at the Center for Catastrophic Preparedness and Response and the International Center for Enterprise Preparedness (New York, 26 April 2005). http://www.dhs.gov/dhspublic/display?content=4479.

central government organizations been established to deal specifically with CIIP.[18]

Most countries in the CIIP Handbook consider CIIP to be a national security issue, and also stress the importance of CIIP for the economy, and crime prevention. In countries such as France, New Zealand, and Sweden, CIIP is mainly led by the defense establishment, whereas in other countries, such as the UK or Switzerland, approaches to CIIP are jointly led by the business community and public agencies. Furthermore, in Australia, the US, and New Zealand, CIIP is integrated into the overall counterterrorism efforts, where the intelligence community plays an important role.[19] In India, CIIP is seen as an essential part of the country's way to becoming an information technology superpower. It is hoped that the promotion of safe IT products and widespread use will benefit the whole nation economically. In the Republic of Korea, in Japan, Malaysia and Singapore, CIIP is considered essential for a prosperous e-economy and e-society. Information technology and information assurance are seen as part of the global power competition. In Russia, information security is closely linked to the safeguarding of state secrets: CIIP is an element of the central government's power politics.[20]

Areas of Governmental Action in CIIP

The challenges that governments must address in the area of CIIP are manifold. There is no doubt that governments have responsibilities as owners and operators of information systems. Their policies usually have two aims: first, to promote the usage of the new information and communication technologies in order to support the information society and the welfare of the nation. Secondly, and at the same time, governments try to protect their citizens and companies from the risks and dangers emanating from the very same technologies.

Different areas of governmental actions have emerged in the field of CIIP, which should all be taken into account when pursuing a comprehensive CIIP

18 In Canada it is Public Safety and Emergency Preparedness Canada (PSEPC); in Germany the Federal Office of Information Security (BSI); in Sweden the Swedish Emergency Management Agency (SEMA); in the UK the National Infrastructure Security Co-ordination Centre (NISCC); and in the United States the Department of Homeland Security (DHS). Dunn/Wigert, op. cit.; and Abele-Wigert/Dunn, op.cit.

19 Dunn/Wigert, op. cit.; and Abele-Wigert/Dunn, op.cit.

20 Ibid.

policy. First of all, reducing the risks to critical infrastructures requires an effort to counter or disrupt the sources of threat through education, civil action, criminal prosecution, or intelligence operation. In addition, it is essential to identify vulnerabilities by research and to reduce the impact of an attack by providing warnings, improved resilience, and disaster recovery. Finally, assessing trends by incident reporting, information sharing, and dialog with infrastructure owners is also an important part of a holistic CIIP policy. Therefore, governments should pay special attention to the following issues:

- Understanding the nature of risks and threats and the resulting vulnerabilities: One of the much-debated difficulties is assessing the threats and risks to critical information infrastructures. From predictions of a "Digital Pearl Harbor" to statements playing down the threats, experts imagine all kinds of scenarios. Governments should provide reliable and well-documented threat and risk assessments in this field, taking into account technical, organizational, legal, and national security factors. A good example of a government agency covering the legal, technical, and security policy aspects of CIIP is the Swiss Reporting and Analysis Center for Information Assurance (MELANI).
- Enhancing vulnerability detection and response: Governments have a role to play by initiating, supporting, or operating information-sharing structures, often based on public-private partnerships. This approach is exemplified by the Computer Emergency Response Teams (CERTs) and Information Sharing and Analysis Centers (ISACs). To gather all the relevant information, governments have to set up formal and informal information-exchange channels with all relevant actors, such as academia, private businesses, and intelligence services. Moreover, governments must handle sensitive information with care. This is certainly one of the reasons why the UK National Infrastructure Security Co-ordination Centre (NISCC) is such a successful model in handling CIIP.
- Promoting more secure products and services, and supporting research and development: Governments should encourage the development of more secure IT-related products and services, particularly securi-

ty standards and certification procedures. It is important that incentives for information security improvements be focused on those who are best able to provide greater security: For instance, if vendors were liable for the security performance of their products, there would be a strong incentive for them to increase the security of their products. Another challenge is how to ensure that officials concerned with the protection of CII understand and catch up with the rapidly changing technological architecture and new industry structures.[21] Since it is difficult for each private company to ascertain whether its security levels are adequate when obtaining software, cryptography, or IT services on the open market, the Japanese Ministry of Economy, Trade and Industry (METI), for instance, has developed several information-security evaluation systems that are conducted through a third party since April 2003. These systems include an information auditing system, an information security management system, certification for the evaluation of security products, and encryption technology evaluation systems. These standards are not only used for the government's procurement of its own software and IT services, but can also be used by the private sector in the future.[22]

- Raising awareness and information-sharing: Governments need to inform individuals and organizations about risks related to cybercrime and the dangers of insufficient security for themselves and for others, as well as available solutions. Information should be shared continuously among governments, industries, and academia, but also within governments. Over many years, some government organizations have created information systems that suited their needs with-

21 TNO report 33680, op. cit., p. 63.

22 Other activities include: Japan Information Processing Development Corporation (JIPDEC) started Information Security Management System (ISMS), a new accreditation system for any kind of services dealing with information, based on ISO/IEC 17799 in April 2002, replacing the Information-Processing Accreditation Scheme (IAS). http://www.meti.go.jp/english/policy/index_information_policy.html.
The Ministry of Internal Affairs and Communications (MIC) and the Ministry of Economy, Trade and Industry (METI) established the CRYPTREC Advisory Committee (chaired by Prof. IMAI Hideki, The University of Tokyo) in May 2001 to promote information security measures by objectively evaluating secure cryptographic techniques. Based on the results of the evaluations, a list of e-Government recommended cryptographic technique was reported. http://www.meti.go.jp/english/policy/index_information_policy.html.

out regard for the requirements of other organizations.[23] Moreover, a common vocabulary has to be defined and sensitive information classified. Some governments have set up special education programs. For instance, in South Korea, information security education has become part of the computer literacy education that begins at primary-school level.[24] For instance the UK government has undertaken initiatives such as "IT Safe - IT Security Awareness for Everyone" and "GetSafeOnline" that particularly address home users and small businesses with advice in plain English and practical tips on protecting computers.[25] In Germany the campaign "Security in the Internet" and the internet service "BSI for the citizen" provide easy-to-understand information on relevant IT security issues.[26] Awareness-raising is also a main activity of the European Network and Information Security Agency (ENISA).[27]

- Developing an adequate legal framework: A sound legal framework and effective law enforcement procedures are essential in deterring cyber-crime. Although many developed countries have discussed the protection and security of information (infrastructures) and related legislation for some years, most of them have only begun to review and adapt their legislation since 11 September 2001. The Republic of Korea enacted a special "Information Infrastructure Protection Act" in January 2001 that outlines the government framework for information infrastructure protection. Because national laws are developed autonomously, there is a need to harmonize national legal provisions and to enhance judicial and police cooperation internationally. Many countries have also set up special cyber-crime units, which are usually part of the national police force and/or the intelligence services, or of another law enforcement agency.[28]
- Emergency preparedness and crisis management: These are important aspects of CIIP. In the past, these goals have been comparatively easy to achieve, as the responsibility and services were in the hands of the

23 White, Gregory B./DiCenso, David J. Information Sharing Needs for National Security. Proceedings of the 38th Hawaii International Conference on System Sciences, 2005, p.4. http://csdl2.computer.org/comp/proceedings/hicss/2005/2268/05/22680125c.pdf.

24 http://www.mic.go.kr/index.jsp.

25 http://www.itsafe.gov.uk.

26 http://www.sicherheit-im-internet.de; and http://www.bsi-fuer-buerger.de.

27 http://www.enisa.eu.int/about/activities/index_en.htm.

28 See CIIP Handbook 2006 Volume I.

government. Today, however, it is less easy to say who is responsible when critical infrastructure services are no longer available, and who has to cover the financial damages incurred by a service failure and repair. As governments and private companies involved in CIIP may have different standards, means, and policies, the responsibilities have to be clearly assigned to those involved in order to ensure a well functioning state and society. Successful emergency management requires clear guidelines and recommendations. Governments should implement adequate legislative regulations, make financial incentives available to the private sector, and create public-private partnerships.[29] In Canada, for example, an all-hazards approach was initiated with the establishment of Public Safety and Emergency Preparedness Canada (PSEPC) and its National Critical Infrastructure Assurance Program (NCIAP) in 2003. The goals are to provide a national framework for cooperative action and overall national leadership and coordination, especially for crisis management. CIIP is pursued in partnership between government organizations, private-sector owners and operators, and others with a stake in the Canada's national critical infrastructure. The partners exchange timely information about risks, vulnerabilities, and threats and thus create a better understanding of interdependencies.[30]

Conclusion

Modern societies are increasingly connected and dependent on critical information infrastructures. The increased speed of the networks has also scaled up the inherent threats and risks. Many actors with different backgrounds and interests are involved in a country's CIIP policy. It is obvious that all actors involved, and especially the government that must deal with these actors, require a common understanding on how to address the issue. So far, different types of government activity have emerged in the field of CIIP, such as awareness-raising and information-sharing, enhancing vulnerability detection and response, promoting more secure products and services, developing an adequate legal framework, and institutionalizing effective crisis management.

29 See contribution of Andersson, Jan Joel and Andreas Malm in this volume.
30 http://www.psepc-sppcc.gc.ca/prg/em/nciap/creation-en.asp.

Considering the complex nature of a comprehensive CIIP policy, the role that states can and should play in handling the issue is manifold and challenging. Sharing of power with non-state actors is not the only difficult issue: like other problems involving security, this one has global origins and implications, and its solution requires transnational institutions. But most states still treat CIIP primarily as a national security issue, even though the information infrastructure transcends many boundaries. Whereas many governments have supported national initiatives and policies and have set up new organizations or working groups for dealing with CIIP, many obstacles remain to be overcome, especially for an international dialog. Best practices and possible solutions to CIIP challenges vary from country to country and are obviously influenced by historical, geographical, political, organizational, or cultural peculiarities and traditions, as well as by the resources at hand.

One of the major challenges that remain is the effective protection by the government of critical information assets that are owned and operated by the private sector. Information exchange between governments and the private sector is a trust issue. Private companies will only share their sensitive information about critical assets and problems they have encountered with other stakeholders or the government if this information is treated confidentially. However, should the information exchange between government and private infrastructure operators be more informal and on an ad-hoc basis, or should it be institutionalized? And what kind of information should be exchanged between different stakeholders? What incentives would encourage the private sector to share sensitive information with governments?

Another challenge for governments is to find the right balance between protection and individual freedom. As there is no absolute security, the aim of a government's CIIP policy should be to make the whole society as robust as possible. It is not always easy to decide whether the most serious, or rather the most likely risks deserve priority in the allocation of financial and other resources. Citizens expect security from governments, but at the same time they are very reluctant to hand over their basic civil rights and freedom to governments for the sake of more security. What kind of residual risks societies are willing to accept remains a matter of debate.

A government's CIIP policy must include a comprehensive strategy as well as the necessary guidelines. An effective CIIP policy needs a holistic approach, taking into account technical, economic, organizational, law-enforcement,

and security-policy aspects of the problem. As there are usually many different agencies involved in CIIP, a clear leadership and allocation of roles within governments becomes essential. In the process, conflicting interests may arise on issues such as what should be protected, by whom, and when. However, especially in emergencies and crises, all stakeholders involved in CIIP need to know their duties and responsibilities. It is also important for the private sector to know whom to talk to and where the competencies lie in the public administration. This is especially vital because major accidents involving information and telecommunication technologies usually happen with very little or no early warning. Not only should public-private partnerships be boosted, but information exchange among public agencies at various levels also needs to be encouraged. An open dialog with academics and research institutes could be essential in finding the appropriate tools for protecting critical infrastructures and analyzing their (inter-) dependencies. In the end, the best way to achieve a satisfactory CIIP policy is probably to find the right balance between the various actors' desire for security and their own capacities to fulfill these requirements.

Part II
CIIP Threat Issues

Terrorist Capabilities for Cyber-attack

*By Clay Wilson**

Introduction

Violent extremists often rely on exploiting vulnerabilities of targets seen as soft and easy to access. A stronger policy for domestic physical security, together with the effectiveness of the US government's so-called "war on terror", has reduced some options for physical attack, and evidence shows that extremists may now be developing new computer skills or forming alliances with cyber-criminals that may give them access to high-level computer skills. In addition, continuing publicity about IT security vulnerabilities on the internet may encourage an interest in attempting a possible computer network attack, or cyber-attack, against the critical infrastructure of the US or other countries.

To date, the US Federal Bureau of Investigation (FBI) reports that cyber-attacks attributed to political extremists have largely been limited to unsophisticated efforts such as email bombing of ideological foes, or defacing of websites. However, their increasing technical competence is resulting in an emerging capability for network-based attacks. Currently, the FBI predicts that terrorists will either develop their own technical skills, or hire hackers for the purpose of complementing large conventional attacks with cyber-attacks.[1]

The IBM corporation has reported that during the first half of 2005, criminal-driven computer security attacks increased by 50 per cent, with government agencies and industries in the US targeted most frequently. Cyber-crime is now a major criminal activity, and in a recent report from the House Homeland Security Committee, officials claimed that members of the al-Qaida network had used online identity theft and credit card fraud to support their opera-

* Opinions expressed in this article are those of the author, not necessarily those of the Congressional Research Service.

1 Lourdeau, Keith. FBI Deputy Assistant Director, Testimony before the US Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security, 24 February 2004.

tions.[2] For example, the 2002 bombings in Bali were reportedly financed in part through online credit card fraud, according to the Indonesian police.

US Department of Defense (DoD) officials have further stated that the internet is now a prime recruiting tool for insurgents in Iraq. Arabic-language websites reportedly contain coded plans for attacks, and also give advice on how to build and operate weapons, and how to pass through border checkpoints.[3] In addition, recent news articles report that the younger generation of extremists, such as those behind the July 2005 bombings in London, are learning new technical skills to help them avoid detection by law enforcement computer technology.[4]

This report reviews publications and government reports to explore the following: (1) examples of vulnerabilities that may raise the level of interest of actors in attempting a coordinated cyber-attack; (2) effects of the so-called "war on terror" that are driving extremists to use the internet more; (3) ways in which criminals may be improving their IT skills.

What is Cyber-terrorism?

Traditional distinctions tend to be inadequate for describing computer network attacks (CNA) in ways that parallel the physical world. For example, if a nation-state were to secretly sponsor non-state actors who initiate CNA to spread fear or to create economic disruption, the distinction between cyber-crime and cyber-war would be blurred. Likewise, the interactions between terrorists and criminals who use computer technology may sometimes blur the distinction between cyber-crime and cyber-terrorism. So far, it remains difficult to determine the sources responsible for most of the annoying, yet increasingly sophisticated attacks that plague the internet.

2 According to FBI officials, al-Qaida terrorist cells in Spain used stolen credit card information to make numerous purchases. Also, the FBI has recorded more than 9.3 million US victims of identity theft in the past 12 months. Democratic Staff of the House Homeland Security Committee. Identity Theft and Terrorism, 1 July 2005, p. 10.

3 Curiel, Jonathan. "Iraq's tech-savvy insurgents are finding supporters and luring suicide-bomber recruits over the Internet". In: San Francisco Chronicle, 10 July 2005, p. A.01.

4 Evans, Michael and Daniel McGrory. "Terrorists Trained in Western Methods Will Leave Few Clues". In: London Times, 12 July 2005.

A terrorist may be defined as an ideological fighter who uses tactics or actions that target the civilian population to produce shock and fear. Some observers feel that the term "cyber-terrorism" is inappropriate, because a widespread cyber-attack may simply produce annoyances, not terror, as might be caused by a bomb, let alone by a chemical, nuclear, or biological (CNB) weapon. However, others feel that since the effects of a widespread computer network attack would be unpredictable, due to interdependencies of network systems, they might cause enough economic disruption, fear, and civilian deaths to qualify as terrorism. There are at least two approaches to defining the term "cyber-terrorism":

a) Effects-based: Computer attacks resulting in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism qualify as "cyber-terrorism", even if they are perpetrated by criminals.
b) Intent-based: Unlawful or politically motivated computer attacks undertaken to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage, constitute acts of "cyber-terrorism".[5]

Objectives for a Cyber-attack

Although current news reports about terrorism center around physical damage, if a widespread cyber-attack were launched against the US, the intention of terrorists might be to destabilize the economy.[6] Death and destruction might be secondary objectives of such an attack. Many security experts also agree that a cyber-attack would be most effective in connection with a conventional bombing, or a CNB attack. Some computer security observers say that a widespread, coordinated cyber-attack is technically very difficult to orchestrate and is unlikely to be effective for furthering terrorists' goals. These experts say

5 For a more in-depth discussion of cyber-terrorism, see Wilson, Clay. Computer Attack and Cyber-terrorism: Vulnerabilities and Policy Issues for Congress. CRS Report for Congress, RL32114 (17 October 2003).

6 Gordon, Sarah and Richard Ford. Cyber-terrorism? Symantec Security Response - White Paper (2003). [http://securityresponse.symantec.com/avcenter/reference/cyber-terrorism.pdf]. Ex-CIA chief Gates warns on cyber-terror, MSNBC.com, 6 December, 2004. http://www.msnbc.msn.com/id/6663555.

that the reason why these groups have undertaken no such attacks is because they cannot directly cause death and destruction.[7] However, other observers say that a large-scale cyber-attack, because of the unknowable interactions of complex computer systems, might affect the economy in ways that could be unpredictable. These observers also say that al-Qaida and associated groups are becoming more technically sophisticated, and that years of publicity about computer security weaknesses have made them aware that the US economy could be vulnerable to a coordinated cyber-attack.[8]

Publicity is also one of the primary objectives for a successful terrorist attack. Extensive coverage has been given to the vulnerability of the US information infrastructure and to the potential harm that could be caused by a cyber-attack. This may lead extremists to feel that a cyber-attack directed at the US may garner considerable publicity. Such groups may also feel that even a marginally successful cyber-attack could gain tremendous publicity.[9]

Internet Security Vulnerabilities

At the July 2005 Black Hat computer security conference in Las Vegas, a security expert demonstrated an exploit of what many consider to be a sig-

7 Evers, Joris. "Cisco Squashes 'Critical' Net Attack Bug." In: Cnet News.com, 2 November 2005. www.pcworld.com/news/article/0,aid,109819,00.asp. Joris Evers, reporting remarks by Bruce Schneier at CeBIT technology trade show in March 2003, "Cyber-terror Threat Overblown", Computerworld, 14 March 2003. http://www.computerworld.com/printthis/2003/0,4814,79368,00.html. Weimann, Gabriel. "Cyberterrorism - How Real Is the Threat?" (Washington, DC: United States Institute of Peace, Special Report 119, May 2004. Dan Ilett reports remarks of Richard Clarke at the Oxford Internet Institute in February 2005, "Clarke joins latest cyber-terror debate", ZDNet UK, 11 February 2005. [http://news.zdnet.co.uk/internet/security/0,39020375,39187582,00.htm].

8 Dan Verton is a former US Marine Corps Intelligence officer. Verton, Dan, Black Ice. The Invisible Threat of Cyber-Terrorism (Emeryville: McGraw-Hill/Osborne, 2003), p. 110. Keith Lourdeau, deputy assistant director of the FBI Cyber- Division, testimony before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security, 24 February 2004. Ryan Naraine, reporting remarks of Roger Cressey at Infosec World 2005, "Cyber-Terrorism Analyst Warns Against Complacency". In: eWEEK.com, 4 April 2005. http://www.eweek.com/article2/0,1895,1782286,00.asp.

9 Office of the Manager, National Communications System. The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Internet Communications (December 2000), p. 31. http://www.ncs.gov/library/reports/electronic_intrusion_threat2000_final2.pdf.

nificant internet security flaw by showing how Cisco Systems internet routers, the most commonly used internet routers, could be quickly hacked.[10] This router vulnerability could allow an attacker to disrupt selected portions of the internet, or even target specific elements of the infrastructure such as banks or power stations.[11] Security expert Bruce Schneier, who has recently criticized the idea of "cyber-terrorism", reportedly agreed that the Cisco router flaw was a "major" internet security vulnerability that could allow criminals to steal identity information or otherwise attack networks. Cisco Systems had released a software patch to fix the problem in April 2005, but over the following four months failed to notify its customers and government agencies, including the DHS, about the seriousness of the vulnerability.[12]

The US presents ample economic targets that are vulnerable to cyber-attack, possibly by extremist groups.[13] A February report by the President›s Information Technology Committee (PITAC) stated that the US information technology infrastructure, which is vital for communication, commerce, and the control of the physical infrastructure, is highly vulnerable to terrorist and criminal attacks. The report also found that the private sector has an important role in protecting national security by deploying sound security products and adopting good security practices.[14] However, a recent survey of 136,000 PCs used in 251 commercial businesses in North America found that a major security software patch known as SP2 had only been installed on nine per cent of the systems, despite the fact that Microsoft had advertised the importance of installing the security patch a year earlier. These businesses will continue to be vulnerable to major security threats until they deploy the software patch throughout their organizations.[15]

10 Storer, Amy. Update: "IPv6 risks may outweigh benefits". SearchSecurity.com, 29 July 2005. [http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1112459,00.html?track'NL-358&ad'525032USCA].

11 Garza, Victor. "Security researcher causes furor by releasing flaw in Cisco Systems IOS", SearchSecurity.com, 28 July 2005. [http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1111389,00.html].

12 Evers, Joris. "Cisco Squashes 'Critical' Net Attack Bug." In: Cnet News.com, 2 November 2005. [http://news.com.com/Cisco+squashes+critical+Net+attack+bug/2100-1002_3-5929498.html].

13 Verton, Black Ice, p. 110.

14 President's Information Technology Advisory Committee. Cyber- Security: A Crisis of Prioritization. Report to the President (Washington, February 2005), p. 25.

15 Foley, John. "Businesses Slow to Deploy Windows XP SP2". In: Information Week, 26 April 2005, p. 26.

Several other recent studies of global computer security issues found that most computer attacks were directed against critical infrastructures such as government offices, financial services, manufacturing plants, and power stations. These reports also show that the US is the most frequent target of computer attacks; during the first half of 2005, US computer systems were attacked 10 times more often than those of the second most targeted nation, China (see section titled "Trends in Cyber-crime", below).[16] US government agencies have come under criticism in past years for the inefficiency of their computer security programs.[17] And despite growing concerns about national security, a May 2005 report by the Government Accountability Office (GAO) stated that because of the growing sophistication of malicious code on the internet, the ability of civilian agencies to respond to cyber-threats could be diminished.[18]

Effects of the "War On Terror"

The DHS has reportedly suggested that increased security measures may force extremist groups to change tactics in attacking US targets.[19] The Search for International Terrorist Entities (SITE) Institute, a research group that monitors extremism on the internet, has reported that because of the effects of the "war on terror", Muslim extremists are gravitating toward the internet, and are succeeding in organizing online where they have been failing in the physical world.[20] Militant groups now use online services for covert messaging through

16 IBM News. "Report finds online attacks shift toward profit", 2 August 2005. http://www.ibm.com/news/us/en/2005/08/2005_08_02.html; Symantec press release. "Symantec Internet Security Threat Report Highlights Rise In Threats To Confidential Information", 21 March 2005. http://www.symantec.com/press/2005/n050321.html.

17 Based on 2002 data submitted by government agencies to the White House Office of Management and Budget, the GAO noted, in testimony before the House Committee on Government Reform (GAO-03-564T, 8 April 2003), that all 24 agencies continue to have "significant information security weaknesses that place a broad array of federal operations and assets at risk of fraud, misuse, and disruption.". Lee, Christopher."Agencies Fail Cyber- Test: Report Notes 'Significant Weaknesses' in Computer Security" 20 November 2002 http://www.washingtonpost.com/ac2/wp-dyn/A12321-2002Nov19?language'printer.

18 GAO report 05-231. "Information Security: Emerging Cyber-security Issues Threaten Federal Information Systems". May 2005.

19 Lipton, Eric. "Homeland Report Says that Threat From Terror-List Nations is Declining". In: The New York Times, 31 March 2005, Section A, p. 9.

20 Moutot, Michel, Radical Islamists use Internet to spread jihad, 2 June, 2005. [http://siteinstitute.org/bin/articles.cgi?ID=inthenews7005&Category=inthenews&Subcategory=0

steganography, anonymous email accounts, and encryption.[21] Many websites resemble online training camps in the sense that they offer instructions for how to create a safe-house, how to clean a rocket-propelled grenade launcher, or what to do if captured.[22] Some websites also include detailed cyber-attack instructions, including lists of email addresses for potential targets, such as Israeli police and government officials.[23]

Changing Concerns about Terrorist Cyber-attack, 2001–2005

Immediately after the 11 September 2001 attacks, public concerns were high about the threat of a possible follow-on cyber-attack from terrorist groups.[24] Subsequently, there has been increasing disagreement among security experts about (1) whether such an attack could possibly be launched by terrorists against the US civilian critical infrastructure, or (2) whether such an attack could seriously disrupt the US economy.[25]

Simulated cyber-attacks conducted by the US Naval War College in 2002 determined that attempts to cripple the US telecommunications infrastructure would be unsuccessful because system redundancy would prevent widespread

21 Suspected extremists are reportedly using encryption techniques to prevent police from accessing vital intelligence on seized computers, according to the British police. Tendler, Stewart. "Encrypted files frustrate police". Times Online, 20 July 2005 [http://technology.timesonline.co.uk/article/0,,20409-1701405,00.html]. See CryptoHeaven: http://www.cryptoheaven.com; and SecretMaker, http://www.secretmaker.com/emailsecurer/steganography/default.html.

22 Spring, Tom. "Al Qaeda's Tech Traps". PCWorld, 1 September 2004. http://www.pcworld.com/news/article/0,aid,117658,00.asp.

23 Stanley, Theodore. "The Online Jihad". The Statesman (New Delhi, 8 March 2005), p. 1.

24 In July 2002, Gartner and the US Naval War College hosted a three-day, seminar-style war game called "Digital Pearl Harbor" (DPH), with the result that 79 per cent of the gamers said that a strategic cyber-attack against the US was likely within the next two years. Gartner Research. "Digital Pearl Harbor: Defending Your Critical Infrastructure", 4 October 2002. http://www.gartner.com/pages/story.php.id.2727.s.8.jsp.

25 Former CIA director Robert Gates has warned that the threat of cyber-terrorism should be taken particularly seriously. Keith Lourdeu, deputy assistant director of the FBI Cyber- Division, stated that "our networked systems make inviting targets for terrorists due to the potential for large-scale impact on the nation". Schweitzer, Douglas. "Be Prepared for Cyber-terrorism". In: Computerworld, 6 April 2005. However, others believe that infrastructure systems are robust and could recover quickly. Forno, Richard. "Shredding the Paper Tiger of Cyber-terrorism". In: Security Focus, 25 September 2002. http://www.securityfocus.com/printable/columnists/111. See also: CRS Report 32114, op.cit.

damage. Many observers suggest that evidence from natural disasters shows that many critical infrastructure systems, including banking, power, water, and air traffic control, would likely recover rapidly from a possible cyber-attack.[26]

To date, there has been no published report of a coordinated cyber-attack launched against the critical infrastructure by a terrorist or terrorist group. Dennis McGrath of the Institute of Security Technology Studies at Dartmouth College has been quoted as saying that: "We hear less and less about a digital Pearl Harbor. Cyber-terrorism is not at the top of the list of discussions."[27]

However, in May 2005, the US Central Intelligence Agency (CIA) conducted a classified war game, dubbed "Silent Horizon", to practice defending against a simulated large scale cyber-attack. The national security simulation was significant because its premise — a devastating cyber-attack that affects government and parts of the economy with the same magnitude as the 11 September 2001 suicide hijackings — contravenes assurances by many US counter-terrorism experts that a cyber-attack is highly unlikely to achieve such far-reaching effects.[28] Some observers believe that tests of countermeasures for unlikely events, such as a coordinated or widespread cyber-attack, may sometimes be considered prudent.

Technical Skills of Terrorists

In April 2002, the CIA stated in a letter to the US Senate Select Committee on Intelligence that cyber-warfare attacks against the US critical infrastructure would become a viable option for terrorists as they become more familiar with the technology required for the attacks. Also according to the CIA, various groups, including al-Qaida and Hizbollah, are becoming more adept at using the internet and computer technologies, and these groups have the intentions and desire to continue to develop the skills necessary for a cyber-attack.[29]

26 Lubow, Eric. "Homeland Security CIO: No Digital Pearl Harbor Likely". Linux Security.com, 7 May, 2003. http://www.linuxsecurity.com/content/view/113925/151. Jackson, William. "War College Calls Digital Pearl Harbor Doable". In: Government Computer News, 23 August 2002. http://www.gcn.com/vol1_no1/daily-updates/19792-1.html.

27 Associated Press. "CIA Overseeing 3 Day Wargame on Internet", 25 May 2005.

28 Bridis, Ted. "Silent Horizon war games wrap up for the CIA". In: USA Today, 26 May 2005. http://www.usatoday.com/tech/news/techpolicy/2005-05-26-cia-wargames_x.htm.

29 From a letter addressed to the US Senate Select Committee on Intelligence, April 2002. Dan Verton, Black Ice, op. cit., p. 87 and p. 110.

Through captured literature, it has become known that many al-Qaida members have been well educated and are familiar with engineering and other technical areas.[30] During the US invasion in November 2001, al-Qaida fighters fled from Kabul, Afghanistan, leaving behind many documents and sensitive information that, upon close examination, reportedly showed that some al-Qaida operatives were well-educated and trained in the use of computer systems. "Technical treatises in Arabic, English, German as well a students' notebooks in Arabic, Turkish, Kurdish, and Russian reflected a consistent interest in and widespread familiarity with electrical and chemical engineering, atomic physics, ballistics, computers, and radios", according to researchers and journalists who examined the documents.[31]

Abu Musab Zarqawi has formed an al-Qaida "information wing" to distribute video clips of terrorist operations using specially designed web pages, with options for viewers to choose Windows Media or Real Player. The videos supplement a regular online al-Qaida news service giving details about recent exploits, and are also included in a monthly internet magazine that offers religious justifications for jihad and military advice on how to conduct it. Zarqawi has been described as one of a "new generation" of terrorists, and is believed to be surrounded by followers in their twenties who are comfortable and familiar with internet technology.[32]

Imam Samudra, convicted of taking part in the 2002 bombings of two Bali nightclubs and now awaiting execution, has written a book titled "Aku Mekawan Terroris!", which translates to "I Oppose Terrorism!". In this widely published book, Samudra advocates that Muslim youth actively develop hacking skills "to attack US computer networks". Samudra names several websites and chat rooms as sources for increasing hacking skills. He also urges Muslim youth to obtain credit card numbers and use them to fund the struggle against the US and its allies.[33] The terrorist attacks in Bali, and recent attacks in several

30 Spring, Tom. "Al Qaeda's Tech Traps". PCWorld, 1 September 2004. http://www.pcworld.com/news/article/0,aid,117658,00.asp.

31 Davis, Anthony. "The Afghan files: Al-Qaeda documents from Kabul". In: Jane's Intelligence Review, 1 February 2002.

32 Glasser, Susan and Steve Coll. "The Web as Weapon". In: The Washington Post, 9 August 2005, p. A.1.

33 Sipress, Alan. An Indonesian's Prison Memoir Takes Holy War into Cyber-space (14 December, 2004). http://www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html.

other countries, are thought to have been funded through financial crimes such as credit card fraud.[34]

In February 2005, FBI director Robert Mueller testified before the Senate Select Committee on Intelligence that terrorists were showing a growing understanding of the critical role of information technology in the US economy and had expanded their recruitment to include students of mathematics, computer science, and engineering.[35]

Possible Insider Threat from Terrorists

Terrorists working as employees could possibly gain authorized access to sensitive computers and data for critical infrastructure systems. A recent study of security incidents, conducted by the US Secret Service and the Carnegie Mellon Software Engineering Institute, found that attacks on computer systems committed by insiders with authorized access had reportedly cost industry millions of US dollars in fraud and lost data.[36] Insider employees with access to sensitive information systems could also use the opportunity to secretly insert hidden vulnerabilities or otherwise sabotage software that is being developed either locally, or under offshore contracting arrangements. As an example, twenty employees of subcontractors working at the Sikorsky Aircraft Corporation were arrested in the US in January 2003 for possession of false identification in order to obtain security access to facilities containing restricted and sensitive military technology. All of the defendants pleaded guilty and have been sentenced, except for one individual who was convicted at trial on April 19, 2004.[37] Also, documents seized from a terrorist group in India, in March 2005, revealed plans to carry out disruptive attacks against software companies in Bangalore, according to police officials in Delhi.[38]

34 Richard Clarke, former counter-terrorism czar for US presidents George W. Bush and Bill Clinton, stated that US citizens were vulnerable to people who would use their identities against them. Rademacher, Kevin. "Clarke: ID theft prevention tied to anti-terrorism efforts". In: Las Vegas Sun, 13 April 2005. http://www.lasvegassun.com/sunbin/stories/text/2005/apr/13/518595803.html.

35 Testimony before the Senate Select Committee on Intelligence, 16 February 2005.

36 Randazzo, Marisa et al. Insider Threat Study: Illicit Cyber- Activity in the Banking and Finance Sector, Carnegie Mellon Software Engineering Institute, August 2004.

37 US Attorney's Office, District of Connecticut. http://www.usdoj.gov/usao/ct/attf.html.

38 Ribeiro, John. "Terrorists target India's outsourcing industry". In: InfoWorld, 7 March 2005. http://www.infoworld.com/article/05/03/07/HNterroristsindia_1.html.

Trends in Cyber-crime

According to an August 2005 computer security report by IBM, more than 237 million overall security attacks were reported globally during the first half of this year. Government agencies were targeted the most, reporting more than 54 million attacks, while manufacturing ranked second with 36 million attacks, financial services ranked third with approximately 34 million, and healthcare received more than 17 million attacks. The overwhelming targets of these attacks, all of which occurred in the first half of 2005, were government agencies and industries in the US (12 million), followed by New Zealand (1.2 million) and China (1 million).[39] Most security analysts agree that the number of security incidents reported are only a small fraction of the total number of attacks that actually occur.

Usually, a cyber-attack is difficult to detect until after it is well under way, and may involve hundreds or thousands of compromised computers that are directed by a cyber-criminal to attack as a swarm from all parts the globe. If the attack is against a still-undisclosed, or newly discovered security vulnerability, the targeted computer systems are usually at a big disadvantage. Most current computer security safeguards operate mainly to prevent the types of attacks that are already known to administrators. A new, unique type of attack against computers may encounter inadequate, untested, or non-existent defenses.

A 2004 survey by Counterpane Internet Security, covering 450 networks in 35 countries, shows that hacking has now become a profitable criminal pursuit. Hackers now sell unknown computer vulnerabilities (commonly called "zero-day exploits") on the black market to criminals who use them for fraud. Hackers with networks of compromised computers rent them to other criminals who use them to launch coordinated attacks against targeted individuals or businesses, including banks or other institutions that manage financial information.[40]

39 The Global Business Security Index reports worldwide trends in computer security from incidents that are collected and analyzed by IBM and other security organizations. IBM press release. IBM Report: Government, Financial Services and Manufacturing Sectors Top Targets of Security Attacks in First Half of 2005, 2 August 2005. http://www-1.ibm.com/press/PressServletForm.wss?MenuChoice'pressreleases&TemplateName'ShowPressReleaseTemplate&SelectString't1.docunid'7815&TableName'DataheadApplicationClass&SESSIONKEY'any&WindowTitle'Press+Release&STATUS'publish.

40 Schneier, Bruce. Attack Trends: 2004 and 2005. 6 June 2005. http://www.schneier.com/blog/archives/2005/06/attack_trends_2.html.

In Autumn 2004, organized cyber-criminals appear to have infiltrated the computer systems of the London offices of the Japanese Sumitomo bank in an attempt to steal £220 million. The cyber-criminals reportedly planned to transfer the money to other bank accounts around the world. Officials at the London police fraud squad reportedly stated that the Sumitomo case had been the only incident so far in which an attack by external cyber-criminals against a major bank nearly succeeded.[41] Figures from the National Hi-Tech Crime Unit in England also show that, in 2003, at least 83 per cent of British companies were targeted by hackers in attempts to seize control of their systems.

Identity theft involving thousands of victims is now easily enabled by advances in computer technology and by poor computer security practices.[42] For example, MasterCard International recently reported that a computer hacker had accessed more than 40 million credit card numbers belonging to US consumers that might now be used for fraud.[43] Some of these account numbers are reportedly now being sold on a Russian web site, and some customers have seen fraudulent charges appear on their statements. Officials at the UFJ bank in Japan reportedly stated that some of that bank's customers may also have become victims of fraud related the same theft of MasterCard information.[44]

Information about stolen credit cards and bank accounts is now traded online in a highly structured arrangement, involving buyers, seller, intermediar-

41 Walsh, Conal. "Terrorism on the cheap - and with no paper trail". The Guardian, 17 July 2005. http://www.guardian.co.uk/alqaida/story/0,12469,1530132,00.html.

42 LexisNexis reported on 12 April 2005 that personal information, such as the Social Security numbers of 310,000 US citizens, may have been stolen in a data security breach that involved 59 instances of unauthorized access to its corporate databases using stolen passwords. ChoicePoint Inc. has reported that since July 2003, personal information for as many as 145,000 citizens may have been viewed by unauthorized individuals. Boston College reported in March 2005 that a hacker had gained unauthorized access to computer database records with personal information for up to 106,000 alumni, and in the same month, Chico State University of California reported that its databases containing the names and Social Security numbers for as many as 59,000 current and former students had been breached. Bank, David and Christopher Conkey. "New Safeguards for Your Privacy". In: The Wall Street Journal, 24 March 2005, p. D1.

43 Krim, Jonathan and Michael Barbaro. "40 Million Credit Card Numbers Hacked". In: Washington Post, 18 June 2005, p. A01. See also the report by the US House of Representative Homeland Security Committee, 1 July 2005, raising concerns about potential ties between identity theft victims and terrorism. Harrington, Caitlin. "Terrorists Can Exploit Identity Theft, Report From House Democrats Says". In: CQ Homeland Security, 1 July 2005.

44 BBC News. "Japan cardholders 'hit' by theft", 21 June 2005 [http://news.bbc.co.uk/1/hi/business/4114252.stm].

45 CCRC staff. "Russia, Biggest Ever Credit Card Scam". Computer Crime Research Center, 8 July 2005. http://www.crime-research.org/news/08.07.2005/1349.

ies, and service industries. These services include offering to change a billing address of a theft victim, through manipulation of stolen PINs or passwords. Estimates by some observers show that, in a highly profitable black market, each stolen MasterCard number can be sold for between US$42 and US$72.[45]

Links Between Terrorism and Cyber-crime

Linkages between criminal and terror groups may allow terror networks to expand and undertake large attacks internationally by leveraging criminal sources, money, and transit routes. For example, ransom money gained from prior kidnappings by terrorists is believed by some to have been used to help fund the 11 September 2001 terrorist attacks. Also, London police officials believe that the perpetrators of the July 2005 public transport bombings obtained high-quality explosives on the Eastern European black market.[46]

According to a recent conference on terrorism and organized crime, a study found that many militant groups become progressively more involved in conventional crime, particularly in the lucrative drug trade.[47] Officials of the US Drug Enforcement Agency (DEA) reported in 2003 that 14 of the 36 groups found on the US State Department's list of foreign terrorist organizations were involved in drug trafficking. DEA officials reportedly argued that the "war on drugs" and the "war on terrorism" were and should be linked.[48]

A 2002 report by the US Library Congress Federal Research Division revealed a "growing involvement of Islamic terrorist and extremists groups in drug trafficking", and limited evidence of cooperation between different terrorist

46 Walsh, Conal. "Terrorism on the cheap — and with no paper trail". The Guardian, 17 July 2005. http://www.guardian.co.uk/alqaida/story/0,12469,1530132,00.html. Lal, Rollie. "Terrorists and organized crime join forces". In: International Herald Tribune, May 25, 2005. http://www.iht.com/articles/2005/05/23/opinion/edlal.php. Porter, Barbara. Forum Links Organized Crime and Terrorism. By George! Summer 2004. http://www2.gwu.edu/~bygeorge/060804/crimeterrorism.html.

47 Préfontaine, Daniel C. and Yvon Dandurand. "Terrorism and Organized Crime: Reflections on an Illusive Link and its Implication for Criminal Law Reform". International Society for Criminal Law Reform, Annual Meeting Montreal, August 8–12, Workshop D-3 Security Measures and Links to Organized Crime (11 August, 2004). http://www.icclr.law.ubc.ca/Publications/Reports/International%20Society%20Paper%20of%20Terrorism.pdf.

48 Ibid.

groups involving both drug trafficking and trafficking in arms.[49] At a Senate hearing in March 2002, US State Department officials also indicated that some political violence movements may be using drug trafficking as a way to gain financing while simultaneously weakening their enemies through exploiting their desire for addictive drugs.[50] Western Europe and North America are regions that have major narcotics markets, optimal infrastructure, and open commercial nodes that increasingly serve the transnational trafficking needs of both criminal and terrorist groups.[51]

Drug traffickers are among the most widespread users of encryption, and often have the financial clout to hire high-level computer specialists capable of using steganography and other means to make Internet messages hard or impossible to decipher. Access to such cyber-crime specialists allows terrorist organizations to transcend borders and operate internationally without detection. Many highly trained technical specialists are available for hire in the countries of the former Soviet Union and in the Indian subcontinent. Some specialists will not work for criminal or terrorist organizations willingly, while others may be misled, or unaware of their employers' political objectives. Still others will agree to provide assistance because well-paid legitimate employment is scarce in their region.[52]

Another significant form of convergence between organized crime and terrorism using information technology is the international movement of money. To facilitate this, members of different terrorist groups are given special training in computer software, and engineers are hired to facilitate communications. International organized criminals and terrorists also require the skills and cooperation of in-house specialists and experienced advisors to continue evading the scrutiny of bank regulators and international investigators. These

49 LaVerle, Berry, Glenn E Curtis, Rex A. Hudson, and Nina A. Kollars. A Global Overview of Narcotics — Funded Terrorist and Other Extremist Groups. Federal Research Division, Library of Congress (Washington, DC, May 2002). http://www.loc.gov/rr/frd/pdf-files/NarcsFunded-Terrs_Extrems.pdf.

50 Beers, Rand and Francis X. Taylor, US State Department. "Narco-Terror: The Worldwide Connection Between Drugs and Terror", testimony before the US Senate Judiciary Committee, Subcommittee on Technology, Terrorism, and Government Information, 13 March 2002.

51 Curtis, Glenn and Tara Karacan. "The Nexus Among Terrorists, Narcotics Traffickers, Weapons Proliferators, and Organized Crime Networks in Western Europe". Federal Research Division, Library of Congress (Washington, DC, December 2002), p. 22. http://www.loc.gov/rr/frd/pdf-files/WestEurope_NEXUS.pdf.

52 Shelly, Louise. Organized Crime, Cyber-crime and Terrorism (Computer Crime Research Center, 27 September 2004). http://www.crime-research.org/articles/Terrorism_Cyber-crime.

include financial advisors, accountants, bankers in offshore zones, and even bankers in major financial centers who may or may not know about the political motives of their clients.[53]

Other Sponsors of Terrorists

The prospect of a nation-state supporting cyber-terrorism activity is worrisome. However, in March 2005, a DHS report indicated that of the six nations currently listed by the State Department as terrorist sponsors, five — North Korea, Sudan, Syria, Libya, and Cuba — are now described as a diminishing concern. Only Iran remains listed as a nation-state that might possibly be motivated in the future to assist terrorist groups in attacking the US homeland. The DHS report also predicts that other potential sponsors of terrorist attacks against the US homeland might include groups such as Jamaat ul-Fuqura, a Pakistani-based organization linked to Muslims of the Americas (MOA); Jamaat al-Tabligh, a Muslim missionary organization; and the Dar Al Islam Movement in the US.[54]

Iraq is also suspected to have direct ties to several terrorist groups, such as Mujahideen-e-Khalq in Iran and the Palestinian Abu Nidal organization.[55]

Efforts to Prevent Cyber-crime

Security product vendors have learned that in order to combat cyber-crime more effectively, it must be treated as a global problem. Many of these security vendors have created their own independent advance-warning systems through linking proprietary security equipment into global networks that share information collected by their distributed customer base. One example is the

53 Shelley, Louise and John T. Picarelli. "Methods Not Motives: Implications of the Convergence of International Organized Crime and Terrorism". Police Practice and Research, Vol. 3, No. 4, (2002), p. 311. http://www.american.edu/tracc/resources/publications/shelle70.pdf.

54 The DHS report, dated January 2005, is entitled "Integrated Planning Guidance, Fiscal Years 2005-2011 Rood, Justin. "Animal Rights Groups and Ecology Militants Make DHS Terror List, Right-Wing Vigilantes Omitted". In: CQ Homeland Security, 25 March 2005. Lipton, Eric. "Homeland Report Says that Threat From Terror-List Nations is Declining". In: The New York Times, 31 March 2005, section A, p. 9.

55 Mueller, Robert, Director of FBI. Testimony before the US Senate Select Committee on Intelligence, February 11, 2003.

early-warning DeepSight Threat Management System, announced in 2003 by the Symantec security company, which is composed of a global network of 19,000 firewall and intrusion-detection devices maintained by thousands of volunteer data partners. The DeepSight threat management system correlates global data to detect the start of a possible swarming internet attack originating simultaneously in different parts of the world, and notifies administrators to help them defend their systems when targeted.[56] However, research by several computer experts has recently concluded that future malicious computer code may soon be able to detect and avoid the global network sensors, and defeat even these newer safeguards.[57]

Cyber-crime is a major international challenge; however, attitudes about what constitutes a criminal act in the IT field still vary from country to country. The EU has set up the Critical Information Infrastructure Research Coordination Office (CI2RCO), which examines how its member states are protecting their critical infrastructures from possible cyber-attack. The project will identify research groups and programs focused on IT security in critical infrastructures.

The Convention on Cyber-crime was adopted in 2002 by the Council of Europe, a consultative assembly of 43 countries based in Strasbourg. The convention, effective from July 2004, is the first and only international treaty to deal with breaches of law "over the internet or other information networks". The Convention on Cyber-crime was adopted by the Council of Europe in November 2001, and requires participating countries to update and harmonize their criminal laws against hacking, infringements on copyrights, computer facilitated fraud, child pornography, and other illicit cyber- activities.[58] To date, eight of the 42 countries that signed the convention have completed the ratification process. A coalition of US industry associations, including the Business Software Alliance, the Cyber- Security Industry Alliance, the American Bankers Association, the Information Technology Association of

56 Roberts, Paul. Symantec Offers Early Warning of Net Threats. PCWorld, 12 February 2003. http://www.pcworld.com/news/article/0,aid,109322,00.asp.

57 Recent reports at the 2005 Usenix Security Symposium show that future worms could probe for the location of global sensors, and then bypass them when launching an attack. Broache, Anne. Worms could dodge net traps, News.com, 4 August 2005. [http://news.com.com/Worms+could+dodge+Net+traps/2100-7349_3-5819293.html].

58 The full text of the Convention on Cyber- Crime may be found at: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm; and at http://www.usdoj.gov/criminal/cyber-crime/coe-hatespeechProtocol.pdf.

America, InfraGard, Verisign, and several others, have urged the US Senate Foreign Relations Committee to ratify the convention.[59]

Although the US has signed the convention, it did not sign a complimentary protocol that contained restrictions to criminalize xenophobia and racism on the internet, which would likely not be supported by the US constitution.[60] The complimentary protocol would require nations to imprison anyone guilty of "insulting publicly, through a computer system" certain groups of people based on characteristics such as race or ethnic origin, a requirement that could make it a crime to email jokes about Polish people or to question whether the Holocaust occurred. The US Department of Justice has said that it would be unconstitutional for the US to sign that addition because of the First Amendment›s guarantee of freedom of expression. Also, the Electronic Privacy Information Center, in a June 2004 letter to the Foreign Relations Committee, objected to US ratification of the convention, because it would "would create invasive investigative techniques while failing to provide meaningful privacy and civil liberties safeguards."[61]

Conclusion

Computer security experts continue to disagree about whether a cyber-attack by terrorists is a near-term or long-term possibility. However, the so-called "war on terror" has driven terrorists to use the internet more, and thus become more skillful with computer systems, and the tools for cyber-attack are becoming faster and more sophisticated. Terrorists are developing links with cyber-criminals that may give them access to engineers with high-level computer skills. The time may be approaching when a cyber-attack may offer advantages that cause terrorists to act, even if the probability of success or level of effectiveness is unknown.

59 Wait, Patience. "Industry Groups urge Senate ratification of cyber-crime treaty". In: Government Computer News, 6 June 2005 [http://appserv.gcn.com/vol1_no1/web/36257-1.html]. McCullagh, Declan. "Tech Firms call for approval of cyber-crime treaty". Cnet.com News, 29 June 2005. [http://news.com.com/2102-7348_3-5768462.html?tag'st.util.print].

60 The US Senate Committee on Foreign Relations held a hearing on the convention on 17 June 2004. Archick, Kristin. Cyber-crime: The Council of Europe Convention. CRS Report for Congress, RS21208 (Washington, DC, 26. April 2002). Durnout, Estelle. "Council of Europe ratifies cyber-crime treaty". ZDNet, 22 March 2004. http://news.zdnet.co.uk/business/legal/0,39020651,39149470,00.htm.

61 http://www.epic.org/privacy/intl/senateletter-061704.pdf.

Future unknown computer vulnerabilities, inadequate deployment of security fixes, and incomplete planning by governments to prevent network attack may allow terrorists to someday launch a cyber-attack that could overwhelm the ability of civilian agencies to respond effectively. Despite efforts to improve computer security, the US government does not have an internet recovery plan or an official assessment of threats to national cyber-security. DHS officials have stated that a draft cyber-security threat evaluation plan will be available in fall 2005, but a finalized cyber-security plan that pinpoints the nation's weakest security links will likely not be available until 2006.[62] Leaders of the US Senate Financial Management, Government Information and International Security Subcommittee also noted that the DHS does not have a robust way to detect a coordinated attack against the critical infrastructure, partly because the DHS has yet to complete the necessary formal resource sharing agreements with other government agencies.[63]

To protect against future threats from cyber-attack, the US government should explore whether the "war on terror" should be linked more closely to international efforts to prevent cyber-crime, and perhaps also to the "war on drugs". The government should also encourage vendors of computer products and services to quickly notify the DHS about any newly discovered, major security vulnerabilities that potentially might threaten the Internet infrastructure, or homeland security. Finally, effective ways should be explored to harmonize laws around the globe and gain more international cooperation for detecting and preventing cyber-crime.

62 Dizard, Wilson. "Cyber-security plans wait for DHS to complete its evaluation of threats". In: Government Computer News, Vol. 24, No. 20 (25 July 2005).

63 Gross, Grant. "Senators Call on DHS to Improve Cyber-security Efforts". In: IDG News Service, 19 July 2005. [http://enterprisesecurity.symantec.com/publicsector/article.cfm?articleid'5862&EID'0].

The Enemy Within: System Complexity and Organizational Surprises

By Michel J.G. van Eeten, Emery Roe, Paul Schulman, Mark de Bruijne

Introduction

The range of threats faced by critical infrastructures has expanded dramatically since 11 September 2001. But external threats are not the only concern. In many ways, the infrastructures themselves are their own worst enemy. For example: field data at a major Dutch telecom operator shows that the company's own maintenance activities were the second-largest cause of service disruptions, right after equipment failure.[1] The reason? Complexity. As Demchak has said, the chief manifestation of complexity is surprise.[2] The fact that planned maintenance, even after careful assessment and approval procedures, manages to cause disruptions qualifies as a prime example of surprise arising out of complexity. From the perspective of maintaining reliable services, it is not that important whether the events that triggered the surprise originated from within or from outside of the infrastructure – should we even consider that to be a clear distinction. Whatever the origin, it is the surprising behavior of the complex system itself that the organization has to respond to.

The term "complexity" is invoked so often that occasionally, it seems to have lost all meaning. For practitioners, the term conveys why they need resources to do their job; for academics and consultants, it explains why their expertise is needed. A plethora of technological and organizational responses has been developed to reduce the complexity of the system being managed. Procedures, rules, training, modeling, design, decision support — the list of such measures can easily be extended by simply looking at engineering curricula.

While technology can be used to manage much of this complexity, the systems are so complex that they can never be made inherently safe and stable. Surprises will occur, and organizational strategies are required if the system is to function reliably. Weick and Sutcliffe call this approach "managing the

1 Verbist, S. Reliability in Mobile Telecommunications under Rapidly Changing Conditions (confidential report) (Delft: Delft University of Technology, 2002).

2 Demchak, C.C. Military organizations, complex machines: Modernization in the U.S. armed services (Ithaca, N.Y.: Cornell University Press, 1991), p. 3.

unexpected".[3] Engineers hate the unexpected. For those who design and analyze the technological systems of their organizations, the unexpected defies their understanding – or even their professionalism, as some of them seem to think. Operators fear the unexpected. Their work under real-time conditions has brought them to experience the unexpected as a normal part of their lives, but also as an element that demonstrates the limits of their understanding of the system, as well as to their ability to control it reliably. In other words, the unexpected reminds them of their vulnerability.

Managing the unexpected is hard enough even for organizations that have command and control over the core infrastructure elements through which they provide their services. Just keeping up with the increasing complexity of these systems is a major challenge. More and more, however, services are provided through interdependent networks of organizations rather than by individual organizations. In fact, the critical information infrastructure is the poster child of this development and the opportunities it presents to us. We find different organizations in virtually every layer of the technology – from the physical connections to the transportation layer and all the way up to the application layer.

How do organizations manage to cope with working under these networked conditions? Here, we can draw on the extensive fieldwork of our Delft-Oakland research team. Over the past years, we have collected data in organizations operating large-scale water systems, electricity grids, and telecommunication networks. All of them depend on critical information infrastructure as part of their overall technological infrastructure – and all of them depend on their ability to reliably manage the surprises that the technology throws their way. This paper reports on some of our findings regarding networked reliability. First, we provide an overview of the literature on organizational reliability. Next, we discuss how these organizations have adapted to the networked conditions in which they increasingly find themselves. Finally, we shall offer a number of concluding thoughts regarding the protection of critical information infrastructure.

3 Weick, K. E. and K.M. Sutcliffe. Managing The Unexpected (San Francisco: Jossey Bass, 2001).

Technology, Risk, and Reliability

Organizational theorists are developing a lively and increasing interest in organizational reliability – the ability of organizations to manage hazardous technical systems safely and without serious error.[4] A number of reasons account for the stepped-up interest.

First, society increasingly depends upon "high-performance", but also highly hazardous technologies ranging from nuclear weapons and nuclear power to large jet aircraft, medical technologies, complex electrical grids, and telecommunication systems. Many of these technical systems impose relatively tight error tolerances upon operators and maintenance personnel, and the consequences of errors can be disastrous, with ramifications that go far beyond the user, extending to by-standers and society at large.[5] Second, concern for reliability among organization theorists has grown because of major high-profile accidents that have become international bywords for preventable disasters, such as Exxon Valdez, Three Mile Island, Bhopal, Challenger, and the Tenerife air disaster. Many of the accidents illustrate all too vividly that technical design alone cannot guarantee safe and reliable performance.[6] That is to say, these technologies are so complex and tightly coupled that their behavior is full of surprises. Finally, in the aftermath of 11 September 2001, there is a heightened

4 LaPorte, T. and P. Consolini. Working In Practice But Not In Theory: Theoretical Challenges of High Reliability organizations. Public Administration Research and Theory, Vol. 1 (1991), pp. 19–47.; LaPorte, T. "High Reliability Organizations: Unlikely, Demanding and At Risk". In: Journal of Contingencies and Crisis Management, Vol. 4 (1996), pp. 60–71; Meier, A. von. "Occupational cultures as a challenge to technological innovation". In: IEEE Transactions on Engineering Management, Vol. 46, No. 1 (1999), pp. 104–114; Schulman, P.R. "The Negotiated Order of Organizational Reliability." In: Administration and Society, Vol. 25 (1993), pp. 353– 372; Perrow C. Normal Accidents (Princeton: Princeton University Press, 1984/1999); Roberts, K. New Challenges To Understanding Organizations (New York: Macmillan, 1993); Sagan, S. The Limits of Safety (Princeton: Princeton University Press, 1993); Sanne, J. M. Creating Safety in Air Traffic Control (Lund: Arkiv Forlag, 2000); Weick, K. E., K.M. Sutcliffe, and D. Obstfeld. "Organizing For High Reliability". In: Research in Organizational Behavior, Vol. 21 (1999), pp. 81–123; Weick and Sutcliffe, Managing The Unexpected, op. cit.; Beamish, T.D. Silent Spill (Cambridge, Mass.: M.I.T. Press, 2002); Evan, W.M. and M. Manion. Minding the Machines: Preventing Technological Disasters (Saddle River, NJ: Prentice Hall, 2002)

5 Perrow, Normal Accidents, op. cit.

6 Weick, K. E. "The Vulnerable System: An Analysis of the Tenerife Air Disaster". In: K. Roberts (ed.), New Challenges To Understanding Organizations (New York: Macmillan, 1993), pp. 173–97; Vaughn, D. The Challenger Launch Decision (Chicago: University of Chicago Press, 1996).

interest in "critical infrastructures" and their reliability in the face of potential terrorist attack.[7]

Despite the recent upsurge in interest, the analytic roots of reliability research in organization theory are deeply set. Some of the earliest investigation in this field appears in quality control (QC) analysis[8] and, later, in human factors analysis.[9] As a general rule, QC has sought to achieve reliability by controlling worker behavior to match task requirements, while the human-factors approach has been directed toward securing reliability by molding strategic organizational and task variables to human requirements.

As important as QC and human factors approaches to organizational reliability have been for analysts and organizations, they addressed reliability concerns in a substantially different way from those that have subsequently come to the fore. Research during the 1980s and the debate it engendered did not directly revolve around production reliability per se. Some organizations have become increasingly concerned about errors, accidents, and failures undermining safety. They are seen by many to jeopardize the survival of the organization itself and its members, as well as that of significant numbers of people outside the organization.

The conventional approach to organizational reliability treats it as a marginal or fungible property whose costs can be traded off against other organizational values. Conventionally, "marginal reliability" has been considered to be an embedded variable — a probability coefficient attached to production estimations.[10] The new reliability analysis is quite different, as it deals with error and failures that have far-reaching and often unacceptable implications for safety – not just inside, but outside of the organization as well. This is not reliability as a probabilistic property that can be traded off at the margin against other organizational values, but reliability directed toward a set of catastrophic events whose occurrence must, as nearly as possible, be completely

7 National Research Council. "Making The Nation Safer: The Role of Science and Technology in Countering Terrorism" (Washington, D.C. National Academy Press, 2002).

8 E.g., Juran, J. M. "The Quality Trilogy: A Universal Approach to Managing for Quality". In: Quality Progress, Vol. 19, No. 8 (August 1986), pp. 19–24.

9 Salvendy, G. Handbook of Human Factors and Ergonomics (New York: Wiley, 1997); Perrow, C. "The Organizational Context of Human Factors Engineering". In: Administrative Science Quarterly, Vol. 28 (1983), pp. 521–41; Norman, D. The Design of Everyday Things (New York: Basic Books, 2002);

10 Schulman, P.R. "Medical Errors: How Reliable Is Reliability Theory?". In: M.M. Rosenthal and K. M. Sutcliffe (eds.), Medical Error (San Francisco: Jossey Bass, 2002), pp. 200–216.

precluded. In this respect, the new organizational reliability analysis is about the high reliability achieved through precluding events — the high standards of performance that can be achieved against a set of unacceptable events. These differences between the marginal and precluded-event reliability are summarized in Table 1 below.

Variable	Marginal Reliability	Precluded Event Reliability
Context	Efficiency	Social dread
Risk	Localized	Widely distributed
Calculation	Marginal (variable cost)	Non-fungible (fixed requirement)
Standards	Average or run of cases	Every last case
Learning	Trial & error learning	Formal learning with limited trial & error
Orientation	Retrospectively measured	Prospectively focused
Control	Probabilistic	Deterministic

Table 1: Marginal and Precluded-Event ("High") Reliability

High-Reliability Theory

The beginnings of the new perspective on organizational reliability can be traced to works by James Reason[11] (1972) and Barry Turner[12] (1978) that connected human and organizational factors as systematic producers of major technical failures. A key anchor point for the new approach, however, is Charles Perrow's *Normal Accidents*.[13] In this work, Perrow added a new dimension to his earlier groundbreaking work on technology and organizations.[14] Categorizing technologies along the dimensions of complexity and tight coupling, Perrow identified a specific class of technologies — complex and tightly coupled — that are particularly problematic from the standpoint of organizational reliability. They pose the risk of "normal accidents", irrespective of the strategies that organizations adopt to manage them. These technologies are in effect accidents waiting to happen — they are capable of changing their conditions or states with a

11 Reason, J. Human Error (Cambridge: Cambridge University Press, 1972).
12 Turner, B. M. Man-Made Disasters (London: Wykeham, 1978).
13 Perrow, Normal Accidents, op. cit.
14 Perrow, C. Complex Organizations: A Critical Essay (New York: Wadsworth, 1979).

speed and a degree of interactivity that defies the understanding in real-time of operators or the anticipation of designers and planners. Further, the changing conditions carry the risk of catastrophic consequences for users, managers, and innocent third parties alike. Perrow's framework, in fact, set a limiting condition for the organizational reliability of large technical systems. Perrow's analytic perspective has been echoed in a number of subsequent studies.[15]

Perrow's argument has been questioned by a group of researchers who have identified in case studies what they assert to be a set of "high-reliability organizations" (HROs). These organizations (a nuclear aircraft carrier, a nuclear power plant, and air traffic control centers) have established comparatively excellent performance records in managing technologies of high complexity and tight coupling.[16] They were found to be surviving in highly unforgiving political and regulatory niches with respect to reliability. They are able to do so, it was argued, because of organizational, managerial, and cultural factors that buffer the organizations from the hazards of tightly-coupled and complex technologies and, in effect, mitigate the risk of managing these systems. Among the factors observed by the HRO researchers are those summarized below:

- Organizationally specified core events that must not occur.
- Established error priorities and trade-offs in support of precluding events.
- Identified set of precursor events or conditions that can funnel through specified chains of causation into precluded events.
- Established set of procedures that specify behavior to guard against both precluded and precursor events.
- Maintained widespread sensitivity and attentiveness toward unanticipated, unspecified events or conditions that might also have a causal connectionto precursor and precluded events.
- Pursued incompatible strategies simultaneously (e.g., buffering against paradoxes).

15 Sagan, op. cit.; Evan and Manion, op. cit.

16 LaPorte, T. and P. Consolini. "Working In Practice But Not In Theory: Theoretical Challenges of High Reliability organizations". In: Public Administration Research and Theory, pp. 19–47; Rochlin, G.I. and A. von Meier. "Nuclear Power Operations; A Cross Cultural Perspective". In: Annual Review of Energy and Environment, Vol. 19 (1994), pp. 153–187; Roberts, New Challenges To Understanding Organizations, op. cit; Schulman. The Negotiated Order of Organizational Reliability, op. cit., pp. 353–372.

- Established formal structure of roles, responsibilities, and reporting relationships that can also be transformed under conditions of emergency or stress.
- Team approach to problem-solving.
- Recognition that key features of strategy and structure are unstable and subject to decay: cycles of reinforcement.
- External supports, constraints, and regulations that allow for all of the above.

These organizations begin with a clear specification of core events that simply must not be allowed happen.[17] To this they add the specification through careful causal analysis of a set of precursor events or conditions that could lead to core events. These precluded and precursor events constitute the "envelope" of reliability within which these organizations seek to operate. They develop elaborate procedures to constrain behavior and task performance within the envelope. At the same time, the organizations feature, through a "culture of reliability", a widespread sensitivity and attentiveness toward previously unspecified conditions that might causally connect specified events. If careful formal specification underlies the identification of core and precursor events, here the organization avoids specific boundary criteria for what constitutes a reliability or "safety" issue.[18]

Additionally, high-reliability organizations are characterized by the simultaneous pursuit of contradictory or paradoxical properties of reliability management.[19] Error protection regimes that guard against one type of error (say an error of omission) are likely to make another type of error (errors of commission) more likely. HROs must clearly specify operational procedures and standards while preserving ambiguity so they do not become insensitive or inattentive to the unexpected. They must pursue simultaneous strategies of anticipation and resilience.[20] Another contradiction that must be managed is one that can arise between formal design principles and actual operational experience. HROs are able to buffer these paradoxes, having to reconcile both

17 LaPorte. High Reliability Organizations, op. cit., pp. 60–71.

18 Schulman. The Negotiated Order of Organizational Reliability, op. cit., pp. 353–372.

19 Rochlin, G.I. "Defining High Reliability Organizations in Practice". In: K. Roberts (ed.), New Challenges To Understanding Organizations (New York: Macmillan, 1993), pp. 11–32.

20 For an elaboration of this paradox, see: Wildavsky, A. Searching For Safety (New Brunswick, NJ: Transaction Books, 1998).

sides of the paradox if high reliability in averting catastrophic failure and securing widespread safety is to be achieved.

Another feature discovered in research on HROs is the ability to transform formal roles as well as reporting and authority relationships under emergency conditions or stress. Typically, this means bypassing formal hierarchy and the development of lateral, less formal modes of communication and coordination.[21] Much of the work of the organizations is generally carried out in teams, and there is a great emphasis throughout the organization on the cultivation of high levels of technical competence through personnel selection and training.

HROs also recognize that key organizational properties such as attention, close coordination, and mutual trust across units that have to rely on one another are not constants and cannot be treated as known factors. They are subject to decay and must be continually renewed to the high levels required in these organizations. Routines will numb mindfulness;[22] shared understanding will erode. As noted in earlier research, it is not invariance, but rather the attention to and careful management of fluctuations that helps define the HRO.[23]

Finally, and perhaps most importantly, HROs exist in environments that share an intense aversion to the events they are trying to preclude. This means that HROs are carefully watched and regulated, and that the wider task environment prevents them from succumbing to internal drift or changing their goals away from high reliability. At the same time, the environment supports the organization in treating reliability as non-fungible, that is, it generally insulates the organization from pressures to trade off reliability against other variables under close market competition. For example, ratepayers absorb the security and reliability costs of nuclear power plants, and all airlines are required to practice similar maintenance procedures under close regulation of the aviation authorities. This regulation and support allows HROs to incorporate redundancy in technical designs and to invest a great deal in anticipatory and contingency analysis.

21 Roberts, K. "Some Characteristics of One Type of High Reliability Organization". In: Organization Science, Vol. 1 (1990), pp. 160–176.

22 Langer, E. Mindfulness (New York: Addison-Wesley, 1989).

23 Schulman. The Negotiated Order of Organizational Reliability, op. cit., pp. 353–372.

High Reliability and Normal Accidents

Whether the above features constitute a sufficient or even necessary set of conditions for preventing "normal accidents", i.e., precluding unacceptable events, is at present an unanswerable question. While the dispute between the normal accident theory and HRO research has continued[24], in its most extreme form the dispute centers on an assertion that cannot be disproved. No amount of good performance can disprove Perrow's viewpoint concerning normal accidents, because it can always be said that the reliability of an organization can only be measured by the first catastrophic failure that still lies ahead, not by the many successful operations that lie in the past. Along these lines, Perrow has insisted there have not been more serious nuclear accidents because "we have not given large plants […] time to express themselves"[25] — that is, given enough time, the complexity of these plants will produce instances of erratic behavior that will prove to be disastrous.

Further, one variable that Perrow regards as independent in his causal analysis — loose and tight coupling — is fraught with ambiguity in terms of its identification and understanding. Loose coupling means that the system can achieve the desired outcomes through multiple paths, so a failure in one place need not disrupt the system. Tight coupling means there is no such slack, and failures can quickly spread through the system, causing other failures.

In Perrow's formal analysis of "tight coupling", he refers to the physical properties of technologies. But at later stages in his analysis, he applies the concept to social organizations themselves. One may disagree as to whether organizations are directly analogous to physical systems, and whether the phenomenon of tight coupling is equivalent in both contexts.[26]

In addition, it is sometimes difficult to distinguish between tight coupling as a cause or as a consequence of failure or accident. In July of 1993, a massive

24 Perrow, C. review of Sagan, S. D. "Limits of Safety". In: Journal of Contingencies and Crisis Management, Vol. 2 (1994), pp. 212–220; LaPorte, T. "A Strawman Speaks Up: Comments on Limits of Safety". In: Journal of Contingencies and Crisis Management, Vol. 2 (1994), pp. 207–11; Rijpma, J.A. "Complexity, Tight Coupling and Reliability". In: Journal of Contingencies and Crisis Management, Vol. 5 (1997), pp. 15–23; Weick, Sutcliffe, and Obstfeld. Organizing For High Reliability, op. cit., pp. 81–123.

25 Perrow, Normal Accidents, op. cit., p. 12.

26 This very point has in fact been the subject of historical debate in organization theory, leading to the shift away from the "machine metaphor" underlying scientific management theory. Cf. Morgan, G. Images of Organization (New York: Sage Publications, 1997).

flooding occurred across the Midwestern states of the US. During the flood, water flows overwhelmed dams and reached levels so high that suddenly a set of spillways, across several states, which had been considered independent state flood protection devices became tightly-coupled relative to the impact of any one water diversion upon the others.[27] The failure of physically separate dams and spillways to contain unprecedented water levels was really the independent variable that turned a loosely-coupled set of elements into a tightly-coupled system. At best, we could ascribe tight coupling as a latent feature of the Midwestern spillways, a feature that follows from a specific magnitude of failure.

On the other hand, the HRO research perspective has had its own conceptual and empirical difficulties. The research has centered on a small number of selective case studies during a specific time period for each organization. This small number of cases does not constitute proof that the features discovered in these organizations are truly necessary ones.[28] Further, HRO research has in some respects asserted high reliability as a defining characteristic, rather than a performance variable, of its organizations. This leaves unanswered the question of which traits, if any, can contribute to higher reliability (along a continuum) in organizations, and to what extent. Fortunately, more recent research is beginning to broaden the analytic focus on reliability from structure to process in organizations, especially the cognitive and sense-making skills and strategies of their members.[29]

The Challenge of Networked Reliability

In the entire debate between normal accident and HRO approaches to reliability research, one issue has been consistently ignored. Many technical systems for which we wish to attain the highest reliability in operation and management, specifically our "critical infrastructures", are not under the control of single

27 Hey, D.L. and N.S. Philippi. "Reinventing Flood Control Strategy." Wetlands Initiative (1994).

28 Schulman, P.R. The Analysis of High Reliability Organizations: a Comparative Framework". In: K. Roberts (ed.). New Challenges To Understanding Organizations (New York: Macmillan, 1993), pp. 33–54.

29 Weick, Sutcliffe, and Obstfeld. Organizing For High Reliability. Research in Organizational Behavior, op. cit., pp. 81–123; Sanne, Creating Safety in Air Traffic Control, op. cit.; Schulman, P.R., E. Roe, M.J.G. van Eeten, and M. de Bruijne. "High Reliability and the Management of Critical Infrastructures". In: Journal of Contingencies and Crisis Management, Vol. 12, No. 1 (2004), pp. 14–28.

organizations. In the areas of electricity transmission and distribution, water resource management, transportation, telecommunication, medicine, and financial services, many critical services we depend on for reliable, error-free performance are derived from networks of organizations. In fact, reliability increasingly is and has to be a property of the network, not a consequence of the structure or behavior of a single organization.

The remainder of this chapter will focus on the formation of networks and their increasing centrality to the understanding of high reliability. We frame our discussion around a single research question: How do networks of organizations and units, many with competing, if not conflicting, goals and interests, provide highly reliable services in the absence of ongoing command and control and in the presence of rapidly changing task environments and technologies?

The short answer to this question is: by relying increasingly on real-time operations. We provide a more detailed answer by looking at one of our field studies: the California electricity system during the energy crisis in 2001 (for more details on this case study, see Roe et al. (2002)[30] and Schulman et al. (2004)[31]).

The Case of the California Electricity Crisis

In 1996, the US state of California adopted a major restructuring in its system of electricity generation, transmission, and distribution. The state moved from a set of large integrated utilities that owned and operated the generation facilities, the transmission lines, and the distribution and billing systems, and set retail prices under a cost-based regulatory system, to a market-based system consisting of independent generators who sell their power on wholesale markets to distributors, who then sell it to retail customers. The key utilities were forced to sell off most of their generating capacity (except for nuclear and hydropower sources) and to place their transmission lines under the control of a new organization, the California Independent System Operator (ISO), which assumed

30 Roe E., M.J.G. van Eeten, P.R. Schulman & M. de Bruijn. Real-Time Reliability: Provision of Electricity Under Adverse Performance Conditions Arising from California's Electricity Restructuring and Crisis. A report prepared for the California Energy Commission, Lawrence Berkeley National Laboratory, and the Electrical Power Research Institute (San Francisco: California Energy Commission, 2002).

responsibility for managing a new state-wide high voltage electrical grid. This grid had been primarily formed by the merger of two separate grids formerly owned and managed by the two utilities Pacific Gas and Electric (PG&E) in the north and Southern California Edison (SCE) in the south.

The restructuring legislation created a new set of institutions and relationships, many without precedent in the experience or culture of electric power provision. We present specific findings on the reliability of electricity provision under performance conditions arising out of California's electricity restructuring. These findings relate most directly to the different organizations charged with the actual provision of reliable electricity under the restructured conditions, namely, the ISO, private generators, and distribution utilities, each with competing if not conflicting goals arising out of the deregulation-based restructuring.

The focus on the control rooms of the ISO, PG&E, and an unnamed private generator allows us to directly address the issue of tight coupling and complex interactivity. There was not one operator in the ISO control room who was not tightly linked to the outside through multiple communications and feedback systems. Everyone constantly used the telephone; pagers were going off all over the place; computers were connected to internal and external servers running everything from market bidding software to congestion scheduling; the AGC (Automatic Generation Control) system connects the ISO generation dispatcher directly to privately-held generators; the ADS (Automatic Dispatch System) connects the dispatcher directly to the bidder of electricity; dynamic scheduling systems in the ISO controls selected out-of-state generators; governors on generators automatically bring frequency back into line; the frequency and ACE (Area Control Error) measurements reflect real-time electricity usage across the grid; all kinds of telemetry measurements come back to the control room in real time; web pages used by the ISO, PG&E, and private generators carried real-time prices and information; an operator in the ISO control room uses software to make the time error correction for the entire grid; and on and on.

The answer to our research question — "How did the California high reliability network maintain reliable electricity, during what proved to be unprecedented turbulent times?" — is: The focal organization, the ISO, balances load and generation in real time (that is, in the current hour or for the hour ahead) by developing and maintaining a repertoire of responses and options in

the face of unpredictable or uncontrollable system instability produced within the network (e.g., by generators acting in a strategic fashion) or from outside through the network's open system features (e.g., temperatures and climate change). "Load" is the demand for electricity and "generation" is the electricity to meet that load, both of which must be balanced (i.e., made equal to each other), since service delivery will otherwise be interrupted due to physical failure or collapse of the grid.

Our research led us to focus on the match between, on one hand, the options and strategies within the HRO to achieve its reliability requirement (namely, balancing load and generation, staying within limits set for key transmission paths, and meeting the other parameter constraints) and, on the other hand, the unpredictable or uncontrollable threats to fulfilling the reliability requirement. A match results from having at least one option sufficient to meet the requirement under given conditions. At any point, there is the possibility of a mismatch between the system variables that must be managed to achieve the reliability requirement and the options and strategies available for managing those variables.

Meeting the reliability requirement involves managing the options and strategies that coordinate the actions of the independent generators, energy traders, and the distribution utilities in the wider network.The options that the ISO control room, as the focal organization, deploys are network-based, e.g., outage coordination is the responsibility of the ISO, but involves the other partners in the network. In other words, the ISO control management can be categorized in terms of the variety of network-based options available to the ISO (high or low) and of the instability of the California electricity system (high or low), as in Figure 1.

		System Volatility	
		High	Low
Network Option Variety	High	Just-in-time performance	Just-in-case performance
	Low	Just-for-now performance	Just-this-way performance

Figure 1: Performance conditions for California Independent System Operator (CAISO)

"Instability" is the extent to which the focal control room in the ISO faces rapid, uncontrollable changes or unpredictable conditions that threaten the grid and service reliability of electricity supply, i.e., conditions that jeopardize the task of balancing load and generation. Some days are characterized by low instability, fondly called in the past "normal days". A clear example of high instability are the days for which a large part of the forecasted loads had not been scheduled through the day-ahead market, which means that for the ISO, actual flows are unpredictable, and congestion will have to be dealt with at the last minute. Additionally, any loss of transmission or generating capacity can introduce instability into the system.

"Option variety" is the amount of HRO resources, including strategies, available to the ISO control room to respond to events in the system in order to keep power load and power generation balanced at any given point in time. It includes available operating reserves, other generation capacity, available transmission capacity, and the degree of congestion. High option variety means, for instance, that a range of resources is available to the ISO, allowing it to operate well within the required regulatory conditions. Low options variety means the resources are below requirements and, ultimately, that very few resources are left and the ISO must operate close to, or even in violation of, some regulatory margins.

These two dimensions together set the conditions under which the ISO control room has to pursue its high-reliability management. As we observed, they demand four different performance modes for achieving reliability (i.e., balancing load and generation) that we term: "just-in-case", "just-in-time", "just-for-now", and "just-this-way". "Low" and "high" are imprecise terms, though they are the terms used and commonly recognized by many of our ISO interviewees. In practice, the variables of system instability and options variety should be better thought of as continua without rigid high/low cut-off points (i.e., they can be thought of in terms of the frequency and duration for which careful adjustments stay within or exceed the bandwidths). Let us turn now to a brief description of each performance mode, each of which represents a dramatically different way of balancing load and generation.

Just-in-case performance, redundancy, and maximum equifinality.
When options are high and instability is low, just-in-case performance is dominant in the form of high redundancy. Large reserves are available to the ISO

control room operators, there is excess plant capacity (the bête noire of many deregulation economists) at the generator level, and the distribution lines are working with ample backups. All operations run much as forecasted, with little or no unpredictability and/or uncontrollability. More formally, redundancy is a state where the number of different but effective options to balance load and generation is high relative to the market and technology requirements for balancing load and generation. There are, in brief, a number of different options and strategies to achieve the same balance. The state of high redundancy is best summed up as one of maximum equifinality, i.e., a multitude of means to meet the reliability requirement.

Just-in-time performance, real-time flexibility, and adaptive equifinality. When options and instability are both high, just-in-time performance is dominant. Option variety to maintain load and generation remains high, but so does the instability of system variables, in terms of both market factors (e.g., rapid price fluctuations leading to unexpected strategic behavior by market parties) and technological variables (e.g., sagging transmission lines during unexpectedly hot weather).

How does just-in-time performance work? Operators told us about days that started with major portions of the loads still not scheduled and with the predictability of operations significantly diminished. Reliability becomes heavily dependent on the ISO control room's ability to pull resources and the balance together up to the last minute. Because of the time pressure this brings with it, operators cannot rely completely on their highly specialized and formalized tasks and procedures, but initiate a great deal of lateral communication to quickly and constantly relay and adapt all kinds of information in order to "maintain the bubble" with respect to the variables that need to be managed given the performance conditions they face. They not only have to respond quickly to unpredictable and uncontrollable events, but have to make sure that their responses are based on understanding the variables so as to ensure that these responses do not exacerbate the balance problem (especially as confusion over what is actually happening can be intense at these times) or the risk of cascading variables. It is no longer possible to separate important and unimportant information beforehand. Support staff are pulled into real-time operations to extend the capability to process information quickly and integrate it into a

"bubble" of understanding the many more variables and complex interactions that are possible in just-in-time performance.

This performance condition demands "real-time" flexibility, that is, the ability to utilize and develop different options and strategies quickly in order to balance load and generation. Since operators in the control room are in constant communication with each other and with others in the network, options are reviewed and updated continually, and informal communications are much more frequent. Flexibility in real-time is the state where the operators are so focused on meeting the reliability requirement, and on the options for doing so, that more often than not, they customize the match between them, i.e., the options are just enough and just in time. The fact that instability is high focuses the operators' attention on exactly what needs to be addressed and clarifies the search for adequate options and strategies. What needs to get done gets done with what is at hand, as it is needed.

More formally, the state of real-time flexibility is best summed up as adaptive equifinality: There are alternative options, many of which are developed or assembled as required to meet the reliability requirement. The increased instability in system behavior is matched by flexibility on the part of the focal organization in using inter-organizational options and strategies for keeping performance within reliability tolerances and bandwidths. Substitutability of options and strategies is high for "just-in-time" performance, an immensely important point to which this paper returns. As one ISO control room shift manager put it, "In this [control room] situation, there are more variables and more chances to come up with solutions." "It's so dynamic," said one of the ISO's market resource coordinators, "and there are so many possibilities […] Things are always changing."

Just-for-now performance and maximum potential for deviance amplification. When option variety is low but instability is high, just-for-now performance is dominant. Options to maintain power loads and generation have become visibly fewer and increasingly insufficient to meet requirements in order to balance load and generation. This state can result from various factors. Unexpected outages can occur, and loads may increase to the physical limits of transmission capacity; furthermore, the use of some options can preclude or exhaust other options, e.g., using stored hydro capacity now rather than later. Just-for-now performance is a state best summed up as one of maximum potential for

"deviance amplification": Even a small deviation in elements of the market, technology or other factors in the system can ramify widely throughout the system. Marginal changes can have maximum impact in threatening the reliability requirement, i.e., the loss of a low-megawatt generator can tip over the system into blackouts. From the standpoint of reliability, this state is untenable over time. Here, operators are under no illusion that they are in control; they understand how vulnerable the grid is, how limited the options are, and how precarious the balance; they keep communications lines open to monitor the state of the network, and they are busily engaged in developing options and strategies to move out of this state. They do not panic, and indeed, they still retain the crucial option of reconfiguring the electricity system itself by declaring a "Stage 3" power emergency – which means controlled blackouts.

"Just-for-now" performance is also very fast-paced and best summed up as "firefighting". When options become few and room for maneuverability is tight (e.g., when loads continue to rise while new power generation becomes much less assured and predictable), control operators become even more focused on the big threats to balancing load and generation. As options become depleted, support staff members in the control room have less and less to add. There is less need for lateral, informal relations. Operators even walk away from their consoles and join the others in looking up at the big board on the side wall. "I'm all tapped out," said the generation dispatcher on the day we were there when the ISO had just avoided issuing a Stage 3 declaration. At this state, operators and support staff wait for new, vital information, because they are out of options for controlling the ACE themselves.

Just-this-way performance, crisis management, and zero equifinality. In this last performance mode for balancing power loads and electricity generation, system instability is lowered to match low options variety, and just-this-way performance is dominant. This performance state occurs in the California electricity system as a short-term "emergency" solution. Here, the main option is to tamp down instability directly by means of crisis controls and forced network reconfigurations. The ultimate instrument of crisis management strategy is the Stage 3 declaration, which requires the interruption of firm load in order to bring back the balance of load and generation from the brink of just-for-now performance. The effect of a Stage 3 declaration is to reconfigure the grid into a more tightly coupled system under command-and-control management.

More formally, just-this-way performance is a state best summed up as one of zero equifinality: Whatever flexibility could be squeezed from the remaining options and strategies is forgone on behalf of maximum control of a single system variable — in this case, load. Once the decision to shed load has been taken, information is centered on compliance. The vertical relations and hierarchy of the control room extend into the network, even to the distribution utilities in their rotating outage blackouts.

In sum, one of the important features of the reliability management of the ISO within the network is the large proportion of that management that occurs in real-time, that is, under conditions of high system instability. Estimates given by ISO participants of time spent in just-in-time and just-for-now performance modes (what we term as "real-time reliability" performance) ranged from 75 to 85 per cent in April 2002 and 50 to 60 per cent in April 2003. This is a departure from the large preponderance of anticipatory, just-in-case management found in much of the earlier HRO research. Indeed, the California system cannot be reliable with respect to grid or service reliability without the options of performing "just-in-time" or "just-for-now", or the ability of control room operators to maneuver across different performance modes as circumstances require. Such real-time reliability is better thought of as a process across organizations, not the property of those organizations or their technology.

The Push to Real-Time Operations

Our findings at CAISO are not unique to this organization. In large-scale water and telecommunications utilities, we have seen developments that are very similar to those in the electricity sector.[32] In response to increased turbulence, organizations are relying more and more on real-time operations to maintain service reliability.

Not that they are pleased with this development. During our extensive interviews and observations at a major Dutch mobile telecommunications

31 Schulman, Roe, van Eeten & de Bruijne. High Reliability and the Management of Critical Infrastructures, op. cit., pp. 14–28.

32 Eeten, M.J.G. van, & E. Roe. Ecology, Engineering and Management: Reconciling Ecosystem Rehabilitation and Service Reliability (Oxford University Press, New York, 2002); Schulman, Roe, van Eeten & de Bruijne. High Reliability and the Management of Critical Infrastructures, op. cit, pp. 263–280.

company, operators and managers told us they felt very uncomfortable regarding their increasing reliance on real-time operations. According to the engineering training that most of them received, real-time operations are only meant to iron out minor shortcomings in service delivery — the small fluctuations that remain after careful planning, design, development, and maintenance. For these professionals, ending up in real-time operations ultimately equals a failure of planning, design, development, and maintenance — or to repeat the more concise phrasing some of them used: of management. Many of them also cited fierce cost-cutting and the rapid market-driven introduction of new services as main causes of being forced to work outside the formal procedures that they were trained to use.

Nevertheless, these organizations have adapted — as evidenced by their performance measures.[33] Performance was not upset even as their customer base skyrocketed, as the number of services they provided grew rapidly, and as the complexity of their system peaked due to layered and overlapping IT and TI infrastructures. During a 400 per cent increase in the number of customers, the number of major incidents had only risen by about 50 per cent. Performance in the area of business continuity, such as Call Completion Rate and Call Success Rate, improved slightly.

There have been other changes, however. Most notably, there has been a steady increase in the number of major incidents whose origin is categorized as "unknown". "Unknown" means that immediately after resolving the incident, its cause remained unclear. In other words, the number of potentially disruptive surprises has risen, but has not caused a higher number of actual disruptions.

How did they adapt? Similar to the case of the California ISO, the mobile telecom operator has learned to cope with just-in-time and just-for-now performance conditions. In practice, this causes a number of shifts within the organizations. First, and perhaps foremost, we expect that organizations concerned with reliability will partially shift organizational resources from long-term planning to real-time management. This shift could be captured in the saying "the prospect of hanging concentrates the mind wondrously." As stated above, the day-to-day operational management of these systems was meant to deal with the few remaining surprises and disturbances. While the idea of preventing surprises through careful planning, design, and construction

33 Verbist, op. cit.

of the technological system certainly remains important, the focus is moving to real-time operations. Increased system complexity and turbulence in their task environment reduces the ability of these organizations to plan and develop robust systems that are intrinsically reliable — not least because critical parts of those systems may now be outsourced.

In practical terms, this implies larger network operating centers with a more diverse set of professionals. During visits to the facilities of several major Dutch mobile telecom providers, we noticed that these control centers have grown rapidly and have strengthened their oversight capabilities within the internal organizational networks.

Related to this development, we witnessed other shifts. When planning gives way to real-time management, we should also expect a shift in emphasis from design to improvisation. Surprises are by definition not covered by the existing procedures and design, and therefore require improvisation by operators if reliability is not to suffer. Organizations face more incidents that defy the logic of the conventional telecommunication paradigm of element, network, and service management. Complex interactions among these levels put a high premium on operators being able to "keep the bubble" — instantly piecing together fragmented and sometimes seemingly contradictory information regarding the behavior of the system. This shift also brings to light the rather different, and at times conflicting, roles of engineers and operators.[34]. The push toward real-time operations implies and requires that discretionary power be shifted from the former to the latter group of professionals.

In more general terms, we could view this entire development as a shift from anticipation to resilience.[35] Anticipation as a risk management strategy relies heavily on the ability to foresee future disturbances. If increased system complexity makes it more difficult to foresee all risks and to deal with them through careful planning and design, then systems will need to be more resilient: that is, their ability to bounce back from disturbances becomes more important, since their ability to prevent disturbances is undermined. This also implies a shift of attention from analysis to operational experience. The more experienced operators are, the larger their repertoire to correctly diagnose surprises when they occur.

34 Von Meier, op. cit., pp. 104 –114.
35 Wildavsky, op. cit.

For those working in critical information infrastructures, a lot of this will sound familiar. The similarities as well as the interconnections that they have with other critical infrastructures expose them to the same dose of the unexpected. During the millennium transition, information infrastructure specialists of the California ISO sat in the control room watching the screens as the clock counted the last seconds of the year 1999. They had worked hard to patch all their systems in time, but they were experienced enough to expect the unexpected. And true enough, a threat did realize and not of the kind they had anticipated. None of the important systems failed, but just around midnight they became bogged down in massive hacking attacks. As it turned out, many hackers were hoping to exploit a window of vulnerability — and the hope itself almost created the window.

One of the implications of the increasing complexity of critical infrastructures, and of the surprises it generates, is the need for operational discretion. In important ways, the governance of these systems is distributed and decentralized — meaning that centralizing and homogenizing government policies to protect critical information infrastructures, however well-intentioned, may well turn out to be harmful rather than helpful.[36] How helpful the current policies to protect critical infrastructures — and the public-private initiatives that accompany them — will be remains an open question. Undoubtedly, these initiatives will receive their own fair share of surprises.

36 For a more elaborate discussion on governance of the security and reliability of information networks, see M. van Eeten, H. de Bruijn, M. Kars, H. van der Voort, J. van Till, "The Governance of E-Security: A Framework for Policy", Report to the Directorate General of Telecommunications and Post (Delft/Den Haag/Amsterdam: TU Delft & Stratix, 2004).

The Aspect of Early Warning in Critical Information Infrastructure Protection (CIIP)

By Thomas Holderegger

Introduction

At the latest since the beginning of the Cold War, timely warning of attacks has become an indispensable component of ensuring the sovereignty and security of nation-states. In response to the threats of nuclear intercontinental missiles and other military dangers, nation-states – led by the US – developed reliable and credible early-warning systems for imminent attacks, capable of discovering military threats worldwide and in real time and, if necessary, initiating countermeasures. Such ingenious detection mechanisms fulfilled multiple tasks: They not only permitted quick reaction to an attack and therefore optimal protection of the population and of strategically important infrastructures, but they also reduced the probability of such an attack. Potential attackers were aware that they would be quickly discovered and, in this way, were simultaneously deterred from implementing their intentions.[1]

After the Cold War, early warning temporarily declined in importance, but – in view of the progress of the "digital revolution", the transition to an information society, the triumphant advance of the internet, and the introduction of information and communication technology (ICT) into business, administration, and research — early warning re-emerged in the 1990s in the context of "Critical Infrastructure Protection" (CIP), which includes "Critical Information Infrastructure Protection" (CIIP). In addition to physical ICT infrastructures (such as computers, networks, satellites), CIIP also protects intangible assets such as information and the availability, integrity, confidentiality, and authenticity of data.[2]

1 Keyes, David. "Cyber- Early Warning: Implications for Business Productivity and Economic Security". In Security in the Information Age: New Challenges, New Strategies, (Washington, DC: Joint Economic Committee, United States Congress, 2002), pp. 42ff. http://www.fas.org/irp/congress/2002_rpt/jec-sec.pdf; Dunn, Myriam. "Sicherheit im Informationszeitalter: Critical Information Infrastructure Protection (CIIP) als gemeinsame Herausforderung für Politik und Wirtschaft". In: digma: Zeitschrift für Datenrecht und Informationssicherheit, Vol. 4, No. 2 (2004), p. 66.

2 For a definition of CIP and CIIP and an overview of the history and theory of CIIP, see: Dunn, Myriam and Isabelle Wigert. International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries (Zurich: Center for Security Studies, 2004), pp. 17–26.

In contrast to the adversary states during the Cold War, which were relatively easy to identify and observe, today's antagonists are often much more difficult to make out. ICT also enables smaller organizations or even individuals to threaten critical infrastructures.[3] This situation is aggravated by the fact that all sectors of the economy and the state, but also private individuals, are increasingly dependent on ICT and that, at the same time, these sectors are becoming increasingly interdependent. If the information infrastructure of a single sector malfunctions, this may lead to major consequences that are difficult to predict in advance for one or more of the other sectors.[4] Moreover, the motivations of today's attackers are not as clear as those anticipated during the Cold War, making an accurate assessment of the threat more difficult: Possible motivations include curiosity, challenge, adventure, malice, criminal intent (especially enrichment), blackmail, revenge, industrial or classical espionage, political motives, terrorism, or interference with military capabilities.[5] Accordingly, nation-states today are confronted with the difficult task of protecting multiple, interlinked sectors that are dependent on a generally vulnerable and extremely complex technology (ICT) from an unclear threat and, at the same time, shielding them from breakdowns, accidents, natural disasters, and sabotage. In light of the underdeveloped security of ICT and the complexity of dependencies and threats outlined above, it is unrealistic to expect that incidents can be prevented altogether.

As a realistic goal within the framework of CIIP, nation-states therefore strive to ensure that a breakdown of important infrastructure, or even only of certain components of ICT, will be limited to an incident that is short, rare, controllable, geographically isolated, or as inconsequential as possible for the national economy and security.[6] In the view of more and more states, the key to

3 Federal Strategy Unit for Information Technology (FSUIT). Verletzliche Informationsgesellschaft: Herausforderung Informationssicherung (Bern 2002), p. 17. http://www.isb.admin.ch/internet/sicherheit/00791/index.html?lang=de. See also: Westrin, Peter. "Critical Information Infrastructure Protection (CIIP)". In: Information & Security, Vol. 7 (2001); Moteff, John D. Critical Infrastructures: Background, Policy, and Implementation (Washington, DC: CRS Report for Congress, Congressional Research Service, The Library of Congress, 2002), p. 1.

4 Within the framework of CIP, the critical infrastructures that require protection are divided into sectors. For a compilation of the sectors by country, see: Dunn and Wigert, International CIIP Handbook 2004, op. cit., pp. 344ff. and the comments in chapter 2.1.6.

5 Keyes, Cyber- Early Warning, op.cit., p. 44.

6 On the goals of CIIP, see: Wigert, Isabelle. "Der Schutz kritischer Informationsinfrastrukturen in der Schweiz: Eine Analyse von Akteuren und Herausforderungen", p. 97. In: Wenger, Andreas (ed.), Bulletin 2005 zur schweizerischen Sicherheitspolitik (Zürich: Forschungsstelle für Sicher-

attaining this goal is a capacity for early warning – and this capacity can only be implemented through a comprehensive, far-reaching exchange of information among numerous players with varying approaches to the problem.[7]

Since most sectors are controlled by private enterprise and ICT infrastructures are generally operated by the private sector, which — unlike the state — is not interested in strategic measures for safeguarding national security, there are differing approaches and perspectives: the technical (ICT) perspective, the business perspective, the perspective of prosecutorial and legislative organs, and the security-policy/analytic-strategic perspective.[8]

This paper discusses the question of early warning in general and therefore ignores other aspects of CIIP, such as prevention, crisis management, and technical troubleshooting. The goal of this article is to identify the individual players, to assign to each of them to a different perspective, and to name tasks and responsibilities. A particular focus will be on the state as a player: What resources are available to the state to reconcile the differing priorities, perspectives, and responsibilities? Since ICT is not restricted to the territory of individual nation-states, since many private enterprises act internationally, and since potential attackers can operate from abroad, international early warning will be discussed next: How can the many national players be brought together and integrated in an international dialog? Finally, following a brief summary, the paper will offer a conclusion and prospects.

Early Warning

As already mentioned in the introduction, early warning is seen as the key to achieving efficient CIIP. To achieve an early-warning capacity, however, far-reaching information exchange is necessary encompassing the most important

heitspolitik, 2005), pp. 97–121. http://www.css.ethz.ch/publications/bulletin; Juster, Kenneth I. and John S. Tritak. "Critical Infrastructure Assurance: A Conceptual Overview". In: Security in the Information Age: New Challenges, New Strategies, (Washington, DC: Joint Economic Committee, United States Congress, 2002), p. 12.

7 See, e.g. the conclusion in Dunn and Wigert, International CIIP Handbook 2004 op. cit., pp. 342ff. and Keyes, Cyber- Early Warning, op. cit. pp. 46 and 50.

8 See contribution of Isabelle Abele-Wigert in this volume for more details on the different perspectives. Cf. also Wigert, op. cit., Der Schutz kritischer Informationsinfrastrukturen in der Schweiz. Due to its modest significance for early warning, the business perspective will be omitted for the purposes of this paper.

players in the field of information assurance. Each of these players adopts a specific perspective in relation to the problem of information assurance. The following three approaches summarize the most important perspectives on early warning, even if in practice they cannot be delineated so clearly:

- The IT-technical perspective, where CIIP is fundamentally understood as IT security.
- The perspective of prosecutors, where CIIP is understood as the protection of society from cyber-crime.
- The security-policy perspective, which perceives CIIP as a policy for combating exceptional incidents and views society as threatened in its entirety: Like the representatives of the technical perspective, the representatives of the security-policy perspective combat ICT incidents every day.[9]

This chapter on early warning will present the players in more detail: The first part will introduce non-state actors, and explain their tasks. The second part will discuss the state as a player, first pointing out its activities and then considering its possibilities for creating an early-warning capacity. The third part will reflect upon how the early-warning capacity created in this way can be internationalized: First, we will examine what form of international information exchange already largely exists; then we will explain how this information exchange could be optimized and simplified by integrating the various perspectives within a single player.

9 See the contribution of Isabelle Abele-Wigert in this volume for more details on the different perspectives. Dunn and Wigert, op. cit., p. 22, enumerate a fourth perspective: the business perspective. This perspective views CIIP as securing e-business or the availability of processes and services, in general employing the resources of the IT perspective, even if certain organizational or staffing aspects are taken into account. Since this perspective is the least significant for the aspect of early warning, it is omitted here. The classification is necessarily an oversimplification. E.g., Metzger, Jan. "The concept of critical infrastructure protection". In: Alyson J. K. Bailes and Isabel Frommelt (eds.). Business and Security: Public-Private Sector Relationships in a New Security Environment (Oxford: Oxford University Press, 2004), p. 200, additionally lists defense-policy and regulation-policy perspectives, which the classification chosen here subsumes under the security-policy perspective; and Wigert, Schutz kritischer Informationsinfrastrukturen in der Schweiz, op. cit.

Non-state Players

Non-state players usually adopt the (IT-) technical perspective and generally limit their exchange of information to other representatives of this perspective (in this regard, see chapter 2.3.1). This chapter will introduce the most important non-state players.

Software and Hardware Manufacturers

This category includes both manufacturers of personal computers, servers, communications hardware (mobile phones, PDAs, IP telephony, etc.), and network hardware (such as routers, switches, satellites, etc.) and manufacturers of operating systems and applications.

Their task within CIIP is limited to the manufacture of systems that are as secure as possible and to the issuing of system-specific instructions, best practices, and later improvements: security notices, handbooks, and training courses, but also security updates (patches) and software updates. It is the systems of these players that are attacked.

Software and hardware manufacturers are representatives of the (IT-) technical perspective on CIIP, and their products primarily target representatives of the business perspective,[10] which is why they are also not unfamiliar with this perspective. Many of them also actively assist prosecutions or support representatives of the security-policy perspective.

Anti-Virus Software Manufacturers

Although the anti-virus software manufacturers also actually produce software, they play a different role than software manufacturers (chapter 2.1.1): They manufacture software that does not have productive characteristics, but that provides additional protection for the products of software and hardware manufacturers.

10 See fn. 9: This perspective is not elaborated in detail here, since it is unimportant to early warning.

The task of anti-virus software manufacturers consists in the search for viruses, worms, Trojan horses, bots, spyware/adware and other malware.[11] As soon as a new pest surfaces, up-to-date "definition lists" are distributed that allow the anti-virus software (search engine) to recognize the pest. In other words, the anti-virus software manufacturers are responsible for discovering and removing as many pests as possible.

Anti-virus software manufacturers are primarily representatives of the (IT-) technical perspective, even though the success of their products also depends on additional considerations related to the business perspective.

IT Security Providers

IT security providers sell know-how for the protection of IT infrastructures, generally without developing programs themselves for the removal of pests — this task falls within the scope of the anti-virus software manufacturers (chapter 2.1.2).[12]

Rather, the IT security experts search for security holes (vulnerabilities) in the products of the hardware and software manufacturers (chapter 2.1.1), develop "proof-of-concept" code showing how vulnerabilities could be exploited, and communicate their findings to the manufacturers, who then generally undertake to distribute a security update (patch) as quickly as possible.[13] In addition, IT security providers also offer services such as penetration tests for systems, integrated security solutions (intrusion detection systems, personal or hardware firewalls, backup systems, etc.).[14] Many operators of critical infra-

11 Additional information on malware and their consequences can be found at: http://www.melani.admin.ch/gefahren-schutz/schutz/index.html?lang=en. Information on bots: http://en.wikipedia.org/wiki/Internet_bot.

12 A precise delineation between IT security providers and anti-virus manufacturers is not always possible. Often, the same company will offer both services.

13 Proof-of-concept code: A source code for a program (a so-called "exploit"), which enables the vulnerability to be exploited. Such codes are developed to demonstrate the exploitability of the discovered vulnerability. Often, exploits emerge within a short period of time on the basis of this source code, with which attackers then attempt to exploit the vulnerability. See: http://en.wikipedia.org/wiki/Exploit_%28computer_security%29. Security holes are defined at: http://www.melani.admin.ch/gefahren-schutz/schutz/00030/index.html?lang=en.

14 For a definition, see: http://en.wikipedia.org/wiki/Penetration_test (penetration test) http://en.wikipedia.org/wiki/Intrusion-detection_system (IDS); http://en.wikipedia.org/wiki/Firewall_%28networking%29 (firewalls).

structure (chapter 2.1.6) and companies (chapter 2.1.7) have outsourced their IT security efforts to IT security providers or use their services to complement their own measures.

IT security providers are representatives of the (IT-) technical perspective, and they support representatives of the business perspective, who often outsource their IT security efforts to them.

Computer Emergency Response Teams (CERTs)

Also called Incident Response Team (IRT) or Computer Security Incident Response Team (CSIRT), CERTs form working groups to coordinate and take measures in response to ICT security incidents.

CERTs consist of IT security specialists with top-rate computer, network, and programming expertise and are specialized on combating breakdowns or attacks against the IT infrastructure of their clients. Each CERT is responsible for a defined group of clients: Many larger companies, governments, organizations, or universities have their own CERT. The type of services offered and their use are governed individually by contract. CERTs usually have good international contacts with other CERTs, exchange information, best practices, and tips among themselves and with their circle of clients, and help each other solve problems.[15]

CERT teams are the typical representatives of the (IT-) technical perspective and constitute an indispensable component of efficient CIIP policy.

Media

This category encompasses mass media such as television, radio, and larger newspapers, magazines, and web information portals, but also relevant computer periodicals.

Of all the players mentioned here, the media have the greatest potential to gain public attention. For this reason, they play an important role in warning and raising the awareness of the public, and they can also perform valuable services in the field of prevention. The following groups can be reached by the

15 FSUIT, Verletzliche Informationsgesellschaft, op. cit., p. 28 (in German). The largest team of this kind is the US CERT/CC (CERT Coordination Center): http://www.cert.org. On the information exchange of CERTs, see also chapter 2.3.1.

various media: the greater public, via reporting in the mainstream media (large newspapers, television, etc.) on larger incidents or trends and dangers; amateur computer users interested in the subject, via computer periodicals providing simple and easily understandable best practices, tips, and instructions; and expert computer users, via sometimes highly specialized periodicals directed at professionals.

In a complex interaction, the media also influence the attackers (who may have a penchant for myth-making and strive for fame, and will switch to new attack vectors when the old approaches achieve widespread coverage), and at the same time, they constitute an important resource for IT security experts (e.g., expert periodicals).

The media cannot be assigned to any CIIP perspective or, depending on the focus of the publication, they can be assigned to all of them.

Operators of Critical Infrastructure

Although the representatives of the security-policy perspective of CIIP are also concerned with the security of citizens, of small and medium-size businesses (SMBs), and of large companies, the operators of critical infrastructure are the focus of the interest of CIIP.

Until approximately the beginning of the 1990s, most infrastructures regarded as important for maintaining the security, productivity, and welfare of the state were controlled by the state; today, many of these infrastructures in many countries are privately operated. A further aggravating factor is that many operators of critical infrastructure operate internationally. While the state used to be able to ensure quality controls in vital areas more easily due to its monopoly, this is no longer as simple today, since private players are not forced to consider security policy and therefore often neglect cross-sector efforts; but in turn, they have more experience in the practical aspects of safeguarding the security of their systems than the state.[16]

Nation-states divide the operators of critical infrastructure into so-called sectors; the following sectors are defined most frequently:

16 Henriksen, Stein. "The Shift of Responsibilities within Government and Society", p. 61. In: CRN-Workshop Report: Societal Security and Crisis Management in the 21st Century (Stockholm: Swedish Emergency Management Agency and ETH Zurich, 2004), pp. 60–63; Wigert, Der Schutz kritischer Informationsinfrastrukturen, op.cit., pp. 98ff.

- finance
- administration
- telecommunication (and information technologies)
- emergency response organizations (protection and rescue, fire service)
- energy
- public health (including water supply)
- transport and logistics[17]

From the CIIP perspective, the spectrum of tasks of the operators of critical infrastructure can be defined as follows: They make services available that are indispensable for maintaining the sovereignty, security, economic productivity, and social welfare of the nation-state. Representatives of this group of players are often very large enterprises with efficient information assurance resources and highly trained specialists. In other words, while they are often very good at ensuring their own information assurance, they are often (still) not integrated into any information exchange and are hardly interested in information assurance outside their own enterprise. In the framework of the public-private partnerships (PPPs) sought by many states, attempts are being made to integrate the operators of critical infrastructure into an information exchange (with the state, but also with each other). In this way, the state receives important information on the situation of the critical infrastructures, the private operators of which in turn benefit from information provided by the state, sometimes also from intelligence sources.[18]

The operators of critical infrastructure often adopt a business perspective[19] on CIIP, even if they approach their own ICT security primarily from an (IT-) technical perspective. Business continuity — one of the main goals of the business perspective — plays a central role in the sectors described above.

Small, Medium-Size and Large Businesses

All businesses not included in any of the other categories belong to this last category of non-state players.

The tasks of these players are not easy to define, since they vary considerably. As a rule, however, it can be said that these businesses also are becoming

17 See fn. 4, supra.
18 See chapter 2.2.3.
19 See fn. 9 for a more detailed explanation of this perspective.

increasingly dependent on ICT, to a similar extent as the operators of critical infrastructure. Like the operators of critical infrastructure, they are responsible for their own information assurance. While large businesses — similar to the operators of critical infrastructure, who also tend to be large — certainly are able to muster the resources, know-how, and personnel to safeguard information assurance, this is not the case for SMBs. These often lack both the human and the financial resources to attend to IT security (or even information assurance) in detail.[20] Accordingly, representatives of this group of players also tend to outsource the maintenance of their own ICT infrastructure to IT security providers (see chapter 2.1.3).

Like the operators of critical infrastructure, small, medium-size, and large businesses mostly adopt a business perspective[21] on CIIP, even though they approach their ICT security primarily from an (IT-) technical perspective.

The Function of the State as a Player

Already in the introduction, the question was raised in what area of CIIP the state functions as a player, and how it should interact with the private sector. As a rule, the operators of critical infrastructure, as well as small, medium-size, and large businesses, bear responsibility for the security and availability of their information systems themselves. At the same time, many operators of critical infrastructure and large businesses have very good information assurance capacities, extensive know-how, and practical experience. How can the state even provide supportive assistance in this context, and where does this obligation derive from?

As already mentioned, it is in the vital interest of the state to protect the productivity of its national economy. The more society, business, and administration become dependent on ICT, and the more individual sectors become dependent on each other due to increasing ICT networks, the more imminent the danger of an ICT breakdown becomes from the perspective of security policy. In Switzerland, for instance, the state has the constitutional mandate to ensure the general welfare of the population, from which it derives its duty

20 Keyes, Cyber- Early Warning, op. cit., p. 48.
21 See fn. 9 for a more detailed explanation of this perspective.

to act – since a massive, long-lasting breakdown of ICT infrastructures would have disastrous effects on the welfare of the economy and the population.[22]

The primary interest of the state may focus on the operators of critical (information) infrastructures. But private users and small, medium-size, and large businesses should not be neglected either. Due to the highly networked nature of ICT, general security can only be promoted when awareness of this problem is raised also among such ICT users. Nowadays, every home computer can be abused, and every business is in danger of suffering data loss, being spied on using ICT, or being affected by a breakdown and the resulting productivity loss. A general enhancement of security is only possible if all players are integrated into the CIIP strategy.

The first part of this chapter will show what tasks the state performs in the area of information assurance. Then, it will be explained how the state can be linked up with the players introduced in chapter 2.1: The second part of the chapter will define "open constituency" and discuss how the state can raise the awareness of the public and of small, medium-size, and large businesses and provide support for maintaining ICT security. The third part will focus on the interaction with operators of critical infrastructure and on ways to approach this interaction: By means of public-private partnerships, this "closed constituency" can be integrated into a far-reaching information exchange process. On the one hand, this serves to create an early-warning capacity to prevent major breakdowns; on the other hand, it enhances communication with known contacts to coordinate measures if incidents occur.

Legislation / Prosecution and Strategic Analysis

Legislation and prosecution are uncontested responsibilities of the state that are also exercised in the field of "cyber-crime". Even if these are two indispensable responsibilities of the state in the context of CIIP and of law enforcement in general, they play a subordinate role for the question of early warning and will therefore not be discussed in detail here.

More significant for a sound early-warning capacity are intelligence efforts and strategic analyses in the field of cyber-crime and information assurance, both of which are also undertaken by the state. In view of the unclear threats,

22 Swiss Federal Constitution, article 2, paragraph 2; available at: http://www.admin.ch/ch/d/sr/1/101.de.pdf (in German).

the unknown potential attackers, and the fact that attacks are sometimes very difficult to discover, this type of information procurement and analysis is becoming extremely important. Only states have the resources and the capability to observe the situation constantly, to share related information with foreign authorities, to conduct studies on possible attackers, and to continuously compile statistics that make it possible to quantify and control the problem in the first place. No other player has this interest in compiling cross-sector analyses: The private sector does obtain (mainly technical) information concerning the security of its own systems, but it has neither the resources nor the interest to undertake more extensive studies of attackers and attacks and to keep track of tendencies and trends in similar sectors abroad. The state is the only player that assumes a comprehensive security-policy perspective on CIIP, and is therefore the only entity that can realize an integration of the differing perspectives.[23]

Open Constituency (Citizens and Small, Medium-size and Large Businesses)

In addition to safeguarding the operators of critical infrastructure, who are the focus of the interest of state CIIP policy, there is also an interest in protecting the public as well as small, medium-size, and large businesses.[24]

Many current threats to ICT, such as spam,[25] distributed denial-of-service attacks (DDoS),[26] identity theft,[27] blackmail, and many others originate in so-called botnets.[28] Botnets consist of many hundred, and sometimes even hundreds of thousands of compromised computer systems that can be remote-controlled by an attacker without the knowledge of the user, after being infected by a Trojan horse, a worm, or other malware.[29] In addition to larger systems with broadband internet connections (e.g., at universities), botnets generally affect private computers. Such botnets represent a serious threat since they can be used to conduct many attacks. If comprehensive protection of ICT and

23 See contribution of Isabelle Abele-Wigert in this Volume for a discussion of the different perspectives.
24 The following considerations apply to large businesses only to a limited extent (in this regard, see chapter 2.1.7).
25 More information on spam can be found at: http://www.melani.admin.ch/gefahren-schutz/schutz/00025/index.html?lang=en.
26 Information on DDoS attacks: http://en.wikipedia.org/wiki/Distributed_denial_of_service.
27 Information on identify theft: http://en.wikipedia.org/wiki/ID_Theft.
28 Information on botnets: http://en.wikipedia.org/wiki/Bot_nets.
29 For information on these malwares, see fn. 11.

especially of the ICT infrastructure of the operators of critical infrastructure is to be possible, the awareness of the private user must also be raised, so that private computers can be better protected. Because of the extensive networking of ICT, no player can be ignored.

Possible tasks of the state with respect to this "open constituency" are to be found in the following areas:

- Awareness-raising: The public can be reached through the publication of configuration instructions, recommendations, and supplemental information, for instance on the internet. In this regard, it must be taken into account that a target audience is being addressed that is actually not interested in the topic (in contrast to information provided to the "closed constituency", see chapter 2.2.3): The instructions should therefore not be overly complex or convey unnecessary information, so that the public does not feel overloaded and does not shy away from obtaining information in the future. By including the media in a targeted manner (see chapter 2.1.5), familiarity with these offerings and their dissemination can be increased. A neutral state authority that is independent of the interests of the IT industry, is perceived differently by the media than other service providers in the field of IT security: A warning or recommendation to the public is often taken up by the media, thereby usually reaching a larger public.
- Warning: Almost every day, web portals and computer periodicals publish new security holes and issue warnings that may be relevant for IT professionals, but that overwhelm amateurs. In the context of the internet-based efforts recommended in the previous point, such warnings can be conveyed selectively. For instance, warnings can be issued only when measures become necessary that go beyond the basic protection recommended in the configuration instructions, which would massively reduce the frequency of warnings. Initial experiences in Switzerland have shown this strategy to be successful: Many (computer) media outlets take up such warnings, which then — not least because of their rather rare occurrence — receive more attention.[30]

30 Details on the information assurance efforts in Switzerland can be found in the Country Survey Switzerland in the CIIP Handbook 2006, Vol. I.

- Assistance: An additional support possibility — especially for businesses — is, for instance, assistance rendered after an incident. If a private person or a business becomes the victim of an ICT incident, this can be reported via the web portal mentioned above or by other means. This not only improves and increases the flow of information, allowing better analytic conclusions concerning the condition of national ICT security, but it also opens up the possibility of active assistance – whether in the form of legal advice, responses to a technical question, or even the deployment of a state CERT to support the victim.[31]

Closed Constituency (Operators of Critical Infrastructure)

As indicated above, a different approach is recommended for dealing with operators of critical infrastructure, namely for what is known as public-private partnerships (PPP).[32]

First, it must be assumed that the operators of critical infrastructure have above-average ICT security competence, employ their own specialists, and are able to mobilize know-how and financial resources to protect their systems optimally. It would not be a successful strategy to bore this circle of clients with awareness-raising campaigns, configuration recommendations, or tips that may only make sense for the open constituency.

Second, the operators of critical infrastructure are not simply ordinary representatives of the business world, but rather, they are the focus of state CIIP interest: A breakdown of these infrastructures threatens to interfere massively with the functioning of the state polity.

While the state's interest with respect to the open constituency lies primarily in awareness-raising, education, and support, the supreme goal for the closed constituency is the uninterrupted provision of services. In order to achieve this or, should the case arise, to learn as quickly as possible of larger incidents, the state depends on continuous information exchange with the operators of critical infrastructure. In addition, this is the only way to ensure that a comprehensive picture of the danger can be obtained.

31 As an example of how this has been implemented in Switzerland, see: http://www.melani.admin.ch.

32 On public-private partnerships, see: Dunn and Wigert, International CIIP Handbook 2004, op. cit., p. 342; Metzger, The concept of critical infrastructure protection, op. cit., p. 209.

Far-reaching information exchange is therefore unavoidable to maintain the ICT security of the operators of critical infrastructure and to create an early-warning capacity.[33] Only when it is known that breakdowns have occurred or are soon to be expected in a particular sector can other representatives of this sector or of other sectors be warned and prepared for a potential emergency situation. At the same time, such an information flow also enables an exchange of experiences, recommendations, standards, and best practices among the operators of critical infrastructure — and since these operators are experienced professional providers of ICT infrastructures, a considerable know-how gain can be realized through exchanges among their ICT experts, leading to a general increase of the ICT security level in a country.

However, since the operators of critical infrastructure are predominantly businesses operated by the private sector, in competition with each other, and often critical concerning the motives of the state for providing support, the expansion of such information exchange constitutes a great challenge.[34] In the United States, for instance, a sobering conclusion was reached just a few months ago, after one year of operation of the "Protected Critical Infrastructure Information Program" (PCII): Hardly any reports have been submitted so far. The main reason indicated is that companies are hesitant to notify the government of vulnerabilities and business secrets — especially since, although the information does not reach the public, the information within the government is no longer subject to the control of the company submitting the report.[35]

Switzerland is attempting to circumvent this problem through the signing of non-disclosure agreements: At all times, the information flow is subject to the control of the company submitting the report. Without the permission of the reporting entity, the state is not allowed to forward information to other

33 For instance, Presidential Decision Directive PDD-63 (22 May 1998) likewise decided to establish so-called Information Sharing and Analysis Centers (ISACs) to facilitate information exchange with the private sector. See: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, 22 May 1998. http://www.fas.org/irp/offdocs/paper598.htm. See also Keyes, Cyber- Early Warning, op. cit., pp. 46f. and p. 50. In the US, for instance, a debate is currently underway to what extent even a notification requirement might be necessary. See the related article in Computerworld: http://www.computerworld.com/databasetopics/data/story/0,10801,101820,00.html. In another article, the US government is accused of having neglected information exchange: http://www.computerworld.com/governmenttopics/government/story/0,10801,102049,00.html.

34 Keyes, Cyber- Early Warning, op. cit., p. 48.

35 Poulsen, Kevin. U.S. Info-sharing initiative called a flop. Security Focus, 11 February 2005. http://www.securityfocus.com/news/10481.

state authorities, other operators of critical infrastructure, or the public. This organizational arrangement aims to enhance the willingness of the private sector to submit reports.

In addition to the services for the open constituency (see chapter 2.2.2), the following offerings are conceivable for the closed constituency:

- Communication channel to the public: Members of the closed constituency can approach the public via the reporting channels for the open constituency (see chapter 2.2.2) and submit certain warnings or recommendations (for instance, those important to their business). They can thereby participate in determining the agenda of state activities in the area of public information. It is important, however, that the neutrality of the government office responsible for receiving reports be maintained, so that it does not allow itself to be instrumentalized.
- Making available an international network of intelligence services, prosecution authorities, and CERTs: The international network of national reporting and analysis offices can be made available to the members of the closed constituency. This proposal will be further elaborated in chapters 2.3.1 and 2.3.2.
- Communication platform for the members of the closed constituency: While most attackers against the ICT infrastructure exchange information and experiences almost constantly, this is still hardly the case for the victims of such attacks. The national reporting and analysis office can act as a communication platform for the members of the closed constituency. In this way, the closed constituency has the possibility of exchanging information and experience under clearly regulated conditions – even with competitors.
- Distribution of exclusive information: Thanks to its intelligence-analysis capacities, the state is able to compile threat analyses, situation reports, statistics, background information, and perpetrator profiles, and to make them available to the closed constituency. For instance, this makes it possible to forward a detected heightened threat of economic espionage directly to the most important representatives of the private sector. As an additional service, it would be possible to conclude far-reaching information agreements with certain manufacturers (see chapters 2.1.1 and 2.1.2) entailing an information gain for the

closed constituency. Only recently, for instance, Microsoft declared its intention to cooperate more frequently and more closely with governments.[36]

- Early warning: The final and most important point is the specific topic of this paper: early warning. Based on mutual trust, efficient early warning arises as a consequence of ongoing information exchange between the state and the members of the closed constituency, particularly in the event of accidents, breakdowns, attacks, or sabotage within the critical infrastructures. With the consent of the reporting member, the state reporting office is able to warn the other members, issue recommendations, or offer support in a timely manner.

International Early Warning

After enumerating the non-state players in chapter 2.1 and introducing the state as a player in chapter 2.2 and examining the state's possibilities of cooperation with other players and with respect to national information exchange, the focus of this chapter will be on the international aspect of early warning. In what way are the previously introduced players already communicating with each other? In what way can these information flows be institutionalized?

In this regard, the first part of the chapter will show to what extent players, predominantly of the same kind and sector, have exchanged information bilaterally (and internationally) so far; the second part will then consider how a concentration of all players and of all CIIP perspectives in a single player can improve international information exchange – and therefore early-warning capacity.

First Step: International Exchange Among Players of the Same Kind (Already Realized)

Most of the players introduced in chapter 2.1 as well as the state already undertake international information exchange: A prominent example can be

36 See the Microsoft press releases: http://www.microsoft.com/presspass/press/2005/feb05/02-02SecurityCooperationPR.mspx and http://www.microsoft.com/emea/pressCentre/PressRelease.aspx?f=SharedSourcePR_210305.

found in the international contacts of the CERTs.[37] Most of the larger CERTs exchange information regularly at conferences, colloquia, or other meetings, discuss the newest attack techniques, technologies, and standards, and receive continuing training in seminars.[38] Also, in the course of their daily work, the teams – who often know each other personally — exchange information and, in this way, are among the most internationally networked players in the field of IT security.

The manufacturers of software, hardware, and anti-virus software are generally large international companies with branches in numerous countries. Their training programs, warnings, technical support and other services are oriented towards a global strategy — which is increasingly also characterized by security considerations — but, thanks to their national presence, they also offer local support, assistance, and often also expert know-how in emergency cases. It is obvious that the national branches of these manufacturers exchange information internationally.

IT security providers also mostly act internationally: When security holes, vulnerabilities, and trends are discovered, they are published internationally, and most of the services offered can be used independently of location. The experiences of a representative of this sector from a particular country are also available to clients from other countries.

More and more, the information compiled or processed by the state is shared internationally. The two core competences of the state — legislation and prosecution — are constantly adapted and standardized internationally.[39] As part of daily information exchange among the intelligence services of nation-states, the results of strategic/analytical investigations in the field of information assurance are also aligned.[40] While the state may be the only player adopting a truly comprehensive security-policy perspective on CIIP, thus already encompassing

37 Internationally, CERTs primarily exchange information at the Forum of Incident Response and Security Teams (FIRST): http://www.first.org.

38 See the information under FIRST Events & Meetings: http://www.first.org/events.

39 The most prominent example of these harmonization efforts in the fields of prosecution and legislation is the Cyber- Crime Convention of the Council of Europe. More information is available at: http://www.coe.int/T/E/Legal%5Faffairs/Legal%5Fco%2Doperation/Combating%5Feconomic%5Fcrime/Cyber-crime/ and at: http://www.iwar.org.uk/law/resources/eu/cyber-crime-final.htm (text of the Convention).

40 Various institutionalized forms of intelligence exchange exist, but they are subject to secrecy and can therefore not be elaborated in more detail here.

a broad spectrum of technical, organizational, personnel, strategic/analytic and security-policy considerations, it nevertheless generally does not (yet) have access to the crucial information of the operators of critical infrastructure and of the SMBs and large companies.

The greatest quantitative deficit in the field of international information exchange exists with respect to the small, medium-size, and large businesses and with respect to the operators of critical infrastructure. Due to the predominance of the business perspective in their approach to information assurance, their desire for international information exchange is low — only reluctantly do they share information with their competitors or with the state concerning their own vulnerabilities and threat potentials. While many of these representatives act internationally and therefore also communicate internationally, this information exchange is limited to the core business and the ICT infrastructure of the enterprise in question.

The greatest qualitative deficit in international information exchange is due to the selective perspective on CIIP that each of the involved players adopts. Most players are representatives of either the business perspective or the (IT-) technical perspective — which is also why their international, mainly bilateral information exchange is also limited to the relevant perspective.[41] CERTs, for instance, address technical questions, evaluate problems, and address their proposed solutions to specialists. CERT warnings are therefore almost always directed at a particular technical problem and generally also offer a (technical) solution to this technical problem.[42] Software and hardware manufacturers, anti-virus software manufacturers, and IT security providers limit their information exchange and their warnings, instructions, and recommendations to their products and to the products they support, and therefore they do not engage in any more extensive information exchange.

Second Step: National Concentration of the Players and Integration of the CIIP Perspectives into an International State Player (in the Process of Implementation)

This chapter will present solutions for remedying the deficits identified in the last chapter in the area of international information exchange — on the one

41 Wigert, Schutz kritischer Informationsinfrastrukturen in der Schweiz, op. cit.
42 FSUIT, Verletzliche Informationsgesellschaft, op. cit., pp. 30ff.

hand, the marginal participation of the private sector (SMBs, large companies, operators of critical infrastructure), and on the other hand, the limitation of information exchanged by actors about their CIIP perspective. How can the operators of critical infrastructure and other representatives of the private sector participate efficiently in the information exchange that is indispensable for securing an early-warning capacity? And how can the various CIIP perspectives be integrated to ensure that the situation can be assessed accurately and information can be exchanged internationally and efficiently?

The added value of the state as an actor was already highlighted in chapters 2.2.2 and 2.2.3, and various measures were considered as to how the state can improve its efforts relating to information exchange. These measures also contain the key to improving international information exchange. While the measures presented in chapter 2.2.2 can integrate all national players to achieve better awareness-raising, warning, and assistance capacities, chapter 2.2.3 illustrated the possibilities of how operators of critical infrastructure could be integrated to compile better situation analyses of the critical infrastructures of a country, and how an early-warning capacity could be realized.

The possibilities for interacting with the operators of critical infrastructure, as introduced in chapter 2.2.3, only create the foundation for an international early-warning capacity. Legal regulations on reporting, communication, and warning procedures can also create the conditions for the operators of critical infrastructure to be integrated into a national, bilateral information exchange with one another, in much the same way that most other players already are.[43] In addition, this approach creates clear rules for dealing with information submitted to the state, thereby helping to reduce prejudices held by the private sector about the state as a player and generating trust as a precondition for mutual information exchange. At the same time, under the arrangement proposed in chapter 2.2.3, the members of a "closed constituency" would receive access to foreign prosecution authorities and to the internationally exceptionally well-connected CERTs, thereby increasing the capacity to solve problems effectively in the event of an incident, and would have an additional channel for communicating with the public.

Thanks to the targeted integration of the operators of critical infrastructure into state protection efforts, the largest gaps in the CIIP efforts so far have been closed: the lack of information available to critical infrastructure operators about

43 See chapter 2.1 and chapter 2.3.1.

the condition of the ICT infrastructure, and the shortcomings that hampered the reporting flow in emergencies. This is because the regulated communication channels between the state and the operators of critical infrastructure also flow in the other direction and support a regulated dissemination of exclusive intelligence information, and especially of early warning.

An international early-warning center can be established by creating a public, national competence center with experts from the technical, intelligence-analysis, and criminal law fields, networked with the public and the general private sector as part of the "open constituency" suggested in chapter 2.2.2, and with the operators of critical (information) infrastructure as part of the "closed constituency" suggested in chapter 2.2.3,.[44] Not only does such a competence center combine the (IT-) technical, prosecutorial, intelligence-analysis, and business perspectives into a comprehensive approach to the problem, but it also constitutes an international communication platform and contact point for information assurance concerns. Thanks to its established contacts with operators of critical infrastructure, technicians, legislators, intelligence officers, and strategic analysts at home and abroad, such a competence center can monitor ongoing situations and realize an early-warning capacity through targeted receipt, evaluation, and dissemination of information – and, if necessary, to issue warnings internationally, directly to the affected players.[45]

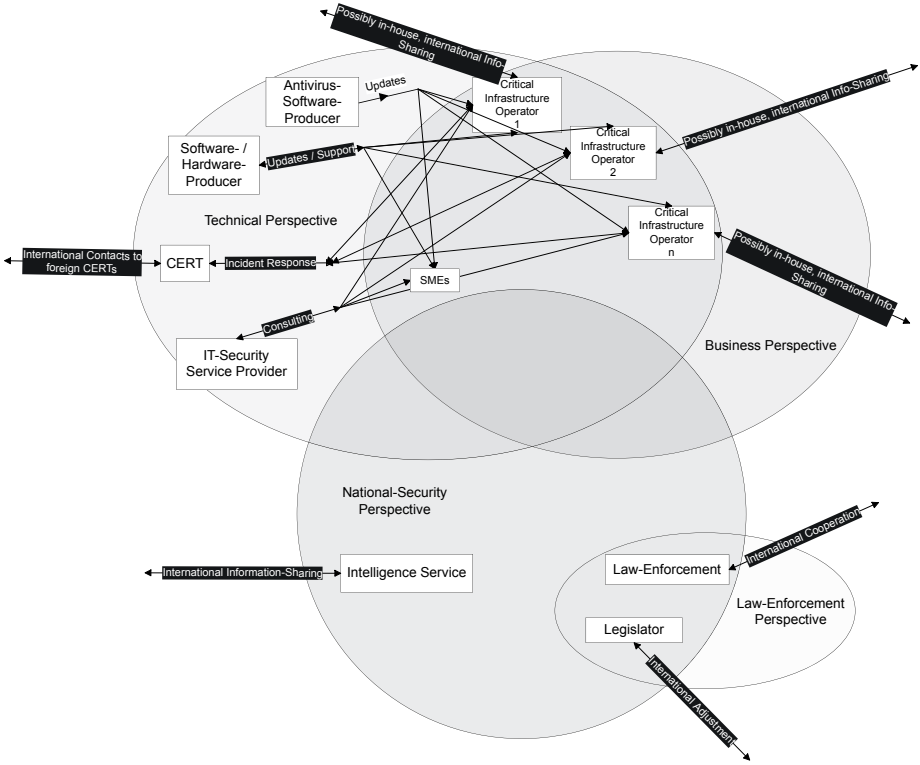
The problem analyses of such competence centers cover different areas than those provided by the CERTs, for instance, which offer primarily technical solutions. A warning may indeed be issued by such a center based on other than technical considerations and — with a focus on the critical infrastructures — may also be issued without being able to supply a technical solution. The problem analysis may therefore, under certain circumstances, be performed far away from the (technical) source of the malfunction; nevertheless, measures are recommended that are as close as possible to their (technical) implementation and are accordingly adapted to the requirements of those affected in business and administration.[46] At the same time, such a center also offers a

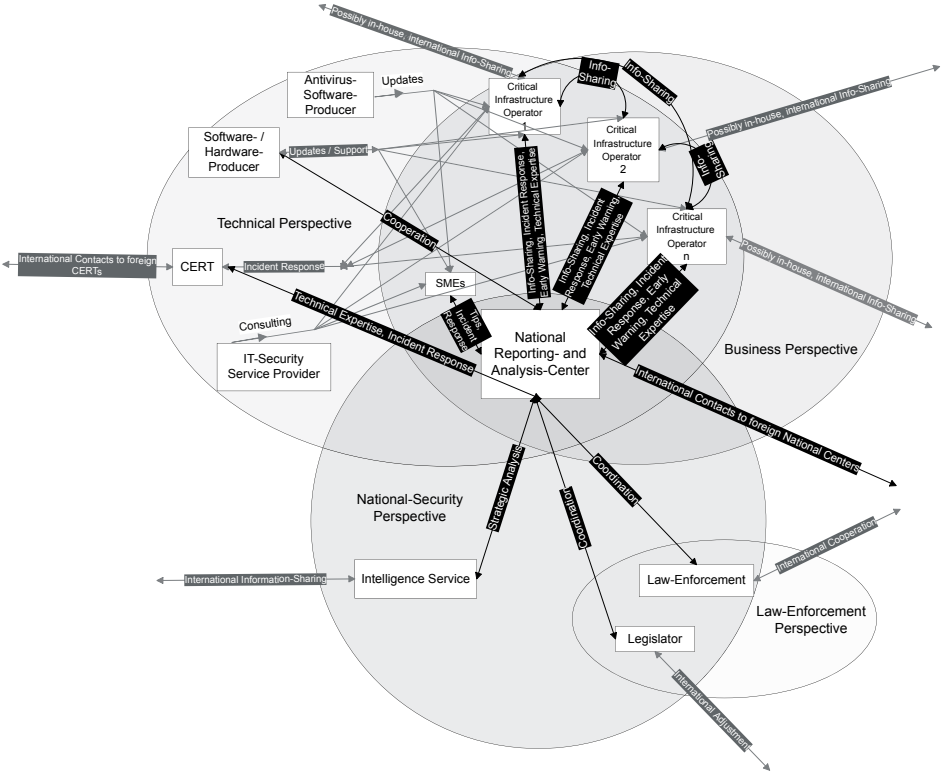
44 The conclusion that the key to success lies in public-private partnerships is also largely shared by the relevant literature and is currently being implemented in practice in many countries. For examples, see the Country Survey section in the CIIP Handbook 2006, Vol. I.

45 A decision of the Swiss Federal Council of 29 October 2003 created precisely such a competence centre named "Melde- und Analysestelle Informationssicherung (MELANI) — Reporting and Analysis Centre for Information Assurance", which is now in operation: http://www.melani.admin.ch.

46 FSUIT, Verletzliche Informationsgesellschaft, op. cit., pp. 31f.

national contact point for requests for assistance and expert know-how in the event of an ICT incident, so that the incident remains short, rare, controllable, geographically isolated, and — if possible — consequences for the national economy and national security can be avoided.





Conclusion

For a long time, a military early-warning capacity has been regarded as indispensable for assuring the sovereignty, security, and economic welfare of nation-states. In addition to timely alerts enabling the organization of defense, the protection of the population, and the initiation of countermeasures, an efficient early-warning capacity gives rise to an additional benefit: deterrence. An attack becomes less attractive the less damage it can cause.

In the most recent topic area of state security policy, namely Critical (Information) Infrastructure Protection, early warning plays a key role, but has not been sufficiently realized anywhere so far. This paper has therefore

considered the question of how such a capacity could be realized, which of the players (who pursue differing priorities and view the problem from correspondingly different perspectives) should participate, where the responsibilities and tasks lie, and which function is assigned to the state. Other important aspects of successful CIIP policy include international harmonization and promotion of research and development, training, education, and the elaboration of common standards, but they have not been the focus of interest of this paper.

Most non-state players, such as software and hardware manufacturers, anti-virus software manufacturers, IT security providers, Computer Emergency Response Teams (CERTs), the media, and the operators of critical infrastructure that are central to this problem focus on an IT-technical perspective and view CIIP fundamentally as a matter of IT security to be solved with technical measures. Business considerations also play an important role for these players. In contrast, prosecutors view CIIP as the protection of society from cyber-crime, and therefore respond primarily in a reactive manner. The security-policy perspective on CIIP adopted by the state perceives a threat to society as a whole, and strives to prevent a large incident in ICT infrastructures, taking into consideration technical, legislative, organizational, and international measures. While policy makers and legislators act upstream with respect to CIIP efforts, the intelligence services and ICT technicians (such as CERTs) are situated in the center and deal with the protection of critical infrastructure and ICT security in their daily work. Prosecutors are downstream and inherently reactive, but a certain deterrence potential can be attributed to them.

The greatest obstacle to achieving an effective early-warning capacity lies in the deficient communication between the representatives of these levels. The greatest quantitative deficit in the field of international information exchange is found in the small, medium-size, and large businesses as well as among the operators of critical infrastructure. Their desire for international information exchange is low – they are reluctant to share information with their competitors or with the state concerning their own vulnerabilities and threat potentials. While many of these representatives operate and therefore also communicate internationally, this information exchange is limited to the core business and the ICT infrastructure of the enterprise in question.

The greatest qualitative deficit in international information exchange is due to the selective perspective on CIIP that each of the involved players adopts. Most players are representatives of either the business perspective (SMBs, large

businesses, operators of critical infrastructure) or the (IT-) technical perspective — which is also why their (inter-) national, mainly bilateral information exchange is also limited to the relevant perspective. CERTs, for instance, address technical questions, evaluate problems, and address their proposed solutions to specialists. CERT warnings are therefore almost always directed at a particular technical problem and generally also offer a (technical) solution to this technical problem. Software and hardware manufacturers, anti-virus software manufacturers, and IT security providers limit their information exchange and their warnings, instructions, and recommendations to their products and to the products they support, and therefore do not engage in any more extensive information exchange.

In the areas of intelligence exchange, security-policy planning, legislation, and prosecution, for example, state offices are confronted with the problem that the infrastructure to be protected is not under their direct control.

By creating a public, national competence center with experts from the technical, intelligence-analysis and criminal law fields, networked with the public and the general private sector as part of the "open constituency" suggested in chapter 2.2.2, and with the operators of critical (information) infrastructure as part of the "closed constituency" suggested in chapter 2.2.3, an (inter-) national early-warning center can be established. Not only does such a competence center combine the (IT-) technical, prosecutorial, intelligence-analysis, and business perspectives into a comprehensive perspective on the problem, but it also offers an (inter-) national communication platform and contact point for information assurance concerns. Thanks to its established contacts with operators of critical infrastructure, technicians, legislators, intelligence officers, and strategic analysts at home and abroad, such a competence center is able to engage in ongoing situation monitoring and to realize an early-warning capacity – through targeted receipt, evaluation, and dissemination of information. At the same time, such a center also offers an (inter-) national contact point for requests for assistance and expert know-how in the event of an ICT incident, so that the incident remains short, rare, controllable, geographically isolated, and if possible without consequences for the national economy and national security.

Part III
CIIP Public Policy Issues

Public-Private Partnerships and the Challenge of Critical Infrastructure Protection

By Jan Joel Andersson and Andreas Malm

Introduction

There have been great shifts in economic policy in Europe over the past two decades. Among the most important of these shifts have been the privatization of public monopolies, infrastructure networks, and the deregulation of service provision — functions traditionally associated with national governments. Driven by poor performance and inspired by neo-liberal economics, public monopolies have undergone dramatic transformation. In many European countries, the provision of energy, communication, transport, financial services, and health care have all been, or are being, privatized and previously protected markets deregulated. These changes are meant to increase competition, improve productivity, provide more consumer choice, and lower prices. However, while liberalization in many cases has improved efficiency and productivity, it has also led to concerns regarding the accessibility, equality, reliability, and affordability of services.[1] Moreover, the privatization of public monopolies and infrastructure networks and the deregulation of services have important implications for national and international emergency preparedness and crisis management.

To survive in a market-driven economy, companies need to minimize costs and maximize profits. With pressure to cut costs, fewer resources are available for security and crisis management. Keeping reserve stock, maintaining redundant systems, and employing back-up staff are measures that cost money. To save money, activities and support functions previously performed by in-house experts and staff are frequently contracted out to external consultants. While this may reduce costs, emergency preparedness measures and crisis management capabilities are also reduced. Yet in a modern society, uninterrupted energy supply, communication, transport, financial services, and health care must be maintained at all times.

1 See, for example Héritier, Adrienne. "Market integration and social cohesion: the politics of public services in European integration." In: Journal of European Public Policy. Vol. 8(5): 825–852, 2001; Id. "Public-interest services revisited." In: Journal of European Public Policy. Vol. 9(6): 995–1019, 2002.

In a non-liberalized economy, the state assumes both the responsibility as well as the costs of guaranteeing functioning systems and services. However, in a liberalized global economy, assigning responsibility for securing such systems and services is more problematic. Who should implement and pay for the protective measures that have to be taken to ensure "homeland security"? Which measures should come under the responsibility of national and local governments and of the private sector, respectively? How do national solutions to these problems fit with the internationalization of markets for goods and services and the emergence of transnational information and communications networks?

The first step towards greater "homeland security" is effective emergency preparedness and crisis management measures. While there is wide agreement that emergency preparedness is important, the question of what should be done and who should pay for it nonetheless remains.[2] Public-Private Partnerships (PPPs) have been proposed as an answer to the questions of responsibility and financing. In fact, PPPs are considered by many to be a panacea for all governance problems in a deregulated economy.[3] As we argue in the following, however, the extent to which such partnerships are a panacea rather than a Pandora's box remains to be seen.

In this paper, we aim to do three things. First, we will first discuss why PPPs have emerged as the preferred choice for governments when it comes to providing market-corrective regulation in a liberalized economy. Second, we will outline some of the prospects and pitfalls of this approach and examine why PPPs might only constitute a secondary, or less desirable, choice for private actors. Rather than a panacea for liberalized economies, such partnerships may instead become a Pandora's box for many governments — an unreliable and unpredictable solution to the problem of under-provision of governance in

2 See, for example: O'Hanlon, Michael, et al. Protecting the American Homeland. One Year On (Washington, D.C.: Brookings Institution Press, 2003).

3 Partnerships between public and private actors to fulfill public functions are on the increase at every level of government. Public-Private Partnerships have been suggested as a way to improve everything from inner city urban development to relations between developing countries and multinational corporations. In the US and Canada, for example, PPPs currently operate in most policy areas, and trial programs in the US are being planned by the Internal Revenue Service, the Census Bureau, and the Social Security Administration. See, for example: Davis, P. Public Private Partnerships — Improving Urban Life. Academy of Political Sciences, USA (1986); Osborne, Stephen P. Public-Private Partnerships: Theory and Practice in International Perspective (Routledge 2000); Vaillancourt Rosenau, Pauline, ed. Public-Private Policy Partnerships (Cambridge, M.A.: MIT Press).

deregulated sectors of society, particularly in the areas of national emergency preparedness and crisis management. We will subsequently explore this argument by examining the cases of the energy and financial services sectors.

The Problem

Why is the provision of emergency preparedness measures in a liberalized economy particularly problematic? A fruitful way to think about emergency preparedness is to view it as a service for managing risks. Basic economic theory tells us that the optimal level of emergency preparedness is reached when consumers' willingness to pay for extra emergency preparedness is just equal to the cost of providing it. In practice, we should think of this level as a "zone of adequacy" within which both the value of emergency preparedness and the cost of providing it will be relatively stable, rather than as a singular point. In a liberalized economy, the main question is whether markets are likely to respond effectively to current and expected future risks.

Proponents of liberalized markets argue that the market can provide appropriate levels of emergency preparedness, and that the threat does not necessarily require any kind of government intervention.[4] Private actors should have a very strong incentive to provide pro-active and effective emergency preparedness and crisis management without any government intervention or regulation. After all, it ought to be any private actor's worst nightmare to fail in providing a key service to its customers because of inadequate emergency preparedness and crisis management.

However, while individuals and companies may have strong incentives to provide effective emergency preparedness and crisis management, private motivation is unlikely to be sufficient to provide an optimal amount of emergency preparedness for society as a whole. In fact, private motivation may not even be enough to provide emergency preparedness and crisis management capabilities to ensure individual corporate safety, let alone the safety of society at large.[5]

4 See for example: Shuttleworth et al. Security of energy supply, Energy Regulation Brief. NERA, produced for Departement of Trade and Industry (2003).

5 Stephen Castella at Morgan Stanley once asked: "Have you ever wondered why you have never heard of a company that did not have a contingency plan?" Stephen Castella, CPM, BCP 102: Continuity of Information Foundations for Successful BCP in Your IT Department, January 2001. http://www.contingencyplanning.com.

A recent disaster research study conducted by the University of Texas shows that only six percent of companies that experience a disaster with catastrophic losses survive in the long run (two years and beyond).[6]

While the market, in theory, may deliver emergency preparedness that could be adequate for society as a whole, there are several reasons to believe that it will not be able to do so. First, market failures and imperfections generally exist to such a degree that they may prevent the market mechanism from functioning efficiently. Second, even with a perfectly functioning market, the assumption that the market clearing level of emergency preparedness is adequate for society at large seems inappropriate from a societal perspective. Since no system can ever be totally secure, the question always remains how much security and preparedness is enough. It does not take much to see that a government may have higher standards of security and emergency preparedness than the market would be willing to contribute on its own accord.

In short, while in theory, individuals and companies in a liberalized economy have strong incentives to provide effective emergency preparedness and crisis management, in reality, private motivation is unlikely to be sufficient to provide an optimal amount of emergency preparedness for society as a whole. There are several reasons why private actors are unlikely to respond to current and expected risks in the provision of emergency preparedness measures in a manner that is sufficient for society as a whole in a liberalized economy. The most important of these reasons are associated with market failures, imperfect information, and moral hazard. We will examine these reasons in more detail before discussing why some form of government intervention is necessary to ensure an optimal level of emergency preparedness for society as a whole.

Market Failures

One reason why private actors are unable to supply adequate national emergency preparedness is because the latter is a public good.[7] If one citizen is protected by national emergency preparedness, no other citizen is less protected. The problem with emergency preparedness (like all public goods) is that once it is

6 University of Texas, Texas A&M University Hazard Reduction and Recovery Center, Business Disaster Recovery Study, 2001. http://hrrc.tamu.edu.

7 Goods are public if they are non-rival in consumption. National defense is a classic example of a public good, because if the armed forces defend one citizen, no other citizen is less defended.

produced, the marginal cost of consuming it is zero. Hence, the price of this good should also be zero. However, if the good is costly to produce, no private firm will produce it, since it can not charge consumers for it. In a free market, private actors will undersupply non-excludable public goods.[8] Since national emergency preparedness measures are a non-rival good and costly to supply, private actors will undersupply them in a liberalized market.

Negative externalities constitute a second reason why markets fail to provide national emergency preparedness measures against large crises. An externality is an effect of actions of an individual that affects the welfare (utility) of others.[9] For example, a poorly maintained power grid can lead to a major power outage. However, the full cost to society that follows from a major power outage is not borne by the power grid operator alone. Hence, power grid operators will not consider the full effect on society as a whole when they decide on the appropriate level of emergency preparedness. As a result, the market rate allocates resources inefficiently.

In general, a negative externality can also arise whenever the emergency preparedness of a firm is adversely affected by poor emergency preparedness on the part of another firm. Such interdependent security problems can lead to "contamination effects", and the lack of appropriate behavior of other firms may affect the willingness of a company to reduce its exposure to risk.[10] In such a case, private actors will under-invest in emergency preparedness and crisis management measures that would be desirable for society as a whole. Private actors deciding how to best prepare for large scale emergencies and crises are unlikely to take the external costs of such an event fully into account. They will therefore generally provide an inefficiently low level of preparedness against major emergencies and crises on their own. Without government involvement, private actors will thus generally under-invest in emergency preparedness and crisis management measures.

8 If public goods are excludable, they will be underutilized. Przeworski, Adam. States and Markets (Cambridge: Cambridge University Press 2003), p. 32.

9 An externality is positive if the action of an actor increases the welfare of other individuals. An externality is negative if the action reduces the welfare of others.

10 See: Kunreuther, Howard, and Geoffrey Heal. Interdependent Security. Journal of Risk and Uncertainty Vol. 26, (March/May 2003), pp. 231–249; Kunreuther, Howard, Geoffrey Heal, and Peter Orszag. Interdependent Security: Implications for Homeland Security Policy and Other Areas. Policy Briefs #108 (Brookings Institution, October 2002).

Imperfect Information

A third reason why the market will be unable to provide the "appropriate" level of emergency preparedness for society as a whole is a lack of perfect information. If information is not perfect, the market is incomplete and inefficient.[11]

It is costly and extremely difficult to accurately evaluate emergency preparedness measures. To do so successfully would require active and consistent collection, analysis, and dissemination of information on current and future risks. It would also require continuous assessment of current emergency preparedness levels in society as whole, in order to create an awareness and verify that implemented emergency preparedness measures lie within the "zone of adequacy". However, neither individuals nor individual companies have the resources or knowledge to evaluate the optimal level of emergency preparedness for major national crises. Arguably, only national governments have the resources to actively and consistently collect, analyze, and disseminate information on current and future risks as well as the current security level in order to stimulate and verify that it lies within the "zone of adequacy". In a situation without any government regulation or minimum standards, it is likely that private actors will under-invest in emergency preparedness and crisis management measures.

Moral Hazard

A fourth reason why private actors will not provide "adequate" emergency preparedness measures is moral hazard. Many companies are unwilling to assume the costs for implementing necessary emergency preparedness measures because they expect the government to bail them out in the case of a major emergency or crisis. There are numerous examples of governments picking up the bill for private industry after major crises. For example, government assistance has been extended to struggling banks in many countries, and the airline industry received massive financial aid after the attacks on 11 September 2001. If the government is unable to credibly commit itself to not bailing out the private sector after a major crisis, it will create a moral hazard. If private firms

11 Greenwald, Bruce C., and Joseph E. Stiglitz. Externaltities in Economies with Imperfect Information and Incomplete Markets. Quarterly Journal of Economics. Vol. 101 (1986), pp. 229–264; Stiglitz, Joseph E. Whither Socialism? (Cambridge, M.A.: MIT Press 1994), chs. 3–4.

expect the government to pick up the bill, they will under-provide emergency preparedness measures.

Moreover, bankruptcy laws limit individual and corporate financial liability for the effects of major crises. Thus, private actors have little incentive to prepare for large-scale emergencies and catastrophes. If a major crisis would lead to losses exceeding a private firm's net assets, and the government refuses to bail it out, the firm would simply declare bankruptcy. Since the outcome of a major crisis for a firm's owner does not vary beyond bankruptcy, the firm has little or no incentive to reduce the effects of the most severe kinds of crises by improving its emergency preparedness, even if the required steps were relatively inexpensive and would greatly benefit society as a whole.

The importance of each of these reasons may of course vary from case to case. However, the fact remains that in a deregulated economy, the market will in general under-provide emergency preparedness measures. At the same time, in a modern society, uninterrupted energy supply, communication, transport, financial services, and health care must be guaranteed at all times.

The Role of Government

National defense is the sole responsibility of the government, but who is responsible for "homeland defense"? In a non-liberalized economy, the state assumes both the responsibility as well as the costs of guaranteeing critical infrastructure systems and services to ensure societal security and public safety. It is more difficult to assign a clear responsibility for securing such systems and services in a liberalized economy, where most of the critical infrastructures are in private hands. Given the importance of the private sector in providing societal security and emergency management, it is paramount to establish where and when private-sector responsibility for societal security and public safety ends, and where and when government responsibility begins. Who should implement and pay for the protective measures that have to be taken to ensure societal security and public safety? Which measures should be the responsibility of national and local governments and which the responsibility of the private sector? Finally, how does the internationalization of markets and services affect these issues?

While the liberalization of previously government controlled sectors and markets — such as energy and communications — has in many cases improved

efficiency and productivity, it has also led to concerns regarding the accessibility, equality, reliability, and affordability of services. Moreover, the privatization of public monopolies, infrastructure networks, and the deregulation of service provision have important implications for national emergency preparedness and crisis management. While costs may have been reduced, redundancies and reserve capacity have also been reduced.[12] Governments no longer have the reserve capabilities, resources, or manpower that were once at their disposal for managing major crises, and private companies are unable and unwilling to assume full responsibility.[13]

Market forces do provide some incentives to firms to avoid the direct financial costs of disruption of their operations due to crises and unforeseen events. All private firms are responsible to their shareholders for operational business risks and have to prepare for contingencies and emergencies. However, in general, market incentives are not compelling enough for private actors to provide the appropriate level of security for society as a whole. To survive in a market-driven economy, companies need to minimize costs and maximize profits. Keeping reserve stock, maintaining redundant systems, and employing back-up staff all cost money. With pressure to cut costs, less resources are available for contingencies and crisis management. Bankruptcy laws and moral hazard further limits the extent to which private actors are willing to extend their emergency preparedness and crisis management capabilities.

The diminishing role of the state in the provision of energy, communications, and financial services, in combination with the need of private companies to minimize costs and maximize profits, create what we describe as a gap between government emergency preparedness measures (which, of course, vary across sectors) and private actors' lack of interest in providing sufficient such measures for society as a whole. This gap is illustrated in figure 1 below.

12 See, for example: Boot, P., et al. European Energy Markets: Challenges for Policy and Research (The Hague: Ministry of Economic Affairs, 2003).

13 Armed forces reductions in many countries have further diminished governments' capability for ensuring societal security, public safety, and emergency management.

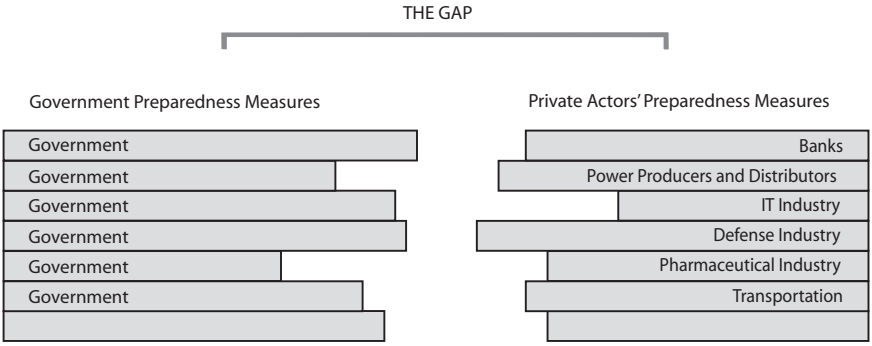


Figure 1: Minding the Gap
Source: Adapted from Andreas Malm, Klas Lindström, & J.J. Andersson, "Finansiella sektorns motståndskraft mot infrastrukturella störningar av samhällshotande art" [Resilience in the Financial Sector]. Report. Stockholm: Finansinspektionen 2003.

The gap between government and private actors' emergency preparedness measures indicates that market incentives are not enough to provide sufficient societal security. Since the market is unlikely to close the gap by itself, the government must "help the market work" by altering the incentive structures to close the gap.[14] While market forces are potent, one must remember that over-reliance on markets is just as dangerous as over-reliance on the powers of direct regulations. In short, markets by themselves do not provide adequate incentives for private actors to invest in societal security at warranted levels.

In order to ensure appropriate emergency preparedness for society as a whole in major crises, some form of government intervention will be necessary in certain markets. However, government intervention does not necessarily imply massive state-led intervention or government takeover of critical infrastructure. The need for some type of government intervention to ensure adequate levels of societal security and emergency preparedness for society as a whole does not determine how or in which situations the government should intervene.

14 For a similar conclusion, see: Orszag, Peter R. Testimony before the National Commission of Terrorist Attacks Upon the United States, November 19, 2003.

Closing the Gap

In principle, there are three ways in which the gap in emergency preparedness between public and private actors could be closed. The first alternative is legislative regulation, the second alternative is to use economic policy instruments, and finally, the third alternative is to turn to PPPs. We will discuss each alternative in turn.

Direct Regulation

Knowing the tendency of private actors to under-invest in emergency preparedness measures, the government could use its legislative power to close the gap by simply forcing the private sector to adhere to certain minimum standards. The government could, for example, impose direct regulation requiring private actors to adopt certain emergency-preparedness features, such as diesel-powered back-up generators and separate data and telecommunication links. Another regulatory option for the government would be to require private utility and service providers to carry insurance against major crises and catastrophic events. Such an insurance requirement would then lead insurance companies to provide incentives for utility operators and service providers to build more robust systems.

The argument for regulation is that it will provide a uniform level of emergency preparedness (assuming that the regulations are followed and enforced) across society as a whole. However, the benefit of regulation must be weighed against its potential costs.[15] A "perfect" government would certainly be able to improve societal security, public safety, and emergency preparedness by imposing the right kind of regulation to counteract negative externalities and moral hazard. In reality, however, it is less clear that governments would be able to do so. All regulators face the problem of imperfect information and must regulate under uncertainty. For example, how will we know that the mandated

15 Lafont, Jean-Jacques and Jean Tirole. A Theory of Incentives in Procurement and Regulation (Cambridge, M.A.: MIT Press, 1994); Baron, David T. The Economics and Politics of Regulation: Perspectives, Agenda, and Approaches. In: Modern Political Economy, edited by Jeffrey S. Banks and Eric A. Hanushek (Cambridge: Cambridge University Press, 1995); Spiller, Pablo T. Regulatory Commitments and Utilities' Privatization: Implications for Future Comparative Research. In: Modern Political Economy, edited by Jeffrey S. Banks and Eric A. Hanushek (Cambridge: Cambridge University Press, 1995).

emergency preparedness measures are set at the "right" level for maximum social welfare?[16] Any form of regulation has distributional consequences, with some gaining and some losing. Different interest groups will therefore seek to influence the government to regulate in their favor. Moreover, while regulation may motivate firms to meet the minimum mandated standards, there are no incentives to exceed these standards. Legislation may also impede innovation in finding new and less costly ways to improve emergency preparedness measures. Finally, the cost of these measures will undoubtedly be passed on to the customers and users.

While many of the negative aspects of any legislation can be avoided by careful attention to its design, the potential for regulatory mistakes is considerable, especially in innovative and rapidly changing sectors such as IT and financial services.[17] The international dimension must also be considered. Internationalized markets and transnational information and communications networks pose considerable challenges to the autonomy and effectiveness of national governments in regulating domestic problems. Given the problems of imperfect information, distributional consequences, and international markets, it is unlikely that governments will prefer regulation as the primary option in ensuring appropriate emergency preparedness across society. Private firms, in turn, will most likely consider regulation to be the *least* desirable form of market intervention to correct the under-supply of emergency preparedness.

Economic Policy Instruments

The government may use economic policy instruments, rather than legislative constraints, to encourage the private sector to invest in emergency preparedness measures voluntarily. If designed appropriately, economic policy instruments – such as direct government subsidies or tax incentives – could affect companies' behavior and improve emergency preparedness. It is likely that different types of incentives will be the preferred choice for private actors, since this model would allow them to improve their emergency preparedness measures on their own terms while avoiding both costs and government control.

16 A standard for emergency preparedness suitable for, say, power grid operators could impose an excessively high standard (which would lead to unnecessary costs) or an excessively low standard (which would lead to insufficient protection) for society as a whole.

17 Malm, Andreas, Klas Lindström och Jan Joel Andersson. Finansiella sektorns motståndskraft mot infrastrukturella störningar av samhällshotande art [Resilience in the Financial Sector]. Report. Finansinspektionen (2003b).

However, in using economic policy instruments, the government faces a trade-off between inducing the firms to behave in the desired way and offering them some socially costly rewards. In fact, economic policy instruments – such as direct subsidies and tax breaks — will likely be the least appealing alternative for governments. If the monetary incentives are too generous, they will encourage unnecessarily costly improvements and the government will pay for unnecessary security (gold plating). On the other hand, if the economic incentives are too small, the private sector will ignore the offer.[18] In short, the government will spend money (directly or by tax breaks) with little control over either process or outcome.

Public-Private Partnership

Given the problems of ensuring adequate levels of emergency preparedness in society by direct regulation or economic policy instruments, PPPs provide a solution that seems to satisfy both government and private actors. Arguably, the organizational principle of the PPP is appropriate for addressing the tension between market forces and non-market forces in the provision of societal security, public safety, and emergency management.

PPPs have a long history and tradition.[19] There are many definitions of PPP, and scholarship on this subject is increasing. In this paper, we adhere to the definition of PPPs as "voluntary cooperation between public and private actors on a common project."

PPPs are rapidly gaining popularity as a form of governance in many areas of society. There are several reasons for this development. Partnerships are seen by both public and private actors as the most effective way of reaching their goals. The basis for any partnership is structural cooperation between equal parties in which both sides gain. For the government, PPPs provide a way of engaging the private sector in public affairs and a means of establishing guidelines and standards without having to resort to regulatory means of "command and control". PPPs are also preferred to direct subsidies or tax incentives because they allow the government to maintain a certain degree of

18 Another reason why the private sector may ignore such an offer is that the government often would want to renege on the promises it makes once the firms do what the government wants them to do. If the private sector suspects this, then the economic policy instruments are not credible. Przeworski, op. cit., p. 101.

19 Davis, op. cit.

control. For private actors, PPPs offer a flexible way of meeting government requirements while avoiding regulation.

However, despite the general consensus on the positive aspects of the PPP model, we argue that for various reasons, it may be an unreliable and unpredictable way of closing the gap in national emergency preparedness and crisis management in deregulated sectors of the economy. It is difficult to achieve tangible results with PPP. The main problem lies in implementation. It is relatively easy for government and private actors in a PPP to agree on the existence of a problem and on the need to resolve it. It is, however, much harder to agree on what should be done about it, who should be responsible for implementing the solution, who should assume legal responsibility for potential damages, and who should bear the costs of implementing countermeasures. Closing the gap in the provision of emergency preparedness measures requires clear guidelines and recommendations, consensus among actors, time, and money.

By refraining from imposing regulation and engaging in PPPs, the government passes on the responsibility for implementation and costs to the industry. The industry, in turn, will be reluctant to accept the responsibility and costs without clear guidance and economic compensation. Without clear guidance and money from the government, there is a distinct possibility that private actors simply participate in PPP as a means to deflect attention from insufficient emergency preparedness measures and to avert outright regulation. The government's and the private sector's respective order of preference concerning alternatives for closing the gap is illustrated in the figure below, where 1 indicates the most favored solution, 2 the second choice solution, and 3 the least-favored solution.

		Alternatives		
		Direct Regulation	Economic Policy Instruments	Public-Private Partnership
Actors	Government	2	3	1
	Private Sector	3	1	2

Figure 2: Closing the Gap
Source: Adapted from Jan Joel Andersson, "Public-Private Partnerships and Emergency Preparedness," paper presented at the conference on National Deregulation and European Reregulation, organized by the Stockholm Centre for Organisational Research, Stockholm, 27 February 2004, p. 8.

In the following sections, we will draw on some of our previous work on PPPs in the financial services and energy sectors to illustrate our argument.[20] In doing so, we will compare and contrast our experience from Sweden with the work that has been undertaken by others in the UK and the US.

Cases: Financial Services and Energy

Resilience in the Financial Sector

The importance of functioning financial systems cannot be overstated in today's global economy. The 11 September 2001 attacks severely disrupted US financial markets, resulting in the longest closure of the stock markets since the 1930s and severe settlement difficulties in the government securities market, but the

20 Malm, Andreas, Jan Softa, Jan Joel Andersson och Klas Lindström. IT och sårbarhet - kritiska beroendeförhållanden i den nationella IT-infrastrukturen. Temaserie 2003:5. Stockholm: KBM (2003); Malm, Andreas, Klas Lindström och Jan Joel Andersson. Kritiska beroendeförhållanden i den nationella IT-infrastrukturen. Opublicerad rapport. KBM (2003a); Malm, Andreas, Klas Lindström och Jan Joel Andersson. Finansiella sektorns motståndskraft mot infrastrukturella störningar av samhällshotande art [Resilience in the Financial Sector]. Report. Finansinspektionen (2003b); Malm, Andreas, Klas Lindström, Jacob Henricson, Jan Softa and Jan Joel Andersson.. Hel Projektet, Dokumentation från samverkansseminarium 23–24 oktober 2003. Unpublished manuscript. Energimyndigheten (2003c).

risk of major operational disruption is not a new threat to financial systems.[21] Both naturally occurring and man-made events over the last 30 years have clearly demonstrated the need for actors in the financial markets to plan for business continuity in case of major crises and disruptions. In comparison to other sectors, the financial market demonstrates a pattern of primarily market-driven adjustments to credit, market, and operational risks.[22] While events such as the 2001 terrorist attacks against the US do not change the basic view in most countries that primary responsibility for managing operational disruption lie with the financial markets, the catastrophic nature of such events has led several governments to examine whether there is a need to modify existing policy instruments to mitigate the effects on society of operational disruption in the financial markets due to major crises.[23]

In order to analyze the appropriateness of any policy instruments, it is necessary to first identify the key features of the market in which the policy instruments will be applied. Financial markets are characterized by some unique characteristics:

- Financial markets are global in nature today. Economic and technological interdependencies have created markets that exceed the scope of national sovereignty. For example, financial contracts increasingly straddle international borders and transactions often involve multiple jurisdictions. A business deal in London between a US and a UK bank could be carried out over the Amsterdam stock exchange, cleared through Clearnet in Paris, and settled in the Netherlands with payment made via a TARGET transfer.[24] Consequently, few financial market problems can be resolved by unilateral action by a single government. An attempt to assert public powers, which would bear on the

21 US Government Accountability Office, GAO-03-251: Additional actions needed to better prepare critical financial market participants, 2003.

22 In general terms, credit risk is the risk that a bank's customers will not repay their loans. Market risk is the risk that a bank will suffer losses due to changes in exchange rates, interest rates, investment costs etc. Operational risk is the risk of unexpected financial losses, which arises from breaches in internal controls, processing errors, inadequate information systems, fraud, or unforeseen catastrophes.

23 See for example: UK Report of the Taskforce on Major Operational Disruption in the Financial System: Do we need new statutory powers? (December 2003).

24 Even this relatively simple transaction involves interconnected contracts under the laws of a number of different countries.

single jurisdiction of a country, could in fact lead to more problems than it would solve.

- Financial markets are large and complex. These facts suggest that those closest to the markets are likely to be in a better position to understand the impact that a decision in one area might have on others.[25]
- Financial markets are characterized by rapid structural change. One consequence of the rapidly changing structure is that any regulatory or statutory response from public authorities is at risk of becoming quickly outdated.
- Financial markets immediately react to events. In order to parry any market reactions, decisions have to be taken in a flexible manner.

Given the global nature, complexity, and uncertainty that characterize financial markets, British, US, and Swedish public authorities have concluded that although governments have an important role to play, the primary responsibility for dealing with operational disruptions should rest with the actors in the financial markets. The actors in the financial markets have themselves supported this view.[26] In the UK and the US, governments have concluded that no additional statutory powers are needed as a consequence of 11 September 2001 to safeguard the functioning of the financial markets in case of major crises.[27] In Sweden, the government has followed the Anglo-Saxon model and has refrained from imposing any new statutory powers to safeguard the functioning of financial markets in case of major crises. However, the lack of new statutory powers does not imply that national governments are doing nothing. It simply means that other policy instruments have been employed.

The US government has, for example, adopted an Interagency Paper on Sound Practices to Strengthen the Resilience of the US Financial System. This paper appears to have focused market infrastructures' attention on planning for wide-scale disruption.[28] In September 2003, the Securities and Exchange Commission (SEC) issued a policy statement suggesting that specific "business

25 See for example: McKinsey & Company's Banking & Securities Practice — Experiences from 9/11 terrorist attacks (November 2001).
26 UK Report of the Task Force, op. cit.
27 Ibid.
28 Press release available at: http://www.federalreserve.gov/boarddocs/press/bcreg/2003/20030408/default.htm, accessed on 21 April 2004.

continuity planning principles" should be applied to certain trading markets.[29] On 7 April 2004, the SEC approved rules proposed by the National Association of Securities Dealers (NASD) and the New York Stock Exchange (NYSE), which require NASD and NYSE members to develop business continuity plans that establish procedures relating to an emergency or significant business disruption.[30] Similar guidelines and rules have been devised in the UK and are under development in Sweden.[31] Such principles are also being discussed internationally in the G10 Central Bank Governors' Committee on Payment and Settlement Systems (CPSS) and within the European System of Central Banks (ESCB). For example, the CPSS' Core Principles for Systemically Important Payment Systems and the CPSS/IOSCO Recommendations for Securities Settlement Systems both address the importance of business continuity and the need for appropriate contingency arrangements. Furthermore, the principles for capital coverage of operational risks that will be introduced under the new Basel and EU Capital Adequacy Standards have strengthened and highlighted the importance of business continuity within financial firms.[32] The former case is particularly interesting, since it ties risk management to annual accounts and thus forces firms to reconcile their accounts by including operational risks in their calculations.

However, in practically every case of direct regulation, individual firms and senior management remain responsible for developing business continuity plans and selecting and estimating those operational risks that will be financially covered, which will prove to be a challenge for the supervisory role of authorities such as FSA, SEC, and Finansinspektionen.[33]

29 Policy statement available at: http://www.sec.gov/rules/policy/34-48545.htm, accessed on 21 April 2004.

30 File Nos. SR-NASD-2002-108 and SR NYSE-2002-35.

31 See, for example, FSA handbooks on operational risks and business continuity such as the FSA Consultation Paper 142. Finansinspektionen was expected to release guidelines in 2004.

32 Although the details of the accord, to be introduced by 2007, are still being worked out, central banks and banking sectors as a whole have commenced seminars and debates on the details of the accord as well as the impact it will have on banking in the future. The US Federal Trade Commission's (FTC) proposed regulation, which will require financial service companies to protect their networks against "anticipated threats" and generally take measures to protect their information, may have a similar impact.

33 For example, the Financial Services Authority (FSA) confirmed in 2003 that it would maintain its non-prescriptive approach to business continuity arrangements by financial firms as outlined in FSA Consultation Paper 142.

Although the primary responsibility for managing operational risk remains with the market, recent catastrophic events such as the terrorist attacks of 11 September 2001 have led the FSA, SEC, and Finansinspektionen to elaborate high-level business continuity planning principles for firms critical to the functioning of the financial system in the specific areas of recovery times, and testing of business continuity arrangements and their preparedness for dealing with legal issues on major operational disruptions. This elaboration requires the cooperation of market actors. Due to the problems associated with detailed direct regulation to provide appropriate emergency preparedness measures in the financial sector, PPPs have emerged as the preferred solution for many governments.

In the financial sector, cooperation between public authorities and the private sector has traditionally been conducted on an informal basis, primarily to facilitate the supervisory roles of authorities such as FSA, SEC, and Finansinspektionen. Furthermore, in countries where antitrust laws are less stringent than in the US, such as the UK and Sweden, informal cooperation between private market actors on security issues has been highly developed, and in some cases well organized, for many years.[34] There are several reasons for this. The most important is the view among the key actors that security is not a factor to be used for competition purposes.[35] Among actors, recent major crises have also highlighted the need for a more developed cooperation and coordination of emergency preparedness and crisis management. For example, one clear lesson from the events of 11 September 2001 was that the "extraordinary levels of cooperation by market participants" helped overcome shortcomings in individual firms' business continuity planning.[36] The established cooperation between private market actors, and between public authorities and market actors has, quite naturally, facilitated the development of PPPs on issues related to security and emergency preparedness in the financial sector. Hence, there are several examples of PPPs under development throughout the countries under consideration.

34 For example, through organizations such as "Bankföreningen" and "Försäkringsförbundet" in Sweden.

35 This trend appears to be shifting in terms of low-level security issues. Increasingly, client and transaction security are used competitively by key actors in financial markets.

36 Federal Reserve, New York State Banking Department, Office of the comptroller of Currency, Securities and Exchange Commission. Summary of 'lessons learned' and Implications for Business Continuity (13 February 2002).

In the US, the Financial and Banking Information Infrastructure Committee (FBIIC) is chartered under the President's Working Group on Financial Markets, and is charged with improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting the concept of public-private partnership.[37] The FI-ISAC and the National BankNet under the Office of the Comptroller of Currency (OCC) constitutes one form of an information sharing partnership launched as a result of the recent emphasis on "Homeland Security".[38] In the UK, following the events of 11 September 2001, the Standing Committee (composed of representatives of the UK's financial authorities: HM Treasury, the Bank of England, and the Financial Services Authority) set up a sub-group on resilience and contingency planning to co-ordinate the work being done by the authorities and by other bodies in this area. Recognizing that the primary responsibility for contingency arrangements lies with the private sector, the authorities' aim was to share information and facilitate work to address any overlaps or gaps.[39] Furthermore in the UK and the US, market participants as well as public authorities are considering the establishment of a single organization that would become the focal point for both ex-ante preparations for major operational disruptions and ex-post responses. Although it has not developed into a full-scale PPP yet, Finansinspektionen in Sweden is pushing for increased cooperation between market players and public authorities to improve resilience in the financial sector. At the international level, we note that much work is also being done in this area, including, for example, the development within the EU of a Memorandum of Understanding on high-level principles of co-operation between banking supervisors and central banks in crisis management situations.

In short, work in the US, the UK, and in Sweden points towards a more cooperative framework for dealing with business continuity in the financial markets, thus supporting our theoretical argument. Our experiences from working with emergency preparedness issues in the financial sector in Sweden also support the predictions of our model.

37 Done to a large extent in cooperation with the Federal Deposit Insurance Corporation (FDIC)

38 The OCC ensures a safe, sound, and competitive banking system that supports the citizens, communities, and economy of the United States.

39 The Committee work under a Memorandum of Understanding (Financial Stability: Memorandum of Understanding), towards the common objective of financial stability. As set out in that MoU, there is a tripartite Standing Committee on financial stability, comprising senior representatives of the three authorities. This meets monthly to consider issues relevant to financial stability.

In Sweden, market actors demonstrate a growing interest in cooperation concerning high-level security issues, i.e., issues beyond the reach of separate financial institutions in terms of the existing risk management policies. In terms of national security issues, market participants want a single point of contact and guidelines. Furthermore, while all the major private actors in the Swedish financial market realize the importance of high levels of emergency preparedness and acknowledge that they have a certain responsibility for providing this preparedness, they are opposed to direct and detailed government regulation, rules, and standards. The main arguments are that:

- Standards would be hard to keep up to date;
- The specific circumstances of each infrastructure necessitate flexibility;
- It would be difficult to strike the correct balance to ensure standards were neither too prescriptive, nor so vague as to be worthless;
- The standards would need to be extremely far-reaching to be effective, which would be difficult to achieve.

As an alternative to regulations, rules, and standards, market actors naturally find PPPs attractive and thus promote their development. However, we can already identify several difficulties in this developing public-private partnership, such as:

- The sharing of information;
- The supervisory vs. advisory role of the government;
- The financing of market infrastructure improvements.

On the basis of work in the US and the UK and of our experience in Sweden, we may conclude that PPPs are being promoted by governments as a solution to "bridging the gap" in the provision of emergency preparedness in the financial service sector. However, within the developing PPPs, several key issues are outstanding. While the exact list of issues will vary from country to country, let us explore the ones mentioned above a bit further:

- The sharing of information. An effective PPP requires sharing of sensitive information. How can private actors be assured that sensitive information regarding their emergency preparedness does not reach

unauthorized users or competitors? In Sweden, for example, the Freedom of Information Act makes it difficult for government agencies to engage in a PPP for information-sharing with the financial sector.
- The advisory vs. supervisory role of the government. The dual role of the government as both advisor and supervisor makes for an unbalanced partnership.
- The sharing of cost for improving emergency preparedness. Who will foot the bill for agreed emergency preparedness measures?

For PPPs to succeed in the financial services sector, these types of issues must be resolved.

Robustness in the Energy Sector

The importance of energy, and in particular electricity, has been underlined by recent major black-outs in North America (eastern Canada; north-east US) and Europe (Italy; south-east England; southern Sweden and eastern Denmark). The costs of a failure of supply in electricity to industry, commerce, and the individual are difficult to fully estimate, but are measured in billions of US dollars of lost output.[40] The social consequences of any failure to supply are potentially even greater.[41] Ensuring the security of energy supply is of central importance to the public interest. It is a crucial underpinning of economic performance and of the quality of life.

The energy sector has recently been liberalized in several countries. When energy market liberalization gathered pace from the late 1980s, energy security still mattered, but seemed initially to need little attention — world fossil fuel markets were slack and there was substantial surplus capacity in the electricity and gas supply industries.[42] However, since the end of the 1990s, attention has focused sharply again on security of supply. Several highly publicized major blackouts (Auckland, Montreal) in combination with increasing international conflicts in important oil-producing regions (The Caspian Sea Region, Central

40 UK Department of Trade and Industry. Cm.5761 White Paper: Our Energy Future – creating a low carbon economy (February 2003).

41 An extended loss of power during a severe winter in Northern Europe or North America could prove catastrophic.

42 Priddle, R. Security of Supply in Liberalized Electricity Markets. Eurelectric Annual Convention (Leipzig, 24–25 June 2002).

Asia, and The Gulf Region) sparked new interest in energy supply and security issues.[43] Other important stimulants of this renewed interest were California's major power crisis and the "fuel protesters" crisis in the UK which came close to shutting down the gasoline distribution network.[44] Moreover, the rise of international terrorism has drawn attention to the vulnerability of energy network infrastructures and production facilities.

A number of factors that are unique to the energy market must be taken into consideration, for instance:

- Electricity is difficult and expensive to store. To meet peak demand, an equivalent amount of generating capacity must exist; and in practice, an extra reserve is required in the event of breakdowns or exceptional levels of demand.
- Some energy markets are geographically constrained — for example, the UK has relatively few international interconnections for gas and electricity supplies, limiting the ability of actors to respond quickly to a shortage by importing energy from abroad.
- An energy market is characterized by relatively low flexibility of prices (meaning that in the short term, very high prices might be necessary to balance supply and demand in response to a supply shortage; this effect was seen in the 1970s oil crises)
- Long lead times and high capital intensity are typical of many energy development projects, which in turn constitute barriers to entry for new actors in an energy market.
- The concentration of world hydrocarbon resources, in particular, in certain countries, that allows those countries to exercise some degree of market power.

These are all reasons why, in view of the over-riding importance of energy security, national governments have a responsibility to ensure adequate levels of energy security. However, none of the governments in the US, the UK,

43 See, for example: Boot, P., et al. European Energy Markets: Challenges for Policy and Research (The Hague: Ministry of Economic Affairs, 2003); Newlove, Lindy, Eric Stern, and Lina Svedin. Auckland Unplugged: Coping with Critical Infrastructure Failure (Baltimore: Lexington Books, 2003).

44 See article in San Francisco Chronicle: http://www.sfgate.com/cgibin/article.cgi (accessed 6 April 2003).

or Sweden believe that these potential complications necessarily present an insuperable problem within a market framework. Quite on the contrary, these governments seem to believe that extensive direct and detailed regulation could hamper the policy objectives of security, efficiency, and environmental sustainability. They refer to several reasons, such as:

- Policies to control consumer costs, protect the environment, tax and subsidize industry, and maintain reliable service all interact with one another. Hence, measures taken to solve one problem may worsen (or ameliorate) another problem: e.g., simply reducing oil use may increase global oil dependence by reducing oil prices. An obvious current example reflecting this complex relationship is the debate on long-term contracts on gas supply within the EU.[45] First, the European Commission wanted to prohibit these contracts. Now, the commission is expected to conclude that long-term contracts are indispensable for security of supply and that a minimum percentage of long-term contracts is therefore required in the directive on security of supply for gas. This confusion has lasted for almost two years now, and has reduced predictability, which is an important factor in the market.[46]
- Both within and across nations, consumers, industry, governments, and international organizations make interrelated choices. The fragmentation of power among localities, states, and the federal government, the fragmentation of jurisdiction among agencies of the federal government, and perhaps even the constitutional separation between the legislative and administrative branches of government, make it difficult to devise and implement integrated solutions to large-scale problems.
- Infrastructure resiliency improvements need not take a full generation, though substantial restructuring would. Significant reductions of oil dependence would take decades preceded by substantial public investments; costs accrue early, benefits later. In many cases, the political system seems unable to address these large, long-term problems. The actual power plants of any domestic energy infrastructure only reach

45 Long-term contracts have traditionally provided the necessary incentive for new energy generation in many European countries. However, the contracts have added inertia to the pricing mechanism.

46 Boot et al., op. cit.

turnover after decades of operation, and there is a low public-political perception of need for change. Election cycles, changes of administration, and voter behavior do not reward continuity and long-term investment.
- Vulnerabilities vary across energy types. Event consequences may be local, regional, national, or international, and therefore blur divisions of responsibilities.

The experience of regulatory initiatives clearly illustrates the intrinsic difficulties of direct regulation, regardless of whether they are carried out on a national or supranational level. The EC directive and the debate on long contracts, as well as the US experiences of price caps, with adverse consequences in California, clearly demonstrate these difficulties.[47]

In general, therefore, governments look to markets, with appropriate economic incentive structures, to ensure that security of supply is maintained. The basic problem here is that social costs (e.g. security, environmental costs of oil dependence etc) are not internalized by the energy market. Entrepreneurs are more familiar with the financial costs of remedial measures than with intangible future benefits, and in some sectors of the industry, different customers may value security of supply differently. In broad terms, the cost of a failure to supply electricity may not be felt by the electricity supplier whose service has broken down; in the absence of appropriate arrangements and incentives, this cost may be spread over the industry more widely or borne by consumers. This could encourage some companies to freeload, which could cause the industry collectively to take inadequate precautions regarding security of supply. Indeed, there are a number of potential obstacles that may make it difficult for markets to determine and deliver the appropriate level of security. Some of these have frequently been discussed in all three of the countries under consideration, and they normally include obstacles such as:

- Economies of scale and natural monopoly effects;
- Network effects (when a group of customers take their supply from a single pipe or wire);
- Transaction costs;
- The fact that full competition in supply has not yet developed.

47 Directive 2003/54/EC of the European Parliament and of the Council of 26 June 2003. The Economist, How to keep the lights on (August 23rd 2003) p 12.

The impact of deregulation has sometimes been felt in the lack of economic incentives for investments in restructuring for robustness or in taking precautions against attack.[48] In recognition of the obstacles mentioned, most governments therefore wish to remove any potential barriers to the achievement of energy security, and to monitor developments in energy markets to determine whether their security is being put at risk in any way.[49] It may be necessary in specific cases for regulators to set security standards or to take steps to remedy any inability of energy markets to provide satisfactory levels of security. However, past experience shows that this can be best achieved through a process of internalization. However, this approach has already demonstrated some weaknesses, due to the specific character of the energy market.

Various strategies to liberalize domestic markets have resulted in a wide range of national market structures, not only in the countries under consideration, but indeed across the whole of Europe. The overall trend is that dominant and vertically integrated companies from relatively sheltered domestic markets expand abroad, while companies in competitive markets merge at home. The latest developments (for instance, the Eon/Ruhrgas merger) suggest an intensification of this trend: The dominant electricity companies are further increasing their level of vertical integration by taking over gas businesses.[50]

If energy markets proceed along this path, they run the risk of ultimately being shaped by a tight oligopolistic structure, where large companies do not compete over each others' home markets, and which display a high level of vertical integration.[51] In the case of the EU, the situation might even deteriorate if some countries aim to stimulate this tendency, as seems to be the case nowadays.[52] In this context, we need to take into consideration the specific characteristics of the electricity sector and of electricity as a product, which make market power easy to abuse, hard to detect, and difficult to prove. Studies of the Californian energy crisis show significant risks of price increases and of

48 See, for example: Karas, Thomas H. Energy and National Security. Sandia Report, SAND2003-3287, Unlimited Release (September 2003).

49 "Though protecting our energy vulnerabilities will largely be accomplished through the private sector, there is a strong national coordinating and analytical role to be filled by the federal government." US FY 2004 Congressional budget.

50 NERA. Consolidation in the EU electricity sector (London, 2003).

51 Boot, op. cit.

52 In the US case, a higher level of concentration is actually suggested as a potential solution to recent power failures. See, for example: The Economist. Bring me your powerless masses, 23 August, 2003, p 20.

reduced levels of security.[53] Furthermore, today's regulatory authorities judging mergers and acquisitions do not aim to engineer competition in markets, but merely to prevent companies from achieving dominant positions. The security of the energy market is threatened by the difficult combination of a trend towards a high level of concentration in the electricity sector, the specific product characteristics mentioned, the inherent limitations of competition policy, and the possibility of implicit objectives of some states. Hence, although the governments under consideration believe that the protection of energy vulnerabilities will largely be accomplished through the private sector, governments have a strong national coordinating and analytical role.[54]

In the energy sector, therefore, many governments consider PPPs necessary for navigating the difficulties imposed by private-sector ownership of critical infrastructures.[55] The motivation for this is multifold:

- To create an information-sharing framework on threats and vulnerabilities affecting the nation's critical infrastructure for the public and private sectors.
- To define the appropriate level of security necessary to protect critical infrastructures, define the levels of security that markets will achieve, and define the role the government should play in closing the gap between desired and market-achievable security.
- To review existing legislation, government capabilities, and private-sector security requirements, at the federal, state, and local levels, to ensure that (a) resources are adequate to support existing policy requirements, and (b) existing policy requirements contribute to improving economic security.

The US and other governments have even gone so far as to consider implementing a regulatory or legislative exemption to anti-trust rules, which limit possibilities for PPPs, in order to improve security without adversely impacting

53 US Government Accountability Office report for period of May 2000-February 2001.

54 See, for example: US FY 2004 Congressional budget; UK Department of Trade and Industry, op. cit.

55 See, for example: section 1(b) of the 16 October 2001 Executive Order on Critical Infrastructure Protection (EO 13231); UK Department of Trade and Industry, op. cit.; and work performed by "Nationella Styrgruppen för privat-offentlig samverkan" in Sweden.

consumers.[56] However, monitoring and analyzing present security levels is one thing; attempting to establish incentives through PPPs is another matter, which of course once again raises questions of how the public and private sectors should share the costs of improvements and correcting measures.[57]

It would be erroneous to believe that only direct regulation raises questions on how the public and the private sectors should share the costs of achieving adequate levels of security. To a certain degree, the willingness of governments to engage in a PPP with the private sector may open a window of opportunity for cost shifting. We are, in general, concerned about the danger that consumers and markets may overly rely on government "rescue packages" in the event of perceived threats to security. If governments hold out the prospect of intervention whenever "the going gets tough", markets may never be able to provide effective risk management. The interesting question is whether PPPs, considered necessary for correcting imperfect information in the market and for monitoring risks and levels of security in general, in fact open a window for government bailouts. Indeed, our experience from working with the energy market in Sweden points towards this dilemma.[58] In view of the "massive investment in energy production and transportation infrastructure" that will be needed over the coming decade, it is naturally tempting for energy markets to shift costs to the government.[59]

Indeed, there are further complications when trying to establish PPPs to close the gap in the energy markets. Among these are:

- **The concrete nature of work on these issues.** There are underlying conflicts of interest between politics and markets, and between micro-power and mega-power, that will have to be resolved. The security of supply problem may very well resolved by market frameworks that are not promoted by incumbent market players, who will naturally lobby against such solutions. Hence, the concrete nature of work on these issues within a PPP may not be easy to outline.

56 Partnership for Critical Infrastructure Security. Draft paper for critical infrastructure assurance (3 April 2002). http://www.pcis.org/index.cfm accessed 21 April 2004.
57 Karas, op. cit.
58 Malm et al 2003 c, op. cit.
59 OECD 2000.

- **Responsibilities.** Within a PPP, responsibilities may often be blurred in the perception of consumers. Collective responsibility may often lead to no-one taking responsibility for the issues at stake.

Paradoxically, the transition to competitive markets seems to necessitate a greater, albeit carefully circumscribed, role for a regulator. This realization among governments has increased the interest in PPPs as a way forward. Work in the US, the UK, and Sweden points towards a more cooperative framework for dealing with security issues in the energy markets, thus supporting our theoretical argument. However, experience demonstrates that PPPs have problems and difficulties of their own that must be resolved to realize the objective of security of supply in energy markets.

Conclusion

PPPs are rapidly gaining popularity as a form of governance in many areas of society. There are several reasons for this development. Partnerships are seen by both public and private actors as the most effective way to reach their goals. The basis for any successful partnership is structural cooperation between equal parties where both sides benefit. For the government, PPPs provide a means of engaging the private sector in public affairs and achieving guidelines and standards without having to resort to regulatory means of "command and control". PPPs are also preferred to direct subsidies or tax incentives, since a certain degree of control can be maintained. For private actors, PPPs offer a flexible way of meeting government requirements while avoiding regulation.

However, despite the general consensus on the positive aspects of PPPs, we have argued in this paper that such partnerships may be an unreliable and unpredictable way of closing the gap when it comes to issues of national emergency preparedness and crisis management in deregulated sectors of the economy. Our conclusion is based on theoretical as well as empirical grounds. First, it is difficult to achieve tangible results with PPPs. The main problem lies in implementation. It is relatively easy for a government and private actors in a PPP to agree that there is a problem and that something must be done to resolve it. It is much harder, however, to agree on what should be done, who should be responsible for doing it, and who should assume legal responsibility

as well as the financial costs involved in implementing new measures. Closing the gap in the provision of emergency preparedness measures requires clear guidelines and recommendations, consensus among actors, time, and money. In other words, governments and private actors must reconcile responsibilities and costs in the provision of societal security.

The Relevance of International Organizations for the Protection of Cyberspace

By Subimal Bhattacharjee

Introduction

Information communication technology (ICT) has revolutionized lives and societies in many countries. Its reach has been phenomenal in terms of information dissemination, reducing geographical constraints, fostering faster and cheaper communications, and facilitating electronic commerce. Its application today has also given a new dimension to governance. Use of ICT tools has been absorbed into almost every activity in society: work at home, business transactions, governmental operations, service delivery mechanisms, national defense, and activities in the outer space. The unleashing of this revolution has been far more spectacular than the Industrial Revolution of the 19th century. The impact has been faster, more pronounced, and more widespread.

The revolution in ICT, the emergence of the new medium of cyberspace,[1] and its extensive use by different user groups have ushered in the cyber-society. The characteristics of this rapidly emerging society are determined more by concepts of a global village and of global reach than by any classical sociological theory. It is a society that has emerged mainly from IT user groups rather than by stratification along religious, ethnic, or geographic lines. Like the physical environment, cyberspace contains objects (files, mail messages, graphics etc.) and offers various modes of transportation and delivery. Unlike real space, though, exploring cyberspace does not require any physical movement other than pressing keys on a keyboard or scrolling a mouse. It is an accepted fact that change is the only constant characterizing the infusion of technology. But technology has often been an issue of debate. ICT enjoys near-uniform acceptance across different parts of the world in different age groups and beliefs. This form of technology can be understood and accepted by all, hence its tremendous popularity and usage in such a short span of time, compared

1 Cyberspace is the total interconnectedness of human beings through computers and communications without regard to physical geography. William Gibson is credited with inventing or popularizing the term "cyberspace" in his novel Neuromancer in 1994.

to other media like television and radio. Where originally only some specific sectors of society had modernized their working procedures with the help of ICT tools, there is now hardly a single part of society that remains untouched by them.

It is an accepted fact that ICT is becoming an extremely important tool for our survival. We shudder to imagine a society that lacks all the amenities that we have today. Most of these amenities depend on the infrastructures that have been built over the years. These infrastructures are largely critical in nature, as they not only make our life easier, but also provide crucial services that we depend on, for example electricity installations. Today, the whole mechanism of electricity generation, distribution, and management is administered using the SCADA system, which depends on ICT. Without electricity, modern life would be impossible. Many other utilities and essential functions also depend on ICT for their running and maintenance, and interdependence is required for the smooth running of the various critical sectors. In other words, ICT has become indispensable for our survival.

Management of Cyberspace

Cyberspace is complex and is becoming more complex day by day. There are multiple stakeholders who have a role in the management and the smooth running of the internet that is the lifeline of cyberspace. These include governments, technical peer groups, the industry, and the user community. These varied groups have to synchronize their work to maintain the infrastructure, and this in turn gives rise to various management issues. Even the classification of these management issues is quite varied. One group[2] classifies the issues under five headings: infrastructure and standardization; legal; economic; development; and socio-cultural issues. Another group identifies the main areas of management as infrastructure; issues of usage; and development. However, for the purposes of the present discussion, we will address the two basic threads of management parameters: The management of internet resources like domain names, protocols, IP addressing, root servers on the one hand, and the day-to-day running of the internet by internet service providers (ISPs) and content providers. Millions of users, ranging from the ordinary user at home to

2 http://www.diplo.org.

the network administrators of root servers, are also indirectly involved in the management of the medium at various levels. Software and hardware vendors, technical integrators, content providers, and service providers all have a role to play in this process.

Management of Internet Resources

It is worth looking at the historical development of the internet to arrive at an understanding of how its resources are managed. The internet started as a US Department of Defense initiative called the Advanced Research Projects Agency Network (ARPANET) in 1958. Until the 1980s, the project was managed by the Ministry of Defense's Advanced Research Projects Agency (DARPA). Then DARPA assigned the task of address management to Jon Postel, a student of the University of California at Los Angeles affiliated with the Stanford Research Institute (SRI). After some time, Postel found the huge data traffic and naming system unwieldy, and started assigning his work to various groups at the SRI. This arrangement was formally called the Internet Assigned Names Authority (IANA). By 1992, the military and civilian portions of the internet had separated. The National Science Foundation undertook the responsibility of managing the civilian part of the internet and assigned the management of domain name registration to US company Network Solutions Inc. under competitive bidding. Towards the end of NSI's contract, there were pressures to change the existing domain naming system and in 1997, US President Bill Clinton[3] authorized the US Commerce Secretary to privatize the DNS in a way that would increase competition and facilitate international participation in its management. Thus in November 1998, ICANN[4] was designated as the institution to look after IANA functions, which included the assignment of technical protocol parameters, coordination of IP address space allocations, the oversight and implementation of policies for DNS registries and registrars, and oversight of the root server system. ICANN still remains a non-profit entity, although its constitution and functioning have changed frequently over the years.

ICANN is still responsible for DNS management as a contractor for the US government, which retains the overall control. The DNS consists of the 13

3 A Framework for Global Electronic Commerce: http://www.ecommerce.gov.
4 http://www.icann.org.

root servers, top domain servers, and a number of DNS servers located around the world. It is based on two types of top-level domains — generic top-level domains (gTLDs) and country codes (ccTLDs). ICANN is in charge of the overall management of the gTLDs like ".com", ".net", and ".org", which includes setting the cost of registration. The ccTLDs are managed by a variety of national institutions such as academic and technical organizations. ICANN's function has been debated from time to time, and its composition, functions, and accountability have been modified to incorporate these views. A Government Advisory Council (GAC) allows government members to advise the ICANN Board on relevant public policy issues, although it does not have any enforcing powers. However, GAC members have provided quality input and thought leadership to the ICANN Board over the last few years, including those on WHOIS policies, cyber-security, and domain names. One of the major highlights of their endeavor is the document "GAC Principles and Guidelines for the Delegation and Administration of Country Code Top-Level Domains".[5]

The standards for TCP/IP protocol are set by the Internet Engineering Task Force (IETF), the main technical body for all internet-related activities. It focuses on developing security protocols, including public-key infrastructures (PKI). The Internet Architecture Board (IAB) and the Internet Engineering Steering Group (IESG) monitor the development of standards. The World Wide Web Consortium (W3C) develops the applications standards that allow the private routing and management of resources, although it is not involved in the management of technical standards. Its applications are based on the internet protocol (IP). At present, TCP/IP management is broadly confined to two areas — the allocation and distribution of IP addresses and the development of new standards. The distribution of IP numbers is hierarchically organized, and ICANN distributes blocks of IP addresses to the five regional internet registries (RIRs), mostly based on geographical considerations. RIRs in turn distribute these addresses to the ISPs. Other internet-specific entities have been established for the smooth and secure running of the cyberspace. Among these are the Asia Pacific Network Information Centre (APNIC) and the North American Network Operators' Group (NANOG).

5 www.icann.org.

Day-To-Day Administration of the Internet

ISPs are companies that supply internet connectivity to homes and business customers. ISPs support one or more forms of internet access, ranging from traditional modem dial-up to DSL and cable modem broadband service, to dedicated T1/T3 lines. At present, many wireless ISPs are emerging that offer internet access through wireless LAN or wireless broadband networks. In addition to basic connectivity, most ISPs also offer related internet services like e-mail, web hosting, and access to software tools. Many of them also offer services like content filtering and anti-spam filtering. Separately, content providers provide all relevant content either to the ISPs or to the various portals.

All these responsibilities and functions need to function in a highly coordinated fashion. So far, these functions have been undertaken by the private sector, with technical management of the internet infrastructure being confined to the respective countries managing their internet exchanges. At the highest end of this complex management spectrum is ICANN, which is responsible for the allocation of IP addresses and the managing the domain-naming system or the internet addressing system. It is under contract from the US Department of Commerce, which has the final control.

Why Cyberspace Needs Protection

While the proliferation and diffusion of ICT and the rapid growth of cyberspace has brought many advantages, it has also generated a plethora of issues that require attention. Cyberspace has grown in various dimensions, and the interaction of the various stakeholders has brought up questions of governance. These issues are social and economic in nature and cannot be avoided. The internet poses a formidable challenge to governance,[6] creating concerns about the safety and sustainability of the medium. Among these challenges are cyber-attacks and attempts to disrupt networks. Some perpetrators attempt to give a new dimension to traditional crimes by variations in cyberspace. While many early cyber-attacks were carried out by pranksters, the perpetrators have now transformed into organized gangs and syndicates. The internet allows corporations and consumers to conduct their financial transactions online. More and more

6 Center for Strategic and International Studies. Cyber Threats and Information Security — Meeting the 21st Century Challenge (Washington, December 2000).

people are using online banking and make online purchases with their credit cards. This is an opportunity for the hackers to steal money from customer accounts and to disrupt networks. Hacking and network disruptions are not only raising concerns of law and order, but are also causing serious thoughts on network infrastructure. This is directly related to the issue of critical information infrastructures and their protection. CI are also vulnerable to such attacks, and need to be protected under clearly defined security policies. As a result, concerns are being expressed across the user spectrum, ranging from the individual user to businesses and government departments. At all these levels, steps are being taken to stem abuses and confront attacks.

Data protection is very important, and security concerns are growing in view of a rapidly growing industry that often outsources its work to offshore companies. There are constant worries among the outsourcing nations about the security standards and practices in the countries that have taken a lead in outsourcing, so that even stray incidents have raised very strong concerns. The rapidly developing hacking techniques and the threat of more attacks have brought forth the fear that with financing and support from organized crime, hackers could even cripple the very functioning of the internet. In a related scenario, spam — which was previously only considered a nuisance — is being eyed with security concerns because of the gradual blending of spamming techniques with virus writing tools. Today, virus writers are paying spammers to infect computers.

Issues for Protection

In identifying some of the issues that are critical for the protection of cyberspace, we distinguish three broad areas of direct intervention and two areas of indirect intervention:
Direct Intervention:

- Cybercrimes and cyberattacks;
- Security of networks and information systems;
- Critical information infrastructure protection.

Indirect Intervention:

- Data protection and privacy;
- Spamming.

Cybercrimes and Cyberattacks

Cybercrimes and cyberattacks have grown in frequency and sophistication. While a decade ago, hacking may have been primarily the domain of thrill-seekers, it has now become a professional activity where people are paid by organized crime syndicates and terrorist organizations to launch cyberattacks. The tools used most frequently for launching cyberattacks are hacking, unleashing of viruses and worms, phishing, distributed denial-of-service (DDOS) attacks, and website defacements. Apart from technological solutions to confront these attacks, there are legal efforts, including attempts to form a global alliance to combat cybercrime. Legislation outlawing specific and pre-defined activities in cyberspace is a global issue, and all national laws to address such issues needs to be suitably harmonized. At the same time, international cooperation in law enforcement must be fostered, and Interpol should be strengthened.

Security of Networks and Information Security

The security of networks has become too crucial to leave it in the hands of the technology vendors who run or maintain these networks. Their smooth functioning should be of equal concern to governments and law enforcement agencies because of the sheer amount of critical data that is stored and transmitted using critical infrastructure. Information security has become critical factor, and so a standardized approach to information security may not be the right solution to address network security holistically. Many stakeholders have important roles and responsibilities in implementing policies and strategies suitable to mitigate their risks. Healthy public-private partnerships are also desirable and promising model for the future. There is a need for raising the awareness and education of all stakeholders, and governments have a major role to play in this area as well.

Critical Information Infrastructure Protection

CIIP is vital for the protection of cyberspace. Many sectors are critical for our survival, and almost all of them depend on robust networks. Most of the advanced nations have defined a CIIP policy defining the critical infrastructures, and their protection strategy is set based on the levels of interdependencies and the nature of operations. These CIIP policies have generally covered the sectors of electricity, communications, transportation, health, and energy.

Data Protection and Privacy

Data protection has become very important in cyberspace. With the increasing outsourcing of work, particularly to offshore locations gaining momentum, the need for secure data storage and transmission has become more urgent. Private data is very sensitive, and the phenomena of identity theft and third-party stealing of data have made all stakeholders realize the need for stringent protection measures. There have also been reports of harassment and extortion attempts using stolen private data. Thus, privacy has become a very important issue in cyberspace. The internet allows easy tracking of and snooping on individuals. Currently, the protection of privacy is covered by national laws. Expectations and rights of privacy protection are often subject to exceptions for reasons of public policy, national security, political expediency, or law enforcement.

Spamming

Spam or unsolicited bulk mail has caused havoc for some time now, and has assumed serious proportions with the blending of spamming with virus writing techniques. Not only does spam mail clog up networks; the occurrence of these unwanted e-mails is now beginning to have serious financial implications. Almost 70 per cent of all e-mail in circulation today is spam, and laws have been passed to control it. As far as spam is concerned, there is a contradiction between the nature of the internet, which has generally been open and free, and the desire of e-mail users to be free from unwanted commercial solicitations. The fact that the cost of sending e-mails is independent of the number of messages sent only encourages marketers to send out as many copies of their e-mail as possible. Billions of spam e-mails are thus distributed every day.

Relevant Multilateral Organizations

A plethora of multilateral organizations are involved in various aspects of cyberspace. These range from the various UN bodies like the ITU, WIPO, and WTO to the regional bodies like APEC, the EU, the G8, etc. Their functions include policymaking, regulating, and setting standards for running the internet as well as creating awareness of the importance of the medium. Financial bodies like the World Bank and the Asian Development Bank have been involved in funding various projects related to the development of the management of cyberspace, including financing of infrastructure for better usage of cyber-resources.

In the following, we will list the various relevant multilateral organizations with a brief description of each as far as their roles in the protection and administration of cyberspace are concerned. The funding agencies have been purposefully left out, since they are not involved in capacity-building efforts, apart from funding some projects to secure networks and develop cyber-security policies.

United Nations (UN)

The UN took on a major role in cyberspace when the UN secretary-general announced the Millennium Development Goals (MDG), which underscore the importance of ICT for development. The 55th UN General Assembly issued Resolution 55/63 on combating the criminal misuse of information technologies in December 2000. This resolution underlined the need for the protection of cyberspace, including international cooperation. The establishment of the UN ICT Task Force in November 2001 was another step forward towards attaining the MDG, and the Task Force took the first major step in cyber-security when it published a comprehensive guide in September 2002 that referred to issues of information insecurity and cyber-security. The document provided solutions for the security of cyberspace as well as response mechanisms and strategies. It laid down best practices and standards for a safe and secure running of cyberspace. The UN also organized the World Summit on the Information Society in two phases, held in Geneva in September 2003 and in Tunis in November 2005. These conferences discussed in depth all issues that are critical for the growth and sustenance of the internet. During

the first phase at Geneva, a decision was taken to set up a Working Group on Internet Governance (WGIG). The UNSG appointed the WGIG in September 2004. In July 2005, the WGIG submitted a report that elaborated in great detail on the security of cyberspace. The WGIG report offered four models of internet governance, including the management of cyber-security issues. In the Tunis phase, the WGIG report was discussed, but a consensus was reached on maintaining the present status of internet governance. It was also decided that the UN would set up an internet governance forum that will examine all policy issues related to internet governance, and that cyber-security would be treated as a primary issue.

International Telecommunications Union (ITU)

The ITU has been at the forefront of all UN organizations for policy-making on technical issues related to the internet. It has been focusing on countering spam; fostering international cooperation, including sharing of information and best practices; analyzing all internet government issues; and also providing support to developing in the field of cyber-security. In late June and early July 2005, the ITU organized the four-day WSIS Thematic Meeting on Cybersecurity, where it considered and debated six broad themes[7] in promoting international dialog and cooperative measures among governments, the private sector, and other stakeholders, including:

- Sharing information on national approaches;
- Good practices and guidelines;
- Developing watch, warning, and incident response capabilities;[8]
- Technical standards and industry solutions;[9]
- Harmonizing national legal approaches and international legal coordination;[10]
- Privacy, data, and consumer protection;[11]
- Developing countries and cyber-security.[12]

7 http://www.itu.int/osg/spu/cybersecurity/index.phtml.
8 http://www.itu.int/osg/spu/cybersecurity/agenda.html#session9.
9 http://www.itu.int/osg/spu/cybersecurity/agenda.html#session12.
10 http://www.itu.int/osg/spu/cybersecurity/agenda.html#session13.
11 http://www.itu.int/osg/spu/cybersecurity/agenda.html#session15.
12 http://www.itu.int/osg/spu/cybersecurity/agenda.html#session16.

The ITU has also undertaken a major initiative to counter spam. In July 2004, it organized the ITU WSIS Thematic meeting on Countering Spam in Geneva, where it analyzed the different aspects of spam and its growing menace and also undertook an assessment of the awareness and the readiness of nations to deal with it from a policy and technical point of view. In April 2005, it published the ITU Survey of Anti-Spam Legislation Worldwide. The ITU has also called on its technical standardization committees to address the issue in cooperation with other bodies such as the IETF.

The ITU's approach and work has set the tone for many present research and development on technical cyber-security issues and current security measures, such as public key infrastructure (PKI) and e-mail-filtering technologies. In addition to technical work in its standardization groups, and educational work in its development sector, the ITU is working to build confidence and security in the use of ICTs and the promotion of a global culture of cyber-security as called for in the WSIS Declaration of Principles and Plan of Action.

World Intellectual Property Organization (WIPO)

The World Intellectual Property Organization (WIPO), another specialized agency of the UN, is responsible for intellectual property protection. It administers 23 international treaties dealing with different aspects of intellectual property protection. These include establishing international standards for intellectual property laws as well as practices and registration services that allow patents, trademarks, and designs to be protected in many countries. The WIPO also provides technical and legal assistance to developing countries, facilitates resolution of intellectual property disputes, and explores new issues arising in the global intellectual property arena. The WIPO fosters cooperation among member states for IP-related issues. It is involved in the implementation of the Uniform Domain Name Dispute Resolution Policy (UDRP) that was developed by the WIPO and adopted by ICANN. It offers capacity-building measures for developing countries, including by online means, aimed at enhancing access to the intellectual property system as a tool for economic development. The WIPO is also focusing on the harmonization of approaches to ISP liabilities. Its efforts in this area include all stakeholders at the national, regional, and international levels. Its area of focus, namely IP-related issues and the related domain of privacy protection, are critical for the smooth functioning of cyberspace.

United Nations Educational Scientific and Cultural Organisation (UNESCO)

UNESCO's role in cyberspace is in the socio-cultural area. It has concentrated its efforts on the freedom of expression and multilingualism in cyberspace. It has also vigorously taken up the debate on ethical issues related to cyberspace. A consensus on ethics in the virtual space is an important part of making cyberspace a decent and secure medium to work in. UNESCO organized the International Conference on Freedom of Expression in Cyberspace in Paris in February 2005. UNESCO has published a document with the title "Recommendation on the Promotion and Use of Multilingualism and Universal Access to Cyberspace"[13] that identifies four points for consideration so that the greatest number of people may profit from the potential of ICT:

- Development and promotion of multilingual content and systems;
- Access to networks and service;
- Development of public domain content;
- Reaffirming and promoting the fair balance between the interests of rights-holders and the public interest.

Asia-Pacific Economic Cooperation (APEC)

Asia-Pacific Economic Cooperation (APEC) is a regional forum for fostering economic growth in the Asia-Pacific region by cooperation in a purely non-binding manner and open dialog. The APEC Telecommunications and Information Working Group (APEC TEL) has a general mandate to develop ICT policies and cooperation strategies for the Asia-Pacific region into an information society and to reduce the digital divide, as well specific tasks in protecting the information and communications infrastructure and providing cyber-security. In May 2002, the 5th APEC Ministerial Meeting on Telecommunications and Information Industry offered a document on information security that would lay the ground for the drafting of a cyber-security strategy. This strategy has offered recommendations in six specific areas: legal issues and cooperation, information-sharing, security and technical guidelines, public awareness, training and education, and wireless security. The need for cooperation among all

13 http://www.netdialogue.org/initiatives/unescocyber.

the regional players, including the CERTs, was stressed, and focus was laid on information-security training programs. APEC TEL has established an e-Security Task Group, which works on coordinating regional activities on a wide range of security-related issues, including spam. A few other areas of specific focus have been PKI interoperability, IT legislation, and strengthening law enforcement agencies for the protection of cyberspace. Another agency of APEC, the APEC Electronic Commerce Steering Group (ECSG), is active in the areas of user-protection measures and privacy.

Organization for Economic Co-operation and Development (OECD)

The Organization for Economic Co-operation and Development (OECD) started focusing on cyber-security in 1992, when it issued a set of information-security recommendations that was reviewed in the year 1997. In July 2002, the OECD published the comprehensive document "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" after it had been formally adopted as a recommendation of the OECD Council. The guidelines highlighted the need for fostering a culture of security among all users and stakeholders. The document suggested nine core principles that purported to support a risk-management approach to information-security issues. The guidelines also stress that information security is a continuous process, where risk analysis and its changing façade need to be dealt with in a dynamic manner. In addition to such topics as spam and privacy, the human dimension of cyber-security is also addressed. The OECD Council also offered policy recommendations to member countries that urged consultation, coordination, and cooperation in dealing with information-security issues, at both national and international levels. The council further identified the need for large-scale distribution of the guidelines across all organizations and among all individual internet users in both member and non-member countries. A review schedule of five years has been established in order to address evolving concerns and to provide a forum for international cooperation and exchange of experience. Apart from establishing policy guidelines and outreach plans to create the right awareness among member countries, the OECD also conducted a survey in 2004 to monitor the implementation of the information security guidelines. In 1980, OECD also published the Recommendation of the Council

Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, which is still of great relevance today.

Group of Eight (G8)

The Group of Eight (G8), consisting of the leading industrialized nations, deals with all issues of cyberspace, including cyber-security, on an informal basis. It has focused on critical infrastructure protection, and the first G8 meeting in March 2003 was devoted to the protection of critical information infrastructures. The G8 has given special attention to critical information infrastructures and to the need to increase international cooperation to ensure their protection against potential terrorist attacks. The meetings resulted in a set of 11 internationally agreed principles for protecting critical information infrastructures that would serve as a foundation for further work in this area. The G8 defined information security in terms of a process approximating a risk management approach, rather than an amalgamation of technologies. From the perspective of direct government involvement, the principles point to the need for countries to have early warning and crisis communications networks and bodies, and indicate a strong role of governments in supporting awareness building and training.

European Union (EU)

The European Union (EU) has been active on many fronts to improve the security and safety of cyberspace. It has focused on multi-faceted policy issues surrounding attacks on computer networks, the propagation of viruses, worms and Trojans, spam e-mails, phishing, and identity fraud. In 2004, the EU established the European Network and Information Security Agency (ENISA) to ensure network and information security within the European Community. ENISA aims to contribute to the development of a culture of network and information security for the benefit of the citizens, consumers, enterprises, and public sector-organizations of the EU. The EU has devoted efforts to building awareness among all stakeholders, including nations and vulnerable groups. In June 2002, it launched the action plan "eEurope 2005: An information Society for All", which recognizes cyber-security as being more than a purely techno-

logical challenge.[14] The EU has been actively deliberating anti-spam measures and banned spam in 2002 through the e-Privacy Directive (2002/58/EC). In a related effort, the EU established the Contact Network of Anti-Spam Enforcement Authorities (CNSA), which will give the necessary teeth and also participate and share experiences and critical information with law enforcement agencies. CNSA meets regularly to cooperate on anti-spam enforcement and has recently agreed to procedures for cross-border complaints.

Council of Europe (CoE)

The Council of Europe (CoE) has been working on cybercrime since 1989. After publishing a report on the adequacy of criminal procedural laws in cyberspace in 1995, it established a Committee of Experts on crimes related to cyberspace in 1997. This committee began drafting a binding convention to facilitate international cooperation in the investigation and prosecution of computer crimes. The first draft of his effort was released in April 2000 for public comment. Several more drafts have been released since then, culminating in the final draft released on 29 June 2001.

The Convention on Cybercrime[15] is divided into four chapters. The first chapter deals with substantive law issues: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, and offences related to copyright. The second chapter deals with law-enforcement issues, including preservation of stored data, preservation and partial disclosure of traffic data, production order, search and seizure of computer data, real-time collection of traffic data, and interception of content data. Chapter III contains provisions concerning mutual assistance between states in both traditional and computer-related crime, as well as extradition rules. Chapter IV contains the final clauses, which deal with standard provisions in Council of Europe treaties. The convention creates a common approach to criminal policy aimed at the protection of society against cyber-crime, the adoption of appropriate legislation, and fostering international co-operation. It recognizes the need for cooperation between governments and the private sector industry in combating

14 Dunn, Myriam and Isabelle Wigert. International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries (Zurich: Center for Security Studies, 2004).

15 http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

cyber-crime. It is a multilateral convention that requires signatory states to comply with and commit to its provisions and implement national legislation that is consistent with the convention. Any country, other than the members of the CoE, can join the convention if a few specific criteria are adhered to. The convention has inspired many of the international discussions on how to achieve a common legal ground for combating cyber-crime.

Analysis of these Efforts

As can be seen from the earlier section, all major multilateral organizations have become increasingly involved, in various capacities, in CIIP in their respective areas of jurisdiction over the last few years. This is due to the increasing importance of cyberspace and to the prevalence of multiple stakeholders that hold key roles for its smooth administration. Today the criticality of cyberspace, which facilitates so many functions for almost every activity on this planet, has added to the responsibility of all stakeholders to secure and protect its underpinnings. As the number of online users increases, so does the incidence of cyber-attacks, making protective measures even more important.

The multilateral organizations listed in the previous section have generally been active in the following areas: legal issues and legal cooperation; concern for network infrastructure; usage issues like spam and privacy; information-sharing; and training and awareness-building. These multilateral organizations have not been directly involved in the running of the technical infrastructure on their own, which generally has been the domain of IETF and ICANN along with national agencies and network operators. However, they have been able to provide policy support to the technical infrastructure of the internet. All these organizations also participated in the deliberations of the UNSG-appointed Working Group on Internet Governance (WGIG),[16] which was established in November 2004 on the basis of the recommendations of the first phase of the World Summit of the Information Society (WSIS-I) in Geneva in September 2003. The WGIG meticulously identified all relevant issues of internet governance, and cyber-security and protection of networks were seen as critical points. The WGIG offered four institutional models for the running and maintenance of the internet infrastructure, against the backdrop of concerns about internationalizing control of the internet, without one nation

16 www.wgig.org.

having the final control. The WGIG also heard many concerns about the role of ICANN and the technical issues involved in the running of the internet. Many commentators strongly suggested that technical issues remain under the responsibility of the industry and vendors.

Based on their activities over the past few years, the roles of multilateral organizations can be summarized as follows:

- UN — overall policy issues, supporting all other bodies under its umbrella;
- UNESCO — socio-cultural dimensions like the privacy of usage, freedom of expression on cyberspace;
- ITU — policy issues and spam;
- OECD — special focus on secure networks, spam, and global cooperation;
- G8 — critical infrastructure protection;
- EU — security of networks, privacy, data protection;
- CoE — legislation on cyber-crime;
- APEC — focus on spam and network security;
- WIPO — intellectual property issues.

Most of these organizations agree on the need for a strong legal regime for protecting cyberspace. The shared view is that national laws need to be harmonized to ensure a common understanding of the need for all global cyber-security concerns to be addressed. Furthermore, since cyber-crimes are transnational, international cooperation is occasionally required for their successful prosecution. At the same time, a strong international legal regime diminishes the possibility of a few nations becoming virtual havens for attackers. In this context, the provisions of the CoE Convention on Cyber-Crime identify issues that provide a useful basis for strengthening national legal frameworks dealing with the cyber-crimes. OECD, ITU, and even the discussions at WSIS-II in Tunis on legal issues have made the Convention as the basis for all further establishment of a common legal regime for cyber crimes.

The focus of many of these organizations has also been on building awareness among all stakeholders of the need for building secure networks and then sustaining these networks as a secure medium. The need for defining security policies at the level of corporate and government networks, and for adhering to best practices, have been clearly outlined. Furthermore, the necessity of auditing

network security regularly has been highlighted. Compliance norms have been offered, and more stringent measures have been suggested for the handling of critical networks. A well-recognized guiding principle is that IT security needs to be proportional. Most of the multilateral organizations have published documents in the form of guidelines and recommendations on the need for secure networks and have offered thought leadership with best practices. These organizations have focused on the role of governments and their requirement for constant updates about security concerns and response strategies. Security involves regular exchanges between governments and other stakeholders and sharing information about the configuration of systems and the availability of network protection tools. The ITU recommendations and OECD guidelines provide a basis for the coordination of efforts at the national, regional, and international levels.

One of the most common targets of most multilateral organizations has been to combat spam. Recognizing that it may be difficult to reach a consensus on a global definition of spam, many agencies are focusing on cooperation and enforcement mechanisms to stop unwanted e-mails that are generally harmful or fraudulent[17]. Anti-spam laws have been passed at the national levels, but they still need to get harmonized at the international level. The degree of cooperation among these organizations in combating spam is also noteworthy. The OECD, ITU, and APEC have shown enough coordination in anti-spam cooperation. It is not necessary to boost these efforts further. The OECD Spam Toolkit comprises legislative, technological, and self-regulatory components. It is the result of much brainstorming and many contributions from stakeholders across the world, including the multilateral organizations. The OECD and ITU have organized a number of workshops on spam to raise awareness and generate maximum attention for this issue. Similarly, UNESCO, WIPO, and the OECD have also addressed privacy issues quite extensively. On data protection, the EU has been most active.

It is apparent that the attention and possible actions of multilateral organizations have been focusing primarily towards criminal prosecution efforts. However, there is still no consensus even in this area, which is why there is still no clear common law to curb global internet crime. The CoE draft Convention on cyber-crimes has no doubt been an important step, but it has

17 http://www.khaleejtimes.com/Displayarticle.asp?section=opinion&xfile=data/opinion/2005/september/opinion_september60.xml.

not moved forward because the legal policies of many nations do not match its benchmarks and because, despite a common understanding of the need to have clearly defined legal framework to combat transnational cyber-crime. Similarly, the response from Interpol and other global law enforcement agencies has not reached a satisfactory level across all stakeholders. No doubt Interpol has given special attention to combating cyber-crimes and is engaged in transnational investigations, but it still falls short of a regime that is in total control of the management of criminal investigations and legal action.

The potential threat to cyberspace from terrorism has been much discussed among the leading nations after the attacks on US landmarks on 11 September 2001. After that event, studies[18] have revealed that terrorism acts in the physical world are preceded by increased terrorist activity in cyberspace. These increased activities may take the form of cyberattacks, usually DDOS attacks against the target websites and networks, and are also observed in the form of increased communications among militant groups. These trends have been witnessed not only in the case of the 9/11 attacks, but also in connection with the Indian parliament attack in December 2001, the Madrid train bombings in March 2004, and the London bombings in July 2005. Likewise, terrorists are using the internet to communicate and to recruit sympathizers. They are also using the internet to raise funds for their activities, and there have been instances of money-laundering using steganographic messages. The fact is that the multilateral organizations need to ensure that neither terrorist groups nor their sympathizers are able to host servers and websites and spread propaganda on the internet. There is no doubt that today, when servers and domain names (except the TLDs) are managed at national levels, it would be possible for one of these multilateral bodies to have oversight over monitoring extremist websites and content on the internet through the networks of many countries. Creating effective legal and political structures and policies to deal with such activities is a multilateral effort; probably, the UN would be the best body for such an assignment. The scope of the UN Security Council Resolution on Terrorism should be extended to cyberspace, the use of which by terrorists should be strictly countered.

While the efforts of all these multilateral organizations have started well, a lot more remains to be done. Cyberspace is dynamic and changing very fast. More and more emerging issues will need to be addressed. The efforts of the

18 http://www.ists.dartmouth.edu/analysis/cyber_a1.pdf.

UN will be more pronounced as the Internet Governance Forum begins its work, allowing for a more comprehensive treatment of many issues. A global consensus will be crucial for the next steps. We need to secure cyberspace and keep it growing, and multilateral solutions will be the preferred way of maintaining its smooth operation.

Conclusion and Recommendations

Towards a Global Culture of Cyber-Security

By Myriam Dunn and Victor Mauer

The information infrastructure – the combination of computer and communications systems that serve as the underlying infrastructure for organizations, industries, and the economy – has become a key asset in today's security environment.[1] All critical infrastructures are increasingly dependent on the information infrastructure for a variety of information management, communications, and control functions. This dependence has a strong national security component, since information infrastructure enables both economic vitality and military and civilian government operations. In particular, the government and military information infrastructures depend on commercial telecommunications providers for everything from logistics and transport to various other functions.[2] Current trends, such as the opening and liberalization of the markets, globalization processes that stimulate the cross-national interconnection of infrastructures, and the widespread access to telecommunications networks, are heightening the security requirements of the infrastructures in countries across the globe.

In addition, there are a number of observations that indicate the danger arising from society's dependence on complex, vulnerable, and critical systems:

- Many of the networks and systems have been built piecemeal by many different people and organizations using a wide assortment of information technologies, and with a wide range of functionalities in mind. Very few have been designed or implemented with assurance or security as primary considerations.[3]
- On the technical level, security will hardly evolve naturally or by the forces of the free market alone, because there are substantial obstacles

1 Computer Science and Telecommunications Board, National Research Council,. Trust in Cyberspace (Washington, D.C.: National Academy Press, 1999).

2 Personick, Stewart D. and Cynthia A. Patterson (eds.). Critical Information Infrastructure Protection and the Law: An Overview of Key Issues (Washington, D.C.: National Academies Press, 2003), p. 1.

3 Goodman, Seymour. E. "The Protection and Defense of Critical Information Infrastructures". Paper presented at the 43rd Annual IISS Conference, "The Strategic Implications of the New Economy" (Geneva, 12–15 September 2001), pp. 3–4.

to IT security: there is no direct return on investment, time-to-market impedes extensive security measures, and security mechanisms often have a negative impact on usability.[4]

- There is a historic lesson to be learned: It is a recurring phenomenon that the conveniences of a new technology are embraced long before its unwanted side-effects are systematically dealt with. The resulting "convenience overshoot" may last for decades.[5] Today, this approach might just be a trifle too dangerous: Too much depends on smooth, reliable, and continuous operation of the CII.
- Historically, many critical national infrastructures have been physically separate systems with little interdependence. Today, however, due to the CII, physical large-scale infrastructures are highly interconnected. But so far, attempts to understand the inter- and intra-connectedness among the various subsystems are completely lacking.
- Credibility, trust, and confidence are key assets in our volatile world.[6] One of the unforeseeable consequences of disruptions in the information infrastructure is likely to manifest itself in indirect and non-quantifiable ways: the destabilization of basic trust among citizens in the mechanisms that govern them.[7]
- In his book on "Normal Accidents", Charles Perrow argues that in an interactively complex system, two or more discrete failures can interact in unexpected ways, thereby affecting supposedly redundant sub-systems. A sufficiently complex system can in fact be expected to have many such unanticipated failure mode interactions, making it vulnerable to inevitable accidents, even without external triggers.[8]

4 Näf, Michael. "Ubiquitous Insecurity? How to "Hack" IT Systems". In: Wenger, Andreas (ed.). The Internet and the Changing Face of International Relations and Security. Information & Security: An International Journal, Volume 7, (2001), pp. 104–18.

5 Examples are: The introduction of the Ford Model T in 1909 and the widespread use of seat belts; the 70-year delay between the introduction of steam locomotives and the first use of pneumatic brakes.

6 Dunn, Myriam. Information Age Conflicts: A Study on the Information Revolution and a Changing Operating Environment. Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung, No. 64 (Zurich: Center for Security Studies, 2002), pp. 33–41.

7 Westrin, Peter. "Critical Information Infrastructure Protection". In: Wenger, Andreas (ed.). The Internet and the Changing Face of International Relations and Security. Information & Security: An International Journal, Vol. 7 (2001), pp. 74–75.

8 Perrow, Charles. Normal Accidents: Living with High-Risk Technologies (New York: Basic Books, 1984).

- Even as our knowledge and competence as regards system reliability increases, new demands of functionality will likewise increase, and thereby system complexity. An inevitable "ingenuity gap" arises.[9]

Seen from this viewpoint, a robust ICT-dependent society requires active intervention, at a stage when a major, society-threatening chain reaction of IT-related events is still only fiction. Active intervention in this case means taking adequate measures to make those systems, and thus society, more secure, which can only be done based on a better and more thorough understanding of the problems we face.

The Challenge of Interdisciplinary Research

At present, however, open, pressing, but unanswered questions abound in the field of CIIP. As a result, there is not just a research gap — there is a veritable Grand Canyon of lacking knowledge to be filled; and the research community is only just beginning to single out the correct and the most important questions that need to be asked. The research field is also highly dynamic, mainly due to the rapid changes in the technological environment. In such a dynamic field, we need to pinpoint the underlying urgent questions that are not subject to erratic change. Also, the question of generalizing and establishing over time the results of studies involving information infrastructure protection is in itself a fundamental issue: Does the topic of CIIP have a classifiable structure and content that is sufficiently stable in time to provide a foundation for durable protection and preparedness planning?[10] At present, it would appear that the answer to this question is "no". In fact, it seems as if the problem complex itself were in flux to a degree that calls for constant observation until this area of research has gained a more stable scientific and methodological base. Academia and practitioners will have to work hand in hand to resolve that problem.

In addressing the topic of critical infrastructures and their protection, one has to understand and assess the relevance of various factors. Issues that demand special attention have become apparent through in-depth analysis

9 An ingenuity gap is a shortfall between rapidly rising need of complex societies for initiative and innovation and the inadequate supply of it. See: Homer-Dixon, Thomas. The Ingenuity Gap (New York: Knopf, 2000), p. 1.

10 Westrin, op. cit., p. 77.

of the subject matter and cross-country comparison of protection practices. The trickiest of these issues are those that demand an integration of various disciplines. These include a number of policy issues, which are addressed in this volume, but also diverse issues such as inter-linkages between CI, the working of complex systems, consequences of interdependencies, possible cascading effects of failures, and newly emerging, insufficiently understood threats and vulnerabilities.

There is no question that technology is one of a number of mediating factors in human behavior and social change, which both affects and is affected by other phenomena. However, one must be very careful not to succumb to technological determinism. The technological determinist view is a technology-led theory of social change: technology is seen as the prime mover in history. Technology, however, is not an abstract, exogenous variable, but rather inherently endogenous to politics.[11] This embeddedness means that ICTs and people can only be fully examined through an overarching theoretical perspective that encompasses an understanding of the social, economic, political, and technical dimensions inherent in it. Therefore, only frameworks that combine socio-economic, socio-political, and socio-technical knowledge can give satisfactory answers to many of the issues at hand, because they alone offer insights into how individual practices are linked to wider socio-political regimes and socio-technical landscapes that evolve in particular cultural and geographical contexts.

However, the interdisciplinarity that this implies is not easily realized. Conceptual frameworks to analyze how digitalization, infrastructures, and various other aspects of CIIP shape a diversity of social processes, and vice versa, are not readily available. In general, research that cuts across disciplines meets with considerable obstacles. Much of the difficulty of interdisciplinarity has to do with the fact that attention, recognition, and authority are channeled by academic institutions of the individual disciplines.[12] A discipline is a scientific domain that has a specific methodology, specific implicit hypotheses justify-

11 Chandler, Daniel. "Technological or Media Determinism". Online resource, created on 18 September 1995. http://www.aber.ac.uk/media/Documents/tecdet/tdet02.html; Herrera, Geoffrey. "Technology and International Systems". In: Millennium, Vol. 32, No. 3, (2003), pp. 559–94; Mackenzie, Donald and J. Wajcman (eds.). The Social Shaping of Technology: How the Refrigerator Got its Hum (Buckingham: Open University Press, 1994, reprint).

12 Sperber, Dan. "Why Rethink Interdisciplinarity?". Online Seminar on Interdisciplinarity, Paper (no date)., a Available at http://www.interdisciplines.org/interdisciplinarity/papers/1/4.

ing it, and a specific vocabulary. Attempts to build interdisciplinary bridges logically lead to the "intersection/union" problem: in order for a result to be accepted by two disciplines, one has to reduce their implicit hypotheses to a set of common ones (intersection), and to extend the justifications to include a complete justification in both disciplines (union). Relaxing the implicit hypotheses, although increasing the generality of the result, will limit its "practical" consequences, and may result in too general a statement.[13]

These obstacles are hard to overcome. However, if we are aware of the need for interdisciplinarity, much might already have been won. In specific areas, disciplinary boundaries and routines stand in the way of optimal research. Openness to interdisciplinarity is thus the most sensible recommendation at this point.[14] The goal is to go ahead with new research programs, and, for this, to reshape the institutional landscape. More generally, it is conceivable that the advancement of science will involve so much reshaping of its institutional forms that the disciplines as we know them will have to go.

In this volume, we have offered an in-depth analysis of key issues in three parts, covered by authors from different disciplines so as to incorporate the viewpoints of an interdisciplinary group of scholars. Rather than wrapping up each of the chapters in this volume individually, we choose to tackle one of the most prominent overarching questions in this concluding chapter of Volume II: What role can and should the state play in protecting these infrastructure systems within their broader environment? More specifically with regard to the three parts of this volume, how can the state foster much-needed research? How can we overcome the problem posed by the differing viewpoints in CIIP? How can governments gain more knowledge on the threat environment? What role can they play in early warning and public outreach, in public-private-partnerships, and concerning legal issues?

13 Mendez, Patrice Ossona de. "The Risks and Challenges of Interdisciplinarity". Online Seminar on Interdisciplinarity, online comment (2 April 2003)., a Available at http://www.interdisciplines.org/interdisciplinarity/papers/1/2#_2.

14 Laudel, Grit. "Collaboration, Creativity and Rewards: Why and How Scientists Collaborate". In: International Journal of Technology Management, Vol. 22, (2001), pp. 762–81.

Finding the Right Role of the State in CIIP

The developments of the past decade have led many observers to assume that the forces driving global change are acutely undermining the state and its political freedom of action. What is clear already is that any conception of security capable of dealing with the current world order needs to be linked to a much wider notion of governance than that which characterized the Cold War. In the realm of CIIP, governments are challenged to operate in unfamiliar ways, sharing influence with experts in the IT community, with businesses, and with nonprofit organizations, because the ownership, operation, and supply of the critical systems are in the hands of a largely private industry. We are thus confronted with a case in which governments cannot carry out their most basic mission, providing security, without the cooperation of the private sector.

The fact that the maintenance of "business continuity" for an individual, corporate or local actor and security efforts in terms of national or even international security often exist side by side in the realm of CIIP and homeland security seems to be a long-term trend rather than an exception. This points to the changing nature of security practices in a world in which the state sees itself as being unable "to go it alone". In fact, the state practice of security is moved from the outside of the border into domestic space: Security is domesticated and privatized, while the private realm is securitized. On the one hand, the practice of securing society is privatized by putting the responsibility partially on the shoulders of the owners and operators of critical infrastructure. On the other hand, the goal or philosophy of the state is still the same, whereby national security practices spill into society.

This development also means that even though the issue of cyber-threat is clearly linked to national security, no measures are envisaged that would traditionally fall within the purview of the national security apparatus. In general, national-security countermeasures stress deterrence and prevention of attacks, while the investigation and pursuit of the attackers is only of secondary importance, since the concept of compensatory or punitive damage is rarely meaningful in a national-security context. Private-sector countermeasures, however, are frequently oriented toward detection, which means developing audit trails and other chains of evidence that can be used to pursue attackers in the courts.[15] This means that even if we consider CIIP to be a national-

15 National Academy of Sciences, Computer Science and Telecommunications Board. Computers at Risk: Safe Computing in the Information Age (Washington D.C.: National Academy Press, 1991), p. 19.

security issue, the tools available to the state are not part of its traditional national security arsenal — on the contrary: In the majority of countries, the law-enforcement/cyber-crime perspective has emerged as the most prominent one, due to the nature of the threat, the resources available to the law enforcement community, and cultural and legal norms that restrict the number of available strategies.

Even more, because CIIP and economic growth are so closely interrelated, any involvement of the state in cyber-security matters is subject to much scrutiny. It has in fact been argued that one solution to the problem of cyber-security is to focus on economic and market aspects of the issue rather than on suitable technical protection mechanisms.[16] If we apply this viewpoint, we quickly realize that the insecurity of the internet can be compared to environmental pollution and that cyber-security in fact shows strong traits of a "public good" that will be underprovided or fail to be provided at all in the private market.

Cyber-Security – A Public Good?

In economics, a public good is a good that is hard or even impossible to produce for private profit, because the market fails to account for its large beneficial externalities. By definition, a public good possesses two properties[17]:

- **Non-rivalrous:** its benefits fail to exhibit consumption scarcity; once it has been produced, everyone can benefit from it without diminishing others' enjoyment.
- **Non-excludable:** once it has been created, it is very difficult, if not impossible, to prevent access to the good.

Public goods provide a very important example of market failure, in which individual behavior seeking to gain profit from the market does not produce efficient results. The production of public goods results in positive externalities,

16 Andersson, Ross. "Why Information Security is Hard: An Economic Perspective". In: IEEE Computer Society (ed.). Proceedings of the 17th Annual Computer Security Applications Conference, New Orleans, 10–14 December 2001. http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/econ.pdf.

17 Stiglitz, Joseph E. and Carl E. Walsh. Principles of Microeconomics (New York, W. W. Norton & Company, 2004, 4th Edition), pp. 236–238; Wikipedia, The Free Encyclopedia. s. v. "Public Goods". Available at: : http://en.wikipedia.org/wiki/Public_goods.

which are not remunerated. In other words, because private organizations cannot reap all the benefits of a public good that they have produced, there will be insufficient incentives to produce it voluntarily. At the same time, consumers can take advantage of public goods without contributing sufficiently to their creation. This is called the free-rider problem, because consumers' contributions will be very small.[18]

Is cyber-security a public good? We can in fact observe that the security of the entire internet is affected by the security employed by all internet users[19]: Insecure nodes not only jeopardize the integrity of their own systems, but also compromise the security of all users, for instance by spreading worms unintentionally and by irresponsibly tolerating distributed attacks from their computers. On the other hand, when a firm or individual has a greater level of cyber-security, their computers are less likely to be hacked into and used to launch spam or other denial of services attacks. The security that the computer owner provides thus benefits other computer users by reducing the probability that they will be attacked through the first owner's computer. However, since individuals are not generally liable for the damage caused when a hacker takes over their computer, they do not benefit from the increased security. Since users do not therefore bear the full costs of their actions, individuals have no incentive to upgrade the security of their systems.[20]

This could, in theory, lead to the free-rider problem. There are in fact various levels on which free-riding could take place: first, individuals are likely to free-ride. Second, companies might also be free-riders, even though some researchers have pointed out that there is little empirical evidence for this in the financial sector, for example.[21] And third, nation states are also prone to free-ride. Because any externality created by unsecured computers is not limited by national boundaries, it is unlikely that any country could respond to such an externality on its own. Pursuing its own interest, each country, state, or region has insufficient incentive to safeguard the global information infrastructure. Cyber-security thus shows some important features of a public

18 Ibid.

19 Anderson, Why Information Security is Hard.

20 Anderson, Ross. "Unsettling Parallels Between Security and the Environment". Economics and Information Security Workshop, Berkeley, 16–17 May 2002. Available at: http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/37.txt.

21 Powell, Benjamin. "Is Cyber-Security a Public Good? Evidence from the Financial Services Industry" The Independent Institute Working Paper, 14 March 2005., a Available at: http://www.independent.org/pdf/working_papers/57_cyber-.pdf.

good, even if it might not be a "pure" one. In addition, cyber-security is fast becoming a global public good.

Solutions, Policy Options, and Recommendations

In the economic literature, there are a number of possible solutions to the free rider problem. Some public choice theorists advocate government intervention and state provision of public goods by providing the difference between the optimal level of cyber-security and the level the private sector voluntarily provides. Also, if voluntary provision of public goods will not work, then the obvious solution is to make their provision mandatory.[22] One general solution to the problem is for governments or states to impose taxation to fund the provision of public goods. A government may also subsidize the production of a public good in the private sector.[23]

However, there is widespread agreement that governments should not get involved too much. Specifically, it is agreed that regulation may not produce optimal results due to various factors:

- Governments are inherently slow to respond or adapt to new situations.
- Governments usually place the emphasis on the tools they know best, in the shape of top-down regulation, which may not be the most effective approach.
- Government regulations are ineffective, since the technology changes too quickly: Often, governments lag behind the private sector in understanding the threats and the state of technology to address them.
- Governments tend to politicize issues rather than remain focused on the substance.
- Governments are always regulating in response to earlier developments and thus lagging behind.

22 Grady, Mark and Francesco Parisi. "The Law and Economics of Cyber-security: An Introduction". George Mason University School of Law and Economics Working Paper Series No 04-54, (November 2004).

23 Wikipedia, The Free Encyclopedia, s. v. "Public Goods"., a Available at: http://en.wikipedia.org/wiki/Public_goods.

In addition, because public goods are not bought and sold on the market, it is impossible to determine the optimal level of cyber-security and then compare it to what the private market has provided. The information problem — figuring out how much provision is optimal — and the incentive problem — making it worth someone's while to provide exactly that amount — are thus unsolved issues in practice. Therefore, public goods will still tend to be produced at suboptimal levels even when the government provides them, though the error will often be in the other direction: In general, many argue the public goods such as national defense tend to be overproduced by governments.[24]

Indeed, there is a fair amount of hype surrounding the topic, in part fueled by government officials: "cyber-war" and related issues are en vogue and have even become a growth market. Producers of information security technology may benefit financially if they can scare more people into purchasing security products. Similarly, professionals competing for the latest homeland security grants may face incentives to overstate the problem. Especially when it comes to CIIP as a national security issue, so-called "professionals of security"[25] also play a considerable role. The institutions that father these professionals of security are bureaucratic ramifications of the state; deprived of their Cold War exterior enemy, these bureaucracies need to legitimize their existence by constantly redefining their role of society's protector and do so by adding new threats to the political agenda, when old ones disappear.[26]

In fact, to look at cyber-security as a mainly economic problem helps to "desecuritze" the issue. Desecuritization as the "unmaking of security" has been considered a technique for "defining down" threats, in other words, a "normalization" of threats previously constructed as extraordinary, as they are when looked upon as a national security issue.[27] This points to the fact that one must be careful not to foment "cyber-angst" to an unnecessary degree and to ensure that threats are seen in appropriate proportions by all involved could be one important role for the state.

24 Goodman, John C. and Philip K. Porter. "Political Equilibrium and The Provision of Public Goods". In: Public Choice, Vol. 120, No. 3–4, (September 2004), pp. 247–266.

25 Aradau, Claudia. "Migration: The Spiral of (In)Security". In: Rubikon, March 2001., a Available at: http://venus.ci.uw.edu.pl/~rubikon/forum/claudia1.htm.

26 Ibid.; Huysmans, Jef. "Revisiting Copenhagen: Or, On the Creative Development of a Security Studies Agenda in Europe". In: European Journal of International Relations, Vol. 4, No. 4, (1998), pp. 479–506.

27 Aradau, Claudia. "Beyond Good and Evil: Ethics and Securitization /Desecuritization Techniques". In: Rubikon, December 2001., a Available at: http://venus.ci.uw.edu.pl/~rubikon/forum/claudia2.htm.http://venus.ci.uw.edu.pl/~rubikon/forum/claudia2.htm.

There is another role for government, linked to a third solution to the free-rider problem that might, in combination with some state intervention where truly needed, produce promising results: The Coasian solution, named after the economist Ronald Coase.[28] The Coasian solution proposes a mechanism by which potential beneficiaries of a public good band together and pool their resources based on their willingness to pay to create the public good. For such solutions, governments can serve as the convener to bring parties to the table. They can compel — either through persuasion or regulation where necessary — the sort of behavior that many believe is needed. Moreover, governments can use purchasing criteria to create a market for products that conform to certain specifications, like security standards. All in all, this points to the fact that global economic development, steered into the right direction, may be the force that best addresses the problem. Below, we will look at how a market for security could be created, and how governments could promote best practices, information sharing, and additional research.

Create a Market for Security: The Role of Insurance

Some commentators have proposed using liability rules and cyber-insurance as solution to cyber-security and CIIP at least at the national level. In fact, economist Hal Varian identifies the situation of responsibility attribution as the main source of weak security.[29] He argues that, in a first step, liability for losses due to security breaches should be transferred to the party who could reduce the risk most easily. Accordingly, manufacturers would be liable for vulnerabilities in their products, but also network nodes – up to the end user — could be called to account if they do not comply with their maintenance duties. Ideally, civil liability allows a victim to recover losses from third parties if such parties were negligent or engaged in intentional misconduct and if such negligence or misconduct was the proximate cause of the loss. As a second step, cyber-risks should be made transferable, so that all parties can buy insurance coverage against possible losses and indemnification claims. The introduction of insurance might thus provide a foundation for market-based

28 Coase, Ronald. "The Lighthouse in Economics". In: Journal of Law and Economics, Vol. 17, no. 2, (1974), pp. 357–376.

29 Varian Hal R. "Managing Online Security Risks". In: New York Times, 1 June 2000., a Available at: http://www.sims.berkeley.edu/~hal/people/hal/NYTimes/2000-06-01.html.

risk analysis and cooperation among infrastructure operators, and can foster best practices.[30]

In this view, a mechanism for gauging the value of stolen information is of critical importance. If companies can assess the value of information, then insurance companies can insure information. In turn, the insurance companies will push companies to better protect their information. However, how to measure the value of information? In general, there is a very limited understanding of the costs of cyber-security attacks and the benefits of preventive measures, for a variety of reasons, not least the fact that it is highly unlikely that detailed access to more than a few such systems will be available to research directed towards this end. Systems for such services as finance and security exchange, or data communication in general, will most probably remain inaccessible for analysis. Governments could play a significant role in sponsoring research on this subject, research that, up to this point, the private sector has been unwilling or unable to conduct. It should also develop mechanisms for systematically collecting information from firms (with appropriate privacy protections) that would allow the government to help develop a better strategy for addressing cyber-security in the future.

Promote Best Practices

Apart from thinking about reforming IT liability to further the development of a cyber-security market, governments might want to promote operational best practices for network administrators and users, combined with ongoing training and enforcement of the practices through random tests, and consider developing standards for software protocols that are more secure than current ones. In addition to playing a role in liability determinations, best practices can also serve as a benchmark against which firms could be audited. Routine audits based on well-accepted principles of testing and analysis can help firms avoid litigation or reduce liability.[31] Such standards could be voluntary or enforced through regulations. At least, governments could serve as an "honest broker", developing and disseminating information that could be expensive

30 Kesan, Jay P.Ruperto P. Majuca, and William J. Yurcik. "Cyber-Insurance as a Market-Based Solution to the Problem of Cyber-Security — A Case Study". 4th Workshop on the Economics of Information Security (WEIS), Harvard University, 2–3 June 2005, a. Available at: http://infosecon.net/workshop/pdf/42.pdf.

31 Personick and Patterson, op. cit., p. 4.

for an individual locality to acquire, but crucial to the prospects of any joint operating agreement. Adopting a nationally or even internationally recognized computer security standard is not, however, a simple process, owing to the evolving nature of security vulnerabilities and the diverse players that have an internet presence.[32] The crucial point is, therefore, to establish "best practices" for industry and government that can be flexible for a variety of users but still provide a basis for liability.

Promote Information Sharing

In addition, governments have a strong role to play in raising awareness and educating all stakeholders about the importance of properly configured systems and available network protection tools as well as about the threat. However, although the sharing of information has been the centerpiece of both the governments' and the private sectors' efforts to protect critical information systems over the past several years, most information sharing still occurs through informal channels. These networks have been plagued by the traditional problems of any "Prisoner's Dilemma", in that members are afraid to cooperate and divulge information because of worries about increased liability due to disclosure, risk of antitrust violations, and the loss of proprietary information.[33]

As a first step, information sharing requires a permissible legal framework, for example regarding both antitrust and liability concerns.[34] In addition, recent research suggests that the membership of these networks should be restricted, making them less broadly based than they presently are. This would allow norms to be developed among actors who have preexisting business connections that would facilitate enforcement, as opposed to the broad networks that currently exist and cannot enforce disclosure.[35] In addition, government

32 Berkowitz, Bruce and Robert W. Hahn. "Cyber-security: Who's Watching the Store?", Iin: Issues in Science and Technology (Spring 2003), a. Available at http://www.issues.org/19.3/berkowitz.htm.

33 Cukier, Kenneth Neil, Viktor Mayer-Schoenberger and Lewis Branscomb. "Ensuring (and Insuring?) Critical Information Infrastructure Protection". KSG Working Paper No. RWP05-055 (October 2005).

34 Personick and Patterson, op. cit., p. 2.; Benson, Bruce L. "The Spontaneous Evolution of Cyber-Law: Norms, Property Rights, Contracting, Dispute Resolution and Enforcement Without the State of Law". In: Journal of Law, Economics and Policy, Vol. 1, No. 2 (2005), a. Available at: http://www2.sjsu.edu/depts/economics/faculty/powell/docs/econ206/Cyber-Law-Evolution.pdf.

35 Grady and Parisi, op. cit.

officials can provide intelligence information about new computer-security threats that might benefit companies involved in information sharing, as is the case for certain early-warning measures.

Promote Research

Finally, governments can fund long-term research into CIIP.[36] They need to spend money to get better information about the threats and about what the available countermeasures can actually achieve. Since the putative new societal risks and vulnerabilities are directly or indirectly related to the development and utilization of new technologies, it would seem natural to follow a chain of analysis beginning with technical specifications and casually running "up" through systems, actors, threats, vulnerabilities, consequences, and finally, countermeasures and mitigation. However, in view of the rapid technological developments constantly taking place, and the particular nature of their implementations, one can raise certain objections to such a synthetic scheme. If, for instance, one carefully examines a relatively localized subsystem from the point of view of risks and threats, thereby identifying certain of its vulnerabilities, in what way can these insights be generalized and established in order to utilize them "beyond" the subsystem itself, on a higher system level?[37]

It may very well be that critical vulnerabilities, and even the worst consequences of infrastructure disruptions, will not be traceable in any useful way to single technical subsystems — perhaps as a consequence of an already overwhelming system complexity of open socio-political systems. Also, in view of the rapid technological developments constantly taking place, and the particular nature of their implementation, even if one carefully examines a relatively localized subsystem from the point of view of risks and threats, thereby identifying certain of its vulnerabilities, these insights can hardly be generalized and established in order to utilize them "beyond" the subsystem itself and on a higher system level.

Effective protection for critical infrastructures, therefore, calls for holistic and strategic threat and risk assessment at the physical, virtual, and psychological levels as the basis for a comprehensive protection and survival strategy, and will thus require a comprehensive and truly interdisciplinary research and development agenda encompassing fields ranging from engineering and

36 Berkowitz and Hahn, op. cit.
37 Westrin, op. cit., p. 74.

complexity sciences to policy research, political science, and sociology. There is no doubt that CIIP will be a major R&D challenge in the future. R&D in the field of CIIP is undertaken by a large variety of actors in each country: research institutes at universities, private-sector research institutes and laboratories, networks of excellence, national research councils, etc. However, so far, there has been rather little coordination and cooperation between R&D actors at the national level.

Furthermore, the inherently transnational nature of CII and the growing international dependency on CII, as well as threats and vulnerabilities to the national CI (a good example is the big blackout in Italy's electric power system in October 2003) make the topic an obvious issue for international cooperation[38] — an issue we turn to in our last chapter.

From the National to the Global

We end this volume as we have ended the first one, by reflecting on what has been called "a global culture of cyber-security". The 2003 WSIS Declaration of Principles calls for such an effort in order to strengthen the trust framework, including information security and network security, authentication, privacy, and consumer protection, all prerequisites for the development of a strong Information Society, a goal pursued in many countries around the world.[39] But, once again, how are we to get there? How can a global culture of cyber-security be fostered? The WSIS Plan of Action proposes to reach that goal mainly by promoting cooperation among governments and by getting them, in close cooperation with the private sector, to prevent, detect, and respond to cyber-crime and the misuse of information and communication technologies by developing guidelines and considering legislation, by strengthening institutional support, and by encouraging education and raising awareness.[40]

38 The rationale for strategic coordination of R&D at the international level was outlined at a December 2001 EU-US workshop on R&D in the field of CIIP. Cf. EU-US Workshop Report, "R&D Strategy for a dependable information society: EU-US collaboration", 1–2 December 2001 (Düsseldorf, Germany), a. Available at: http://www.ddsi.org.

39 World Summit on the Information Society. "Declaration of Principles Building the Information Society: A Global Challenge in the New Millennium",. D document WSIS-03/GENEVA/DOC/4-E, 12 December 2003, a. Available at: http://www.itu.int/wsis/docs/geneva/official/dop.html.

40 World Summit on the Information Society, "Plan of Action". Document WSIS-03/GENEVA/DOC/5-E, 12 December 2003., a Available at: http://www.itu.int/wsis/docs/geneva/official/poa.html.

Solutions to international public-goods problems should consider furnishing an international organization with sufficient funds to subsidize abatement, and empowering it with sharp enough teeth to penalize non-compliance. At the World Summit on the Information Society 2005 held in Tunis, it was suggested that the UN for example could govern the internet, and devise treaties to address issues such as cyber-security. Some support the idea, others feel that it will add more bureaucracy and further delay dealing with cyber-security issues, as UN treaty-making is inordinately cumbersome and certainly unduly time-consuming if the treaty-making effort were to start from scratch. An alternative method for moving towards a global framework would be to take an existing treaty and broaden its affiliation: This procedure is advocated by many who refer to the model of the Council of Europe Convention on Cyber-crime. For the existing convention with its broad coverage to be put to a more global use and thus to save precious negotiation time, it would be necessary to focus on its intrinsic merits and built-in flexibilities.[41]

In addition, governments should make sure that "cyber-crime havens" cease to exist. Different nationalities have different legal systems and criminal laws; therefore, arrangements and cooperation mechanisms between enforcement agencies are the appropriate way to deal with cyber-crime that crosses borders. States should review their laws in order to ensure that abuses of modern technology that are deserving of criminal sanctions are criminalized and that problems with respect to jurisdiction, enforcement powers, investigation, training, crime prevention, and international cooperation with respect to such abuses, are effectively addressed. Liaison between law enforcement and prosecution personnel of different states should be improved, including the sharing of experience in addressing these problems. These measures will ensure that the international community can move swiftly towards a much-needed international and global culture of cyber-security.

41 World Federation of Scientists Permanent Monitoring Panel on Information Security. "Information Security in the Context of the Digital Divide: Recommendations submitted to the World Summit on the Information Society at its Tunis phase" (16 to 18 November 2005)". , Document WSIS-05/TUNIS/CONTR/01-E, 2 September 2005, p. 23., a Available at: http://www.itu.int/wsis/docs2/tunis/contributions/co1.doc.

Appendix

Author Biographies

Isabelle Abele-Wigert

Isabelle Abele-Wigert is research fellow at the Center for Security Studies at the Swiss Federal Institute of Technology (ETH Zurich). She is part of the Center's Comprehensive Risk Analysis and Management Network (CRN) team. She has written on Critical Information Infrastructure Protection (CIIP), focusing on national policy approaches to CIIP. Together with her colleague Myriam Dunn, she is co-author of the CIIP Handbook, which is published every two years. She has a Master's degree from the University of Zurich (modern history, political science and English literature).

Jan Joel Andersson

Dr. Jan Joel Andersson is a research fellow at the Swedish Institute of International Affairs and an associate at 4C Strategies AB. He holds a Ph.D. in political science from the University of California at Berkeley and is a member of the International Institute for Strategic Studies in London. A specialist on security policy, his research currently focuses on public-private partnerships and the challenge of critical infrastructure protection in a globalizing world economy.

Subimal Bhattacharjee

Subimal Bhattacharjee, vice president of Argus Integrated Systems Pvt Ltd., New Delhi, India, is involved in various projects involving high-level cyber-security strategy for governments and large corporations both in India and abroad. He was previously the chairman of the Task Force on Cyber Security for the premier industry body, Associated Chambers of Commerce and Industry of India (ASSOCHAM). He also served in a government assignment as IT adviser to the chief minister of Assam in India. He has authored more than 100 publications on the subject, which includes policy analysis on the complex issues of global internet governance. He has been an international consultant with some of the major multilateral organisations besides being a member of various high-level committees in India related to information security.

Mark de Bruijne

Dr. Mark de Bruijne studied public administration at Erasmus University in Rotterdam (1999) and specialized in safety management. His graduation paper focused on the influence of stress and bureau politics on the collection and processing of warning signals by the Dutch government during the crisis that developed around Dutch New-Guinea (1959–1962). His research on "networked reliability" explores the consequences of institutional fragmentation with regard to the reliability of service provision in critical infrastructures. The focus of this research specifically described how the operators and organizations that manage these infrastructures cope with these changes.

Myriam Dunn

Dr. phil. Myriam Dunn heads the New Risks Research Unit at the Center for Security Studies (CSS), ETH Zurich and is the coordinator of the Comprehensive Risk Analysis and Management Network (CRN), a subject-focused platform through which experts explore common aims and interests in the field of strategic risk analysis. The CRN Initiative links the scientific expertise of the New Risks Research Unit with national and international risk analysis and management authorities. Members of the team serve as consultants and policy advisors in various working groups. On the international level, the CRN's goal is to provide and expand an international partner network to exchange knowledge on risks and risk analysis methodology, and to share and review national experiences in an open, non-hierarchical dialog. Dr. Dunn has published extensively on the impact of the information revolution on security policy issues. She holds a degree in political science, history, and international law from the University of Zurich.

Michel J.G. van Eeten

Michel J.G. van Eeten is an associate professor at the School of Technology, Policy and Management, Delft University of Technology, the Netherlands. He is also the leader of the Critical Infra Program of the Next Generation Infrastructures Foundation (www.nginfra.nl). He has published on large technical systems, ecosystem management, high reliability theory, land use planning,

transportation policy, internet governance, and recasting intractable policy issues. His recent work as a practicing policy analyst includes advice to the Directorate General of Telecommunications and Post, the Ministry of Economic Affairs, KPN Mobile, Rabobank, and the Civil Aviation Authority.

Thomas Holderegger

Thomas Holderegger is an analyst in the Reporting and Analysis Centre for Information Assurance (MELANI), Switzerland (MELANI: www.melani.admin.ch), part of the Service for Analysis and Prevention (SAP) of the Swiss Federal Office of Police (fedpol.ch: www.fedpol.ch). SAP performs the function of preventive state security. He has a degree in general history (specializing in modern history, in particular the Cold War, international relations, US foreign and security policy, and Swiss foreign and security policy), computer science (specializing in communications and distributed systems, and IT security), and social and economic history from the University of Zurich.

Andreas Malm

Andreas Malm is the chief executive officer of 4C Strategies AB, a company assisting governments and corporations in securing their operational continuity in an uncertain world. An expert on risk management and business continuity planning, he has considerable experience with public-private partnerships and critical infrastructure protection in a wide range of sectors, including the finance, telecom, and energy sectors.

Victor Mauer

Dr. phil. Victor Mauer is the deputy director and head of research of the Center for Security Studies (CSS), ETH Zurich, and heads the Center's European Security and Defense Policy (ESDP) Project. He studied at the Universities of Bonn, Oxford, and Cambridge. He specializes in European security, European integration, and transatlantic relations. He has written on European and transatlantic affairs and on various other subjects. Prior to joining the CSS, he worked at the International Secretariat of the NATO Parliamentary Assembly, Brussels.

Emery Roe

Emery Roe is Professor of Public Policy at Mills College. He has a Ph.D. in public policy from the University of California and writes widely on domestic an international public policy and management issues. His recent research includes critical infrastructure reliability, especially with respect to homeland security and deregulated electricity markets. He is also working on a "professional challenges" approach in policy education to managing complexity in real-time.

Paul Schulman

Paul R. Schulman is Professor of Government at Mills College. He received his Ph.D. in political science from John Hopkins University, and his interests are in science and technology and their challenges to the public policy-making process

Clay Wilson

Clay Wilson received his M.S. in telecommunications management at the University of Maryland in 1994, and his Ph.D. from the School of Public Policy at George Mason University in May 2001. From 2001 to 2003, he taught computer security and risk analysis at the University of Maryland University College. He served as a government representative to the Critical Infrastructure Coordination Group (CICG) from 1998-2000, to improve industry and government cooperation for better national computer security. He is currently an advisor on the Virginia Commonwealth Joint Commission on Technology and Science, subcommittee on Nanotechnology. Dr. Wilson also served previously as the computer security officer for the Congressional Research Service (CRS) of the Library of Congress, and now works for the CRS as a research specialist in technology and national security for the Foreign Affairs, Defense, and Trade Division.

Bibliography

Monographs and Journal Articles

Abele-Wigert, Isabelle and Myriam Dunn. International CIIP Handbook 2006, Vol. I.: An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies (Zurich: Center for Security Studies, 2006).

Akintoye, Akintola, Matthias Beck and Cliff Hardcastle (eds). Public-Private Partnerships: Managing Risks and Opportunities (Oxford: Blackwell, 2003).

Alberts, Christopher and Audrey Dorofee. OCTAVESM Method Implementation Guide, version 2.0, vols. 1–18 (Carnegie Mellon University, June 2001).

Allen, Julia H. and Carol A. Sledge. "Information Survivability: Required Shifts in Perspective". In: CrossTalk: The Journal of Defense Software Engineering (July 2002), pp. 7–9.

Anderson, Ross. "Unsettling Parallels Between Security and the Environment". Economics and Information Security Workshop (Berkeley, 16–17 May 2002). Available at: http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/37.txt.

Andersson, Jan Joel. "Public-Private Partnerships and Emergency Preparedness". Paper presented at the conference on National deregulation and European reregulation, organized by Stockholm Centre for Organisational Research (Stockholm, 27 February 2004).

Andersson, Jan Joel. States, Markets and National Autonomy (Stockholm: ÖCB, 2000).

Andersson, Ross. "Why Information Security is Hard: An Economic Perspective". In: IEEE Computer Society (ed.). Proceedings of the 17th Annual Computer Security Applications Conference (New Orleans, 10– 14 December 2001). Available at: http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/econ.pdf.

Aradau, Claudia. "Beyond Good and Evil: Ethics and Securitization /Desecuritization Techniques". In: Rubikon, December 2001. Available at: http://venus.ci.uw.edu.pl/~rubikon/forum/claudia2.htm.http://venus.ci.uw.edu.pl/~rubikon/forum/claudia2.htm.

Aradau, Claudia. "Migration: The Spiral of (In)Security". In: Rubikon, March 2001. Available at: http://venus.ci.uw.edu.pl/~rubikon/forum/claudia1.htm.

Archick, Kristin. Cyber-crime: The Council of Europe Convention. CRS Report for Congress, RS21208, 26 April 2002) (Washington, DC: Congressional Research Service, 2002).

Arquilla, John. "The Great Cyberwar of 2002. A WIRED Scenario". In: WIRED (6 February 1998), pp. 122–127, 160–170.

Barnekov, Timothy, Robin Boyle and Daniel Rich. Privatism and Urban Policy in Britain and the United States (New York: Oxford University Press, 1989).

Baron, David T. "The Economics and Politics of Regulation: Perspectives, Agenda, and Approaches". In: Banks, Jeffrey S. and Eric A. Hanushek (eds.). Modern Political Economy (Cambridge: Cambridge University Press, 1995), pp. 10–62.

Beamish, T.D. Silent Spill (Cambridge: M.I.T. Press, 2002).

Beers, Rand and Francis X. Taylor. "Narco-Terror: The Worldwide Connection Between Drugs and Terror". Testimony before the US Senate Judiciary Committee, Subcommittee on Technology, Terrorism, and Government Information, 13 March 2002.

Bendrath, Ralf. "Critical Infrastructure Protection in the United States". ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead (Zurich, 8–10 November 2001).

Bendrath, Ralf. "The American Cyber-Angst and the Real World – Any Link?" In: Robert Latham (ed.), Bombs and Bandwidth: The Emerging Relationship between IT and Security (New York, The New Press, 2003), pp. 49–73.

Benson, Bruce L. "The Spontaneous Evolution of Cyber-Law: Norms, Property Rights, Contracting, Dispute Resolution and Enforcement Without the State of Law". In: Journal of Law, Economics and Policy, Vol. 1, No. 2 (2005). Available at: http://www2.sjsu.edu/depts/economics/faculty/powell/docs/econ206/Cyber-Law-Evolution.pdf.

Berkowitz, Bruce and Robert W. Hahn. "Cyber-security: Who's Watching the Store?" In: Issues in Science and Technology (Spring 2003). Available at http://www.issues.org/19.3/berkowitz.htm

Berkowitz, Bruce D. American Security (Yale: Yale University Press, 1986).

Bertalanffy, Ludwig von. General Systems Theory: Foundations, Development, Applications (New York: George Braziller Publishing, 1968).

Bertalanffy, Ludwig von. Perspectives on General System Theory: Scientific-Philosophical Studies (New York: George Braziller Publishing, 1975).

Boot, Pieter. European Energy Markets: Challenges for Policy and Research (The Hague: Ministry of Economic Affairs, 2003).

Bozeman, Barry. All Organizations are Public: Bridging Public and Private Organizational Theories (San Francisco: Jossey-Bass Inc., 1987).

Bundesamt für Sicherheit in der Informationstechnik. IT Baseline Protection Manual: Standard Security Safeguards (updated July 2001). Available at: http://www.iwar.org.uk/comsec/resources/standards/germany/itbpm/menue.htm.

Bundesministerium des Innern. Schutz Kritischer Infrastrukturen – Basisschutzkonzept: Empfehlungen für Unternehmen (Berlin, 2005). Available at: http://www.bmi.bund.de/cln_012/nn_165104/Internet/Content/Themen/Terrorismus/DatenundFakten/Basisschutzkonzept__fuer__Unternehmen__und__kritische__Infrastrukturen.html.

Center for Strategic and International Studies. Cyber Threats and Information Security - Meeting the 21st Century Challenge (Washington D.C: Center for Strategic and International Studies, December 2000).

Cerny, Philip J. "Globalization and the Changing Logic of Collective Action". In: International Organization, Vol. 49, No. 4 (1995), pp. 595–625.

Chandler, Daniel. "Technological or Media Determinism". Online resource, created on 18 September 1995. http://www.aber.ac.uk/media/Documents/tecdet/tdet02.html.

Chapman, Gary. "National Security and the Internet". Paper presented at the Annual Convention of the Internet Society (Geneva, July 1998).

Charters, David. "The Future of Canada's Security and Defence Policy: Critical Infrastructure Protection and DND Policy and Strategy". Research Paper of the Council for Canadian Security in the 21st Century (Canadian Security Intelligence Service, July 2001).

Clinton, William J. Executive Order 13010 on Critical Infrastructure Protection (Washington, 15 July 1996).

Coase, Ronald. "The Lighthouse in Economics". In: Journal of Law and Economics, Vol. 17, No. 2 (1974), pp. 357–376.

Commonwealth of Australia, Information Security Group. Australian Communications-Electronic Security Instruction 33 (ACSI 33) Handbook 3, Risk Management. Available at: http://www.dsd.gov.au/library/infosec/acsi33.html.

Computer Science and Telecommunications Board, National Research Council. Trust in Cyber-space (Washington, D.C.: National Academy Press, 1999).

Crutchfield, James P. "Is Anything Ever New? Considering Emergence". In: Cowan, G., D. Pines, and D. Melzner (eds). Complexity: Metaphors, Models, and Reality, SFI Series in the Sciences of Complexity XIX (Addison-Wesley: Redwood City, 1994), pp. 479–497.

Cukier, Kenneth Neil, Viktor Mayer-Schoenberger and Lewis Branscomb. "Ensuring (and Insuring?) Critical Information Infrastructure Protection". KSG Working Paper No. RWP05-055 (October 2005).

Curtis, Glenn and Tara Karacan. "The Nexus Among Terrorists, Narcotics Traffickers, Weapons Proliferators, and Organized Crime Networks in Western Europe". Federal Research Division, Library of Congress (Washington, DC, December 2002).

Davis, Anthony. "The Afghan Files: Al-Qaeda Cocuments from Kabul". In: Jane's Intelligence Review, 1 February 2002.

Davis, Perry. Public Private Partnerships — Improving Urban Life (New York: Academy of Political Science, 1986).

Demchak, C.C. Military Organizations, Complex machines: Modernization in the U.S. Armed Services (Ithaca, N.Y.: Cornell University Press, 1991).

Denning, Dorothy. "Is Cyber Terror Next?" In: Calhoun, Craig, Paul Price, and Ashley Timmer (eds.). Understanding September 11 (New York: W. W. Norton, 2002).

Dizard, Wilson. "Cyber-security plans wait for DHS to complete its evaluation of threats". In: Government Computer News, Vol. 24, No. 20 (25 July 2005).

Dunn, Myriam and Isabelle Wigert. International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries (Zurich: Center for Security Studies, 2004).

Dunn, Myriam. "Critical Information Infrastructure Protection (CIIP). Sicherheit im Informationszeitalter als gemeinsame Herausforderung für Politik und Wirtschaft". In: digma: Zeitschrift für Datenrecht und Informationssicherheit (June 2004).

Dunn, Myriam. "Cyber-Threats and Countermeasures: Towards an Analytical Framework for Explaining Threat Politics in the Information Age". Conference paper, SGIR Fifth Pan-European IR Conference, The Hague, 10 September 2004.

Dunn, Myriam. "The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP)". In: International Journal for Critical Infrastructure Protection, Vol. 1, No. 2/3 (2005), pp. 58–68.

Dunn, Myriam. "Threat Frames in the US Cyber-Terror Discourse". Conference paper, British International Studies Association (BISA) Conference. Warwick, 21 December 2004.

Dunn, Myriam. "Part II: Overview of Methods and Models to Assess Critical Information Infrastructures". In: Dunn, Myriam and Isabelle Wigert.

International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries (Zurich: Center for Security Studies, 2004), pp. 219–297.

Dunn, Myriam. Information Age Conflicts: A Study on the Information Revolution and a Changing Operating Environment. Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung, No. 64 (Zurich: Center for Security Studies, 2002).

Eeten, M. van, H. de Bruijn, M. Kars, H. van der Voort, J. van Till. "The Governance of E-Security: A Framework for Policy". Report to the Directorate General of Telecommunications and Post (Delft/Den Haag/ Amsterdam: TU Delft & Stratix, 2004).

Eeten, M.J.G. van and Emery Roe. Ecology, Engineering and Management: Reconciling Ecosystem Rehabilitation and Service Reliability (New York: Oxford University Press, 2002).

Ellison, R. J., D. A. Fisher, R. C. Linger, H. F. Lipson, T. Longstaff, and N. R. Mead. Survivable Network Systems: An Emerging Discipline. Technical Report. CMU/SEI-97-TR-013. ESC-TR-97-013 (November 1997), pp. 4–6.

Emergency Management Australia. Critical Infrastructure Emergency Risk Management and Assurance Handbook (Mt. Macedon, 2003). Available at: http://www.ema.gov.au/agd/EMA/emaInternet.nsf/Page/Emergency_Management_ERM_ERM.

Erickson, Jon. Hacking: The Art of Exploitation (San Francisco: No Starch Press, 2003).

Evan, W.M. and M. Manion. Minding the Machines: Preventing Technological Disasters (Saddle River, NJ: Prentice Hall, 2002).

Federal Reserve, New York State Banking Department, Office of the comptroller of Currency, Securities and Exchange Commission. Summary of 'lessons learned' and Implications for Business Continuity (13 February 2002).

Federal Strategy Unit for Information Technology (FSUIT). Verletzliche Informationsgesellschaft: Herausforderung Informationssicherung (Bern 2002). Available at: http://www.fgsec.ch/events/ft2003.03/pia_d.pdf.

Government Accountability Office (GAO). "Information Security: Emerging Cyber-security Issues Threaten Federal Information Systems". GAO report 05-231, May 2005.

Gartner Research. "Digital Pearl Harbor: Defending Your Critical Infrastructure", 4 October 2002. Available at: http://www.gartner.com/resources/110500/110534/digital_pearl_h.pdf.

Goodman, John C. and Philip K. Porter. "Political Equilibrium and The Provision of Public Goods". In: Public Choice, Vol. 120, No. 3–4 (September 2004), pp. 247–266.

Goodman, Seymour. E. "The Protection and Defense of Critical Information Infrastructures". Paper presented at the 43rd Annual IISS Conference, "The Strategic Implications of the New Economy" (Geneva, 12–15 September 2001).

Gordon, Sarah and Richard Ford. "Cyber-terrorism?" Symantec Security Response, White Paper (2003). Available at: http://www.symantec.com/avcenter/reference/cyberterrorism.pdf.

Grady, Mark and Francesco Parisi. "The Law and Economics of Cyber-security: An Introduction". George Mason University School of Law and Economics Working Paper Series No 04–54 (November 2004).

Gran, Bjørn Axel. The CORAS Methodology for Model-Based Risk Assessment, version 1.0, WP2, Deliverable 2.4 (29 August 2003).

Greenwald, Bruce C., and Joseph E. Stiglitz. "Externalitities in Economies with Imperfect Information and Incomplete Markets". In: Quarterly Journal of Economics, Vol. 101 (1986), pp. 229–264.

Haimes, Yacov Y. and Pu Jiang. "Leontief-Based Model of Risk in Complex Interconnected Infrastructures". In: Journal of Infrastructure Systems, Vol. 7, No. 1 (2001), pp. 1–12.

Haimes, Yacov Y. Risk Modeling, Assessment, and Management (New York, 1998).

Henriksen, Stein. "The Shift of Responsibilities within Government and Society". In: CRN-Workshop Report: Societal Security and Crisis Man-

agement in the 21st Century (Stockholm: Swedish Emergency Management Agency and ETH Zurich, 2004), pp. 60–63.

Héretier, Adrienne. "Market Integration and Social Cohesion: The Politics of Public Services in European Integration". In: Journal of European Public Policy Vol. 8, No. 5 (2001), pp. 825–52.

Héretier, Adrienne. "Public-Interest Services Revisited". In: Journal of European Public Policy Vol. 9, No. 6 (2002), pp. 995–1019.

Herrera, Geoffrey. "Technology and International Systems". In: Millennium, Vol. 32, No. 3, (2003), pp. 559–94.

Hey, Donald L. and Nancy S. Phillipi. "Reinventing Flood Control Strategy". Wetlands Initiative (September 1994). Available at: http://www.wetlands-initiative.org/images/pdfs_pubs/reinvent.pdf.

Homer-Dixon, Thomas. The Ingenuity Gap (New York: Knopf, 2000).

Huysmans, Jef. "Revisiting Copenhagen: Or, On the Creative Development of a Security Studies Agenda in Europe". In: European Journal of International Relations, Vol. 4, No. 4 (1998), pp. 479–506.

Joint Economic Committee, United States Congress. Security in the Information Age. New Challenges, New Strategies (Washington, May 2002).

Juran J. M. "The Quality Trilogy: A Universal Approach to Managing for Quality". In: Quality Progress, Vol. 19, No. 8 (August 1986), pp. 19–24.

Juster, Kenneth I. and John S. Tritak. "Critical Infrastructure Assurance: A Conceptual Overview". In: Security in the Information Age: New Challenges, New Strategies (Washington, DC: Joint Economic Committee, United States Congress, 2002).

Karas, Thomas H. Energy and National Security. Sandia Report, SAND2003-3287, Unlimited Release (September 2003).

Kesan, Jay P.Ruperto P. Majuca, and William J. Yurcik. "Cyber-Insurance as a Market-Based Solution to the Problem of Cyber-Security – A Case Study". 4th Workshop on the Economics of Information Security (WEIS), Harvard University, 2–3 June 2005. Available at: http://infosecon.net/workshop/pdf/42.pdf.

Keyes, David. "Cyber- Early Warning: Implications for Business Productivity and Economic Security". In: Security in the Information Age: New Challenges, New Strategies, (Washington, DC: Joint Economic Committee, United States Congress, 2002), pp. 42–43.

Knill, Christoph, and Dirk Lhemkuhl. Private Actors and the State: Internationalization and Changing Patterns of Governance. Governance: An International Journal of Policy, Administration, and Institutions. Vol. 15, No. 1 (2002), pp. 41–63.

Marwick, Peat. Vulnerability Assessment Framework 1.1. Prepared under contract for the Critical Infrastructure Assurance Office (October 1998).

Krasner, Stephen D. (ed.). International Regimes (Ithaca: Cornell University Press, 1984).

Kunreuther, Howard, and Geoffrey Heal. "Interdependent Security". In: Journal of Risk and Uncertainty, Vol. 26, No. 2–3 (March/May 2003), pp. 231–249.

Kunreuther, Howard, Geoffrey Heal, and Peter Orszag. "Interdependent Security: Implications for Homeland Security Policy and Other Areas". Policy Briefs #108 (Brookings Institution, October 2002).

Lafont, Jean-Jacques and Jean Tirole. A Theory of Incentives in Procurement and Regulation (Cambridge, M.A.: MIT Press, 1994).

Langer, E. Mindfulness (New York: Addison-Wesley, 1989).

LaPorte, Todd. "High Reliability Organizations: Unlikely, Demanding and At Risk". In: Journal of Contingencies and Crisis Management, Vol. 4, No. 2 (1996), pp. 60–71.

LaPorte, Todd. and P. Consolini. "Working In Practice But Not In Theory: Theoretical Challenges of High Reliability Organizations". In: Public Administration Research and Theory, Vol. 1, No. 1 (1991), pp. 19–47.

LaPorte, Todd. "A Strawman Speaks Up: Comments on Limits of Safety". In: Journal of Contingencies and Crisis Management, Vol. 2 (1994), pp. 207–211.

Laudel, Grit. "Collaboration, Creativity and Rewards: Why and How Scientists Collaborate". In: International Journal of Technology Management, Vol. 22, No. 7/8 (2001), pp. 762–81.

LaVerle, Berry, Glenn E Curtis, Rex A. Hudson, and Nina A. Kollars. "A Global Overview of Narcotics - Funded Terrorist and Other Extremist Groups". Federal Research Division, Library of Congress (Washington, DC, May 2002).

Levy, Steven. Hackers: Heroes of the Computer Revolution (New York: Anchor Press, 1984).

Lewis, James A. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats (Washington, DC: Center for Strategic and International Studies, 2002).

Lourdeau, Keith. FBI Deputy Assistant Director, Testimony before the US Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security, 24 February 2004.

Luiijf, Eric A.M., Helen H. Burger, and Marieke H.A. Klaver. "Critical Infrastructure Protection in The Netherlands: A Quick-scan". In: Gattiker, Urs E., Pia Pedersen, and Karsten Petersen (eds.). EICAR Conference Best Paper Proceedings 2003.

Mackenzie, Donald and J. Wajcman (eds.). The Social Shaping of Technology: How the Refrigerator Got its Hum (Buckingham: Open University Press, 1994, reprint).

Malm, Andreas, Jan Softa, Jan Joel Andersson, and Klas Lindström. IT och sårbarhet — kritiska beroendeförhållanden i den nationella IT-infrastrukturen. Temaserie 2003:5 (Stockholm: KBM, 2003).

Malm, Andreas, Klas Lindström, and Jan Joel Andersson. Finansiella sektorns motståndskraft mot infrastrukturella störningar av samhällshotande art [Resilience in the Financial Sector]. Report. Finansinspektionen (Stockholm: KBM, 2003).

Malm, Andreas, Klas Lindström, and Jan Joel Andersson. Kritiska beroendeförhållanden i den nationella IT-infrastrukturen. Opublicerad rapport (Stockholm: KBM, 2003).

Malm, Andreas, Klas Lindström, Jacob Henricson, Jan Softa, and Jan Joel Andersson.. Hel Projektet, Dokumentation från samverkansseminarium 23–24 Oktober 2003. Unpublished manuscript. Energimyndigheten (2003c).

Meier, A. von. "Occupational cultures as a challenge to technological innovation". In: IEEE Transactions on Engineering Management Vol. 46, No. 1 (1999), pp. 104 –114.

Mendez, Patrice Ossona de. "The Risks and Challenges of Interdisciplinarity". Online Seminar on Interdisciplinarity, online comment (2 April 2003). Available at http://www.interdisciplines.org/interdisciplinarity/papers/1/2#_2.

Methods to Achieve Information Systems Security. Expression of Needs and Identification of Security Objectives (EBIOS). Available at: http://www.ssi.gouv.fr/en/confidence/methods.html.

Metzger, Jan. "The Concept of Critical Infrastructure Protection (CIP)". In: A.J.K. Bailes/I. Frommelt (eds.). Business and Security: Public-Private Sector Relationships in a New Security Environment (Oxford University Press: Oxford, 2004), pp. 197–209.

Mihata, Kevin. "The Persistence of 'Emergence'". In: Eve, Raymond A., Sara Horsfall, and Mary E. Lee (eds.). Chaos, Complexity, and Sociology: Myths, Models, and Theories (Thousand Oaks (etc.): Sage Publications, 1997), pp. 30–38.

Minihan, Kenneth A. Prepared statement by Lt. Gen. Kenneth A. Minihan, Director, National Security Agency, before the Senate Governmental Affairs Committee, 24 June 1998.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Critical Infrastructure Protection in the Netherlands: Quick Scan on Critical Product and Services (April 2003).

Morgan, G. Images of Organization (New York: Sage Publications, 1997).

Moteff, John D. Critical Infrastructures: Background, Policy, and Implementation (Washington, DC: CRS Report for Congress, Congressional Research Service, 2002).

Moteff, John, Claudia Copeland, and John Fischer. Critical Infrastructures: What Makes an Infrastructure Critical? CRS Report for Congress RL31556 (Washington, DC: CRS Report for Congress, Congressional Research Service, updated 29 January 2003).

Mueller, Robert. Testimony before the US Senate Select Committee on Intelligence, February 11, 2003.

Näf, Michael. "Ubiquitous Insecurity? How to "Hack" IT Systems". In: Wenger, Andreas (ed.). The Internet and the Changing Face of International Relations and Security. Information & Security: An International Journal, Volume 7, (2001), pp. 104–18

Narich, Richard. Critical infrastucture protection : importance, complexity, results. In: Défense national et sécurité collective, No. 11 (Novembre 2005).

National Academy of Sciences, Computer Science and Telecommunications Board. Computers at Risk: Safe Computing in the Information Age (Washington D.C.: National Academy Press, 1991),

National Contingency Planning Group. Canadian Infrastructures and their Dependencies (March 2000).

National Research Council. "Making The Nation Safer: The Role of Science and Technology in Countering Terrorism" (Washington, D.C. National Academy Press, 2002).

New South Wales Office of Information and Communications Technology's (OICT). Information Security Guideline for NSW Government Part 1 — Information Security Risk Management. No. 3.2 (first published in September 1997, current version: June 2003).

Newbury, David M. Missing Markets: Consequences and Remedies. In The Economics of Missing Markets, Information and Games (Oxford: Clarendon Press, 1990).

Newlove, Lindy, Eric Stern, and Lina Svedin. Auckland Unplugged: Coping with Critical Infrastructure Failure (Baltimore: Lexington Books, 2003).

Nicander, Lars and Magnus Ranstorp (eds.). Terrorism in the Information Age — New Frontiers? (Stockholm: Swedish National Defence College, 2004).

Norman, D. The Design of Everyday Things (New York: Basic Books, 2002).

O'Hanlon, Michael, Peter R. Orszag, and Ivo H. Daalder. Protecting the American Homeland. One Year On (Washington, D.C.: Brookings Institution Press, 2003).

OECD. World Energy Outlook 2000 (Paris: OECD 2000).

Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP). Tool to Assist Owners and Operators to Identify Critical Infrastructure Assets (19 December 2002).

Office of Critical Infrastructure Protection and Emergency Preparedness. "Threats to Canada's Critical Infrastructure", Threat Analysis TA03-001 (12 March 2003).

Office of the Manager, National Communications System. The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Internet Communications (December 2000).

Osborne, Stephen P. Public-Private Partnerships: Theory and Practice in International Perspective (London: Routledge, 2000).

Parsons, T.J. "Protecting Critical Information Infrastructures. The Co-ordination and Development of Cross-Sectoral Research in the UK". Plenary address at the Future of European Crisis Management Conference (Uppsala, March 2001).

Perrow, Charles. "The Organizational Context of Human Factors Engineering". In: Administrative Science Quarterly, Vol. 28 (1983), pp. 521–541.

Perrow, Charles. Complex Organizations: A Critical Essay (New York: Wadsworth, 1979).

Perrow, Charles. "Review of S. D. Sagan's 'Limits of Safety'". In: Journal of Contingencies and Crisis Management, Vol. 2 (1994), pp. 212–220.

Perrow, Charles. Normal Accidents: Living with High-Risk Technologies (New York: Basic Books, 1984).

Personick, Stewart D. and Cynthia A. Patterson (eds.). Critical Information Infrastructure Protection and the Law: An Overview of Key Issues (Washington, D.C.: National Academies Press, 2003)

Porteous, Holly. "Some Thoughts on Critical Information Infrastructure Protection". In: Canadian IO Bulletin, Vol. 2, No. 4 (October 1999).

Powell, Benjamin. "Is Cyber-Security a Public Good? Evidence from the Financial Services Industry" The Independent Institute Working Paper, 14 March 2005. Available at: http://www.independent.org/pdf/working_papers/57_cyber.pdf.

Préfontaine, Daniel C. and Yvon Dandurand. "Terrorism and Organized Crime: Reflections on an Illusive Link and its Implication for Criminal Law Reform". International Society for Criminal Law Reform, Annual Meeting, Workshop D-3 Security Measures and Links to Organized Crime (Montreal, 8–12 August, 2004).

President's Commission on Critical Infrastructure Protection (PCCIP). Critical Foundations: Protecting America's Infrastructures (Washington, DC, October 1997).

President's Information Technology Advisory Committee. Cyber- Security: A Crisis of Prioritization. Report to the President (Washington, February 2005).

Priddle, R. "Security of Supply in Liberalized Electricity Markets". Eurelectric Annual Convention (Leipzig, 24–25 June 2002).

Przeworski, Adam. States and Markets (Cambridge: Cambridge University Press 2003).

Randazzo, Marisa (et al). "Insider Threat Study: Illicit Cyber- Activity in the Banking and Finance Sector". Technical Report, CMU/SEI-2004-TR-021 Carnegie Mellon Software Engineering Institute, August 2004.

Reason, J. Human Error (Cambridge: Cambridge University Press, 1972).

Reinermann, Dirk and Joachim Weber. "Analysis of Critical Infrastructures: The ACIS Methodology (Analysis of Critical Infrastructural Sectors)".

Paper presented at the Critical Infrastructure Protection (CIP) Workshop (Frankfurt, 29–30 September 2003).

Remarks by US Secretary of Homeland Security Michael Chertoff at the Center for Catastrophic Preparedness and Response and the International Center for Enterprise Preparedness (New York, 26 April 2005).

Rijpma, J.A. "Complexity, Tight Coupling and Reliability." In: Journal of Contingencies and Crisis Management, Vol. 5 (1997), pp. 15–23.

Rinaldi, Steven M., James P. Peerenboom, and Terrence K. Kelly. "Complex Networks. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies". In: IEEE Control Systems Magazine, Vol. 21, No. 6 (December 2001), pp. 11–25.

Roberts, K. "Some Characteristics of One Type of High Reliability Organization". In: Organization Science, Vol. 1, No. 2 (1990), pp. 160–176.

Roberts, K. New Challenges To Understanding Organizations (New York: Macmillan, 1993).

Rochlin, G.I "Defining High Reliability Organizations in Practice". In: K. Roberts (ed.). New Challenges To Understanding Organizations (New York: Macmillan, 1993), pp. 11–32.

Rochlin, G.I. and A. von Meier. "Nuclear Power Operations: A Cross Cultural Perspective". In: Annual Review of Energy and Environment, Vol. 19 (1994), pp. 153–187.

Roe, E., M.J.G. van Eeten, P.R. Schulman & M. de Bruijne. Real-Time Reliability: Provision of Electricity Under Adverse Performance Conditions Arising from California's Electricity Restructuring and Crisis. A report prepared for the California Energy Commission, Lawrence Berkeley National Laboratory, and the Electrical Power Research Institute (San Francisco: California Energy Commission, 2002).

Roe, E., P. Schulman, M. van Eeten and M. de Bruijne. "High Reliability Bandwidth Management in Large Technical Systems." In: Journal of Public Administration Research and Theory, Vol. 15, No. 1 (2005), pp. 263–280.

Rood, Justin. "Animal Rights Groups and Ecology Militants Make DHS Terror List, Right-Wing Vigilantes Omitted". In: CQ Homeland Security, 25 March 2005.

Sagan, S. The Limits of Safety (Princeton; Princeton University Press, 1993).

Salvendy, G. Handbook of Human Factors and Ergonomics (New York: Wiley, 1997).

Sanne, J. M. Creating Safety in Air Traffic Control (Lund: Arkiv Forlag, 2000).

Schmitz, Walter. ACIP D6.4 Comprehensive Roadmap - Analysis and Assessment for CIP. Work Package 6, Deliverable D6.4, Version 1 (European Commission Information Society Technology Program, May 2003).

Schneier, Bruce. Attack Trends: 2004 and 2005. 6 June 2005.

Schulman, P.R. "Medical Errors: How Reliable Is Reliability Theory?" In: Rosenthal, M.M. and K. M. Sutcliffe (eds.). Medical Error (San Francisco: Jossey Bass, 2002), pp. 200–216.

Schulman, P.R. "The Analysis of High Reliability Organizations: a Comparative Framework". In: Roberts, K. (ed.). New Challenges To Understanding Organizations (New York: Macmillan, 1993), pp. 33–54.

Schulman, P.R. "The Negotiated Order of Organizational Reliability". In: Administration and Society, Vol. 25, No. 3 (1993), pp. 353–372.

Schulman, P.R., E. Roe, M.J.G. van Eeten, and M. de Bruijne. "High Reliability and the Management of Critical Infrastructures". In: Journal of Contingencies and Crisis Management, Vol. 12, No. 1 (2004), pp. 14– 28.

Schwartau, Winn. Information Warfare. Cyberterrorism: Protecting Your Personal Security in the Electronic Age (New York: Thundermouth Press, 1994, 2nd ed.).

Shelley, Louise and John T. Picarelli. "Methods Not Motives: Implications of the Convergence of International Organized Crime and Terrorism". In: Police Practice and Research, Vol. 3, No. 4, (2002).

Shelly, Louise. Organized Crime, Cyber-crime and Terrorism (Computer Crime Research Center, 27 September 2004).

Shuttleworth et al. Security of energy supply, Energy Regulation Brief. NERA, produced for Departement of Trade and Industry (2003).

Sperber, Dan. "Why Rethink Interdisciplinarity?". Online Seminar on Interdisciplinarity, Paper (no date). Available at http://www.interdisciplines.org/interdisciplinarity/papers/1/4.

Spiller, Pablo T. "Regulatory Commitments and Utilities' Privatization: Implications for Future Comparative Research". In: Banks, Jeffrey S. and Eric A. Hanushek (eds.) Modern Political Economy (Cambridge: Cambridge University Press, 1995), pp. 63–79.

Standards Australia/Standards New Zealand. Risk Management AS/NZS 4360:1999 (Strathfield, 12 April 1999).

Stigler, George. The Citizen and the State. Essays on Regulation (Chicago: University of Chicago Press, 1975).

Stiglitz, Joseph E. and Carl E. Walsh. Principles of Microeconomics (New York: W. W. Norton & Company, 2004, 4th Edition).

Stiglitz, Joseph E. Whither Socialism? (Cambridge: MIT Press 1994).

Stoneburner, Gary, Alice Goguen, and Alexis Feringa. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-30 (Washington, January 2002).

Strogatz, Steven H. "Exploring Complex Networks". Nature, 410 (8 March 2001), pp. 268–276.

Symantec press release. "Symantec Internet Security Threat Report Highlights Rise In Threats To Confidential Information", 21 March 2005.

Technical Analysis Group (TAG), Institute for Security Technology Studies. Examining the Cyber Capabilities of Islamic Terrorist Groups (Dartmouth College, 2003).

The White House. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (Washington, February 2003).

Thomas, Timothy L. "Al Qaeda and the Internet: The Danger of 'Cyberplanning'" In: Parameters Spring (2003), pp. 112–123.

TNO Information and Communication Technology. TNO report 33680. International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues (30 June 2005).

Turner, B. M. Man-Made Disasters (London: Wykeham, 1978).

UK Department of Trade and Industry. Cm.5761 White Paper: Our Energy Future – Creating a Low Carbon Economy (February 2003).

US Secret Service and Carnegie Mellon University Software Engineering Institute. Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors (2005).

Vaillancourt Rosenau, Pauline (ed.). Public-Private Policy Partnerships (Cambridge: MIT Press).

Vaughn D. The Challenger Launch Decision (Chicago: University of Chicago Press, 1996).

Verbist, S. Reliability in Mobile Telecommunications under Rapidly Changing Conditions (confidential report) (Delft: Delft University of Technology, 2002).

Verton, Dan. Black Ice: The Invisible Threat of Cyber-Terrorism (Emeryville: McGraw-Hill/Osborne, 2003).

Waltzer, N. and B. Jacobs (eds.). Public-Private Partnerships for Local Economic Development (Westport: Praeger, 1998).

Weick, K. E. "The Vulnerable System: An Analysis of the Tenerife Air Disaster". In Roberts, K. (ed.). New Challenges To Understanding Organizations (New York: Macmillan, 1993), pp. 173–97.

Weick, K. E. and K.M. Sutcliffe. Managing The Unexpected (San Francisco: Jossey Bass, 2001).

Weick, K. E., K.M. Sutcliffe, and D. Obstfeld. "Organizing For High Reliability". In: Research in Organizational Behavior, Vol. 21 (1999), pp. 81–123.

Weimann, Gabriel. "Cyberterrorism - How Real Is the Threat?" United States Institute of Peace, Special Report 119, May 2004.

Weimann, Gabriel. www.terror.net. How Modern Terrorism Uses the Internet. United States Institute of Peace. Special Report 116, March 2004.

Wenger, Andreas, Jan Metzger and Myriam Dunn (eds.). The International CIIP Handbook: An Inventory of Protection Policies in Eight Countries (Zurich: Center for Security Studies, 2002).

Westrin, Peter. "Critical Information Infrastructure Protection". In: Wenger, Andreas (ed.): The Internet and the Changing Face of International Relations and Security. Information & Security: An International Journal, Vol. 7 (2001), pp. 67–79.

White Paper on PDD-63. The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 (Washington, 22 May 1998).

White, Gregory B. and David J. DiCenso. "Information Sharing Needs for National Security." In: Proceedings of the 38th Hawaii International Conference on System Sciences, 2005.

Wigert, Isabelle. "Der Schutz kritischer Informationsinfrastrukturen in der Schweiz: Eine Analyse von Akteuren und Herausforderungen". In: Bulletin zur schweizerischen Sicherheitspolitik 2005 (Zurich: Center for Security Studies, 2005), pp. 97–121.

Wikipedia, The Free Encyclopedia. s. v. "Public Goods". Available at: http://en.wikipedia.org/wiki/Public_goods.

Wildavsky, A. Searching For Safety (New Brunswick: Transaction Books, 1998).

Wilson, Clay. Computer Attack and Cyber-terrorism: Vulnerabilities and Policy Issues for Congress. CRS Report for Congress, RL32114 (Washington D.C., 17 October 2003).

Wolfers, Arnold. "National Security as an Ambiguous Symbol". In: Idem. Discord And Collaboration: Essays on International Politics (Baltimore: Johns Hopkins, 1962), pp. 147–165.

World Federation of Scientists Permanent Monitoring Panel on Information Security. "Information Security in the Context of the Digital Divide: Recommendations submitted to the World Summit on the Information Society at its Tunis phase (16 to 18 November 2005)". Document WSIS-05/TUNIS/CONTR/01-E, 2 September 2005, p. 23. Available at: http://www.itu.int/wsis/docs2/tunis/contributions/co1.doc.

World Summit on the Information Society, "Plan of Action". Document WSIS-03/GENEVA/DOC/5-E, 12 December 2003. Available at: http://www.itu.int/wsis/docs/geneva/official/poa.html.

World Summit on the Information Society. "Declaration of Principles Building the Information Society: A Global Challenge in the New Millennium". Document WSIS-03/GENEVA/DOC/4-E, 12 December 2003. Available at: http://www.itu.int/wsis/docs/geneva/official/dop.html.

Zimmermann, Doron. The Transformation of Terrorism. The "New Terrorism," Impact Scalability and the Dynamic of Reciprocal Threat Perception. In: Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung No. 67 (Zurich: Center for Security Studies, 2003).

Newspaper Articles

Associated Press. "CIA Overseeing 3 Day Wargame on Internet", 25 May 2005.

Bank, David and Christopher Conkey. "New Safeguards for Your Privacy". In: The Wall Street Journal, 24 March 2005.

BBC News. "Japan cardholders 'hit' by theft", 21 June 2005.

Bridis, Ted. "Silent Horizon war games wrap up for the CIA". In: USA Today, 26 May 2005.

Broache, Anne. "Worms could dodge net traps". In: News.com, 4 August 2005.

CeBIT technology trade show in March 2003. "Cyber-terror Threat Overblown". In: Computerworld, 14 March 2003.

Christensen, John. "Bracing for guerrilla warfare in cyberspace". In: CNN Interactive, 6 April 1999.

CNN. "FBI: Al Qaeda may have probed government sites", 17 January 2002.

Dizard, Wilson. "Cyber-security plans wait for DHS to complete its evaluation of threats". In: Government Computer News, Vol. 24, No. 20 (25 July 2005).

Douglas Schweitzer. "Be Prepared for Cyber-terrorism". In: Computerworld, 6 April 2005.

Durnout, Estelle. "Council of Europe ratifies cyber-crime treaty". In: ZDNet, 22 March 2004.

Evans, Michael and Daniel McGrory. "Terrorists Trained in Western Methods Will Leave Few Clues". In: London Times, 12 July 2005.

Evers, Joris. "Cisco Squashes 'Critical' Net Attack Bug." In: Cnet News.com, 2 November 2005.

Evers, Joris. "Does Cyber-terrorism Pose a True Threat". In: PCWorld, 14 March 2003.

Foley, John. "Businesses Slow to Deploy Windows XP SP2". In: Information Week, 26 April 2005.

Forno, Richard. "Shredding the Paper Tiger of Cyber-terrorism". In: Security Focus, 25 September 2002.

Garza, Victor. "Security researcher causes furor by releasing flaw in Cisco Systems IOS", SearchSecurity.com, 28 July 2005.

Glasser, Susan and Steve Coll. "The Web as Weapon". In: The Washington Post, 9 August 2005.

Gross, Grant. "Senators Call on DHS to Improve Cyber-security Efforts". In: IDG News Service, 19 July 2005.

Harrington, Caitlin. "Terrorists Can Exploit Identity Theft, Report From House Democrats Says". In: CQ Homeland Security, 1 July 2005.

IBM News. "Report finds online attacks shift toward profit", 2 August 2005.

IBM press release. IBM Report: Government, Financial Services and Manufacturing Sectors Top Targets of Security Attacks in First Half of 2005 (2 August 2005).

Kelley, Jack. "Terror groups hide behind Web encryption". In: USA Today, 6 February 2001.

Krim, Jonathan and Michael Barbaro. "40 Million Credit Card Numbers Hacked". In: Washington Post, 18 June 2005.

Lal, Rollie. "Terrorists and organized crime join forces". In: International Herald Tribune, May 25, 2005.

Lipton, Eric. "Homeland Report Says that Threat From Terror-List Nations is Declining". In: The New York Times, 31 March 2005.

Lubow, Eric. "Homeland Security CIO: No Digital Pearl Harbor Likely". In: Linux Security.com, 7 May, 2003.

McCullagh, Declan. "Tech Firms call for approval of cyber-crime treaty". In: Cnet.com News, 29 June 2005.

McWilliams, Brian. "Suspect Claims Al Qaeda Hacked Microsoft — Expert". In: Newsbytes, 17 December 2001.

Newsweek. "Islamic Cyberterror. Not a Matter of If But of When". 20 May 2002.

Poulsen, Kevin. U.S. Info-sharing initiative called a flop. Security Focus, 11 February 2005.

Rademacher, Kevin. "Clarke: ID theft prevention tied to anti-terrorism efforts". In: Las Vegas Sun, 13 April 2005.

Ribeiro, John. "Terrorists target India's outsourcing industry". In: InfoWorld, 7 March 2005.

Roberts, Paul. "Symantec Offers Early Warning of Net Threats". In: PCWorld, 12 February 2003.

Rood, Justin. "Animal Rights Groups and Ecology Militants Make DHS Terror List, Right-Wing Vigilantes Omitted". In: CQ Homeland Security, 25 March 2005.

Schweitzer, Douglas. "Be Prepared for Cyber-terrorism". In: Computerworld, 6 April 2005.

Spring, Tom. "Al Qaeda's Tech Traps". In: PCWorld, 1 September 2004.

Stanley, Theodore. "The Online Jihad". In: The Statesman, New Delhi, 8 March 2005.

Storer, Amy. Update: "IPv6 risks may outweigh benefits". In: SearchSecurity.com, 29 July 2005.

Tendler, Stewart. "Encrypted files frustrate police". In: Times Online, 20 July 2005.

The Economist. "Bring me your powerless masses", 23 August 2003.

Varian Hal R. "Managing Online Security Risks". In: New York Times, 1 June 2000. Available at: http://www.sims.berkeley.edu/~hal/people/hal/NYTimes/2000-06-01.html.

Wait, Patience. "Industry Groups urge Senate ratification of cyber-crime treaty". In: Government Computer News, 6 June 2005.

Walsh, Conal. "Terrorism on the cheap - and with no paper trail". In: The Guardian, 17 July 2005.

The Center for Security Studies at ETH Zurich (Swiss Federal Institute of Technology) was founded in 1986 and specializes in the fields of international relations and security policy. The Center coordinates and develops the Comprehensive Risk Analysis and Management Network (CRN), a Swiss-Swedish initiative for open dialog on risks and vulnerabilities that is aimed at enhancing knowledge of the causes, interactions, probabilities, and costs of risks in modern societies.

The International Critical Information Infrastructure Protection (CIIP) Handbook is a joint effort within the CRN partner network, which currently includes: The Swedish Emergency Management Agency (SEMA), Sweden; the Directorate for Civil Protection and Emergency Planning (DSB), Norway; the Federal Office for National Economic Supply (NES), Federal Department of Economic Affairs, Switzerland; and the Swiss Federal Department of Defense, Civil Protection, and Sports (DDPS), Switzerland.

The CIIP Handbook focuses on national governmental efforts to protect critical information infrastructure and provides an overview of CII protection practices in a range of countries and international organizations (Vol. I). Vol. II offers more in-depth analysis of key issues related to CIIP.