Part IV
Analysis and Conclusion

Analysis and Conclusion

The International CIIP Handbook provides an overview of issues of high importance in the field of *critical information infrastructure protection* (CIIP), serves as a reference work for the interested community, and provides a basis for further research by compiling relevant material. The book has two main parts and one supplement part:

- *Part I* reviews national policy approaches to CIIP, namely the definition of critical sectors and the CIP/CIIP conceptual framework; initiatives and policy; organizational structures; and early-warning approaches;
- *Part II* addresses methods and models used in the surveyed countries to analyze and evaluate various aspects of CII and CIIP;
- *Part III* includes overview chapters on international organizations, current topics in law and legislation as well as a brief summary of EU and US research and development in the field of CIIP.

The authors have omitted a concluding remark on best practices in CIIP on purpose, not only due to the great discrepancies protection efforts between the various states. The US is still far ahead of most other countries due to its head start and its role as a forerunner in this policy field. However, the US view of CIIP since 11 September 2001 has been strongly shaped by the threat of terrorism – a perspective that is not necessarily shared by other countries, which are mostly still in the process of finding their own "CIIP identity". What we are therefore looking at are snapshot moments of a still very dynamic policy field. Efforts that are touted as best practices today might be considered insufficient tomorrow. In this light, it seems far wiser to keep on carefully observing the field without judging prematurely.

Analysis and Conclusion Part I: Country Surveys

Part I of this Handbook gives an overview of national approaches to CIIP at the level of policy. In conclusion, each of the four sections (critical sectors, initiatives and policy, organizational overview, and early-warning approaches) is wrapped up, incorporating some important findings from Part III. Due to the great differences in protection practices and the constant advancement of existing policies, a true comparison between the fourteen countries is difficult to undertake, especially since many aspects of existing CIIP poli-

cies give the impression of "unfinished business". Still, some basic common features can be observed:

- CIIP is mostly seen as a subset of CIP, including protection, detection, response, and recovery activities at both the physical and the cyber level. However, a clear distinction between CIP and CIIP is lacking in most countries. Often, a seemingly random use of both concepts is found. Additionally, the concepts of CII and CIIP are seldom clearly defined.
- The definition of what constitutes a critical sector is an ongoing process. This can be interpreted as a sign that the topic is still being shaped as a policy field and that a lot of (common) definitions and conceptual boundaries still need to be found. Additionally, we can observe that the list of critical sectors released by the US in 1997 initially left a great impression on every country that began to deal with the subject of CIIP. The list was then tailored to country-specific needs and concepts of criticality.
- The development of the Internet, a global network that is often perceived to be inherently insecure, into the main pillar for the advancement of the information society, for e-Government, and e-Commerce/-Business was in many cases a catalyst for protection efforts, sometimes under the heading of CIIP, sometimes under the more general banner of information security.
- In a few countries, central governmental organizations have been created to deal with CIIP specifically. Mostly, however, responsibility lies with multiple authorities and organizations in different governmental departments. These actors often look at CIIP from contrasting perspectives, which is a major obstacle to academic and practical dialog.
- In some countries, the public and private sectors have jointly raised concerns over the protection of CII. Coordination and cooperation between these stakeholders is seen as indispensable for a successful CIIP policy.
- The issue of *Public-Private Partnerships* (PPP) is therefore recognized as being absolutely crucial. Governments actively promote information-sharing with the private sectors, since large parts of critical infrastructures are owned and operated by the business sector. Some of these efforts look promising, but many unresolved issues remain.
- Early warning is perceived as one of the key CIIP issues. Information-sharing schemes such as *Computer Emergency Response Teams*

(CERTs) as well as *Information Sharing and Analysis Centers* (ISACs) play an increasingly important role. This mirrors the understanding of CIIP as related mainly to IT- and Internet security. However, some countries have chosen a slightly different approach in establishing early-warning systems: the development of permanent analysis and intelligence centers, which often focus on more than just technical aspects.

- The attacks on the US on 11 September 2001 had a strong impact on CIIP – many countries have since reviewed their CIIP policies.
- Legislation concerning CIIP has been under particularly close scrutiny since 11 September 2001. The development of effective regulations, laws, and criminal justice mechanisms are seen as essential in deterring cyber-abuse and other offences against information infrastructures.
- Efforts are being made to achieve an international harmonization of procedural criminal law and to improve police cooperation. Several international organizations, such as the EU, the G8, the OECD, and the UN are committed to this development.
- In the field of CIIP-related research and development (R&D), the US and the EU are the "big players". The US has a leading role in identifying and promoting important R&D topics, which are then often propagated to other parts of the world. The EU plays a crucial role in supporting cross-national R&D and information exchange in Europe. CIIP will continue to be a major R&D challenge in the future.

Critical Sectors

In most countries, the definition of critical sectors is subject to ongoing discussions. Accordingly, the lists of critical sectors provided are not definite. In comparing the country surveys in the first and second editions of the CIIP Handbook respectively, it will also become obvious that these definitions are not static. It is indeed likely that the definition of criticality will continue to change, for example due to events such as the 11 September 2001 attacks or general changes in the conceptualization of CIIP.

Variations between countries can be seen not only in the definition of critical sectors, but also in the definition of CIIP. Some countries, such as Australia, Canada, the Netherlands, the UK, or the US, provide clear definitions, while other countries offer none at all. While superficially, it is always the sectors that are defined and listed as critical, in reality, the products, services, and functions provided by these sectors are the actual focus of protection

efforts. This is clearly the case with recent additions such as "National Icons and Monuments", listed by Australia, Canada, and the US. These are deemed critical because of their inherent symbolic value.

Table 1 shows which country defines which sectors as critical. One must be careful, however, to avoid misleading comparisons: While Australia, Canada, the Netherlands, the UK, and the US are very precise in identifying critical sectors and sub-sectors as well as products and services that these sectors provide, others, such as Austria, Italy, or Sweden, have no official list of CI sectors. Often, identified critical sectors lack clear definitions, and it remains unclear which sub-sectors are included. Furthermore, the fact that similar or even identical assets can be labeled differently in different countries may hamper straightforward comparison.

However, a rough comparison of CI sectors across the selected countries is possible without over-interpreting the collected information. The most frequently mentioned critical sectors in all countries are listed below. These are the core sectors of modern societies, and possibly the ones which large-scale interruption would be most devastating:

- Banking and Finance,
- Central Government/Government Services,
- (Tele-) Communication/Information and Communication Technologies (ICT),
- Emergency/Rescue Services,
- Energy/Electricity,
- Health Services,
- Transportation/Logistics/Distribution, and
- Water (Supply).

Variations in terminology can not only be explained in terms of different threat perceptions or conceptualization of what is critical, but also by country-specific peculiarities and traditions. Individual sectors, for example "Social Security/Welfare", "Insurance", or "Civil Defense", are influenced by *socio-political factors* and traditions, while others, for example "Water/Flood Management" in the case of the Netherlands, are subject to *geographical and historical preconditions*. Some sectors have newly been added after disturbing incidents. This is the case for the categories of "National Icons and Monuments" or the "Post Systems", introduced after 11 September 2001, or the "Meteorological Services", identified as a specific critical sub-sector in Canada after an ice storm in 1998 that severely affected Eastern Canada and Quebec. As mentioned above, these lists can be expected to change slightly over the years, especially due to incidents and events.

Country / Sector	AUS	A	CAN	CH	DE	F	FIN	I	NL	NO	NZ	SE	UK	USA	Total
Air Control Systems												✔			1
Banking and Finance	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	14
Central Government / Government Services	✔		✔		✔		✔	✔	✔	✔	✔	✔	✔	✔	11
Civil Defense				✔				✔							2
(Tele)Communications / ICT	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	14
Dams														✔	1
(Higher) Education														✔	1
Energy / Electricity	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	14
Emergency / Rescue Services	✔	✔	✔	✔	✔		✔			✔	✔		✔	✔	10
Food / Agriculture	✔		✔		✔		✔		✔				✔	✔	7
Hazardous Materials / CBRN			✔										✔	✔	3
Health Services	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔	12
(Defense) Industry / Manufacturing	✔		✔	✔		✔	✔							✔	6
Information Services / Media /Broadcasting	✔	✔	✔	✔			✔		✔			✔	✔		8
Insurance	✔				✔									✔	3
Justice / Law Enforcement					✔				✔		✔		✔	✔	5
Military Defense / Army / Defense Facilities	✔	✔			✔				✔	✔					5
National Icons and Monuments	✔		✔											✔	3
Nuclear Power Plants						✔								✔	2
Oil and Gas Supply	✔		✔		✔			✔	✔	✔	✔		✔	✔	9
Police Services	✔	✔	✔				✔			✔			✔		6
Post Systems		✔												✔	2
Public Administration		✔		✔	✔		✔	✔	✔				✔	✔	8
Public Order / Public Safety						✔			✔				✔		3
Sewerage / Waste Management	✔		✔							✔			✔		4
Social Securtiy / Welfare		✔					✔			✔	✔				4
Transportation / Logistics / Distribution	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔	✔	13
Utilities	✔	✔								✔					3
Water (Supply)	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔	12
Water / Flood Management									✔						1

Table 1: Overview of the Critical Sectors and Sub-sectors Identified by Surveyed Countries

Initiatives and Policy

Decision-makers launched myriad initiatives to come to terms with the newly-perceived risks of information and communication technologies during the late 1990s. CIIP is usually just one aspect of the overall topic of information security. Practical and academic dialog is hampered by vastly differing terminology and viewpoints of what constitutes the problem. Most countries consider CIIP to be a national security issue of some sort. In parallel, however, they often pursue a business continuity strategy under the "information society" label. The law enforcement/crime prevention perspective is also found in most countries. Furthermore, data protection issues are a major topic for civil rights groups. While all of the perspectives can be found in all countries, the emphasis given to one or more of the perspectives varies to a considerable degree.

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 as well as the US and New Zealand, CIIP is integrated into the overall counterterrorism efforts, where the intelligence community plays an important role.

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 (Y2K problem). This led to the establishment of (interdepartmental) committees, task forces, and working groups. Their mandate often included scenario work, the evaluation of a variety of measures, or assessments 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 laying down basic CIIP policies.

In the aftermath of 11 September 2001, several countries have launched further initiatives to strengthen and allocate additional resources to their CIIP efforts. Nevertheless, a comprehensive and fully adequate CIIP policy is still lacking in all countries. All countries examined have recognized the importance of public-private partnerships (PPP), early warning, and research and development for CIIP, but not all countries have implemented their plans.

Organizational Overview

In most countries, responsibility for CIIP rests with more than one authority and with organizations from different departments, and thus involves many different players from different communities. This factor, together with events such as on 11 September 2001, increases the urgency of reorganizing the existing structures by establishing new organizations with a distinct CIIP focus and coordination roles. The following are examples of organizations with at least a partial focus on CIIP:

- The Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) in Canada;
- The Federal Office for Information Security (BSI) in Germany;
- The Centre for Critical Infrastructure Protection (CCIP) in New Zealand;
- The Swedish Emergency Management Agency (SEMA) in Sweden;
- The National Infrastructure Security Co-ordination Centre (NISCC) in the UK;
- The Department of Homeland Security (DHS) in the US.

The establishment and location within the government structures of these key organizations is influenced by various factors such as civil defense tradition, the allocation of resources, historical experience, and the general threat perception of key actors in the policy domain.

Due to the importance of public-private partnerships, the location of new organizations is often constrained by the need to assure private-sector companies that their sensitive commercial and security information will be adequately safeguarded, and by the need to provide a secure environment that can adequately protect intelligence information to which the organization must have access. As the US example shows, the affiliation of CIIP organizations with law-enforcement agencies can cause problems with private-sector companies due to the above reasons.

The following is a short overview of country-specific findings with regard to organizational structure in CIIP:

- In *Australia*, several organizations are responsible for CIP/CIIP. Since terrorism was identified as the most likely threat to arise against Australia's critical infrastructure (considering attacks on both virtual and physical structures), CIIP has been seen as part of the country's overall counter-terrorism effort. Therefore, the Critical Infrastructure Protection Group's members also include the Defence Signals Directorate, the Australian Security Intelligence Organisation, and the Australian Federal Police all operational military, security, and policing intelligence services.

- In *Austria*, there is no single authority responsible for CIP/CIIP – all ministries have their own specific security measures to defend against outside attack and to prevent the unauthorized usage of data. CIIP is mainly perceived as an issue of data protection, as the Austrian E-Government Program, the Official Austrian Data Security Website, or the Pilot Project Citizen Card indicate.
- *Canada's* Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), integrated into the new portfolio of Public Safety and Emergency Preparedness, is the key organization responsible for both CIP/CIIP as well as Civil Emergency Planning. Hence, Canada has a centralized organizational model for CIP/CIIP.
- In *Finland*, CIIP is seen as a data security issue and as a matter of economic importance, closely related to the development of the Finnish information society. Several organizations deal with CIIP, including the Communications Regulatory Authority, the Emergency Supply Agency, the Board of Economic Defense, and the Committee for Data Security.
- In *France*, CIIP is seen both as a high-tech crime issue and as a matter of developing the information society. Overall responsibility for CIIP lies with the General Secretary of National Defense.
- In *Germany*, the Federal Office of Information Security (BSI), which is part of the Ministry of the Interior, is the lead authority for CIIP matters within the organizational structure.
- In *Italy*, CIIP is part of the advancement of the information society. There is no single authority dealing with CIIP. A Working Group on CIIP was recently set up at the Ministry for Innovation and Technologies that includes representatives of all ministries involved in the management of critical infrastructures and many Italian infrastructure operators and owners as well as some research institutes.
- In *the Netherlands*, responsibility for CII lies with a number of authorities, but the Ministry for Interior and Kingdom Relations coordinates CIP/CIIP policy across all sectors and responsible ministries.
- In *New Zealand*, the Centre for Critical Infrastructure Protection (CCIP), located at the Government Communications Security Bureau, is the central institution dealing with CIIP, and the main actor in charge of formulating New Zealand's security policy, including CIIP, is the Domestic and External Secretariat, DESS (that is the support secretariat for the Officials Committee for Domestic and External Security Co-ordination, ODESC).

- In *Norway*, the national key player in Civil Emergency Planning, the Directorate for Civil Defense and Emergency Planning (DSB), subordinated to the Ministry of Justice and Police, is also a key player for CIP/CIIP-related issues.
- In *Sweden*, a number of organizations are involved in CIP/CIIP. The Swedish Emergency Management Agency (SEMA) at the Ministry of Defense has a key role.
- In *Switzerland*, there are a number of different organizational units dealing with CIP/CIIP. Public-private partnerships are among the central pillars of Switzerland's CIIP policy.
- In the *UK*, the key interdepartmental organization dealing with CIP/CIIP is the National Infrastructure Security Co-ordination Centre (NISCC). The NISCC has strong ties with the private sector.
- In the *US*, the Department of Homeland Security (DHS) has the leading role in CIP/CIIP. However, several other organizational units are also involved in CIP/CIIP. Public-private partnerships, e.g., Information Sharing and Analysis Centers (ISACs), are regarded as key elements in CIP/CIIP policy.

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. In Switzerland, the UK, and the US, strong links have already been established between the private business community and various government organizations.

One of the future challenges in many countries will be to achieve a balance between security requirements and business efficiency imperatives. Satisfying shareholders by maximizing company profits has often led to minimal security measures. This is because like many political leaders, business leaders tend to view cyberattacks on infrastructures as a tolerable risk. Additionally, public-private partnerships are mainly based on trust, so that information-sharing is arguably one of the most significant issues in CIIP.

Early Warning Approaches

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), e.g., special CERTs for government departments, CERTs for small and medium-sized businesses, CERTs for specific sectors, and others. CERT functions include handling of computer security incidents

and vulnerabilities or reducing the probability of successful attacks by publishing security alerts.

In some countries, permanent analysis and intelligence centers have been developed in order to make tactical or strategic information available to the decision-makers within the public and private sectors more efficiently. Tasks of early-warning system structures include analysis and monitoring of the situation as well as the assessment of technological developments. Examples can be found in Canada (*Integrated Government of Canada Response Systems*), in Switzerland (*Reporting and Analysis Center for Information Assurance*, MELANI), and in the US (*Directorate for Information Analysis and Infrastructure Protection*, IAIP). Furthermore, there is cross-border cooperation in early warning between Australia and New Zealand. Such international cooperation is sensible when considering the cross-boundary nature of cyberthreats, which are inherently transnational.

Analysis and Conclusion Part II: Analysis of Methods and Models for Critical (Information) Infrastructure Assessment

Part II of the Handbook describes methods, models, and approaches used to analyze and evaluate various aspects of CII in the surveyed countries. Even though the focus of the Handbook is on CII, the majority of the discussed methods and models are designed and used for the larger concept of CI. This reflects the practice of addressing CIP as a comprehensive set of issues, of which CIIP is only a sub-category.

The huge variation in the granularity of methods and models makes a meaningful comparison rather difficult, also because they exist for all of the four hierarchies of CI systems, namely the system of systems, individual infrastructures, individual systems or enterprises, and technical components. A pragmatic approach was chosen in the Handbook by distinguishing between the most important or most-used approaches, which are (1) sector analysis; (2) interdependency analysis; (3) risk analysis; (4) threat assessment; (5) vulnerability assessment; (6) impact assessment; and (7) system analysis. Each is briefly recapitulated below after some general remarks on the state of the art in CII assessment.