Conclusion

The International CIIP Handbook provides an overview of issues of high importance in the field of CIIP, serves as a reference work for the interested community, and provides a basis for further research. The book has two focal points: security policy and methodology. It reviews national approaches to critical information infrastructures protection, namely the CII conceptual framework, policies and initiatives, the regulatory and legal framework, the organizational structure, early warning efforts, and actors involved in research and development (Part I). Furthermore, it addresses methods and models used in the surveyed countries to analyze and evaluate various aspects of the critical information infrastructure (Part II).

In conclusion of this handbook, each of the two parts is shortly wrapped up. The eight countries are briefly compared in terms of the six focal points, and some general thoughts on methodological matters are offered.

Part I: CIIP Country Surveys

Concept of CIIP and Description of System

A comparison of the conceptual understanding of CIIP in the 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.

CIIP Initiatives and Policy

After the Cold War, CIIP came to be perceived as an increasingly pressing issue by many governments. Political decision-makers have launched a plethora of initiatives to come to terms with newly perceived risks of the information and communication technologies. Most countries consider CIIP to be a national security issue, and some also stress the importance of CIIP for the economy and crime prevention.

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.

Law and Legislative Action

All countries under consideration have a variety of legal acts dealing with CIIP-related issues. Apart from old laws that are applied to new criminal offenses, some pieces of legislation cover attacks against computer and telecommunication systems or seek to define a framework for the handling of electronic signatures. As a result of 11 September 2001, many countries are in the process of reviewing their legislation to make it applicable to possible terrorist attacks. In most countries, the need for international action is also acknowledged, and the EU Cyber Crime Treaty is often used as a basis for new legislation.

Organizational Analysis

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 establish-

ing 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.

Early Warning

The general trend in early warning points towards establishing central contact points for the security of information systems and networks. Among the existing early warning organizations are various forms of Computer Emergency Response Teams (CERTs). CERT functions include handling of computer security incidents and vulnerabilities, reducing the probability of successful attacks, and publishing of security alerts. However, no specific CIIP early warning institutions are in place, even though some countries are at the planning stage. Examples include Sweden (National Center for the Reporting of IT incidents) and Switzerland (Analysis and Reporting Center for IT related incidents). The United States plan to incorporate a division focusing on information analysis and infrastructure protection into the Department of Homeland Security.

Research and Development

There is a wide range of CIIP Research and Development activities. Most R&D institutions are not doing research for CIIP issues exclusively, but work on a wider range of topics. Some government and/or other public actors are encouraging a stronger collaboration between government, industry, and academia in order to foster both interdisciplinary research and bundle resources. Topics being examined include vulnerability and risk analysis, development of system protection tools, intrusion detection, monitoring, development of regulations and standards, special academic programs for IT security, and the development and analysis of legislative tools. In general, R&D is done at academic organizations. Additionally, there are R&D institutions within government agencies and private industry. Since 11 September 2001, more funds have been made available for CIP/CIIP projects. However, the need for more research, and for interdisciplinary and international research in particular, is acknowledged.

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.

National Efforts for CII Analysis

Countries such as Australia and Canada 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.

- In Australia, a defense-specific multi-step vulnerability assessment process was developed involving various experts from industry and defense,
- In Canada, a first effort resulted in infrastructure profiles, including criticality and probability of failure studies. Building on this, a comprehensive infrastructure protection process was developed, focusing on the identification of interdependencies. Dependency matrices and algorithms are used to measure and model the ripple effects of direct dependencies (RAFLS),
- In the Netherlands, two consultant reports deal with segments of the country's CI. They focus on the ICT infrastructure and the Internet. These qualitative studies develop a number of layer models in

order to clarify the role of actors involved, as well as to enhance the understanding of interdependencies,

- In Norway, the government program for the protection of society uses a multi-criteria model in order to perform a cost-effectiveness analysis, to study vulnerabilities in the telecommunication system, and to suggest cost-effective measures to reduce these vulnerabilities,
- In Switzerland, a step-by-step analysis with seven elements remains hypothetical to date, and there are no quantitative implementations of this model. However, a rough process and technology analysis was conducted for various sectors by InfoSurance representatives,
- In the US, research on interdependency matters is ongoing. Computer simulations are currently being developed that will predict interactions among critical infrastructure elements. Apart from the Department of Energy, which is very active in the field, a vulnerability assessment process was developed by CIAO for civilian federal departments and agencies.

All countries are at very different stages of assessing their CII, and the amount of manpower and resources allocated varies greatly. Many countries recognize the need for more in-depth research and more comprehensive development of methods and models to analyze various aspects of their national CII.

Models for CII Analysis

The overall objective of the methods and models introduced in the CIIP Handbook is to enhance the security of information systems. Apart from that, they vary greatly. Technical approaches mainly aim to assure that IT-security objectives – such as availability, integrity, confidentiality, and accountability – are complied with at all times. Other approaches, such as layer models and interdependency matrices, have a strong descriptive orientation and often serve to illustrate interdependencies. Risk analysis methodology appears in a variety of forms, some specifically developed for the analysis of CII (such as IRAM, Leontief-based Model of Risk). In its general form, risk analysis has a whole range of applications, from risk identification and assessment of the technical systems level to the analysis of more complex infrastructure systems. As risk assessments often include various elements such as threat, likelihood, vulnerability, or consequences of an event, the amount of time needed to conduct a risk assessment may be considerable.

One of the most pressing but least understood issue in CIIP are interdependencies. A couple of the studied approaches aim to enhance the understanding of this matter. The dimensional interdependency analysis, for example, which describes various types and characteristics of interdependencies, is an interesting starting point for further research. Sector and layer models often display interdependencies between sectors and may also serve as a basis for more thorough analysis. Dependency/Interdependency Matrices can serve as visualization tools for interdependencies between different sectors. Other approaches do not address the issue at all: Technical security models, for example, assume that sufficient protection at the technical system level can prevent threats to larger and more complex systems, and are therefore not concerned with interdependency issues. Risk analysis methodology in general also fails to address interdependencies directly. However, the modified Leontief-Based Model of Risks includes interdependencies by forecasting the effect of change in one infrastructure element on others.

Table 1 provides a final overview of the most important of the discussed methods and models, their application areas, and their objectives.

Model / Method	Application Area	Objective
Dependency / Interdependency Matrix	Complex infrastructure system, special focus on interdependencies	Visualization of strength of interdependencies between sectors
Dimensional Interdependency Analysis	Complex infrastructure system, special focus on interdependencies	Identification, understanding, and analysis of interdependencies.
Hierarchical Holographic Modeling	Complex infrastructure system	Modeling large-scale, complex systems
Infrastructure Profiles	Single infrastructure	Detailed description of various characteristics of infrastructure
Infrastructure Risk Analysis Model (IRAM)	Infrastructure component or whole infrastructure sector	Risk analysis approach especially created for the analysis of CIP
Leontief-Based Model of Risks	Single infrastructure to complex infrastructure system, with special focus on interdependencies	Forecast the effect of one aspect of change on another
Process and Technology Analysis	Infrastructure sector (isolated) and interdependencies between sectors	Identify dependencies between different layers of a sector and between different sectors
Risk Analysis Methodology	From technical systems level to more complex infrastructure systems	Identify risks, assess risks, and take steps to reduce risks to an acceptable level
Scenario Technique	From technical systems level to more complex infrastructure systems	Generation of scenarios to determine strategies
Sector Analysis	Single infrastructure sector	Add to the understanding of the functioning of sectors
Sector and Layer Model	Parts of complex infrastructure system or the totality of a nation's critical infrastructures	Picture interdependencies between elements of infrastructure
Technical IT-Security Models	Technical systems level	Optimal protection of IT assets, local in nature
Vulnerability Assessment	From technical systems level to more complex infrastructure systems	Either part of risk analysis (exposure to threats) or as a combination of risk analysis and emergency management evaluation
Vulnerability Profile Chart	Single infrastructure to complex infrastructure system, with special focus on interdependencies	Visual representation of vulnerability rankings

Table 1: Overview of Models for CII Analysis