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.