Critical Information Infrastructure Protection (CIIP) Policies in Selected Countries:
Findings of the CIIP Handbook

Isabelle Wigert / Myriam Dunn

Center for Security Studies
ETH Zürich
ETH-Zentrum WEC
CH-8092 Zürich
Switzerland

wigert@sipo.gess.ethz.ch
dunn@sipo.gess.ethz.ch

Abstract: The International Critical Information Infrastructure Protection Handbook addresses the subject of critical information infrastructure protection (CIIP), a growingly important topic on the security policy agenda. The CIIP Handbook focuses on aspects of CIIP related to security policy and methodology. The security policy perspective evaluates policy efforts for the protection of critical information infrastructure in different countries. The methodological perspective discusses selected methods and models to analyze and evaluate various aspects of critical information infrastructure.

The International CIIP Handbook: Project Description

Key sectors of modern society, including those vital to the national security and the essential functioning of industrialized economies, are dependent on a spectrum of highly interdependent national and international software-based control systems for their smooth, reliable, and continuous operation. This information infrastructure underpins many elements of the critical infrastructure (CI), and is hence called critical information infrastructure (CII). The CII is facing a continuous change towards new ways of interaction with societies: Most evident is the growing use of open systems to monitor and control operations of the CI as well as the convergence of the media, information technology, and telecommunications technology towards integrated information and communication technologies (ICT).

The increasing value of information and the availability of electronic means to manage its ever-growing volume have not only made information and information systems an invaluable asset, but a lucrative target, too. Whereas the opportunities of ICT are well-known and exploited, the consequences of the inter-linkages among CI through CII are not yet sufficiently understood. Information systems are exposed to failures, are attractive targets for malicious attacks, and susceptible to cascading effects. These new risks and vulnerabilities have become a crucial security issue throughout the world.

A number of issues indicate an urgent need to effectively protect the CII. These include

- inter-linkages among CI,
- consequences of interdependencies,
- possible cascading effects of failures, and
- newly emerging, insufficiently understood vulnerabilities.

Within the last few years, many countries have taken steps to better understand the vulnerabilities of and threats to their CII and have drafted possible solutions for the protection of these critical assets (critical information infrastructure protection, CIIP). These national protection efforts are the subject of the CIIP Handbook.

The first CIIP handbook was published in 2002 with an inventory of protection policies in eight countries[16] and their methods and models employed. The next edition of the handbook, (forthcoming in 2004) includes an update and covers additional countries as well as methodological issues. The overall purpose of the International CIIP Handbook is to provide an overview of CII protection practices in developed countries. It is guided by two key questions:

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

Those two questions are answered in two separate parts:

- *Part I ("CIIP Country Surveys")* looks at policy efforts for the protection of critical information infrastructure in eight countries. Each survey contains six focal points: (1) Concept of CIIP and Description of System, (2) CIIP Initiatives and Policy, (3) Law and Possible Legislative Action, (4) Organizational Analysis, (5) Early Warning, and (6) Research and Development.

- *Part II ("CII Methods and Models")* introduces methods and models to analyze and evaluate various aspects of CII, looking at both specific national efforts and abstract considerations.

[16] Australia, Canada, Germany, the Netherlands, Norway, Sweden, Switzerland, and the United States.

Findings of the 2002 Edition

1) Part I: CIIP Country Surveys

A comparison of the conceptual understanding of CIIP in eight countries shows that even the most basic perception of CIIP varies considerably. A clear distinction between CIP and CIIP is lacking in most cases, and very often, a seemingly random use of both concepts is found. Furthermore, the definition of critical sectors is subject to ongoing discussions in most countries. This is a clear sign that the topic is still being shaped as a policy field and that a lot of definitions and conceptual boundaries still need to be found.

Whereas in some countries, the concept of CIIP is defined very broadly and includes numerous CI elements (e.g., in the Netherlands and in Switzerland), other countries seek to restrict the number of critical sectors (e.g. the United States). A direct comparison of all CI sectors shows that the most frequently mentioned sectors in all countries are: Banking and finance; (tele-) communication; energy and utilities; and transport/ distribution.

Many of the national CIIP efforts were triggered by the Presidential Commission on Critical Infrastructure Protection (PCCIP), set up by former US president Bill Clinton in 1996, and to some extent by the preparations for anticipated problems on the threshold of the year 2000. This led to the establishment of (interdepartmental) committees, task forces, and working groups. Their mandate often included the elaboration of scenarios, suggesting countermeasures, or the structuring of early warning systems. These efforts resulted in policy statements - such as recommendations for the establishment of independent organizations dealing with information society issues - and reports, which serve as a basis for CIIP policy formulation. In the aftermath of 11 September 2002, several countries introduced stronger measures to protect CII, and the event resulted in the provision of additional resources for CIIP. The topic is so new, however, that a comprehensive and fully adequate CIIP policy is still lacking in all countries.

Responsibility for CIIP rests with more than one authority and with organizations from different departments in all surveyed countries. Generally, the organizational structure is very complex and even confusing, and there are many players engaged in CIIP. This is one of the reasons why many nations are currently reorganizing existing structures by establishing new organizations with a distinct CIIP focus. Examples for this are the Department of Homeland Security in the United States or the Swedish Emergency Management Agency.

Furthermore, public-private partnerships are becoming a strong pillar of CIIP policy. Different types of such partnerships are emerging, including government-led partnerships, business-led partnerships, and joint public-private initiatives.

2) Part II: CII Methods and Models

In general, a broad range of methods and models is available for the analysis of critical information infrastructure. However, each approach or methodological element can only be applied to certain aspects of the problem, meaning that no single one is sufficient to address the whole array of pressing issues in CIIP. This necessitates a combination of different methodological elements as employed by all the studied countries.

The applications and the grade of sophistication of the methods and models differ greatly. Some focus on the technical system or the network, others on single elements or components within the overall infrastructure system, or on the analysis of an infrastructure sector, while the most comprehensive of them try to account for the complexity of the entire critical infrastructure system. This diversity makes comparison difficult.

Some countries have developed complex multi-step processes for infrastructure protection, tailored specifically to their needs. However, approaches that are specifically suitable for the analysis of CII are scarce, and most methodological elements originate in risk analysis and modeling.

In all surveyed countries, expert involvement is predominant. This shows that crucial knowledge resides in actors that are often outside the state's sphere of influence. As a rule, this knowledge is not academic, but "owned" by practitioners. Also, academic institutions play a minor role compared to consultants and experts in the assessment of CIIP matters.