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 "GetSafe-Online" 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.