Introduction

Evolution of the Critical Information Infrastructure Protection (CIIP) Issue

Critical information infrastructure protection (CIIP) is perceived as a key part of national security in numerous countries today and has become the nucleus of the US terrorism and homeland security debate after 11 September 2001. A *critical infrastructure* (CI) is commonly understood to be an infrastructure or asset the incapacitation or destruction of which would have a debilitating impact on the national security and the economic and social welfare of a nation.[2] Protection concepts for strategically important infrastructures and objects have been part of national defense planning for decades, though at varying levels of importance. Towards the end of the Cold War and for a couple of years thereafter, the possibility of infrastructure discontinuity caused by attacks or other disruptions played a relatively minor role in the security debate – only to gain new impetus around the mid-1990s.[3]

One reason for the resurgence of concepts for the protection of vital infrastructures has been the so-called *information revolution*, which has caused an ongoing transformation of all aspects of life through saturation with *Information and Communication Technologies* (ICT), and has led to a considerable broadening of the threat spectrum.[4] These two aspects reinforce one another, since it is perceived that the overall capability of malicious actors to do harm is enhanced by inexpensive, ever more

[2] The definition of critical infrastructure varies from country to country. Part I of the Handbook on Country Surveys shows in detail how each country defines the critical infrastructure and what sectors are included.

[3] Cf. 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.

[4] 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, 2002).

sophisticated, rapidly proliferating, easy-to-use tools in cyberspace.[5] This and the anticipated Y2K problem highlighted a new, delicate problem: the dependency of modern industrialized societies on a wide variety of national and international information infrastructures, characterized by highly interdependent software-based control systems.[6]

First Steps in the Protection of Critical Information Infrastructure

The US was the first nation to broadly address the new vulnerability of the vital infrastructures in a concerted effort. New risks in designated *sectors*[7] like information and communications, banking and finance, energy, physical distribution, and vital human services were identified by the *Presidential Commission on Critical Infrastructure Protection* (PCCIP).[8] The PCCIP concluded in 1997 that the security, economy, way of life, and perhaps even the survival of the industrialized world are now dependent on the interrelated trio of electrical energy, communications, and computers. The commission found that advanced societies rely heavily upon critical infrastructures, which are susceptible to classical physical disruptions and new virtual threats.[9]

Vulnerabilities in these infrastructures are believed to be on the rise due to increasing complex interdependencies. As most of the critical infrastructures are either built upon or monitored and controlled by vulnerable ICT systems, the "cyber-" infrastructure has become the new focal point

[5] The perception of a severe risk to national security grew parallel to the development of offensive information operations capabilities and strategies in the US. The twofold debate was triggered by the benefits of the "information differential" provided by C4I component systems employed in the first Gulf War on the one hand, and experiences with the threat of data intrusion as perpetrated by hacker attacks during the conflict on the other (cf. Eriksson, E. Anders. "Information Warfare: Hype or Reality?" *The Nonproliferation Review* (Spring-Summer 1999). http://cns.miis.edu/pubs/npr/vol06/63/erikss63.pdf).

[6] Cf. Mussington, David. *Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development*. (Santa Monica, 2002).

[7] A sector is defined as "A group of industries or infrastructures which perform a similar function within a society", see: President's Commission on Critical Infrastructure Protection (PCCIP). *Critical Foundations: Protecting America's Infrastructures.* (Washington, October 1997): Appendix B, Glossary, B-3.

[8] President's Commission on Critical Infrastructure Protection (PCCIP). *Critical Foundations: Protecting America's Infrastructures.* (Washington, October 1997). Publication quoted in the following as PCCIP.

[9] Ibid.

of protection policies. This part of the global or national information infrastructure, which is essential for the continuity of critical infrastructure services, is called *critical information infrastructure* (CII).

Following the PCCIP's publication, US President Bill Clinton started initiatives to increase the protection of critical infrastructure in the US, on the premise that a joint effort by government, society, organizations, and critical industries was needed to prepare for defending these vital assets.[10] The issue of CIIP has remained a high priority on the political agenda ever since; the events of 11 September 2001 merely served to further increase the awareness of vulnerabilities and the sense of urgency in protecting critical infrastructures.[11]

Within the last few years and following the example of the US, many countries have taken steps of their own to better understand the vulnerabilities of and threats to their CII, and have proposed measures for the protection of these assets. The CIIP Handbook will focus on these *national governmental efforts* to protect critical information infrastructure.

Distinction between CIP and CIIP

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. Accordingly, the reader will find both terms used in the CIIP Handbook. This is not due to a lack of accuracy or random use of the two concepts. Rather, the parallel use of terms reflects the stage of political discussion in the surveyed countries and points to the deficiencies in understanding conceptual differences between the concepts. But why would it be useful and desirable to arrive at a better distinction between the two concepts of CIP and CIIP? And what is their relation to each other?

[10] Clinton, William J. *Defending America's Cyberspace: National Plan for Information Systems Protection. An Invitation to a Dialogue.* Version 1.0 (Washington, 2000); 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.

[11] Bush, George W. *Executive Order 13228. Establishing the Office of Homeland Security and the Homeland Security Council.* (Washington, 8 October 2001). http://www.fas.org/irp/offdocs/eo/eo-13228.htm; Bush, George W. *Executive Order 13231. Critical Infrastructure Protection in the Information Age.* (Washington, 16 October 2001). http://www.fas.org/irp/offdocs/eo/eo-13231.htm.

In our view, CIP is more than CIIP, but CIIP is an essential part of CIP. There is at least one characteristic for the distinction of the two concepts: 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 definition of exactly what should be subsumed under CI, and what under CII, is another question: Generally, the CII is that part of the global or national information infrastructure that is essentially necessary for the continuity of a country's critical infrastructure services. The CII, to a large degree, consists of, but is not fully congruent with the information and telecommunications sector, and includes components such as telecommunications, computers/ software, the Internet, satellites, fiber-optics, etc. The term is also used for the totality of interconnected computers and networks and their critical information flows.

Protection of the CII has become especially important due to two reasons: 1) their invaluable and growing role in the economic sector; and 2) their interlinking role between various infrastructure sectors and the essential requirement that other infrastructures function at all times.[12] There are, moreover, several features that demand a clear distinction between CI and CII: First of all, the system characteristics of the emerging information infrastructure differ radically from traditional structures, including earlier information infrastructures: They differ in terms of scale, connectivity, and dependencies.[13] This means that understanding them will require new analytical techniques and methodologies that are not yet available.[14] Secondly, it appears that cyber-threats are evolving rapidly both in terms of their nature and of their capability to cause harm, so that protective measures require continual technological improvements and new approaches.

Moreover, there are several "drivers" that will likely aggravate the problem of CIIP in the future: these are the interlinked aspects of market forces, technological evolution, and emerging risks.[15] On the one hand, we are facing an ongoing dynamic globalization of information services, which in connection with technological innovation (e.g., localized wireless communication)

[12] Wenger, Andreas, Jan Metzger, and Myriam Dunn. "Critical Information Infrastructure Protection: Eine sicherheitspolitische Herausforderung». In: Spillmann, Kurt R. and Andreas Wenger (eds.). *Bulletin zur Schweizerischen Sicherheitspolitik* (Zurich, 2002), pp. 119–142.

[13] 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*, Uppsala, Sweden, March 2001.

[14] See also Part II of this Handbook.

will result in a dramatic increase of connectivity and lead to ill-understood behavior of systems, as well as barely understood vulnerabilities.

This assessment ties into the fact that security has never been a design driver. And since pressure to reduce time-to-market is intense, a further explosion of computer and network vulnerabilities is to be expected.[16] We are therefore faced with the potential emergence of infrastructures with in-built instability, critical points of failure, and extensive interdependencies. Additionally, increasingly large parts of the CI will be in the private sector and even in the hands of another nation-state.

This 'prospective' view clearly indicates a need to distinguish conceptually between the two concepts of CIP and CIIP. However, the two cannot and should not be discussed as completely separate concepts. As stated above, CIIP is an essential *part* of CIP. An exclusive focus on cyber-threats that ignores important traditional physical threats is just as dangerous as the neglect of the virtual dimension – what is needed is a sensible handling of both interrelated concepts.

CIP/CIIP: A Multifaceted Issue

CIP is an issue composed of many different branches of knowledge and includes an array of multi-faceted sub-categories. CIIP – understood as concerning the protection of the ICT sector and the CII underlying all other sectors – is thus an issue of high relevance to many different, very diverse, and often overlapping communities. These different groups do not necessarily agree on the nature of the problem or on what needs to be protected, so that the actual meaning of "CIIP" depends very much on the speaker.

The resulting veritable quagmire of definitions and discussions at cross-purposes is only the beginning of our difficulties. The differing positions also complicate the allocation of *responsibility* when it comes to the protection of critical information infrastructures and, by implication, in defining appropriate political tools for dealing with the problem. To complicate the picture, the boundaries between the different perspectives are by no means

[15] 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*, Uppsala, Sweden, March 2001.

[16] 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. 104–118.

clear-cut. Among the most important ones, we can list the following ideal-type and simplified perspectives:

- *The system-level, technical 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 detection software. The establishment of so-called *Computer Emergency Response Teams* (CERTs) and similar early-warning approaches in various countries is an example of this perspective.
- *The business perspective:* 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 outlined 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. Cybercrime is a very broad concept that has various meanings, ranging from technology-enabled crimes to crimes committed against individual computers, and including issues such as infringements of copyright, computer fraud, child pornography, and violations of network security. Cybercrime is fought with more or less traditional law-enforcement strategies, especially by adopting appropriate legislation and fostering international co-operation.
- *The national-security perspective*: This is a "grab-bag" view of CIIP. Usually, the whole of society is perceived as 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. This is the perspective adopted in assembling this Handbook.

In accordance with the different perspectives outlined above, information infrastructures are seen variously as a tool for maintaining a competitive edge over business adversaries, as technical-operational systems, as facilitators of criminal activities, as defense-relevant strategic assets, or more generally, as objects of national and international security policy. Depending on one's perspective, the issue may be perceived either as the private/corporate sector's responsibility or as the responsibility of specific governmental agencies, ranging from law enforcement to the defense establishment, or a mixture of all of the above; hence the diversity of approaches that can be found in the country surveys in this Handbook.

All of these perspectives have vital implications for protection policies. The 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[17] – and the answers may vary depending on the scenario –, and subsequently to the question of which protection efforts, goals, strategies, and instruments are appropriate for problem solution.[18] The fact that so many 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. It follows that, even if CIIP is perceived as politics of the extraordinary, states can no longer assure security on their own – rather, they must find new ways of interaction and cooperation with different national and international actors that have not traditionally been in the security arena, which is a much wider notion of governance than that which characterized the Cold War.

Key Terms and Concepts

The diversity of approaches to CIIP means that common understanding of pressing issues and the definition of common values and goals can only be achieved through precise use of language and frank statement of one's point of view. A critical evaluation of key terms and concepts is therefore required to reduce the confusion in taxonomy. To this end, two main points are further explained below: (1) The meaning of the term "critical" in the context of critical information infrastructure; and (2) the suitability of the concept of CIP, especially the focus on infrastructures as objects of protection.

[17] Metzger, Jan. "The Concept of Critical Infrastructure Protection (CIP)". In: Bailes, A. J. K. and Frommelt, I. (eds.). Stockholm International Peace Research Institute (SIPRI), *Business and Security: Public-Private Sector Relationships in a New Security Environment* (Oxford, forthcoming 2004).

[18] Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis*. (Boulder, 1998).

The Meaning of "Critical" in Critical Infrastructure Protection

The classification of what is "critical" lies mainly in the eye of the beholder. Having said that, the concept of criticality itself is also undergoing constant change. A look at CIP documents and at the many definitions and lists of critical infrastructures shows us great variety of conceptions. The main reason is that the criteria for determining which infrastructures qualify as critical have expanded over time; the PCCIP, for example, defined assets whose prolonged disruptions could cause significant military and economic dislocation as critical.[19] Today, critical infrastructures in the US also include national monuments (e.g., the Washington Monument), where an attack might cause a large loss of life or adversely affect the nation's morale.[20] This development shows two differing but interrelated ways of understanding criticality:[21]

- *Criticality as systemic concept*: This approach assumes that an infrastructure or an infrastructure component is critical due to its structural position in the whole system of infrastructures, especially when it constitutes an important link between other infrastructures or sectors, and thus reinforces interdependencies;
- *Criticality as a symbolic concept*: This approach assumes that an infrastructure or an infrastructure component is inherently critical because of its role or function in society; the issue of interdependencies is secondary – the inherent symbolic meaning of certain infrastructures is enough to make them interesting targets.[22]

The symbolic understanding of criticality allows the integration of non-interdependent infrastructures as well as objects that are not man-made into the concept of critical infrastructures, including significant personalities or natural and historical sights with a strong symbolic character. Additionally, the symbolic approach allows us to define essential (security policy–relevant) assets more easily than the systemic one, because it is not the interdepen-

[19] PCCIP, Appendix B, Glossary, B-2.

[20] Moteff, John, Claudia Copeland, and John Fischer. *Critical Infrastructures: What Makes an Infrastructure Critical?* CRS (Congressional Research Service) Report for Congress RL31556. (30 August 2002). http://www.fas.org/irp/crs/RL31556.pdf.

[21] The following is based on Metzger, Jan, "The Concept of Critical Infrastructure Protection (CIP)".

[22] For an example (critical assessment without interdependencies), see: United States General Accounting Office. Testimony before the Subcommittee on National Security, Veterans Affairs, and International Relations; House Committee on Government Reform, *Homeland Security: Key Elements of a Risk Management*, Statement of Raymond J. Decker, Director Defense Capabilities and Management, 12 October 2001, p. 6. http://www.house.gov/reform/ns/statements_witness/GAO-02-150T.pdf

dencies as such that are defining in a socio-political context, but the role, relevance, and symbolic value of specific infrastructures.[23]

Moreover, 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.[24] 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.

The Concept of Infrastructures as Focus of Protection

Is it really the infrastructures that we want to protect? Infrastructures are defined by the *Presidential Commission on Critical Infrastructure Protection* (PCCIP) as "network[s] of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services".[25] In Presidential Decision Directive (PDD) 63, they are described as "the framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security […]."[26]

If we compare the two concepts, the most striking similarity is the focus on "essential goods/products and services". That means that the actual objects of protection interests are not static infrastructures as such, 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. While infrastructures are constructed, maintained, and operated by humans and can be relatively easily illustrated in terms of organizational

[23] Metzger, Jan, "The Concept of Critical Infrastructure Protection (CIP)".

[24] 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, Volume 7 (2001), pp. 67–79.

[25] PCCIP, Appendix B, Glossary, B-2.

[26] Clinton, William J. *Protecting America's Critical Infrastructures: Presidential Decision Directive 63.* (22 May 1998).

and institutional hierarchies, services, flows, and values are a lot more complex, harder to capture, and more difficult to understand.[27]

This also shifts attention away from man-made assets, which makes perfect sense in the age of medial saturation in which the symbolic value of things has become over-proportionally important. To conclude this short excursion into terminology, it makes more sense both from the point of view of system dynamics and actual protection interest to speak of "*critical services robustness*" or "*critical services sustainability*".[28]

Purpose and Key Questions

The overall purpose of the International CIIP Handbook 2004 is to provide an overview of CII protection practices in a range of countries. The initial eight (Australia, Canada, Germany, the Netherlands, Norway, Sweden, Switzerland, and the United States) have been supplemented by six additional surveys (Austria, Finland, France, Italy, New Zealand, and the United Kingdom).

The Handbook is aimed mainly at security policy analysts, researchers, and practitioners. It can be used either as a reference work for a quick overview of the state of the art in CIIP policy formulation and CIIP methods and models, or as a starting point for further, in-depth research. Even though it now covers fourteen countries, the Handbook does not claim to offer a comprehensive analysis of the topic: It is still only a sketchy effort to collect existing policies, show broad developments in the field of CIIP, and assemble some of the methods and models used for CII analysis.

[27] Metzger, Jan, "The Concept of Critical Infrastructure Protection (CIP)".

[28] Cf. CRN Workshop on "Critical Infrastructure Protection in Europe – Lessons Learned and Steps Ahead", Zurich 9–10 November 2001), proceedings available online at: www.isn.ethz.ch/crn.

Structure of the Handbook

The book is guided by two main questions:

1) What national approaches to critical information infrastructure protection exist?
2) What methods and models are used in the surveyed countries to analyze and evaluate various aspects of the critical information infrastructure?

Accordingly, the Handbook focuses mainly on the security policy perspective and on the methodological perspective, which are treated in two separate parts. A third, additional part has been included, which contains a number of short overview chapters.

Part I features six newly added country surveys in addition to updated versions of the eight national profiles included in the first edition of this Handbook. The focal points have been reduced from six to four in order to give the surveys more focus. The chapters on legislation and on research and development both appear as overview chapters in the new Part III. Part II has also been restructured: It no longer addresses methods and models in two separate chapters (National Efforts for CII Analysis/ Models for CII Analysis), but discusses the most commonly used approaches, with concrete examples from assessments developed by the countries profiled:

- *Part I: CIIP Country Surveys* – Part I looks at policy efforts for the protection of critical information infrastructure in fourteen countries. Each survey has four focal points: (1) the definition of critical sectors; (2) CIIP initiatives and policy; (3) organizational structures; and (4) early-warning approaches.
- *Part II: Analysis of Methods and Models for the Assessment of Critical (Information) Infrastructure* – Part II looks at methods and models used in the fourteen countries to analyze and evaluate various aspects of CII. Seven major aspects of CI/CII assessment are discussed: (1) sector analysis; (2) interdependency analysis; (3) risk analysis; (4) threat assessment; (5) vulnerability assessment; (6) impact assessment; and (7) system analysis.
- *Part III: Overview Chapters* – Part III provides short overviews of three focal points: (1) protection efforts in a range of international organizations; (2) current topics in law and legislation, at both the international and the national levels; and (3) common themes in research and development in the EU and the US.

The Handbook still includes an extensive appendix, which contains key terms, a bibliography, a collection of links, and a list of experts involved.

The contents of the Handbook are based on open-source information only. Material was collected from the Internet, official government documents, workshops, and conferences.[29] However, the starting position was not the same for all countries: whereas some provide a wealth of material on the Internet, others do not. In both cases, the surveys were reviewed by at least one national CIIP expert – and expert input was of particular importance when little material could be collected beforehand.[30]

Outlook and Planned Updates

As the information revolution is an ongoing and dynamic process that is fundamentally changing the fabric of security and society, continuing efforts to understand these changes are necessary. This requires a lot of research into information-age security issues, the identification of new vulnerabilities, and new ways for countering threats efficiently and effectively. The International CIIP Handbook is a small contribution towards this ambitious goal. In order to stay abreast of the dynamics in the field, more updates of the CIIP Handbook are planned. These updates will include revised country surveys, new surveys, a modified methodological section, and additional features and analysis.[31]

[29] All links last checked on 1 December 2003.

[30] The authors tried to include all the opinions of the persons contacted. In the final version, however, the Handbook represents solely the authors' views and interpretations. Without the invaluable support and help of these experts, however, this work would not have been possible. The deadline for information-gathering and expert input was 30 November 2003. More recent developments could not be considered in this edition.

[31] The entire publication is available on the Internet (www.isn.ethz.ch/crn). We kindly ask the reader to inform us of any inaccuracies or to submit any comments regarding the content.

Center for Security Studies, ETH Zurich
Volume 2, Zürich 2004.

The International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries

Myriam Dunn and Isabelle Wigert

edited by
Andreas Wenger and Jan Metzger