International

CIIP Handbook

An Inventory of Protection Policies in Eight Countries

Critical

Information

Infrastructure

Protection

Edited by
Andreas Wenger, Jan Metzger, Myriam Dunn

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Contents

Preface

The nature of risks and vulnerabilities in modern societies is becoming more and more transnational today. An open, non-hierarchical dialog on newly recognized vulnerabilities at the physical, cyber, and psychological levels is needed to create new knowledge and a better understanding of new risks and of their causes, interactions, probabilities, and costs.

It is on the basis of these premises that the "Comprehensive Risk Analysis and Management Network" (CRN, www.isn.ethz.ch/crn) was launched two years ago as a joint Swiss-Swedish initiative. The CRN is an internet and workshop initiative for international dialog on national-level security risks and vulnerabilities. As a complementary service to the International Relations and Security Network (ISN, www.isn.ethz.ch), the CRN is coordinated and developed by the Center for Security Studies and Conflict Research at the Swiss Federal Institute of Technology (ETH) Zurich, Switzerland in cooperation with the current CRN partner institutions:

- The Swedish Emergency Management Agency (SEMA), Sweden,
- The General Directorate for Security Policy, Federal Ministry of Defense, Austria,
- The Directorate for Civil Defense and Emergency Planning (DCDEP), Norway,
- The Federal Office for National Economic Supply (NES), Federal Department of Economic Affairs, Switzerland,
- The Swiss Federal Department of Defense, Civil Protection, and Sports (DDPS), Switzerland.

The International Critical Information Infrastructure Protection (CIIP) Handbook is the product of a joint effort within the CRN partner network. The CIIP Handbook provides an inventory of national protection policies in eight countries: Australia, Canada, Germany, the Netherlands, Norway, Sweden, Switzerland, and the United States. It is an important step towards a comprehensive overview of existing efforts in critical information infrastructure protection. Work on this first CRN publication started in 2001. Portions of the study were reviewed and validated by international experts before, during, and after the 2nd CRN workshop "Critical Infrastructure Protection in Europe – Lessons Learned and Steps Ahead", which took place in Zurich from 8–10 November 2001. A major part of the coordination as well as the editorial and administrative work was shared

with Ernst Basler + Partners Ltd. (www.ebp.ch), a leading government consulting company in Switzerland.

Because of the dynamics in the field and in order to include additional country surveys and models, a regular update of the CIIP Handbook is planned. We therefore ask the reader to inform us of any inaccuracies or to submit any comments regarding the content. Those countries not yet included are especially encouraged to submit information to us. Please see the front inside cover for contact information. The entire publication plus additional features will also be available on the Internet (http://www.isn.ethz.ch/crn).

The editors would like to thank all the partners involved, in particular the national experts who generously shared their experience and knowledge with us.* We are looking forward to continuing the development and coordination of the CRN partnership.

Zurich, September 2002

Prof. Dr. Andreas Wenger
Deputy Director,
Center for Security Studies
and Conflict Research

Dr. Jan Metzger
CRN Coordinator,
Senior Researcher

Myriam Dunn, lic. phil. I
Researcher CIIP
Center for Security Studies
and Conflict Research

* We also thank the following for their help in the completion of this project: Daniel Bircher, Stefano Bruno, and Robert Ladner (all from Ernst Basler + Partners Ltd.), Christopher Findlay, Barbara Gleich, Liv Minder, Leo Niedermann, Michelle Norgate, Reto Wollenmann, and Marco Zanoli (all from the Center for Security Studies and Conflict Research at the Swiss Federal Institute of Technology, ETH Zurich).

Introduction

Background

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.

Research Subject

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 this handbook.

A clear and stringent distinction between the two key terms CIP (critical infrastructure protection) and CIIP is desirable, but very hard to obtain. In official publications, both terms are used inconsistently. It often remains unclear whether policy papers are referring to CIP or CIIP, since both concepts are frequently interchanged in an unsystematic manner. Accordingly, the reader will find both terms used in the 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. However, 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 critical information infrastructure.

Purpose and Key Questions

The overall purpose of the International CIIP Handbook is to provide an overview of CII protection practices in eight countries: Australia, Canada, Germany, the Netherlands, Norway, Sweden, Switzerland, and the United States.[1] The book 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?

The handbook's target group consists principally of 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. However, the handbook does not claim to offer a comprehensive analysis of the topic: It is only an initial sketch of developments in the field of CIIP and does not provide a comprehensive compilation of existing policies, or methods and models.

1 Although the study concentrates exclusively on national efforts, it is recognized that important initiatives have been undertaken by international organizations such as NATO or the EU.

Structure of the Handbook

The handbook focuses on a security policy perspective and a methodological perspective, which are treated 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.

The appendix of the handbook contains a glossary of key terms, a bibliography, a collection of links, a list of national experts, and abbreviations. The contents of the handbook are based on open sources of information. These include websites, government documents, workshops, and conference proceedings.[2] For part I, extensive use has been made of the EU-sponsored Dependability Development Support Initiative DDSI (see http://www.ddsi.org). Additionally, expert interviews were conducted between November 2001 and July 2002. Draft versions of the surveys were reviewed by national experts. Without the invaluable support and help of these experts, the handbook would not have been possible.[3]

Outlook

The deadline for information-gathering and expert input was 31 July 2002. More recent information and developments could not be included in this first edition. However, in order to stay abreast of the dynamics in the field, regular updates of the CIIP Handbook are planned. These updates will include continuous work on the existing country surveys, additional country surveys, and more profound methodological analysis. To support this effort, an online version of this handbook with additional features and the possibility to give feedback is in planning.[4]

2 All links last checked by 31 July 2002.

3 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.

4 Available at http://www.isn.ethz.ch/crn.

Part I

CIIP Country Surveys

by Dr. Stefano Bruno

Dr. Stefano Bruno is consultant at Ernst Basler + Partners Ltd.

Introduction

Part I of this handbook surveys critical information infrastructure protection (CIIP) efforts in eight countries (Australia, Canada, Germany, the Netherlands, Norway, Sweden, Switzerland, and the United States). For each survey, six subjects of high importance covering conceptual, organizational, and legal aspects of CIIP are considered:

(1) Concept of CIIP and Description of System

The first section discusses the main assumptions and premises underlying the CIIP policy concept. It lists country-specific critical sectors and provides definitions of CII and CIIP.

(2) CIIP Initiatives and Policy

The second section gives an overview of the most important steps taken since the late 1990s at the governmental level to handle CIIP. A first subsection focuses on initiatives, a second highlights the main elements of CIIP policy. This includes descriptions of specific committees, commissions, task forces, and working groups, main findings of key official reports and fundamental studies, and important national programs.

(3) Law and Legislative Action

The third section lists important pieces of legislation enacted for the promotion of CIIP. This includes acts defining the responsibilities of the government authorities in case of emergencies as well as legislation dealing with issues such as technical IT security, data protection, damage to data, fraudulent use of a computer, the handling of electronic signatures, etc. Several countries have begun reviewing their legislation since 11 September 2001. These developments are considered as far as possible.

(4) Organizational Analysis

The fourth section gives an overview of important public actors in the national CIIP organizational framework. It only characterizes the specific responsibilities or public actors at the state (federal) level (such as ministries, national offices, agencies, coordination groups, etc.). Public actors at the lower state level and private actors (companies, industry, etc.) are omitted. Due to the growing importance of public-private partnerships, the most important of these are presented.

(5) Early Warning

The fifth section describes national organizations responsible for CIIP early warning, namely CIIP-related information-sharing organizations such as CERTs, ISACs, etc. Furthermore, reference is made to plans for the development of comprehensive early warning alert and incident report structures.

(6) Research and Development

The sixth section provides an overview of important public and private actors involved in CIIP-related research and development (R&D). This includes national research councils, network centers of excellence, universities, industry research laboratories, etc. In addition, depending on the information available, the main R&D fields are summarized for each country.

CIIP Country Surveys

Australia

Concept of CIIP and Description of System

In Australia, critical information infrastructure protection (CIIP) is perceived as vital to the maintenance of community and business confidence. The prime minister has defined the aim of CIIP as "to assure Australians that both the physical safety of key assets as well as the information technology systems on which so many of them depend are protected"[1].

The Australian national information infrastructure (NII)[2] is seen as the backbone of the information society, and therefore as the crucial element of CIIP. Some of the elements of the NII are critical to Australia's defense and the country's economic and social well-being. In many cases, attacks on the NII would impact those elements depending on the NII. Serious disruptions to the functioning of society or an inability to govern effectively could result.[3]

The following are the CI sectors in Australia:[4]

- Banking and finance,
- (Tele-) Communications,
- Energy and utilities,
- Information services,
- Transport and distribution,
- Other critical government services (including defense and emergency services).

1 Media release from Australian Prime Minister Howard's office, see http://pm.gov.au/news/media_releases/2001/media_release1367.htm.

2 The NII is defined to include the national network within and through which information is stored, processed, and transported; the people who manage and service the network; and the information itself.

3 Protecting Australia's National Information Infrastructure. Report of the Interdepartmental Committee on Protection of the National Information Infrastructure. Attorney-General's Department. (Canberra, December 1998), 7–8.

4 NII Report 1998, 7.

CIIP Initiatives and Policy

CIIP Initiatives

Since the end of the 1990s, several important steps have been taken to better manage CIIP in Australia. In the 2002/2003 budget, the Commonwealth government allocated AUS$ 24.9 million over four years to continue its efforts to protect the national information infrastructure (NII), which is largely in private hands. The budget allocation will enhance the capability of agencies within the Attorney-General's office, as well as the Defence and Communications, Information Technology, and Arts portfolios to protect critical infrastructure. In addition, the government will form a partnership with industry to minimize potential harm to these crucial systems.[5]

"Australia's National Information Infrastructure: Threats and Vulnerabilities"

The report "Australia's National Information Infrastructure: Threats and Vulnerabilities" was published in February 1997 by the Defence Signals Directorate (DSD). The report contains detailed studies about the strengths and vulnerabilities of key CII sectors. The main conclusions of the report were:[6]

- The potential vulnerability of society to significant NII disruptions is increasing,
- There is a lack of formal structure for the coordination and implementation of a national policy for protecting and assuring the continued operation of critical elements of the NII in peacetime and during hostilities,
- More can be done within affordable limits to minimize existing threats.

The most important recommendation in the DSD report was the establishment of a formal structure involving the government and the private sector to coordinate and implement national policy for the protection of the NII. Further recommendations focused on the collection and assessment

5 For more information see the media release at: http://www.ag.gov.au/publications/Budget2003/mediareleases/nii.htm.

6 NII Report 1998, 11 and 56.

of information, awareness-raising and protection, and on the establishment of a national CERT and a vulnerability analysis team.[7]

Interdepartmental Committee on the Protection of the National Information Infrastructure (IDC)

In August 1997, the Secretaries' Committee on National Security (SCNS) accepted the recommendations of the DSD report and tasked the Attorney-General's Department with the establishment of an Interdepartmental Committee on the Protection of the National Information Infrastructure (IDC). The IDC report of 1998 proposed the establishment of a framework to protect against and minimize the impact of attacks, and to detect and respond to attacks on the NII.

Consultative Industry Forum (CIF)

Since much of the NII lies within the private sector, the IDC report proposed the establishment of an industry forum. It was argued that such a forum would provide a link between the government and the industry and would also provide industry input to policy development and facilitate the development of industry responses to government policy in this area. To this end, the Consultative Industry Forum (CIF) was established.[8] Initially, the CIF provided a valuable mechanism for dealing with the industry. However, concerns have been raised by industry and government representatives over the group's size, composition, and lack of strategic direction.[9]

As a result of the discussions with the industry, the Australian government decided to pursue a collaborative relationship with the industry based on the following lines:

- To hold a Business-Government Task Force meeting with the owners of NII elements,
- To encourage the development of small trust-based information-sharing groups with links to the Commonwealth in key sectors,
- To conduct an awareness-raising program,
- To hold ongoing consultations with industry interests on specific policy initiatives as they arise.

7 NII Report 1998, 1.
8 NII Report 1998, 1.
9 Interview with a representative of the National Office for the Information Economy (NOIE), April 2002.

In the aftermath of 11 September 2001, the Australian authorities have introduced stronger measures to protect CI. Those measures include airport and airline security, heightened intelligence service, additional training for staff in areas such as postal services, and increased protection for major public buildings and diplomatic posts.[10]

CIIP Policy

The Commonwealth has the authority to protect its owns interests, including national security interests. It may provide advice to the state, territory, and local governments, and to the private sector on measures to prevent or respond to attacks that have the potential to impact on the economic and social well-being of Australia. The issue is one for law enforcement unless the government decides, in the case of a specific incident, that it is a defense matter.[11]

NII Report of 1998

The Australian NII report of 1998 states that while the concept of information warfare has been largely focused on malicious attacks, information assurance can be used to protect against, or respond to, natural or accidental as well as malicious disruptions. The report argues that "unlike the physical world, where government-supplied services such as police or defense forces may be the main line of defense, information assurance is a tool that is equally relevant to both the public and the private sectors and needs to be applied accordingly".[12] The protection of the NII is seen as a joint public and private-sector responsibility.

E-Security National Agenda

In 2000, an increased rate of referrals of computer network attacks to the Australian Federal Police and a four-fold increase in reports of computer incidents to the Australian Computer Emergency and Response Team (AusCERT) could be observed. This was the government's main reason for taking a new approach. The "E-Security National Agenda" will involve the National Office for the Information Economy (NOIE) as the key player

10 Media release from the Australian prime minister's office, see http://pm.gov.au/news/media_releases/2001/media_release1367.htm.
11 NII Report 1998, 15.
12 NII Report 1998, 8.

in coordinating e-security activities across the Commonwealth and with a number of other government bodies.[13]

The 2002 Australian Computer Crime and Security Survey reported that computer security incidents or attacks had approximately doubled in the last 12 months compared to 1999 figures.[14] Case studies on e-crime are being developed in Australia as an education tool. It is expected that these case studies will educate businesses, SMEs, and consumers about the need for better protective security practices.

Law and Legislative Action

Crimes Act 1901 Part VIA

This act deals with attacks against Commonwealth computers, and with all computer attacks using the Australian telecommunications system.

Telecommunications (Interception) Act 1979

This act prohibits the interception of telecommunications (including data transmissions) within Australia except under warrant.

Crimes Act 1901 Parts II and VII

This act deals with national security offences such as treason and espionage.

Radiocommunications Act 1992

This act covers offences relating to radio emission, including interference likely to prejudice the safe operation of aircraft or vessels, interference with certain radio communications, and interference likely to cause danger, loss, or damage.

Electronic Transactions Act 1999

This act provides a liberal regulatory regime for the use of electronic communications for legal and government transactions.

There are also provisions in the Telecommunications Act of 1997 requiring a carrier or carriage service provider to enter into an agree-

13 Dependability Development Support Initiative (DDSI). *European Dependability Policy Environments*, *Country Report Australia*. (version April 2002).

14 http://www.auscert.org.au/Information/Auscert_info/2002cs.pdf.

ment with the Commonwealth about planning for network survivability or operational requirements in time of crisis, and providing that rules and licenses for carriers or service providers may require compliance with a disaster plan.

The government has introduced new computer crime legislation, the Cybercrime Bill 2001, to implement the rulings on computer offences proposed in the recently released Model Criminal Code Report. This is an important step toward achieving national consistency in this area and remedying the deficiencies in existing laws. Mirror legislation has already been implemented in New South Wales, and other states are also expected to follow suit. The proposed legislation on computer offences is designed to protect the security, integrity, and reliability of computer data and electronic communications. The penalties will provide a strong deterrent to those who engage in cyber-crime such as hacking, computer virus propagation, and denial of service attacks. Serious offences such as stalking and fraud are also covered.[15]

Organizational Analysis[16]

Public Agencies

So far, there is no single Australian authority responsible for CIIP. Rather, there are several organizations including both public and private actors that own and operate the CII. Until now security imperatives have not been as relevant as economic and commercial motivations in arriving at arrangements for infrastructure governance.[17]

Two central coordination bodies have been established in Australia to oversee the government's CIIP efforts: the E-Security Coordination Group (ESCG) and the Critical Infrastructure Protection Group (CIPG).[18]

15 Interview with a representative of the National Office for the Information Economy (NOIE), July 2002.

16 This section relies strongly on the findings of the Dependability Development Support Initiative (DDSI). *European Dependability Policy Environments*, *Country Report Australia*. (version April 2002).

17 Cobb, Adam. *Thinking about the Unthinkable: Australian Vulnerabilities to High-Tech Risks.* Foreign Affairs, Defence and Trade Group, Research Paper 18. (29 June, 1998).

18 http://www.asio.gov.au/Media/Contents/protecting%20NII.htm.

E-Security Coordination Group (ESCG)

The ESCG is the government's core policy development and coordination body on e-security matters for the public and private sectors. Its main tasks are the development of a secure and trusted electronic operating environment, awareness-raising on e-security, reporting of incidents, and information-sharing. The ESCG is chaired by the National Office for the Information Economy (NOIE) (see below). The E-Security Policy Section of the ESCG provides administrative support to the E-Security Coordination Group. The Section also manages the consultative industry arrangements on behalf of, and in conjunction with, other Commonwealth agencies.[19]

Critical Infrastructure Protection Group (CIPG)

The CIPG is a sub-committee of the ESCG. While the ESCG is interested in e-security issues affecting the broader economy and community, the CIPG concentrates on issues relating to the impact of critical incidents on the NII. The CIPG's main task is to conduct threat and vulnerability assessments of key participants in the telecommunications, finance, and electricity sectors, and of air traffic control.[20] Recently, the CIPG started a study on the degree of threat to Australia's NII from critical incidents. This is to become the centerpiece of the government's policy. The CIPG is chaired by the Attorney-General's Department.

Attorney-General's Department

The main task of the Attorney-General's Department[21] is to coordinate governmental efforts to identify and protect the NII and to coordinate the development of the CII policy. The Attorney-General's Department gives the CIPG executive, policy, and secretariat support. It ensures that critical NII elements are protected in accordance with the government's priorities.

National Office for the Information Economy (NOIE)

The National Office for the Information Economy (NOIE) is the lead Commonwealth agency for information economy issues. Established in 1997, it was tasked with the establishment of a globally leading online econo-

19 Dale, Tom. "Who's Who in eSecurity and eCrime". *eSecurity and eCrime Conference at Baker & McKenzie Cyberspace Law and Policy Centre*. (Sydney, 19–20 July, 2001). http://www.austlii.edu.au/au/other/CyberLRes/2001/17.

20 http://www.asio.gov.au/Media/Contents/electronic%20environment.htm.

21 See http://www.ag.gov.au/aghome/aghome.htm.

my and society.[22] On 11 October 2000, the Minister for Communications, Information Technology and the Arts announced that the government will expand the functions of the NOIE and establish it as an executive agency within the Communications, Information Technology and Arts portfolio. The NOIE has direct responsibility for the development and coordination of advice to the government on issues related to the information economy. The NOIE's strategy consists of:

- The development of cooperative arrangements between the public and private sectors,
- The integration of electronic and physical protective security and response arrangements,
- Encouraging further development of a response capability in the private and public sectors,
- The build-up of a database on threats and vulnerabilities,
- The development of review arrangements.

Office of Government Information Technology (OGIT)

The OGIT was established in 1995 with the task of developing efficient and effective IT strategies and systems within the government. Its principal role is "getting the government on-line". The OGIT was eventually renamed the Office for Government On-line (OGO).[23] In late 2000, the functions of the OGO were incorporated into the NOIE as part of the NOIE's expanded functions. This provided a coordinated approach to technical, regulatory, and social issues affecting government, business, and consumers in the take-up of online services and the development of an information economy.[24]

Australian Security Intelligence Organisation (ASIO)

The Australian Security Intelligence Organisation (ASIO) is Australia's security service.[25] Its primary mission is to provide advice to protect Australia from threats to national security. ASIO gathers information and produces intelligence enabling it to warn the government about situations that might endanger Australia's national security. It focuses on terrorists, political violence, and people who may clandestinely obtain sensitive government information or otherwise harm the country's interests. Further

22 http://www.noie.gov.au.
23 NII Report 1998, 7.
24 http://www.noie.gov.au/about/index.htm.
25 Its functions are set out in the Australian Security Intelligence Organisation Act 1979.

ASIO functions include the provision of security assessments and protective security advice.

Cooperation between Public and Private Sectors

Cooperative arrangements between the public and the private sectors have been a fundamental part of Australia's CIIP framework since the late 1990s. A recent government initiative to develop links with industry was the inaugural meeting of the Prime Minister's Task Force on Critical Infrastructure. Held in Sydney in March 2002, the meeting was very successful in providing business input for the assessment of current arrangements to protect the CI/CII sectors.

Business-Government Task Force on Critical Infrastructure[26]

In Australia, the most important public-private partnership is currently the Business-Government Task Force on Critical Infrastructure. The overall aim is to raise awareness among the key players from the public and private sectors. The Task Force also seeks to ensure business input into the development of policies to protect Australia's CII. The Business-Government Task Force on Critical Infrastructure is co-chaired by the Attorney-General's Department, which is responsible for national security, and the NOIE, which is responsible for the promotion of the information society. However, so far, the organizational and legal framework for the Business-Government Task Force on Critical Infrastructure remains undecided. The members of the Task Force include Commonwealth government agencies, state and territory governments,[27] major companies from the private sector, and major trade associations (e.g., the water, petroleum, electrical, and internet sectors). A deliberate effort was made to ensure that participants were Australian companies rather than branch offices of US companies.[28]

26 Mainly based on an interview with a representative of the National Office for the Information Economy (NOIE), April 2002.

27 Primarily Attorney-General/Justice Departments.

28 Rathmell, Andrew: *Trip Note, Australian Business-Government Task Force on Critical Infrastructure*, 26–27 March 2002 (thanks to the author for the provision of this note).

Early Warning

AusCERT

The Australian Computer Emergency Response Team (AusCERT) is a non-profit organization located at the University of Queensland. As a single, trusted point of contact in Australia for the Internet community, it provides an important information security service to the private sector and to some government agencies. AusCERT's aims are to reduce the probability of successful attacks, to reduce the direct costs of security to organizations, and to lower the risk of consequential damage.[29]

ISIDRAS

ISIDRAS is an IT incident-reporting scheme for Commonwealth government agencies specifically concerned with high-level incidents that could cause damage to the government's IT infrastructures. ISIDRAS is run by the Defence Signals Directorate (DSD).[30]

Warning Alert and Incident Reporting Scheme

Discussions are underway for the development of an early warning alert and incident reporting scheme. This would be targeted at SMEs and some members of the NII. The arrangements for the alert scheme are likely to commence in mid-2002. Some corporate organizations and critical infrastructure sectors that are not members of AusCERT and who do not receive global CERT and open-source information will also be included as part of the target audience.[31]

Research and Development

In Australia, CIIP research and development (R&D) is undertaken by Commonwealth government agencies, the academic community, and commercial e-security businesses. The Commonwealth has a number of industry development polices and programs that positively impact

29 http://www.auscert.org.au, and NII Report 1998, 2.
30 http://www.dsd.gov.au.
31 Interview with a representative of the National Office for the Information Economy (NOIE), July 2002.

on e-security R&D in Australia. In order to position e-security R&D as a national priority, NOIE is presently investigating additional means of augmenting these policies and programs, including through facilitating linkages between researchers in the commercial, government, and academic sectors, and increasing awareness of funding opportunities. The Defence Signals Directorate (DSD) and the Defence Science and Technology Organisation (DSTO) are looking to establish regular, targeted funding of specific e-security R&D projects.[32]

32 Interview with a representative of the National Office for the Information Economy (NOIE), July 2002.

CIIP Country Surveys

Canada

Concept of CIIP and Description of System

In Canada, CI is defined as "those physical and information technology facilities, networks, and assets whose disruption or destruction would have serious impact on the health, safety, security, and economic well-being of Canadians or on the effective functioning of governments in Canada".[1] Based on efforts made in anticipation of Y2K, the Critical Infrastructure Protection Task Force (CIPTF, see below) modified its results to settle on a characterization of CI/CII in six critical sectors. These critical sectors are the following ones:[2]

- (Tele-) Communications,
- Government,
- Energy and utilities,
- Financial services,
- Safety,
- Transport.

CIIP Initiatives and Policy

CIIP Initiatives

The Canadian government has recognized the importance of CIIP and that all elements of the CI are highly dependent on information technology.[3] This adds a new set of CII vulnerabilities and risks to natural hazards such as risk of earthquakes, floods, or ice storms. In the late 1990s, Canada intensified its CIIP efforts. The following list gives an overview of the main initiatives taken:

1 Grenier, Jacques. "The Challenge of CIP Interdependencies". *Conference on the Future of European Crisis Management.* (Uppsala, Sweden, 19-21 March 2001). http://www.ntia.doc.gov/osmhome/cip/workshop/ciptf_files/frame.htm.

2 http://www.epc-pcc.gc.ca/critical/index_e.html.

3 Purdy, Margaret. *Cyber-Sabotage for Government. Speech at the Ottawa Congress Centre.* (Ottawa, 20 February, 2001).

National Infrastructure Risk Assessment (NIRA)

The National Contingency Planning Group (NCPG) was formed in October 1998. Part of its mandate was to develop a National Infrastructure Risk Assessment (NIRA). The NIRA's objective was to better position Canada for the transition to the year 2000. It set out to examine critical Canadian infrastructures.[4] In May 1999, excerpts of the NIRA were published in the book "Canada's Critical Infrastructure: An Overview".

Y2K Efforts

Later, the NCPG was given the mandate to monitor and coordinate federal organizations through the Y2K transition. One of the groups formed under the NCPG was the Infrastructure Analysis Group (IAG). Its mandate was to predict potential impacts of any Y2K failures on the Canadian infrastructure and critical government functions.[5] Drawing on lessons from the Y2K roll-over period, the Canadian federal government in April 2000 created the interdepartmental Critical Infrastructure Protection Task Force (CIPTF). The Task Force was charged with the development of proposals for a national CIP/CIIP policy framework.[6]

Strategic Infrastructure Initiative (SII)

The Treasury Board Secretariat[7] leads the Strategic Infrastructure Initiative (SII) in partnership with key departments and agencies. The SII will satisfy the government's accountability for the security of its IT infrastructure and allow it to meet its government on line objectives. Under the responsibility of the Chief Information Officer, the SII is focusing on designing a robust IT security architecture, establishing optimal IT security standards and practices, and developing the capabilities needed to more fully protect government-held information and communications with Canadians.

CIIP Policy

Based on the perception of the new risks such as IT dependencies/ interdependencies, spectacular terrorism, and mass casualty/urban

4 National Contingency Planning Group. *Canadian Infrastructures and their Dependencies*. (March 2000), iv.
5 National Contingency Planning Group. (March 2000), iv.
6 http://www.dnd.ca/archive/2001/feb01/06protect_b_e.htm.
7 http://www.tbs-sct.gc.ca.

destruction attacks, the federal government has taken several steps towards a better risk management policy.[8]

Government-on-line (GoL)

The government will put in place a technology and policy framework that protects the security and privacy of Canadians in their electronic dealings with their government. This is part of the GoL policy. Canadians will be able to transmit applications and financial transactions securely on-line and in real-time. GoL must address the principal security requirements for electronic transactions (data integrity, data confidentiality, availability, authentication, and non-repudiation).

"All Hazards" Approach

The establishment of the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP, see below) implicated the merging of the CIP/CIIP and emergency preparedness functions. With this process, the Canadian government pointed to the new national security policy agenda, which went beyond the realm of cyberspace. The setting of the new national security agenda was also influenced by the lessons learned from the 1998 ice storm affecting Eastern Canada and Quebec. The Canadian policy emphasizes decentralized, collaborative "bottom-up" approaches, because most of the CI/CII are under the jurisdiction of provincial governments or owned by the private sector.[9] The "all hazards" approach to CIP/CIIP in Canada adds a heightened awareness of physical infrastructure threats analogous to recent discussions on US homeland security.[10] The OCIPEP sees Canada's CI/CII potentially affected by both physical and virtual threats. It is also fully recognized that Canada's CI are heavily dependent on IT.

National Critical Infrastructure Protection Program (NCIPP)

The events of 11 September 2001 have accelerated the implementation of the National Critical Infrastructure Protection Program (NCIPP). The Canadian government is working on this program together with the provinces and the territories. The overall aim is to identify CI/CII of national interest, so that appropriate measures can be taken to protect them and

8 http://faso.nrcan.gc.ca/newsfe_e.htm.

9 Dependability Development Support Initiative (DDSI). *Global Overview – Countries, International and Inter-Governmental Organisations.* (version April 2002), 19.

10 Dependability Development Support Initiative, Global Overview, (version April 2002), 16.

to mitigate and plan for the potential impact in case of failures. The objective of the NCIPP is to catalogue elements of the physical infrastructure as well as of cyberspace that could be at risk from a variety of hazards.[11] The government seeks to involve the provincial, territorial, and local authorities in this process, since it is crucial that these authorities be aware of CI/CII and of the possible significant impacts to their region in case of failures.

Law and Legislative Action[12]

The Constitution Act

This act defines the areas of federal and provincial authority and determines the leadership responsibilities of the different governmental agencies for emergency preparedness.

The Emergency Preparedness Act

This act is a major element of the federal framework. It charges Canadian ministers with the responsibility of making plans for emergencies that may fall under their jurisdiction.

The Emergencies Act

This act is a multi-part statute describing four types of national emergencies: (1) public welfare emergencies (including severe natural disasters and major accidents affecting public welfare), (2) public order emergencies (emergencies that constitute threats to the security of Canada), (3) international emergencies (acts threatening Canada's sovereignty, security, or territorial integrity), (4) war emergencies (real or imminent armed conflict against Canada or its allies).

Following 11 September 2001, Canada is reviewing its legislation, as are many other countries. A new OCIPEP legislative is being drafted to replace the Emergency Preparedness Act. The new legislation will include provisions for CIIP.

11 http://www.gov.yk.ca/depts/community/pdf/3200-1129web.pdf.

12 For this section, the author is indebted to ÖCB (ed.), *International CEP Handbook: Civil Emergency Planning in the NATO/EACP Countries 1999–2000*, (Stockholm, 2000), 33–36.

Organizational Analysis

Public Agencies

Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP)

The Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) is Canada's main governmental organization responsible for CIP/CIIP. The OCIPEP, being embedded within the Department of National Defence, has the ability to call on specialized computer security expertise within the military and national security community. The Office is headed by the associate deputy minister of national defense.[13] The OCIPEP has the objective of developing and implementing a comprehensive approach to protecting Canada's CI/CII. The Office is also the government's primary agency for ensuring national civil emergency preparedness and therefore also encompasses the existing functions of Emergency Preparedness Canada.[14] However, the OCIPEP has no law enforcement and no investigative power. Its approach includes promoting awareness and education, research and development, information-sharing, and partnerships with other governments and the private sector.[15]

National CIO Subcommittee on Information Protection (NCSIP)

In 1998, the National CIO Subcommittee on Information Protection (NCSIP) was established at the behest of the Public Sector Chief Information Officer's Council (PSCIOC), representing all federal, provincial, and territorial governments and a Municipal Information Systems Association (MISA) representative. This forum enables participating governments to exchange information, policies, security awareness program practices, and architecture initiatives related to information protection.

Cooperation between Public and Private Sectors

Canada's CIIP policy is based on a broadly collaborative approach. The Canadian government seeks to create partnerships with private sector actors to enhance information-sharing between the public and the pri-

13 The Minister of National Defence is responsible for the OCIPEP.

14 http://www.epc-pcc.gc.ca/whoweare/index_e.html.

15 Dependability Development Support Initiative, Global Overview (version April 2002), 19.

vate sectors.[16] The current policy postulates that the CIIP challenge has to be tackled by efforts on the part of the federal government and the provinces and territories, as well as individual CII owners. One part of that approach is international collaboration (above all with the US).[17] The public-private partnership approach of the Canadian government is largely based on the structures and contacts developed during the Y2K rollover. During this period, the Canadian government worked together with private actors responsible for the security of CII.[18]

OCIPEP Approach

An important cooperation approach in Canada between the public and private sectors are the regular meetings of OCIPEP and representatives of CI/CII. These meetings are a trigger for the building of trust and for fostering information-sharing. OCIPEP's tries to create Information Sharing and Analysis Centres (ISACs) within governments and within infrastructure sectors.[19]

Information Operations Working Group (IOWG)

The Information Operations Working Group (IOWG) is an activity of the Department of National Defence.[20] The group seeks to build partnerships with industry actors as part of its own CIP/CIIP efforts. The IOWG addresses the Department's own dependence on civilian communications infrastructure.[21]

16 Dependability Development Support Initiative, Global Overview (version April 2002), 20.
17 "Cyber-Sabotage for Government", speech by Margaret Purdy at the Ottawa Congress Centre, 20 February 2001.
18 Dependability Development Support Initiative, Global Overview (version April 2002), 20.
19 "Cyber-Sabotage for Government", speech by Margaret Purdy at the Ottawa Congress Centre, 20 February 2001 and http://www.cfcsc.dnd.ca/irc/nh/nh9798/0034.html.
20 http://www.dnd.ca.
21 Dependability Development Support Initiative, Global Overview (version April 2002), 20.

Early Warning

CanCERT

The OCIPEP provides subscribers with a range of services designed to support responses to computer security breaches. The OCIPEP promotes the collection, analysis, and reporting of statistics on Canadian IT security incidents. The CanCERT team and its subscribers are contributors to these goals.[22] CanCERT is a member of the international Forum of Incident and Security Response Teams (FIRST).

Research and Development

Research and development (R&D) in the field of CIIP is largely financed by the private sector, and partly by the public sector. The following are some of the most important government-funded R&D activities:[23]

The OCIPEP promotes CIIP R&D across the branches of the Canadian government. The OCIPEP encourages collaborative work among governments, the industry, and academia to address crucial requirements in such areas as intrusion detection.[24]

The Canadian National Research Council (NRC) operates the Institute for Information Technology (IIT) and the Institute for Microstructural Sciences (IMS). These institutes conduct their research mostly in collaboration with private firms and universities.

Research at the Communications Research Centre (CRC) is focused on advanced communications. The research programs provide a technical basis for the development of regulations and standards in support of telecommunications and broadcast policy.

The Networks of Centers of Excellence (NCE) is a unique federal program in Canada that facilitates partnerships between industry and universities.

The Defence Research and Development Branch of the Department of National Defence Research and Critical Infrastructure Protection has several responsibilities. They include facilitating and enhancing the ability of decision-makers to make informed decisions on defense policy.

22 http://www.cancert.ca.
23 Dependability Development Support Initiative, Global Overview (version April 2002), 22.
24 Purdy, *Cyber-Sabotage for Government*.

CIIP Country Surveys

Germany

Germany

Concept of CIIP and Description of System

The main premise underlying CIIP in Germany is that the government and society as a whole heavily depend on a secure infrastructure to function. Infrastructure that meets this definition is defined as critical.[1] The following infrastructure sections are defined as critical in Germany:[2]

- Banking and finance,
- (Tele-) Communications,
- Energy and utilities,
- Public administration,
- Public health,
- Rescue services,
- Transport.

CIIP Initiatives and Policy

CIIP Initiatives

AG KRITIS

Initiated by the report of the President's Commission of Critical Infrastructure Protection (PCCIP) in the US, an inter-ministerial working group on CI (AG KRITIS) was established in 1997 by the Federal Minister of the Interior.[3] It consisted of the ministerial representatives, a steering committee, and a permanent office at the Federal Agency for Security in Information Technology (see below).

The mandate of AG KRITIS was:[4]

- To describe possible threat scenarios for Germany,
- To conduct a vulnerability analysis of Germany's crucial sectors,

1 http://www.bsi.de/literat/faltbl/kritis.pdf.
2 http://www.bsi.de/literat/faltbl/kritis.pdf, and http://userpage-fu-berlin.de/~bendrath/Kritis-12-1999.html, 6.
3 http://userpage-fu-berlin.de/~bendrath/Kritis-12-1999.html, 6.

- To suggest countermeasures,
- To sketch an early warning system.

The objective was to deliver the results in a report. The following findings are taken from a draft version of this report;[5] the report itself was never published.[6] In the first half of 1998, AG KRITIS conducted a survey of the federal public administration with a focus on the identification of the specific CII situation in the individual administrative agencies, an analysis of the IT dependency of each infrastructure sector, and an assessment of possible damages.[7] The following is an overview of the main results:[8]

- The awareness of IT threats varies heavily from agency to agency,
- There was a strong reluctance among the interviewees to reveal vulnerabilities in the IT security structure,
- Generally, the main threats for the IT systems are hacking and unauthorized access to data.

The creation of AG KRITIS was an important basis for all the later activities of public agencies in Germany. Its work is carried on, e.g., by the Federal Agency for Security in Information Technology.[9] Furthermore, the Y2K rollover together with the "Melissa" and "I Love You" virus incidents have increased public awareness.

Enquête Commission

In mid-1998, the so-called Enquête Commission on "The future of the media in business and society – Germany's progress towards the information society"[10] issued its fourth progress report, "Security and Protection in the Internet" (Sicherheit und Schutz im Netz).[11] The commission contributed to the collection and assessment of major risks linked to the

4 http://userpage-fu-berlin.de/~bendrath/Kritis-12-1999.html, and http://ww.isn.ethz.ch/crn/extended/workshop_zh/ppt/jantsch/sld003.htm.

5 See, e.g., http://userpage-fu-berlin.de/~bendrath/Kritis-12-1999.html, also available at http://cryptome.org/Kritis-12-1999.html or http://www.iwar.org.uk/cip/resources/Kritis-12-1999.html.

6 Dependability Development Support Initiative (DDSI). *European Dependability Policy Environments*, *Country Report Germany.* (version April 2002).

7 http://userpage-fu-berlin.de/~bendrath/Kritis-12-1999.html.

8 http://userpage-fu-berlin.de/~bendrath/Kritis-12-1999.html.

9 http://www.bsi.bund.de/fachthem/kritis/index.htm (in German) or (in English) http://www.bsi.bund.de/literat/faltbl/kritis_e.htm.

10 The commission was established by the German Bundestag (federal parliament).

11 http://www.bundestag.de.

new information technologies. Furthermore, it made some important proposals for risk management.[12]

Campaign "Security in the Internet"

The campaign "Security in the Internet"[13] is a combined initiative by the Ministry of the Interior, the Ministry of Economics and Technology and the Federal Agency for Security in Information Technology (since 2000). Its main objectives are to promote awareness among citizens and companies, to recommend improvements to Internet security for private and corporate users, and to act as a forum for information-sharing.[14]

Task Force "Secure Internet"

As a reaction to the DDoS-attacks in February 2000 against commercial Internet sites like yahoo.com, cnn.com, ZDNET.com, etc., an inter-ministerial task force called "Secure Internet" was established. Its main goals are to identify possible threats and to study countermeasures. By June 2002, its publications included recommendations on protection against DDoS-attacks and information on 0190-dialers.[15]

Comprehensive Threat Analysis

In the fall of 2001, a comprehensive threat analysis for Germany was published by the Ministry of the Interior.[16] Besides other threats, information security is defined as crucial for the security of the society and the success of the economy. The risk management approach for information security as proposed in this paper assumes responsibility will be mainly delegated to the company providing information infrastructure services.

Infrastructure Analysis Studies

In mid-2002, the Ministry of the Interior and the Agency for Security in Information Technology (see below) launched a series of studies to systematically analyze the CI/CII sectors. These will give an overview of each sector and its internal structures, identify the critical processes,

12 http://userpage-fu-berlin.de/~bendrath/Kritis-12-1999.html.

13 http://www.sicherheit-im-internet.de.

14 http://www.sicherheit-im-internet.de/home/home.phtml, and http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/jantsch/sld005.htm.

15 http://www.bsi.de/taskforce/index.htm.

16 Bundesministerium des Innern. *Zweiter Gefährdungsbericht der Schutzkommission beim Bundesminister des Innern. Bericht über mögliche Gefahren für die Bevölkerung bei Grosskatastrophen und im Verteidigungsfall*. (Berlin, October 2001).

name the dependencies within and across sectors, and list preventive measures. The results of this comprehensive, structured analysis will be used as an important knowledge base for further activities and deeper research.

Further Activities

Besides the above-mentioned activities, the armed forces (Bundeswehr)[17] have initiated various steps within the field of CIIP.

Presently, there are no comprehensive interdependency studies publicly available in Germany.[18] A survey of representatives of CI/CII business sectors was taken in an initial step to systematically collect threats and expected damages to CII. The collected data was summarized in a matrix.[19] Some sector-specific studies have been published in the meantime, e.g. for the financial sector.[20]

CIIP Policy

Though CIIP is a growing issue in Germany, a comprehensive policy document was still lacking by mid-2002. But priorities are named in the framework of the different initiatives mentioned above. Generally speaking, they are:[21]

- To identify new vulnerabilities in Germany's national security,
- To conduct a detailed analysis of IT threats,
- To develop appropriate detection measures,
- To push the process of information-gathering,
- To upgrade the IT basic security (Grundschutz).

Concept "Critical Infrastructure"

The Federal Agency for Security in Information Technology (Bundesamt für Sicherheit in der Informationstechnik, BSI) has defined a security concept "Critical Infrastructure" that includes possible measures going beyond basic IT security measures. Though the importance of such mea-

17 http://www.iwar.org.uk/cip/resources/Kritis-12-1999.html.

18 Interview with a representative of the consulting company Industrieanlagen-Betriebsgesellschaft (IABG), May 2002.

19 For details see Hutter, Reinhard. "Cyber-Terror: Risiken im Informationszeitalter". In: *Aus Politik und Zeitgeschichte* (vol. 10/11, 2002): 36.

20 Bundesamt für Sicherheit in der Informationstechnik (BSI). *IT-Sicherheitsstrukturen in der deutschen Kreditwirtschaft.* (Ingelheim, 2002) http://www.bsi.de/presse/pressinf/itkredit.htm.

sures is well recognized, they have to be limited to a selection of issues due to cost and effectiveness constraints. To define these issues, the BSI recommends the following step-by-step procedure:[22]

- To define a business strategy for trade using CII,
- To assemble a stock of IT techniques and components in consideration of mutual dependencies,
- To define the criticality,
- To verify and facilitate decision-making,
- To define appropriate measures and concepts.

Combating Terrorism

The events of 11 September 2001 made additional resources available under the heading of the "campaign against terrorism". Part of these additional funds will be used for combat against cyber terrorism in the future. Thanks to these additional resources, current and probably also new initiatives in Germany will be funded.[23]

Law and Legislative Action

Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations[24]

The purpose of this law is to create the conditions for electronic signatures. This law deals with issues such as technical security, voluntary accreditation, supervision, liability, and data protection.

Information and Telecommunications Services Act[25]

The Information and Telecommunications Services Act of 1997 was the starting point for the liberalization of the German telecommunications market.[26]

21 http://www.iwar.org.uk/cip/resources/Kritis-12-1999.html.
22 http://www.bsi.de/literat/faltbl/kritis.pdf.
23 Dependability Development Support Initiative, Country report Germany (version April 2002).
24 http://www.iid.de/iukdg/gesetz/Signaturg_engl.pdf.
25 http://www.iid.de/iukdg/gesetz/iukdge.html.
26 Interview with a representative of the consulting company Industrieanlagen-Betriebsgesellschaft (IABG), May 2002.

Act on the Utilization of Teleservices[27]

This act will be the basis for the establishment of uniform economic conditions for the various applications of electronic information and communication services.

Teleservices Data Protection Act[28]

The purpose of this act is to define provisions for the protection of teleservice users' personal data within the framework of the Act on the Utilization of Teleservices, which governs the collection, processing, and utilization of such data by service providers.

Electronic Signature Act[29]

In May 2001, this act (which conforms to EU regulations) replaced the existing pioneer Digital Signature Act of 1997. The main purpose of the act is to define a framework for the handling of electronic signatures.

Organizational Analysis

Public Agencies

Ministries and Agencies

The main ministries involved in CIIP at the national level in Germany are the Ministry of the Interior, the Ministry of Economics and Technology, and the Ministry of Defense. They are supported by the Agency for Security in Information Technology (BSI) and the Reg TP (regulation authority for telecommunications and postal services).

Agency for Security in Information Technology[30]

One of the most important agencies dealing with CIIP in Germany is the Federal Agency for Security in Information Technology (Bundesamt für Sicherheit in der Informationstechnik, BSI), which was founded in 1991. The agency is subordinated to the Federal Ministry of the Interior. Its technical leadership is widely accepted and recognized. Within the BSI, there is a section responsible for CII. This section focuses its work on

27 http://www.iid.de/iukdg/aktuelles/fassung_tdg_eng.pdf.
28 http://www.iid.de/iukdg/aktuelles/fassung_tddsg_eng.pdf.
29 http://jurcom5.juris.de/bundesrecht/sigg_2001/inhalt.html.
30 http://www.bsi.bund.de.

the dependability of CII in the work of the government and the public administration. Efforts are being made in the field of vulnerability and threat assessment. A CERT (called CERT-Bund) is also part of the Federal Agency for Security in Information Technology.

Further Important Actors

Further actors involved within the Federal Administration are the Federal Law Enforcement Agency (Bundeskriminalamt, BKA)[31] and some other ministries.[32] The Federal Intelligence Service (Bundesnachrichtendienst, BND)[33] is responsible for compiling threat analyses.

Cooperation between Public and Private Sectors

The prevalent premise in Germany is that cooperation between the public and the private sectors is the best strategy.[34] In general, the private sector sees little need for initiatives that focus on the private sphere only. The most important input from the private sectors is given in the context of cooperation with actors from the public sector. There are several cooperation initiatives in Germany between public and private actors related to CIIP.

Initiative D21[35]

The Initiative D21 is the largest private-public partnership in Germany. This economic initiative also deals with dependability issues. The Initiative D21 is a neutral platform, independent of party allegiance or the industrial sector. The work of the Initiative D21 is based on the premise that the transition of the country from an industrial society to an information society is a task for both politics and the economy.

D21 is a model of an "activating government". There are 226 participants; all sectors of industry (not only IT providers), institutions, and politics are represented.[36] The Initiative D21 has formed 5 task forces and 15 sub-task forces. In the task forces, important topics are discussed and

31 http://www.bka.de.
32 http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/jantsch/sld004.htm.
33 http://www.bundesnachrichtendienst.de/start.htm.
34 http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/jantsch/sld009.htm.
35 http://www.initiatived21.de.
36 Including 94 member companies, 33 sponsors, 59 supporters, and 43 advisory council members.

agreements are implemented. Some of the main activities of the task force on "Security and Trust in the Internet" include:

- The campaign "Internet for Everyone" with the aim of promoting trust and confidence,
- The study "Internet Access in Germany",[37]
- Recommendations for linking up the different CERTs.

Partnership for Secure Internet Business

The Partnership for Secure Internet Business ("Partnerschaft Sichere Internet-Wirtschaft") is supported by the Ministry of Economics and Technology (Bundesministerium für Wirtschaft and Technologie, BMWi) [38] and was founded in May 2000. The partnership was initiated by the Minister of Economics and Technology together with ten prominent trade associations and companies.[39] The main actors in the "Partnerschaft Sichere Internet-Wirtschaft" are the Ministry of Economics and Technology from the public sector, and up to 40 trade associations and companies from the private sector.

The purpose of the "Partnership for Secure Internet Business" is to ensure a secure and trustworthy Internet for e-business and to promote security as a quality factor. Some of the objectives set until the end of 2002 are:

- A comprehensive awareness campaign on typical security-relevant business mishaps,
- Better transparency through security-relevant standards,
- Observation of trends in sensitive infrastructure as well as increasing awareness of the dangers presented by industrial espionage,
- Improvement of precautionary measures and assistance for small and midsize companies through suitable CERT structures (Computer Emergency Response Teams).

Working Group on Infrastructure Protection (AKSIS) [40]

Based on the premise that the increasing dependability of society on CII means the linked risks must be studied in a comprehensive approach, the Working Group on Infrastructure Protection (Arbeitskreis zum Schutz

37 This was adapted from Tony Blair's "Digital Divide" study.
38 http://www.sicherheit-im-internet.de/themes/themes.phtml?ttid=48&tdid=1616.
39 See http://www.sicherheit-im-internet.de.
40 See http://www.aksis.de, and http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/jantsch/sld010.htm.

von Infrastrukturen, AKSIS) was established in 1999 on the initiative of the Zentrum für Strategische Studien (ZES), which belongs to the company IABG (Industrieanlagen-Betriebsgesellschaft). The main purpose of AKSIS is to provide a forum for information exchange to analyze and to assess the dependability of CI/CII sectors. AKSIS has no official government or industry mandate. It is purely voluntary and informal. There are two meetings per year at which representatives of the public and private sectors (ministries, armed forces, police, telecommunication, energy, transport, banks, academia, etc.) participate.

In November 2001, AKSIS organized the Cyber Terror Exercise (CYTEX) at IABG in Ottobrunn near Munich. Participants came from several federal ministries, other bodies of the public administration, and the industry. The core element of the exercise was a scenario of a series of attacks on the abovementioned public and private actors' IT systems and a large bank in the Berlin area with possible blackmail.[41]

Early Warning

The study "CERT Infrastructure Germany"[42] was published in January 2002. It determined that besides the already existing CERTs (such as dCERT,[43] DFN-CERT,[44] S-CERT,[45] secu-CERT,[46] Telekom-CERT,[47] CERT-Bund,[48] etc.), a CERT following the needs of SME was required. This is being established together with the industrial association "BITKOM".[49]

CERT-Bund

The so called "Referat CERT-Bund" was established on 1 September 2001 at the Agency for Security in Information Technology. The CERT-Bund is a central contact point charged with the security of data processors and networks of the federal public administration. The CERT-Bund also offers

41 For details see Hutter, "Cyber-Terror", 37–38.
42 See http://www.initatived21.de.
43 http://www.dcert.de/index_e.html.
44 http://www.cert.dfn.de.
45 http://www.s-cert.de.
46 http://www.secunet.de.
47 http://www.telekom.de/dtag/home/portal.
48 http://www.bsi.de/certbund/index.htm.
49 http://www.bitkom.org.

some of its services to clients from the private sector. However, several services are only available to the federal administration (e.g., incident response).[50] The CERT-Bund's main tasks include warning and information-sharing, data collection, analysis and processing of information, documentation and dissemination, sensitization of IT decision makers, and cooperation with existing CERTs.[51]

Research and Development

In 2000, the Federal Ministry for Education and Research (BMBF) published its "Concept for action – Information technology in education". The concept is a core element in the implementation and strategic refinement of the action program "Innovation and Jobs in the Information Society of the 21st Century". Likewise, the concept is the BMBF's contribution to the implementation of the EU's action plan within the framework of the eEurope Initiative.[52]

Research and development (R&D) related to the field of CIIP is mainly done at universities. Some of the most important of these are the Technical University Munich (Computer Sciences),[53] the University of Hamburg (Computer Sciences),[54] and the Fachhochschule Bonn-Rhein-Sieg (Applied Computer Sciences and IT Security).[55] Furthermore, at the Ruhr University of Bochum, the faculty for electrical engineering and information technology offers a special academic program for IT security.[56] The Institute for Information, Telecommunications, and Media Law (ITM) at the University of Münster focuses on legal problems concerning the information society.[57]

50 Ennen, Günther. "CERT-Bund – eine neue Aufgabe des BSI". In: *KES Zeitschrift für Kommunikations- und EDV-Sicherheit*. Bundesamt für Sicherheit in der Informationstechnik (BSI). (Bonn, June 2001): 35 and http://www.bsi.bund.de/certbund/index.htm.
51 Ennen, CERT-Bund, 35.
52 http://www.bmbf.de/pub/itkon_e.pdf.
53 http://www.tu-muenchen.de.
54 http://www.uni-hamburg.de.
55 http://www.fh-rhein-sieg.de.
56 http://www.eurubits.de.
57 http://www.uni-muenster.de/Jura.tkr/betaversion/oer/schwerpunkte/index.htm.

CIIP Country Surveys

The Netherlands

The Netherlands

Concept of CIIP and Description of System

In the Netherlands, CIIP is defined as the measures to protect the country, its society, its international allies, and its economic (inter)national interests against the effects of deliberate or inadvertent disturbances or intrusions of CII.[1] The following are the critical sectors in the Netherlands:

- Banking and finance,
- (Tele) Communication,
- Defense,
- Drinking water,
- Energy and utilities,
- Food,
- Government,
- Justice,
- Objects with high risk in case of emergency,
- Public health,
- Public order and safety,
- Social sector,
- Transport,
- Water management.

Given their vital role for the Dutch and international society, for most of these sectors, CIIP is of high importance.

CIIP Initiatives and Policy

CIIP Initiatives

CIIP is being perceived more and more as a crucial issue of national security in the Netherlands. Since the end of the 1990s, several efforts have been made to better manage CIIP.

1 Interview with a representative of the Netherlands' Organization for Applied Scientific Research (TNO), April 2002.

Infodrome Initiative and BITBREUK

In March 2000, the key essay "BITBREUK" (English version "In Bits and Pieces") was published by the government-sponsored think tank Infodrome to stimulate the discussion on CII. The essay offered an initial vulnerability analysis and postulated a number of hypotheses for further discussion and examination by the Dutch authorities in cooperation with the appropriate national public and commercial organizations.[2] In mid-2001, this document was used as a starting point for a so-called 24-hour cabinet session. This was a 24-hour workshop with a selected group of experts that created a manifesto on CI/CII issues with a set of recommendations for all political parties. This KWICT-manifest document is available only in Dutch.[3]

KWINT Report and Memorandum

The report entitled "Kwetsbaarheid op Internet – Samen werken aan meer veiligheid en betrouwbaarheid" (KWINT), written by Stratix/TNO[4] for the Ministry of Transport, Public Works, and Water Management (V&W), was completed in 2001. The report concluded that the Dutch Internet infrastructure is extremely vulnerable. Final recommendations on policy measures were made with regard to awareness and education, coordination of incidents, protection, security, etc. It was concluded that the measures should be taken within a public-private partnership approach, while the government should play a facilitating and coordinating role.[5]

The findings and recommendations of this report triggered the implementation of an interdepartmental working group of members of the Ministries of Economic Affairs, Defense, Finance, Interior, Justice, and Transport (Telecom and Post Directorate). As a result, the KWINT government memorandum (Vulnerability of the Internet) was endorsed by the cabinet on 6 July 2001. It includes a number of recommendations for action.

2 Luiijf, Eric, M. Klaver. *In Bits and Pieces: Vulnerability of the Netherlands ICT-Infrastructure and Consequences for the Information Society.* (Translation of he Dutch Infodrome essay "BITBREUK", de kwetsbaarheid van de ICT-infrastructuur en de gevolgen voor de informatiemaatschappij). (Amsterdam, March 2000).

3 http://www.infodrome.nl.

4 TNO is the Netherlands' Organization for Applied Scientific Research.

5 De Bruin, Ronald. "From Research to Practice: A Public-Private Partnership Approach in the Netherlands on Information Infrastructure Dependability". *Dependability Development Support Initiative (DDSI) Workshop.* (28 February 2002).

Anti-Terrorism Plan

In the aftermath of 11 September 2001, the minister of the interior was tasked by the cabinet in early October 2001 with developing a coherent set of measures to protect CI/CII as part of the nation's anti-terrorism plan.[6] A ministerial steering group including all ministers responsible for aspects of CI/CII will investigate the extent of the vital sectors first. In a second step, the critical parts of the sectors will be defined. Current measures will be assessed and additional measures proposed where necessary. Interdependencies and cross-sector aspects will be taken into account. The six-step project will last till 2004 and is scheduled to proceed as follows:

- Quick scan,
- Public-private partnership kickoff workshop,
- Formulation of availability band integrity requirements,
- Risk analysis generating a list of measures,
- List of measures already taken,
- Plan for measures to be taken. This includes ICT/information infrastructure of all sectors.

In June 2002, 17 working groups were formed, one for each vital sector and three for international, legal, and cross-sector dependencies.

Hacking Emergency Response Team (HERT)

In June 2002, the cyber-crime unit of the Dutch police (KLPD) founded a special response group to be activated if the ICT part of a CI is attacked. The priorities of the Hacking Emergency Response Team (HERT) will be to restore CI services and assist in recovery and logistics while collecting evidence. The intention is to have public-private cooperation in this area, bringing in experts from other organizations in order to analyze and mitigate the problem. HERT is to be fully operational in a few years. The 2002 initial phase is called "Bambi".

CIIP Policy

The Dutch CIIP policy is based on three premises: measures should not decrease innovation, the dynamic character of threats should be taken into account, and there is no 100 per cent reliability.[7] The government policy is aimed at fostering wider application of ICT and an understanding

6 House of Parliament (Tweede Kamer). Dossier 27925 – action line 10.
7 De Bruin, From Research to Practice.

of the consequences. In its report, entitled "Government losing ground", the WRR,[8] a government advisory body, analyzed some of the political aspects of the further advance of ICT across society.[9]

"The Digital Delta"

The publication "The Digital Delta" (June 1999) offers a framework for a range of specific measures regarding government policy on information and communications technology (ICT) for the next three to five years.[10] This memorandum notes the increasing importance of ensuring the security of information systems and communications infrastructure and of mastering the growing complexities of IT-applications that are already advanced in nature.[11]

Defense White Paper 2000

Likewise, the increasing importance of ICT is also explicitly mentioned in the Dutch Defense White Paper 2000: "Given the armed forces' high level of dependence on information and communication technology, it cannot be ruled out that in the future attempts will be made to target the armed forces in precisely this area."[12]

Law and Legislative Action

Penal Code

The Penal Code prohibits attacks against (non-ICT) CI (e.g., sabotage, intervening with water management systems, electricity, railways, etc.).

Cyber Crime Law I and Cyber Crime Law II

Both laws are under development and will include all the provisions of the EU Cyber Crime Treaty.[13]

8 Wetenschappelijke Raad voor het Regeringsbeleid.
9 http://www.infodrome.nl/english/missie-eng.html.
10 http://www.gbde.org/egovernment/database/netherlands.html.
11 Luiijf, Klaver, In Bits and Pieces, 5.
12 Ministerie van Defensie, *Defensienota 2000*, (1999), 59.
13 See http://www.minjust.nl/DOWNLOAD/COMPCRIM.DOC.

Telecommunications Law

This law states requirements of the public telecommunication operators regarding capacity, quality, and other properties of the services offered (e.g., free access to the 112 emergency number), as well as regulations with respect to safety and privacy precautions regarding their network and services.[14]

Organizational Analysis

Public Agencies

Ministry of the Interior and Kingdom Relations (BZK)[15]

The duties of the Ministry of the Interior include the promotion of public order and safety and the provision of centralized management of the countries' police forces. It includes the National Coordination Center (NCC), in charge of emergencies with nationwide impact.

Directorate General Telecommunications and Post[16]

The Directorate-General for Telecommunications and Post is subordinated to the Ministry of Transport, Public Works, and Water Management (V&W). The two most important goals are the strengthening of the Netherlands' competitive position in the field of telecommunications, telematics, and postal services, and to make sure that these facilities remain available to citizens and companies.[17] Other parts of the same ministry are responsible for the CI of transport and water management.

General Intelligence and Security Service

The General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst, AIVD) is a division of the Ministry of Interior and is tasked with information security and the protection of vital sectors of Dutch society.[18] The focus areas of the AIVD change in accordance with social and political changes. One of its new tasks is to uncover forms of improper competition such as economic espionage, which could harm

14 http://www.minvenw.nl/dgtp/home/data/tweng.doc.
15 In December 2000, a total of 594 personnel were employed by the BVD.
16 http://www.minvenw.nl/cend/dco/home/data/international/gb/index.htm.
17 http://www.minvenw.nl/cend/dco/home/data/international/gb/brief.htm#dgtp.
18 http://www.fas.org/irp/world/netherlands/bvd.htm.

Dutch economic interests.[19] Another new task is foreign intelligence. In the interests of national security, it will carry out investigations abroad, though only in the non-military sphere.[20]

Cooperation between Public and Private Sectors

In general, public-private partnerships in the Netherlands are organized by agreement between the actors. The government is usually a facilitator bringing the respective actors together. The other actors cooperate according to their responsibility.[21]

The above-mentioned KWINT study of 2001 has led to a flurry of policy recommendations, which will be elaborated in further detail on a public-private partnership platform. These recommendations include awareness-raising, research and development, alarm and incident response, and integrity of information.

Platform Electronic Commerce in the Netherlands (ECP.nl)[22]

ECP.nl (the Platform for Electronic Business in the Netherlands) has been asked to set up a public-private partnership program. Its activities cover six major areas: awareness, trust, interoperability, national projects, research and development, and international coordination. The first duty of ECP.nl is to inform a broad public about the application of electronic commerce for congresses, seminars, conferences, the own website, helpdesks, training, and electronic newsletters. ECP.nl also works on building trust. To this end, it is involved in several projects, including the implementation of various KWINT action lines.

Infodrome[23]

Infodrome is a think tank sponsored by the Dutch government. Started in 1999, it will run for three years. Infodrome serves a threefold objective: (1) to develop an understanding of the social implications of the information revolution (this requires the gathering of empirical, quantitative knowledge and information on information-related developments, and a systematic analysis thereof), (2) to stimulate social awareness of the

19 http://www.minbzk.nl.
20 http://www.minbzk.nl.
21 Interview with a representative of Netherlands' Organization for Applied Scientific Research (TNO), April 2002.
22 http://www.ecp.nl/ENGLISH/index.html.
23 http://www.infodrome.nl/english/missie_eng.html.

importance of having a government policy that meets the requirements of the information society, and (3) to examine the priorities given by parties and interest groups to activities (public or private) undertaken in relation to the information society. This requires an understanding of the political and social value of knowledge, experience, and insights.

The organizational structure of Infodrome reflects the program's ambitious targets. The program is conducted under the direction of a steering group and presided over by a member of cabinet. In addition, participants include members of important policy think tanks. All ministries are represented in the supervisory committee. The structure ensures that politicians, (political) scientists, and representatives of the administrative system are actively engaged in the development of government strategy vis-a-vis the information age.

Early Warning

CERT-NL (part of SURFnet)

CERT-NL is the Computer Emergency Response Team of SURFnet, the Internet provider for institutes of higher education and many research organizations in the Netherlands. CERT-NL handles all computer security incidents in which a SURFnet customer is involved, either as a victim or as a suspect. CERT-NL also disseminates security-related information to SURFnet customers on a structural basis (e.g. distributing security advisories) as well as on an incidental basis (distributing information during calamities).[24] CERT-NL disseminates information coming from CERT-CC/FIRST.

NLIP Security Coordination Group[25]

Some 55 ISPs are organized within the NLIP (Brancheverenigingvan Nederlandse Internet Providers), the Netherlands Internet Providers' trade association. This independent association exists since 1997.

CERT-RO

A computer emergency response team for government departments (CERT-RO) was established in June 2002. It is operated under the respon-

24 http://cert-nl.surfnet.nl/home-eng.html.
25 http://www.nlip.nl.

sibility of the Ministry of Interior (BZK[26]) under its ICT-agency ICTU. CERT-RO will be co-located and co-operating with an entity that is responsible for issuing alarms and advice memoranda to the public and SME about viruses, Trojan Horse codes, and other malicious software, or "malware". Public radio and TV channels will used for communication. This body will become operational at the end of 2002 and is funded by the Ministry of Transport, Public Works, and Water Management (V&W).[27]

Research and Development

The government of the Netherlands aims to engage the business community more actively in European research initiatives. This goal is to be reached through the provision of information on these initiatives and support for the submission of project proposals. The government will give more encouragement to systematic research. Some research has already been carried out at TNO (the Netherlands Organization for Applied Scientific Research).[28] Research at the universities in the field of Internet dependability and security should also be intensified.[29] The overall aim is to promote research into and development of new methods and aids for ensuring the security of information. Further important actors involved in CIIP research and development are the Dutch Ministry of Defense and the think tank Infodrome, as well as the Rathenau Institute.[30]

26 http://www.minbzk.nl.
27 Dutch Ministry of Transport, Public Works and Water Management / Dutch Ministry of Economic Affairs. Internet Vulnerability. (July 2001).
28 http://www.tno.nl/homepage_nl.html.
29 Dutch Ministry of Transport, Public Works and Water Management / Dutch Ministry of Economic Affairs, Internet Vulnerability.
30 http://www.rathenau.nl.

CIIP Country Surveys

Norway

Norway

Concept of CIIP and Description of System

A central premise underlying the Norwegian CIIP policy concept is that nowadays, the production of most goods and services depends in some way or other on information and communication technology (ICT) systems. This dependency may be as a part of the production process itself or as a part of the logistics to make the goods or services available to consumers. ICT forms an important part of the production of goods and services in a number of critical sectors of society. In Norway, the critical sectors are the following:[1]

- Banking and finance,
- (Tele-) Communications,
- Defense,
- Energy and utilities,
- Oil and gas supply,
- Police,
- Public health,
- Rescue services,
- Social security,
- Transport.

The main challenges for society concerning information infrastructure are seen in the areas of rapid technological development, deregulation, globalization, interdependencies, and the lack of expertise and outsourcing of manpower and systems.[2]

1 Ministry of Trade and Industry. *Society's Vulnerability due to its ICT-Dependence – Abridged Version of the Main Report*, (Oslo, October 2000), 9-10.

2 http://www.ntia.doc.gov/osmhome/cip/workshop/norway.ppt.

CIIP Initiatives and Policy

CIIP Initiatives

Since the end of the 1990s, CIIP has been seen as a safety issue in Norway. In fact, CIIP was put on the political agenda by the government commission on "A Vulnerable Society". The Ministry of Trade and Industry on the other hand perceives CIIP as an economic issue.[3]

Commission "A Vulnerable Society"

The governmental commission "A Vulnerable Society" was established by Royal decree on 3 September 1999. It was active from 1999 until 2000. The findings gave important input to the national planning process.[4] The duty of the commission was to study vulnerabilities in society with a broad perspective. The mandate was to assess the strengths and weaknesses of current emergency planning, to assess priorities and tasks, and to facilitate increased awareness, knowledge, and debate about vulnerabilities.[5]

The government commission identified several areas that should be focused on. One of these areas was CI.[6] In its green paper, NOU (2000: 24) – "A Vulnerable Society", the commission placed great emphasis on the significance of ICT for the vulnerability of society in general. The commission, in what was probably its most controversial proposal, recommended that the field of safety, security, and emergency planning should be concentrated in one single ministry.[7] Furthermore, a strategy based on the following pillars was proposed:[8]

- Partnership between public and private sectors,
- Promotion of information exchange,
- Establishment of early warning capacity,
- Harmonization and adjustments of laws and regulations,
- Public responsibility for CIP vital to ICT systems.

3 Interview with a representative of the Danish Directorate for Civil Defense and Emergency Planning (DSB), March 2002.
4 Interview with a representative of the Danish Directorate for Civil Defense and Emergency Planning (DSB), March 2002.
5 http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/Henriksen/sld001.htm.
6 http://www.ocb.se/dokument/filer/5b_gjengsto_henriksen_abstract.pdf.
7 http://www.ocb.se/dokument/filer/5b_gjengsto_henriksen_abstract.pdf.
8 http://www.ocb.se/dokument/filer/5b_gjengsto_henriksen_abstract.pdf.

ICT-Vulnerability Project [9]

The ICT vulnerability project consisted of an interdepartmental group commissioned by the Ministry for Trade and Industry. The project collaborated with the government commission on the "Vulnerable Society". Together, they coordinated their findings on ICT vulnerabilities.[10] In the ICT vulnerability project, each sector authority evaluated the risks linked to specific functions in that sector.[11]

eNorway Plan

The government produced the eNorway (eNorge) plan that describes the needs, responsibilities, and required action for the development of an information society.[12] With the eNorway plan, the government ensures that the country has equally ambitious objectives as those formulated by the EU in the eEurope Plan.[13]

"*Safety and Security of Society*"

On 5 April 2002, the Ministry of Justice and the Police presented report no. 17 on the "Safety and Security of Society" to the Norwegian Storting (Parliament). The report is a comprehensive statement on the government's proposals regarding the reduction of vulnerabilities in modern society and measures to increase safety and security in the future. It states that when assessing the vulnerability of society, it is important to "consider the consequences of lapses in CI, such as a lapse in the distribution of power or a lapse in telecommunication".[14] The recommendations will form the basis for the government's process of initiating measures.

9 Ministry of Trade and Industry, Society's vulnerability, 10.

10 Dependability Development Support Initiative (DDSI). *European Dependability Policy Environments*, *Country Report Norway.* (version April 2002).

11 A common feature of these evaluations is that each individual sector operation is dependent on its own ICT user systems as well as on the public telecommunications services. Therefore, robust access to telecommunications seems to be very important to most sectors. The telecommunications services are dependent on ICT systems in order to function.

12 Dependability Development Support Initiative, Country Report Norway (version April 2002).

13 http://odin.dep.no.

14 Report No. 17 to the Storting (2000-2001). *Statement on Safety and Security of Society (Summary)*, (April 2002).

CIIP Policy

Over the past few years, and as a result of technological developments, there has been an increased focus on CIIP. Moreover, US policy has been an important trigger in putting CIIP on the political agenda in Norway as a political, security, and economic issue.[15]

Policy Statements

In 1998, the State Secretary Committee for ICT (Statssekretærutvalget for IT – SSIT) formed a subcommittee with a mandate to report on the status of ICT vulnerability efforts being carried out in Norway. Furthermore, the importance of CIIP is also stressed by the Defense Review 2000 and the Defense Policy Commission 2000.[16] In the aftermath of 11 September 2001, the government considered it necessary to increase national safety and security, particularly within the civil defense, in the Police Security Service, and in emergency planning within the health sector.[17]

Definition of CIIP Goals

Norway's CIIP policy is based on the following goals:[18] CII must reach a level of robustness that does not degrade important society functions during a "normal" peacetime situation. And in crisis or war, the infrastructure has to be sufficiently robust to maintain functions that are critical for society. Due to the wide range of threats against the society and the challenges to many CII sectors, the government has initiated several relevant measures concerning CIIP.[19]

Law and Legislative Action

Penal Code, Paragraph 151b

The penal code states that whosoever causes comprehensive disturbances to the public administration or other parts of society by disrupting the collection of information, or by destroying or damaging power sup-

15 Interview with a representative of the Directorate for Civil Defense and Emergency Planning (DSB), March 2002.
16 Interview with a representative of the Directorate for Civil Defense and Emergency Planning (DSB), March 2002.
17 Report No. 17 to the Storting (2000-2001).
18 http://www.ocb.se/dokument/filer/5b_gjengsto_henriksen_abstract.pdf.
19 Report No. 17 to the Storting (2000-2001).

ply plants, broadcasting facilities, telecommunications services, or other kinds of communication, will be punished by incarceration for a maximum of 10 years. Unlawful negligence as mentioned in the first instance will be punished by incarceration for a maximum of 1 year. Accessories will be punished in the same manner. This section became law on 12 June 1987.[20]

In Norway, the laws generally tend to place the blame firmly with the operator in cases of accidents such as rail crashes or fires. However, during the last years, systemic errors and bad leadership have become apparent as the underlying causes of many accidents.[21]

Organizational Analysis

Public Agencies

The Ministries of Defense, Justice and Police, Communications, and Trade and Industry are involved to varying degrees in inter-ministerial cooperation.[22]

Directorate for Civil Defense and Emergency Planning (DSB)[23]

The Directorate for Civil Defense and Emergency Planning (direktoratet for sivilt beredskap, DSB) was established in 1970. The directorate works under the authority of the Ministry of Justice and the Police. The main task is to be a center of resources and expertise for emergency contingency planning. The DSB is a point of contact between central authorities and regional commissioners in peacetime disasters.

To ensure adequate preparedness measures in the community, the DSP devotes considerable efforts to ensure that all Norwegian municipalities carry out risk and vulnerability analyses. The DSB works to ensure that activities involving preparedness responsibilities lead to the implementation of internal control systems to ensure the quality of emergency planning at local government level. The DSB also supervises the planning in the ministries and offices of the regional commissioners.

20 Interview with a representative of the Directorate for Civil Defense and Emergency Planning (DSB), March 2002.
21 http://www.ocb.se/dokument/filer/5b_gjengsto_henriksen_abstract.pdf.
22 Interview with a representative of the Directorate for Civil Defense and Emergency Planning (DSB), March 2002.
23 http://www.dsb.no/presentation/index.asp.

OKOKRIM

The National Authority for Investigation and Prosecution of Economic and Environmental Crime is responsible for issues concerning cybercrime.[24] OKOKRIM has a unit called "IKT-teamet", which focuses on ICT-related crimes.

Changes in the Organizational CIIP Structure

Currently, several changes are taking place within the Norwegian organizational CIIP structure. For instance, part of the Chief Headquarters of Defense (CHO) will be established as an agency under the Ministry of Defense with double reporting lines: one to the Ministry of Defense on military issues and one to the Ministry of Justice on civilian issues. Furthermore, a Unit on Telecom Infrastructure Security has been established at the Post and Telecommunications Authority. In the future, the Ministry of Justice will have a greater coordinating role regarding security in civilian society, which will require several steps towards reorganization in civilian agencies.[25] The government also plans to establish a Directorate of National Protection, which will include CIIP tasks.

Cooperation between Public and Private Sectors

The most important public-private initiatives in Norway are the SIS (Ministry of Trade and Industry Initiative) and the VDI (Intelligence services initiative) projects. Both projects, the VDI (which is already operational) and the SIS (which is to be started in 2002), have clear public-private partnership participation profiles and roles.

Center for Information Security (SIS)

The Norwegian government decided some years ago to establish a Center for Information Security. In 2001, a pilot study was commissioned to investigate options for the establishment of this center.[26]

The main tasks of the SIS will include the exchange of information, competence, and knowledge about threats and countermeasures, and a

24 http://www.okokrim.no.

25 Interview with a representative of the Norwegian Ministry of Trade and Industry, June 2002.

26 Dependability Development Support Initiative (DDSI). *Public-Private Co-operation: Business Governmental Actions Towards Achieving a Dependable Information Infrastructure in Europe*. Issues and background paper for the DDSI workshop on Public-Private Co-operation (Stockholm, 6–7 June, 2002), 10.

holistic threat image generation.[27] The future clients of the SIS will be government agencies, security services, politicians, and private enterprises as a basis for assessing national security status. The SIS will not be operating as a government agency and will not be involved in privacy issues.

VDI (Intelligence Services Initiative)[28]

At the beginning of the new millennium, several agencies and business actors began cooperating with the Norwegian intelligence and security services to prevent computer crimes. The whole project is intended to enable intelligence and security professionals to chart the extent of the threat to vulnerable information infrastructure. One of these measures is the "Warning System for Digital Infrastructure" (VDI). The implementation of the VDI was clearly a cabinet reaction to the commission "A Vulnerable Society" and the Ministry of Trade and Industry report in summer/autumn 2000. The VDI will alert clients to breaches and attempted breaches of computer networks. Each member is free to report the incident to the police. Due to the success of the project, the government wants to prolong it. The success of the VDI is, to a great extent, attributed to its control structures, which alleviate possible concerns about business privacy and other issues.

Early Warning

UNINETT CERT

UNINETT CERT is the Norwegian computer emergency response team and the academic network for research and development. It was formed in 1995. The constituency is made up of the Norwegian state universities, colleges and R&D institutions.[29] The main motivations were to contribute to a better Internet security for UNINETT member institutions, and the perceived need of a focal point for security issues regarding UNINETT member institutions.[30] The basic duty of UNINETT CERT is to provide assistance on handling and investigating incidents involving one or more

27 http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/Henriksen/sld001.htm.
28 http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/Henriksen/sld001.htm.
29 Dependability Development Support Initiative, Country report Norway (version April 2002).
30 http://cert.uninett.no/policy.html.

members of the constituency. Examples of incidents are spamming, suspicious port-scanning, denials of service, etc.[31]

Research and Development

The government commission "A Vulnerable Society" suggested that one ministry should have the main responsibility for research in the field of safety and security, that the Norwegian Research Council should initiate and coordinate research, and that safety and security must be integrated in ICT education.[32] The main research since 1994 has been in the area of the protection of the society, based on the works of BAS (Beskyttelse av samfunnet; Protection of the Society).[33]

Since 1994, BAS has been an ongoing research activity. It is a joint project of the Directorate for Civil Defense and Emergency Planning (DSB) and the Norwegian Defense Research Establishment (FFI). The overall purpose is to make central decision-makers more aware and give them insights into the vulnerabilities of Norwegian society, and to point out cost-effective measures to reduce these vulnerabilities. The first BAS project focused on general trends toward increased vulnerabilities.[34] All the following research activities are based on these basic findings. The second BAS project (BAS2) performed an analysis of public telecommunication services in the period 1997-1999. The results of the project formed the basis for the Norwegian government's new strategy concerning security and emergency preparedness in the telecommunications sector.[35] The third BAS project (BAS3) focused its research on vulnerabilities in the electric power supply.[36] The findings recommended measures to reduce the increasing vulnerabilities in the Norwegian electric power supply. BAS4 is a still ongoing project seeking to map vulnerabilities and the impact of failures in the transportation sector. Furthermore, in recent years, the research papers published by the Defense Research Institute have provided a significant basis for the promotion of safety and security in society.[37]

31 http://cert.uninett.no/policy.html.
32 http://www.ocb.se/dokument/filer/5b_gjengsto_henriksen_abstract.pdf.
33 http://www.ntia.doc.gov/osmhome/cip/workshop/norway.ppt.
34 Four sectors were identified as particularly critical: telecommunications, electric power supply, transportation, and management/information.
35 This strategy was proposed in May 2001.
36 The Norwegian electric power market was deregulated in 1991.
37 Report No. 17 to the Storting (2000–2001).

CIIP Country Surveys

Sweden

Sweden

Concept of CIIP and Description of System

In Sweden, CIIP is understood as the protection of essential electronic information services. The Swedish Commission on Media Convergence defines electronic information services as including IT systems, telecommunications, and radio and television services.[1] However, in a broader sense, the CI sectors in Sweden are the following:[2]

- Banking and finance,
- (Tele-) Communication,
- Food,
- Energy,
- (Electronic) Information services,
- Public health,
- Social welfare,
- Transportation,
- Water supply.

In an earlier joint study, power supply, telecommunication, governmental command and control, financial services, and air traffic were mentioned as the vital sectors for IT incidents.[3]

1 Interview with a representative of the Swedish Agency for Civil Emergency Planning (ÖCB), April 2002.
2 Interview with a representative of the Swedish Defense Research Agency (FOI), July 2002.
3 Interview with a representative of the Swedish Defense Research Agency (FOI), July 2002.

CIIP Initiatives and Policy

CIIP Initiatives

Cabinet Working Group on IO-D

On 12 December 1996, the government decided to appoint a working group within the cabinet. This Cabinet Working Group on IO-D was tasked with the identification of threats and risks due to information warfare, the dissemination of knowledge, proposals for sharing responsibility, and guidelines for a strategy. Today, besides representatives of the cabinet office and ministries, the Cabinet Working Group on IO-D also includes representatives of relevant private companies and organizations.[4]

Commission on Media Convergence

In July 1997, the Swedish government appointed a special investigator to study the implications of convergence between the telecommunications, media, and information technology (IT) sectors. The inquiry was prompted by technical developments that are making the boundaries between IT, telecommunications, and media increasingly fluid, whereas the existing legislation essentially presumes that those boundaries can be maintained.[5]

The ÖCB Infrastructure Report

In the letter of regulation for the year 1998, the former Swedish Agency for Civil Emergency Planning (ÖCB) was tasked to report – in consultation with the relevant authorities and the Swedish armed forces – on the extent to which vulnerabilities in the civilian CI could be assumed to limit the total defense ability under certain conditions. The report identified mutual interdependencies between power grids, telecommunications networks, and IT systems.[6]

4 Interview with a representative of the Swedish Agency for Civil Emergency Planning (ÖCB), July 2002.
5 Interview with a representative of the Swedish Agency for Civil Emergency Planning (ÖCB), July 2002.
6 Interview with a representative of the Swedish Agency for Civil Emergency Planning (ÖCB), July 2002.

Commission on Vulnerability and Security

In June 1999, the Swedish government authorized the defense minister to appoint a commission to ensure an integrated approach to civil defense and emergency preparedness planning as related to CI in the society. This has been the most important step concerning CIIP in Sweden during the last years. Eventually, the Commission on Vulnerability and Security began its work in March 2000.[7] The commission was charged with exploring the options for an organizational or structural separation of functions, and with proposing ways and means of enhancing IT security and protection against attacks.[8] The commission conducted an analysis of trends and problems in the field of crisis management.

In its report, the commission concluded that "as a result of changes in society, the vulnerability of the technical infrastructure is now perceived as a more significant threat both in peacetime and in a security crisis"[9].

CIIP Policy

Expanding the Total Defense Concept

As a consequence of the broadened concept for security policy, the Swedish parliament in 1997 decided on a specific ambition for the preparedness against what was called severe strains on the society. The reorientation of the defense and emergency management system implies an expansion of the Swedish Total Defense Concept. The changes in the Total Defense Concept not only affect the military sector, but, to a large extent, the civil sector and the security and preparedness of Swedish society as well. The main emphasis is no longer on the supporting role of civil defense in relation to military defense. The CI, rather than military resources, could be the primary target for a potential aggressor. It is the Swedish policy to take measures to meet both military and other threats (e.g., terrorist attacks).[10]

7 The Swedish Commission on Vulnerability and Security. *Vulnerability and Security in a New Era – A Summary.* (SOU 2001:41, Stockholm, 2001). http://forsvar.regeringen.se/propositionermm/sou/pdf/sou2001_41eng.pdf, 7.

8 http://www.cesi.it/Vulnerabilitypdf/Interventi/roundtable_ottosson.pdf.

9 Swedish Commission on Vulnerability and Security, Vulnerability and Security, 8.

10 Interview with a representative of the Swedish Agency for Civil Emergency Planning (ÖCB), April 2002.

"Emergency Management Concept"

Part of the Swedish CIP/CIIP policy is that each government authority must make a vulnerability and risk analysis of its own sphere of responsibility. The purpose of such an analysis is to enhance the capacity to manage crisis, situations which come under the heading of "severe peacetime emergencies". This concept refers to an event or number of events that develop or escalate to affect multiple sectors of society.[11]

Organizational Change Process

The ongoing process of changing organization and control in crisis management and CIP/CIIP is based on three principles: responsibility, parity, and proximity. Under the principle of responsibility, whoever is responsible for an activity in normal conditions should assume corresponding responsibility in crisis or war situations. The principle of parity means that as far as possible, during a crisis or war, authorities should be organized and stationed as in peacetime. The principle of proximity means that crises should be dealt with at the lowest possible level.

Government Bill "An Information Society for All"

The Government Bill 1999/2000:86 ("An Information Society for All") defines the Swedish overall IT policy objective. It states that Sweden should become the first country to create an information society for all. The Swedish government proposes that for the purpose of creating an information society for all, state investment be focused primarily on three areas. These areas are (1) regulatory systems, (2) education and training, and (3) infrastructure.[12] An essential element of CIIP-planning is that the agency responsible in peacetime should also be responsible in times of crisis and war, and that the system should be built up from below. This means that the system has its foundation in society's basic capacity and that measures are then taken on the basis of the entire threat perspective, from severe peacetime emergencies to war.

11 Interview with a representative of the Swedish Agency for Civil Emergency Planning (ÖCB), April 2002.

12 Ministry of Industry, Employment and Communication. *An Information Society for All. Fact Sheet No. 2000.018.* (March 2000).

Four New Fields of Activity

Based on the Government Bills 2001/02:158 ("Society's Security and Preparedness")[13] and 2001/02:10 ("Continued Renewal of the Total Defense"),[14] the government will establish four new fields of activity in order to enhance information security and protection against attacks on information systems.

- An advanced intelligence and analysis unit in the field of IT security and protection against attacks on information systems,
- A Computer Emergency Response Team (engaged in monitoring, gathering statistics, and warning system owners where necessary),
- An Information Security Technical Support Team (manned by expert and support staff with a high level of technological expertise),
- A system for security-oriented evaluation and certification of IT products and systems.

Overall Responsibility Approach

The Parliamentary Standing Committee for Defense has for several years recognized the importance of CIIP. With the establishment of the Swedish Emergency Management Agency (SEMA, see below) and the reformed system for emergency management, an important organizational basis has been created to deal with the threats and risks of the information and network society. From 1 July 2002, overall responsibility for IT-security and for policy intelligence and analysis in the public sector rests with SEMA.

Law and Legislative Action

In Sweden, there are three important laws regarding CIIP in general:[15]

- The Telecommunications Act (SFS 1993:597),
- The Swedish Penal Code (SFS 1962:700),
- The Personal Data Act (1998:204).

In its report, the Commission on Vulnerability and Security concluded that there is a need for legislative amendments in order to support the pro-

13 Ministry of Defense. *Society's Security and Preparedness. Fact Sheet.* (March 2002). http://forsvar.regeringen.se/pressinfo/pdf/FB_p200102_158_eng.pdf.

14 See, e.g., http://forsvar.regeringen.se/inenglish/issues/civil.htm.

15 Interview with a representative of the Swedish Agency for Civil Emergency Planning (ÖCB), July 2002.

posals with respect to IT security and the protection against IO. A need for legislative amendments is particularly seen in the following areas:[16]

- Statutory and administrative provisions relating to the activities of local authorities and country administrative boards during major crises,
- The possibility of reallocating resources in the health services during major crises,
- The need for stricter safety regulations and for more effective supervision of the power supply sector.

The government has decided to review the legislation relevant to CIIP and Emergency Management.

Organizational Analysis

Public Agencies

The Swedish Emergency Management Agency (SEMA)[17]

The Swedish Emergency Management Agency (SEMA) was established on 1 July 2002. It is the government authority with overall responsibility for information security. SEMA took over some of the tasks of the Swedish Agency for Civil Emergency Planning (ÖCB)[18] and the National Board of Psychological Defense (SPF).[19] SEMA analyzes the development of society, international conditions, and the interdependency of important operations in society. It also coordinates research and development in the emergency management area. Furthermore, SEMA supports municipalities, county councils, county administrative boards, and other authorities in their emergency management work. The agency also promotes interaction between the public and private sectors. Planning and resource allocation for peacetime emergency preparedness and civil defense are organized in six "coordination areas":

- Technical infrastructure,
- Transport,

16 Swedish Commission on Vulnerability and Security, Vulnerability and Security, 20–21.

17 Interview with a representative of the Swedish Agency for Civil Emergency Planning (ÖCB), July 2002.

18 http://www.ocb.se.

19 http://www.psycdef.se/english.

- Spreading of dangerous infectious substances, toxic chemicals, and radioactive matter,
- Economic security,
- Overall coordination, interaction and information by area,
- Protection, rescue, and care.

In each area, a number of public authorities are represented. They have to coordinate their activities to reduce vulnerabilities and to enhance emergency management capabilities in the areas. SEMA is responsible for the overall integration of planning systems.

The ICT Commission

The ICT Commission was set up by the government as an advisory board in the field of information technology. The commission's task is to analyze the impact of information technology on Swedish society and promote the dissemination of information about new opportunities in the information society. The commission is actively monitoring, initiating, and supporting the development and use of information technology in society.

The National Center of IO/CIP (CIOS)

The National Center of IO/CIP (CIOS) is an office within the National Defense College.[20] CIOS carries out the National Defense College's (NDC's) research and education in the area of Information Operations/Information Warfare, and partly in the area of Command and Control Warfare. It is the NDC's point of contact for external customers regarding IO/CIP.

Information Security Technical Support Team

An Information Security Technical Support Team will be set up as an independent authority answerable to the National Defense Radio Establishment. The Defense Materiel Administration is instructed to establish a Swedish evaluation and certification system.

Swedish Security Service and National Criminal Investigation Department

The Swedish Security Service and the National Criminal Investigation Department are units of the National Police Board. Both units have import tasks in the field of information security and cyber-crime. The Swedish Security Service is responsible for the protection of sensitive objects, counter-espionage, anti-terrorist activities, and the protection of

20 http://www.fhs.mil.se/about/en/about.html.

the constitution. The National Criminal Investigation Department (NCID) provides support for investigations and intelligence support in cases of crimes involving nationwide or international ramifications.[21]

Further Organizations

The Swedish intelligence community, coordinated by the government offices, is of significant importance for Swedish CIIP. The National Communications Security Unit (TSA) provides important services within the field of signals security.

Cooperation between Private and Public Sectors

SEMA Approach

There is a long tradition of public-private cooperation within the framework of the Swedish Total Defense System. Based on this tradition, SEMA is tasked with building up a public-private partnership in the future. There will be two advisory councils connected to SEMA: the Private Sector Partnership Advisory Council and an Information and Operations Security Advisory Council based on the experiences from the Cabinet Working Group on IO-D. However, it has not yet been defined how the CIIP public-private partnership will be institutionalized.[22]

Industry Security Delegation (NSD)

The Industry Security Delegation (NSD) is a delegation within the Confederation of Swedish Enterprises whose objective is to increase cooperation and promote a comprehensive view of vulnerability and security issues. The overall goal of this network structure is to enhance security and risk awareness within the general public and the enterprises. The NSD has drawn up a policy for the establishment of a private sector CERT.[23]

Swedish Alliance for Electronic Commerce (GEA)

The Swedish Alliance for Electronic Commerce (GEA) was founded in 1999 as a non profit organization. The projects are funded by members

21 Interview with a representative of the Swedish Agency for Civil Emergency Planning (ÖCB), July 2002.

22 Interview with a representative of the Swedish Agency for Civil Emergency Planning (ÖCB), July 2002.

23 Dependability Development Support Initiative (DDSI). *European Dependability Policy Environments*, *Country Report Sweden.* (version April 2002).

and government agencies. The GEA focuses on electronic identification, signature, and secure payments issues.

Early Warning

National Center for the Reporting of IT Incidents

The Swedish National Post and Telecom Agency has been tasked with the establishment of a National Center for the Reporting of IT Incidents. This will be comparable to a CERT. The national center should be established by the end of 2002.[24]

Important existing CERTs are Telia CERT, the main telecommunications operator in Sweden, and SUNET CERT, the university network CERT.

Research and Development

CIIP-related research and development (R&D) in Sweden is mainly conducted in the area of academic research, corporate research, and Total Defense research. The Commission on Vulnerability and Security concluded that there is a need for more R&D to improve the capacity for managing major crises. The efforts in R&D have to be made in an interdisciplinary manner. The Commission made several proposals as to how to best promote R&D:[25]

- A broad cross-section of research groups should be encouraged,
- Public bodies should be encouraged to commission and purchase R&D,
- Purchasers and providers should be linked in subject- or problem-oriented networks that include public authorities and research groups.

SEMA has the leading role in Swedish CIIP research and development coordination and will develop a number of R&D programs in that area.

24 Interview with a representative of the Swedish Agency for Civil Emergency Planning (ÖCB), July 2002.

25 Swedish Commission on Vulnerability and Security, Vulnerability and Security, 19.

SEMA is also a contributing partner of the Swiss-Swedish CRN initiative.[26]

The Swedish Defense Research Agency (FOI)[27] is an assignment-based authority under the Ministry of Defense. FOI focuses its R&D efforts on the entire field of applied science from advanced computer models, physics, aerodynamics, and electronics to chemistry, microbiology, and medicine, as well as security policy and defense analysis. One important initiative is the SAVI (Säkring Av Viktig Infrastructur), which is a long term research program at the FOI.[28] The research areas are divided into five major aspects: systems, threats, vulnerabilities, consequences, and measures.

Further important actors involved in CIP/CIIP research and development are the Chalmers University of Technology (Gothenburg),[29] the Linköping Institute of Technology,[30] The Royal Institute of Technology (KTH),[31] Stockholm University,[32] Karlstad University,[33] and the Swedish Institute of Computer Science (SICS).

26 The CRN (Comprehensive Risk Analysis and Management Network") is an internet and workshop initiative for international dialog on national-level security risks and vulnerabilities, see www.isn.ethz.ch/crn.

27 http://www.foi.se.

28 Interview with a representative of the Swedish Defense Research Agency (FOI), April 2002.

29 http://www.chalmers.se.

30 http://www.lith.liu.se/en.

31 http://www.kth.se/eng.

32 http://www.su.se.

33 http://www.kau.se.

CIIP Country Surveys

Switzerland

Switzerland

Concept of CIIP and Description of System

Since the end of the Cold War, risks and vulnerabilities involving information and communications technologies have become a growing issue in Switzerland's debate on security policy. Switzerland's high density of information and communication technology (ICT) in the public and private sectors offers a high potential for vulnerabilities. To date, the critical sectors in Switzerland are the following:

- Administration,
- Civil defense,
- (Tele-) Communication,
- Finance,
- Food,
- Industry,
- Information distribution,
- Military defense,
- Public health,
- Research and education,
- Social security,
- Transport,
- Utilities,
- Water supply.

The definition of these sectors is very broad. A more refined and more official definition is only at the stage of planning.

CIIP Initiatives and Policy

CIIP Initiatives

Since the end of the 1990s, several important steps have been undertaken to better manage CIIP in Switzerland.[1]

Strategic Leadership Exercise 1997

A key experience, and in fact the kick off for all the later steps in Switzerland, was the Strategic Leadership Exercise in 1997 (SFU 97).[2] The main topic of the exercise was the ICT revolution and the related challenges to modern society, politics, economics, and finance as well as to other critical sectors.[3] The results of the exercise unveiled that Switzerland's CI was facing new threats. One of the results was the call for an independent organization dealing with information security issues.[4]

"Strategy for the Information Society Switzerland"

In 1998, the Federal Council defined its "Strategy for the Information Society Switzerland". The four governing principles are: (1) access to information for everyone, (2) empowerment for everyone to use information technologies, (3) freedom of development of the information society, and (4) acceptance of new technologies. Developments triggered by ICT were perceived as a high priority issue for Switzerland.[5]

1 See also Sibilia, Ricardo: "Informationskriegführung. Eine schweizerische Sicht" In: *Institut für militärische Sicherheitstechnik (IMS)*. (Nr. 97-6, Zurich, 1997); Generalsekretariat VBS (Ed.). *Risikoprofil Schweiz. Umfassende Risikoanalyse Schweiz.* (Draft, Bern, August 1999); Spillmann, Kurt R.; Libiszewski, Stefan; Wenger, Andreas; et al. "Die Rückwirkungen der Informationsrevolution auf die schweizerische Aussen- und Sicherheitspolitik". In: *NFP 42 Synthesis*, *Nr. 11. Schweizerischer Nationalfonds*, Bern, 1999). http://www.snf.ch/nfp42/public/resume/rspillmanninfo_d.html; and Bircher, Daniel. "Informationsinfrastruktur – Verletzliches Nervensystem unserer Gesellschaft". In: *Neue Zürcher Zeitung*, 7 *July*, *1999*.

2 The SFU which is subordinated to the Swiss Federal Chancellery is responsible for the periodical training of the federal decision makers. See http:// www.sfa.admin.ch.

3 Schweizerische Bundeskanzlei. *Strategische Führungsübung 1997 – Kurzdokumentation über die SFU 97.* (Bern, 1997), 2.

4 See http://www.infosurance.org.

5 http://www.admin.ch/bakom/news/pm_stratInfoges_d.htm.

Exercise "INFORMO 2001"

After a two-year planning process, the Strategic Leadership Training conducted the three-day exercise "INFORMO 2001". The goals were to review the information assurance process established after 1997 and to coach a newly-established special staff for IT related crisis.[6]

Annual Events

The two most important annual events in Switzerland concerning information security are the Bernese Conference on Information Security and the Symposium on Privacy and Security.

The Bernese Conference on Information Security[7] is organized by the Special Interest Group on Information Security and the Swiss Federal Strategy Unit for Information Technology. Every year, the event covers a specific topic.[8] The Symposium on Privacy and Security[9] aims at offering an international discussion platform for important topics of privacy and security in the fields of science, business, administration, and politics. The event covers various aspects of privacy and security.[10]

CIIP Policy

Security Policy Report 2000

In the Security Policy Report 2000, the Swiss Federal Council defined CIP as a primary goal of its security policy. The Federal Council defined its objectives regarding CIP as follows: "The Federal Council's primary objective regarding the security of this infrastructure is to maintain Switzerland's ability to decide and to act, and to create the conditions ensuring the functioning of the Swiss 'information society'".[11]

6 See http://www.sfa.admin.ch.

7 German translation: Berner Tage für Informationssicherheit

8 For example, the topic in 2002 was 'information assurance', in 2001 'public key infrastructures' and in 2000, 'man as an important security factor'.

9 Symposium on Privacy and Security 2001, available at http://www.privacy-security.ch.

10 The 2001 event topics were 'consumer control – consumer privacy', 'security infrastructure and solutions', 'areas of conflict between e-future and privacy', and 'surveillance'.

11 *Security through Cooperation – Report of the Federal Council to the Federal Assembly on the Security Policy of Switzerland*. (Berne, June 1999). http://www.vbs.admin.ch/internet/SIPOL2000/E/index.htm, 54-55.

Coordination Group for Information Society

The Coordination Group for Information Society defined security and availability of information infrastructure as one of the high-priority operative elements. The key policy document, "Concept Information Assurance", was published in 2000. It recommended the establishment of a crisis management system and the establishment of a special task force "Information Assurance".[12] This strategy of the Swiss Federal Council was accompanied by a large number of parliamentary initiatives. More than 30 initiatives dealing with the information society were proposed by members of parliament between 2000 and 2001, two of them dealing with information and Internet security.[13]

Information Assurance

The current information assurance policy in Switzerland is based on four pillars:

- In order to foster command and control in crisis situations, a concept for a "Task Force Information Assurance" has been developed. The task force's primary duty is to support strategic decision-making in crisis situations. In addition, the creation of a permanent analysis and reporting center for information security is considered to be a core element of the Swiss information assurance concept. This center relies on a broad array of sensors to collect and analyze relevant information,[14]
- Governmental support is provided if the private sector is unable to resolve provisioning problems (the "subsidiary principle"). The ICT Infrastructure Unit's tasks are risk analysis and emergency planning for CI,[15]

12 See Koordinationsgruppe Informationsgesellschaft (KIG): Konzept "Information Assurance", Mai 2000.

13 3rd Report of the Information Society Coordination Group (ISCG) to the Federal Council, 28–30.

14 The federal decree states the establishment of a special Task Force (Sonderstab) "Information Assurance". See *Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (BinfV) vom 23. Februar 2000.* (Bern, 2000). http://www.admin.ch/ch/d/sr/1/172.010.58.de.pdf. The basic concept is available at http://www.isb.admin.ch/dok/dokumente/informatiksicherheit/einsatzkonzept_ia.pdf.

15 The main task of the NES is to guarantee the provision of vital goods and services to the Swiss population. The NES works closely with the private sector as well as with cantonal and municipal authorities.

- The third pillar of Switzerland's current Information Assurance policy is trust and confidence building as well as building networks to tackle information assurance issues,
- The idea of an "Information Assurance" coordination body with the task of coordinating the various initiatives by the federal administration to secure CII is the fourth pillar.

Law and Legislative Action

Swiss Penal Code,[16] *Article 143bis (unauthorized access to a computing system)*

This article states that any person that, by means of a data transmission device, gains unauthorized access to a computing system belonging to others, and specially protected against access by the intruder, shall be punished by imprisonment or a fine if a complaint is made.[17]

Swiss Penal Code, Article 144 (damage to property)

The article states that any person that damages, destroys, or renders unusable any property belonging to others, shall be punished by imprisonment or a fine if a complaint is made.[18]

Swiss Penal Code, Article 144bis (damage to data)

The article states that any person that alters, deletes, erases, or renders unusable data stored or transferred by electronic or similar means without authorization, shall be punished by imprisonment or a fine if a complaint is made.[19]

Swiss Penal Code, Article 147 (fraudulent use of a computer)

The article states that any person that, with the intention of unlawfully obtaining financial rewards for himself or another, interferes with an elec-

16 Although the Swiss Penal Code is up to date, only a few cases have been prosecuted so far. Switzerland's laws against virus creation and the use of malicious software in general are widely applicable. However, the legal structure in Switzerland makes prosecution difficult, due to the complexities of different laws (comprised of laws on both the federal and cantonal level) and law enforcement procedures.

17 Based on the official English translation of the Swiss Penal Code.

18 Based on the official English translation of the Swiss Penal Code.

19 Based on the official English translation of the Swiss Penal Code.

tronic procedure through the unauthorized use of data, shall be punished by community service of up to five years or imprisonment.[20]

Swiss National Economic Supply Law (protection of communication channels)

This law makes specific mention of the protection of communication transfer.

Telecommunication Law

This law regulates the management of IT and telecommunication in the federal administration.

Further laws or legislative activities are presently being discussed. These are the Federal Law on Digital Signature, the Federal Law on e-commerce, and the Law on Data Privacy.

Whereas legislation is written to be widely applicable, prosecution in Switzerland is difficult due to the administrative structure (resulting in the applicability of both federal and cantonal laws). In November 2001, the Federal Council accepted the "Convention on Cybercrime of the Council of Europe".[21] It should be noted that the Swiss Penal Code is already in agreement with the corresponding international articles on infringements of copyright, computer-related fraud, child pornography, and offences related to unauthorized intrusion into protected computer systems.

Organizational Analysis

Public Agencies

The CIP/CIIP issue has been raised mainly by government agencies and by associations and societies. The main responsibilities and the corresponding financial obligations for CIIP presently lie within the public sector.

Federal Strategy Unit for Information Technology (FSUIT)

One of the main bodies is the Federal Strategy Unit for Information Technology (FSUIT). It is subordinated to the Swiss Federal Department

20 Based on the official English translation of the Swiss Penal Code.

21 *ISPS News (Infosociety.ch)*, *Press Release: Gemeinsam die Cyber-Kriminalität bekämpfen. Bundesrat genehmigt Konvention des Europarats*. http://www.isps.ch.

of Finance (FDF). The FSUIT reports to the FDF and is charged with producing instructions, methods, and procedures for the federal administration's information security during normal times. It collects data on incidents within the Swiss federal government[22] and is responsible for the "Task Force Information Assurance".

Division for Information Security and Facility Protection (DISFP)

The Division for Information Security and Facility Protection (DISFP) reports to the Federal Department of Defense, Civil Protection, and Sports (DDPS) . Its main tasks are to gather and analyze information and to provide adequate IT security within the DDPS.[23]

Federal Office of Information Technology, Systems, and Telecommunication (BIT)

The Federal Office of Information Technology, Systems, and Telecommunication (BIT) is subordinated to the Swiss Federal Department of Finance (FDF). BIT is the federal provider for IT. Its responsibilities include security and emergency preparedness.

Federal Office for Communication (OFCOM)

The Federal Office for Communication (OFCOM) is the main regulatory body in the field of telecommunications and ICT in Switzerland. The OFCOM looks at different aspects of the information revolution. It includes consumer protection and management of the frequency spectrum as well as conformity assessment rules in the telecommunications equipment area. The OFCOM deals with information society risks, such as the formation of a new two-tier society, information overload and the resulting inability to analyze problems and make decisions, and new opportunities for the manipulation of information of a technical, political, or economic nature.

Federal Office for National Economic Supply (NES)

The Federal Office for National Economic Supply (NES), which includes an ICT Infrastructure Unit, reports to the Swiss Federal Department of Economic Affairs (FDEA). Its main task is to ensure that the Swiss population is able to obtain vital goods and services at all times. The NES pro-

22 Informatikstrategieorgan Bund ISB, available at http://www.isb.admin.ch.

23 Division for Information Security and Facility Protection (DISFP) available at http://www.vbs.admin.ch/internet/GST/AIOS/e/index.htm.

vides governmental support should the private sector be unable to resolve supply problems on its own. However, measures to ensure national economic supply would only be undertaken if the system of free competition were seriously disrupted.

Federal Office of Information Technology, Systems, and Telecommunication (FOITT)

The Swiss Federal Office of Information Technology, Systems, and Telecommunication (FOITT) reports to the Swiss Federal Department of Finance (FDF). Its responsibilities include security and emergency preparedness.[24]

Strategic Leadership Training (SLT)

The Strategic Leadership Training is part of the Federal Chancellery. It is responsible for the periodical training of federal decision-makers, including instruction for crisis management of security incidents.

Cooperation between Public and Private Sectors

Switzerland has a long-standing tradition of public-private partnerships. Historically, this is due to the tradition of part-time service both in the military and in politics. Moreover, certain Swiss institutions have never been managed by a fully professional staff.

InfoSurance Foundation

The most prominent example of a body promoting cooperation between industry and administration is the InfoSurance foundation.[25] It is supported simultaneously by leading companies and the Swiss government. The foundation seeks to link closely the organizational and structural conditions for recognizing and analyzing the risks for Switzerland and its growing dependency on information technologies. It also aims to inform decision-makers as well as public and private IT users as to the risks and dangers of information technologies.

24 The Federal Office of Information Technology, Systems and Telecommunication, available at http://www.efd.admin.ch/e/dasefd/aemter/bit.htm.

25 The Foundation for the Security of Information Infrastructure in Switzerland. See http://www.infosurance.ch.

ICT Infrastructure Unit (ICT-I)

Another important player regarding public-private partnerships is the National Economic Supply (NES). Its main task is to ensure the provision of vital goods and services to the Swiss population at all times. NES is working in close cooperation with the private sector as well as with cantonal and municipal authorities. The federal government has requested the NES to create a new ICT Infrastructure Unit (ICT-I) to deal with all prolonged disruptions of the information and communications infrastructure affecting the whole of Switzerland and to continuously conduct risk analyses.

Early Warning

SWITCH- CERT

On a technical level, the Computer Emergency Response Team of the Swiss Academic and Research Network (SWITCH-CERT) helps its customers (mainly universities and other institutes of learning) to manage problems concerning information security.

Analysis and Reporting Center for IT-related Incidents

The Federal Strategy Unit for Information Technology (FSUIT, see above) has made efforts to fill the "early warning gap" for Swiss CIIP issues. FSUIT has started the project "Analysis and Reporting Center for IT-related incidents". The planned analysis center will rely on a broad array of sensors to collect and analyze relevant information. This requires well-established contacts to IT operators in the corporate world as well as in public administration. It will also supply the "Task Force Information Assurance" with relevant information in an emergency situation.[26]

26 Informatikstrategieorgan Bund, Einsatzkonzept Information Assurance Schweiz, November 2001, available at http://www.isb.admin.ch/dok/dokumente/informatiksicherheit/einsatzkonzept_ia.pdf.

Research and Development

The Information and Communication Management Research Group[27] at the University of Zurich's Department of Computer Science concentrates on the application of computer science in enterprises, especially problems of information processing within companies where security is an important issue. Some of their current research topics include secure transmission of data and secure access to the Internet.

The Institute of Theoretical Computer Science, Information Security and Cryptography at the Swiss Federal Institute of Technology Zurich, Department of Computer Science, is focusing on cryptography.

The Center for Security Studies and Conflict Research at the Swiss Federal Institute of Technology (ETH Zurich) is developing the Comprehensive Risk Analysis and Management Network (CRN)[28] in order to support the international dialog on risks, vulnerabilities, and risk analysis methodology, and to share and review national experiences. The CRN initiative links the scientific expertise of the ETH Zurich with national and international emergency preparedness and planning authorities.[29] Based on the International Relations and Security Network (ISN),[30] the CRN provides various Internet services and develops training capabilities based on information and communications technology for national and international security analysts, researchers, and practitioners. Research is conducted in the following areas: Risk/Interdependency Modeling, Critical Infrastructure Protection (CIP), Interdependencies and Vulnerabilities in Critical Information, Infrastructure (CII), Political Violence Movements/International Terrorism, International Critical Information Infrastructure Protection (CIIP) Handbook.

The Laboratory for Safety Analysis at the Swiss Federal Institute of Technology has developed a methodology for quantitative vulnerability assessments that can be used to describe dependencies within CI.

27 Information and Communication Management Research Group, available at http://www.ifi.unizh.ch/ikm/research.html: IKM and research activity.

28 http://www.isn.ethz.ch/crn.

29 In Switzerland, the CRN team supports the ongoing process of risk identification and evaluation (Risikoanalyse Schweiz XXI project) with scientific expertise and methodological research.

30 http://www.isn.ethz.ch.

The Security and Cryptography Laboratory at the Swiss Federal Institute of Technology, Lausanne, aims at the promotion of research and education in the field of communication and information system security.[31]

The University of Fribourg's International Institute of Management in Telecommunications (iimt) focuses its research activities on mobile electronic business, information security management, information and communication management, and technology management.

The activities of the Department of Information Technology at the University of Applied Sciences, Lucerne, include technical IT security projects, product testing, and consulting and design of secure ICT system architectures.[32]

The Institute for Internet Technologies and Applications at the University of Applied Sciences, Rapperswil, deals with information security.[33]

The activities of the IBM Research Lab at Rüschlikon (near Zurich) range from cryptographic foundations to the implementation of standards-based cryptographic algorithms.[34]

31 The Security and Cryptography Laboratory (LASEC) was formed in 2000 at the Department of Communication Systems (DSC) of the Federal Institute of Technology at Lausanne (EPFL). Various aspects are considered, including critical security analysis, security strengthening methods, and fundamental research on security and cryptography. Available at http://lasecwww.epfl.ch.

32 Institute for Internet Technologies and Applications (ITA), http://www.ita.hsr.ch.

33 See Homepage, available at http://www.hta.fhz.ch.

34 Source: IBM Research Laboratory, available at http://www.zurich.ibm.com/csc/infosec/index.html.

CIIP Country Surveys

United States

Concept of CIIP and Description of System

CIP in the US is about the protection of infrastructure critical to the people, economy, essential government services, and national security. The main goal of the US government's efforts is to ensure that any disruption of the services provided by this infrastructure is infrequent, of minimal duration, and manageable.[1] In the US, the following are defined as the critical sectors:

- Banking and finance,
- Energy,
- Information and communications,
- Transport,
- Vital Human Services.[2]

The five sectors are highly interdependent, both physically and in their greater reliance on CII.

CIIP Initiatives and Policy

CIIP Initiatives

There have been several efforts since the 1990s to better manage CIIP in the US.

Presidential Commission on Critical Infrastructure Protection (PCCIP)

Based on the recommendations of the Critical Infrastructure Working Group (CWIG), which was appointed as a reaction to the Oklahoma City bombing, President Bill Clinton set up the Presidential Commission on Critical Infrastructure Protection (PCCIP) in 1996,[3] the first national

1 Moteff, John D. *CRS (Congressional Research Service) Report for Congress. Critical Infrastructures: Background, Policy, and Implementation.* (Updated February 4, 2002). http://www.fas.org/irp/crs/RL30153.pdf.

2 Including emergency services, government services, and water supply systems.

3 http://www.ciao.gov/PCCIP, and http://www.ciao.gov/PCCIP/eo13010.pdf.

effort to address the vulnerabilities of the information age. Its tasks were to

- Report to the president on the scope and nature of vulnerabilities and threats to the nation's CI, focusing primarily on cyber-threats,
- Recommend a comprehensive national CIP plan,
- Determine legal and policy issues raised by proposals to increase protections,
- Propose statutory and regulatory changes necessary to effect recommendations.[4]

The PCCIP included representatives from all relevant government departments as well as from the private sector. The PCCIP presented its report to the president in October 1997.[5] The commission's most urgent recommendation was that greater cooperation and communication was required between the private sector and the government.

Presidential Decision Directives (PDD) 62 and 63

Clinton followed the recommendations of the PCCIP in May 1998 with his Presidential Decision Directives (PDD) 62 and 63.[6] They established policy-making and oversight bodies making use of existing agency authorities and expertise, and addressed operational concerns. PDD 63 set up groups within the federal government to develop and implement plans to protect government-operated infrastructure, and called for a dialog between the government and the private sector to develop a National Infrastructure Assurance Plan.[7]

CIIP Policy

National Plan for Information Systems Protection

On 7 January 2000, Clinton presented the first comprehensive national master plan for CIP as "Defending America's Cyberspace. National Plan

4 The President's Commission on Critical Infrastructure Protection (PCCIP). *Critical Foundations: Protecting America's Infrastructures.* (Washington, D.C., October 1997).

5 President's Commission on Critical Infrastructure Protection, Critical Foundations.

6 http://www.fas.org/irp/offdocs/pdd-62.htm, Clinton, William J. *Protecting America's Critical Infrastructures: Presidential Decision Directive 63.* (May, 22 1998). http://www.fas.org/irp/offdocs/pdd-63.htm.

7 Clinton, Presidential Decision Directive 63.

for Information Systems Protection, Version 1.0".[8] This plan reinforced the perception of cyber-security as a responsibility shared between the government and the private sector.[9] Version 2.0, due out in fall 2002, will be a comprehensive document that examines CIP at the level of federal, state, and local government, as well as the private sector.[10]

Homeland Security

In the aftermath of 11 September 2001, President George Bush signed two Executive Orders (EO) affecting CIP. EO 13228, signed 8 October 2001, established the Office of Homeland Security, headed by the Assistant to the President for Homeland Security.[11] One of its functions is the coordination of efforts to protect the US and its CI from terrorist attacks. The EO further established the Homeland Security Council, which advises and assists the president in all aspects of homeland security.

The second Executive Order (EO 13231), signed 16 October 2001 established the President's Critical Infrastructure Protection Board. The board's responsibility is to "recommend policies and coordinate programs for protecting information systems for critical infrastructure"[12]. Finally, the EO also established the National Infrastructure Advisory Council (NIAC). Its task is to provide advice to the president on the security of information systems. The council's functions include enhancing public-private partnerships, monitoring the development of so-called Information Sharing and Analysis Centers (ISACs), and encouraging the private sector to conduct periodic vulnerability assessments of CII systems.[13]

Information Analysis and Infrastructure Protection

In a recent development since June 2002, one of the four divisions of the planned Department of Homeland Security has been dedicated to "Infor-

8 Clinton, William J. *Defending America's Cyberspace: National Plan for Information Systems Protection. An Invitation to a Dialogue.* Version 1.0 (The White House: Washington, D.C., 2000).

9 Three new institutions work together for the security of the state's computer systems.

10 http://www.ciao.gov and interview with a representative of the US Chamber of Commerce, June 2002.

11 Bush, George W. *Executive Order 13228. Establishing the Office of Homeland Security and the Homeland Security Council.* (Washington, D.C., 8 October 2001). http://www.fas.org/irp/offdocs/eo/eo-13228.htm.

12 Bush, George W. *Executive Order 13231. Critical Infrastructure Protection in the Information Age* (Washington, D.C., 16 October 2001). http://www.ncs.gov/ncs/html/eo-13231.htm.

mation Analysis and Infrastructure Protection". It plans to merge the capability to identify and assess current and future threats to the homeland, map those threats against current vulnerabilities, inform the president, issue timely warnings, and immediately take or effect appropriate preventive and protective action. It would coordinate a national effort to secure the entire CI of the US.[14]

Law and Legislative Action

Defense Production Act of 1950

This act is aimed at management of consequences, rather than prevention, which is associated with the more modern approach to risk management that is necessary for CIP.[15]

Computer Fraud and Abuse Act (CFAA) of 1986

Legislative awareness of computer crimes grew dramatically in the early 1980s, as computers became increasingly important for the conduct of business and politics. The CFAA was the conclusion of several years of research and discussion among legislators.[16] It established two new felony offenses consisting of unauthorized access to "federal interest" computers[17] and unauthorized trafficking in computer passwords. Violations of the CFAA include intrusions into government, financial, most medical, and "federal interest" computers.

Computer Abuse Amendments Act of 1994

This act expanded the 1986 CFAA to address the transmission of viruses and other harmful code.[18] The measures provided by this act were further tightened on 26 October 2001 by the USA PATRIOT anti-terrorism legisla-

13 Bush, Executive Order 13231.
14 http://www.whitehouse.gov/deptofhomeland/sect6.html.
15 President's Commission on Critical Infrastructure Protection, Critical Foundations.
16 http://www4.law.cornell.edu/uscode/18/1001.html.
17 Federal interest computers are defined as two or more computers involved in a criminal offense, if they are located in different states.
18 See also http://www.digitalcentury.com/encyclo/update/comfraud.html Jones Telecommunications and Multimedia Encyclopedia.

tion.[19] Violations of the CFAA are investigated by the National Computer Crimes Squad at the FBI and supported by its Computer Analysis and Response Team (CART), a specialized unit for computer forensics.[20]

Much of the federal legislation concerning CI/CII was written before the emergence of "cyber-threats". Thus, it is questionable whether a timely and efficient response would be possible under the existing legal frameworks at both federal and state/local levels.[21]

Organizational Analysis

Public Agencies

The attacks of 11 September 2001 have given the crucial impulse to change the overall CIIP organizational structure in the US. The most important change will be the establishment of the Department of Homeland Security. It will incorporate 22 existing federal agencies. The department will be divided into four divisions: (1) Border and Transportation Security, (2) Emergency Preparedness and Response, (3) Chemical, Biological Radiological, and Nuclear Countermeasures, and (4) Information Sharing and Analysis Centers. In addition to consolidating the existing functions of various federal agencies and departments, the new department will also create a single "all hazards" emergency response plan and a center to collect, review, and analyze intelligence information submitted by the FBI, the CIA, the NSA, and other intelligence services.[22]

Since the final outcome of this change is not yet entirely clear, the next section includes a selection of public actors that play an important role in CIIP today. Under the Bush plan, the Critical Infrastructure Assurance

19 USA PATRIOT stands for: *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*. For full text version see http://www.cdt.org/security/usapatriot/011026usa-patriot.pdf. Privacy and civil liberty advocacy groups have expressed concern over a number of legislative developments.

20 http://www.fbi.gov/hq/lab/org/cart.htm. Of further importance is also the recent enactment of the Gramm-Leach-Bliley (GLB) Act and the regulations that implement GLB, which address privacy concerns by setting forth a range of requirements to protect customer information. For text of GLB see http://www.ftc.gov/privacy/glbact.

21 President's Commission on Critical Infrastructure Protection, Critical Foundations, 81.

22 Interview with a representative of the US Chamber of Commerce, June 2002.

Office (CIAO) and the National Infrastructure Protection Center (NIPC) will be moved into the Department of Homeland Security. These agencies will maintain their current functions but move their entire operations to the new Department of Homeland Security.

Critical Infrastructure Assurance Office (CIAO)[23]

The Critical Infrastructure Assurance Office (CIAO)[24] was created in May 1998 in response to the Presidential Decision Directive (PDD-63) to coordinate the federal government's initiatives on CIP. The CIAO's main tasks are to

- Coordinate and implement the national strategy,
- Assess the government's own risk exposure and dependencies on CI,
- Raise awareness and public understanding and participation in CIP efforts, and
- Coordinate legislative and public affairs to integrate infrastructure assurance objectives into the public and private sectors.

Federal Computer Incident Response Center (FedCIRC)[25]

The Federal Computer Incident Response Center (FedCIRC) is the central coordination and analysis facility dealing with computer security issues affecting the civilian agencies and departments of the federal government. The FedCIRC's incident response and advisory activities bring together elements of the Department of Defense, law enforcement agencies, the intelligence community, academia, and computer security specialists from federal civilian agencies and departments.[26]

National Infrastructure Protection Center (NIPC)[27]

In 1998, the Office of Computer Investigations and Infrastructure Protection (OCIIP) was expanded to become the inter-agency National Infrastructure Protection Center (NIPC). The NIPC is located at the FBI headquarters. Its mission is to serve as the US government's focal point for threat assessment, warning, investigation, and response for threats or attacks against CI. It facilitates and coordinates the federal government's response to incidents, mitigating attacks, investigating threats, and moni-

23 http://www.ciao.gov.
24 It is currently part of the Department of Commerce.
25 http://www.fedcirc.gov.
26 http://www.fedcirc.gov.
27 http://www.nipc.gov.

toring reconstitution efforts. It is linked electronically to the rest of the federal government, including other warning and operation centers. In addition, private-sector Information Sharing and Analysis Centers (ISAC) have informal relationships with the NIPC. Also, the NIPC offers private sector firms from across all industries a program called INFRAGARD.

Office of Homeland Security

The Office of Homeland Security was established by Executive Order 13228 in October 2001. It is headed by the Assistant to the President for Homeland Security. Its mission is to "develop and coordinate the implementation of a comprehensive national strategy to secure the US from terrorist threats and attacks". Among its functions is the coordination of efforts to ensure rapid restoration of CI after a disruption by a terrorist threat or attack.[28] The Office of Homeland Security will remain an entity of its own within the Executive Office, as the administration sees the need for it to continue coordination among federal agencies.[29]

President's Critical Infrastructure Protection Board

The Board was established by Executive Order 13231 in October 2001. Its responsibility is to recommend policies and to coordinate programs for protecting information systems for CI.[30] The Board is directed to propose a National Plan, and, in coordination with the Office of Homeland Security, to review and make recommendations on that part of agency budgets that fall within the purview of the Board. The Board is to be chaired by a Special Advisor to the President for Cyberspace Security. The special advisor may, in consultation with the Board, propose policies and programs to appropriate officials to ensure the protection of the nation's CII.

The Department of Homeland Security[31]

The new department will concentrate all efforts in a single government agency, responsible for coordinating a comprehensive national plan for protecting the US infrastructure. An especially high priority will be placed on protecting the infrastructure of cyberspace from terrorist attacks by unifying and focusing the key cyber-security activities of the CIAO and the NIPC. The department will augment those capabilities with

28 Bush, Executive Order 13228.
29 Interview with a representative of the US Chamber of Commerce, June 2002.
30 Bush, Executive Order 13231.
31 http://www.whitehouse.gov/deptofhomeland.

the response functions of the Federal Computer Incident Response Center. Because information and telecommunications sectors are increasingly interconnected, the department will also assume the functions and assets of the National Communications System (Department of Defense), which coordinates emergency preparedness for the telecommunications sector.[32]

Cooperation of Public and Private Sectors

The government has very actively sought cooperation between the public and private sectors. As the federal government alone cannot protect CI, the goal is a close private-public partnership.[33] One of the new Department of Homeland Security's main tasks will be to facilitate partnership efforts between the government and private sectors. It will give state, local, and private entities one primary contact point. So far, unresolved legal issues – such as the Freedom of Information Act, as well as antitrust and liability issues – impede the comprehensive sharing of information between the public and private sectors. According to experts, resolving these issues should enhance information-sharing and spur the growth of ISACs.[34]

Information Sharing and Analysis Center (ISAC)

While the PDD 63 envisioned a single center serving the entire private sector, namely the NIPC, each sector is now establishing its own Information Sharing and Analysis Center (ISAC). Private sector ISACs are membership organizations managed by private companies. Each ISAC has a board of directors that determines its institutional and working procedures. The function of an ISAC is to collect and share incident and response information among ISAC members, and to facilitate information exchange between the government and the private sector. The following list gives an overview of important existing ISACs:

- A number of the nation's largest banks, securities firms, insurance companies, and investment companies have joined together in a limited liability corporation to form a Financial Services Information Sharing and Analysis Center (FS/ISAC),[35]

32 http://www.whitehouse.gov/deptofhomeland/sect6.html.

33 President's Commission on Critical Infrastructure Protection, Critical Foundations, 104.

34 Interview with a representative of the US Chamber of Commerce, June 2002.

35 http://www.fsisac.com.

- The telecommunications industry has agreed to establish an ISAC through the National Coordinating Center (NCC). Each member firm of the NCC monitors and analyzes its own networks. Incidents are discussed within the NCCs and members decide whether the suspected behavior is serious enough to report to the appropriate federal authorities,[36]
- The electric power sector has established a decentralized ISAC through its North American Electricity Reliability Council (NERC). Much like the NCC, the NERC already monitors and coordinates responses to disruptions in the nation's supply of electricity,[37]
- The IT ISAC started operations in March 2001. Members include 19 major hardware, software, and e-commerce firms, including AT&T, IBM, Cisco, Microsoft, Intel, and Oracle. The ISAC is overseen by a board made up of members and operated by Internet Security Systems,[38]
- New ISACs include the Surface Transportation ISAC [39] and an Oil and Gas ISAC.[40]

National Cyber Security Alliance (NCSA)

The NCSA fosters awareness of cyber-security through educational outreach. It tries to raise citizens' awareness of the critical role computer security plays in protecting the nation's Internet infrastructure, and to encourage computer users to protect their home and small business systems.[41]

Partnership for Critical Infrastructure Security (PCIS)

The PCIS grew out of initiatives outlined in Presidential Decision Directive-63. It works to secure CI and examines cross-sector issues.[42]

There are some additional efforts in public-private partnerships. For example, the San-Francisco-based Computer Security Institute has been working together with the FBI's Computer Intrusion Squad on conduct-

36 http://www.ncs.gov/ncc.
37 http://www.nerc.com; Energy Information Sharing and Analysis Center, http://www.energyisac.com.
38 https://www.it-isac.org.
39 http://www.surfacetransportationisac.org.
40 http://www.energyisac.com.
41 http://www.staysafeonline.info.
42 http://www.pcis.org.

ing an annual Computer Crime and Security Survey, a widely recognized study of dangers, cases, and countermeasures in IT security.

Early Warning

Federal Bureau of Investigation (FBI)

The 1997 PCCIP Report stated that efforts were required to establish a system of surveillance, assessment, early warning, and response mechanisms.[43] The Clinton administration envisaged an enormous database of every hacking or computer-hijacking incident. By 2003, they hoped to have created a constantly updated tool to forecast, identify, and combat cyber attacks that would be developed and maintained in close cooperation between the private and the public sector. The Federal Bureau of Investigation (FBI) was chosen to serve as the preliminary national warning center for infrastructure attacks and to provide law enforcement, intelligence, and other information needed to ensure the highest quality possible. PDD 63 assigned responsibility for developing analytical capabilities to provide comprehensive information on changes in threat conditions and newly identified system vulnerabilities, as well as timely warnings of potential and actual attacks, to the NIPC at the FBI.[44]

Federal Computer Incident Response Center (FedCIRC)

The responsibility for detecting and responding to cyber-attacks while they are in progress lies with the Federal Computer Incident Response Center (FedCIRC), which gives agencies the tools to detect and respond to such attacks, and coordinates response and detection information.

The Information Sharing and Analysis Centers (ISACs)

The Information Sharing and Analysis Centers (ISACs) were planned to help create the early warning database. The idea is that owners and operators will survey incidents and pass the information on to the NIPC, which serves as the private sector point of contact for information-sharing and coordinates and bundles reports from all different ISACs.

43 President's Commission on Critical Infrastructure Protection, Critical Foundations.
44 Clinton, Presidential Decision Directive 63.

Department of Homeland Security

The planned Department of Homeland Security will have a division focusing on information analysis and infrastructure protection. Set up with a special focus on systematically analyzing all information and intelligence on potential terrorist threats within the US, this division will fuse and analyze legally accessible information from multiple sources to provide early warning of terrorist attacks.[45]

Research and Development

CIIP research and development (R&D) efforts in the US focus on issues such as interdependency analyses, threat, vulnerability and risk assessment studies, system protection and information assurance, reconstitution of damaged or compromised systems, the security of automated infrastructure control systems; and intrusion detection and monitoring.[46] Generally, the private sector funds R&D to develop tools to address infrastructure outages, but the federal government does more fundamental R&D. The Department of Defense, which provides the bulk of information security R&D funding because of its mission needs, is sponsoring research at universities in its University Research Initiatives Centers of Excellence program.[47]

Investigation of the need for and solutions to CIIP R&D since the publication of Version 1.0 of the *National Plan for Information System Protection* is conducted under the auspices of the CIP R&D Inter-Agency Working Group (IWG), which includes a number of subgroups. The information and communications (I&C) sector subgroup deals with CII; it was established to further the development and exchange of information between the federal government and private sector regarding I&C CIP R&D programs.[48]

After 11 September 2001, the Bush administration took steps to develop a capability to coordinate cyber-security activities with the nation's

45 http://www.whitehouse.gov/deptofhomeland/sect6.html.

46 http://www.ciao.gov/CIAO_Document_Library/Report_on_Federal_CIP_R&D.pdf.

47 Kneso, Genevieve J., *CRS (Congressional Research Service) Report for Congress. Federal Research and Development for Counter Terrorism: Organization, Funding and Options.* (November 2001). http://www.ieeeusa.org/forum/PAPERS/CRSterrorismresearch.pdf.

48 http://www.ciao.gov/CIAO_Document_Library/2001Cong/05-CIP_RD.pdf.

counter-terrorism effort and to better link information security R&D to these efforts. The mechanism established parallels with the organization created by the Clinton administration. However, it differs in important ways and, potentially, has more authority, because it is closely linked to both the anti-terrorism effort and to the Office of Science and Technology Policy (OSTP), and has specific authority to work with agencies to develop priority R&D programs and budgets.[49] One of the tasks of the interagency President's Critical Infrastructure Board was to coordinate with the director of the OSTP to develop a federal R&D program to protect information systems for critical infrastructure.

49 For more information see Kneso, Federal Research and Development for Counter Terrorism.

Part II
Selected CII Methods and Models

by Myriam Dunn

Myriam Dunn is researcher at the Center for Security Studies and Conflict Research at the Swiss Federal Institute of Technology (ETH) Zurich.

Introduction

Part II of the handbook introduces different methods and models employed in the surveyed countries to analyze and evaluate various aspects of their critical information infrastructure (CII).* The selection of methods and models is neither systematic nor comprehensive, but is closely linked to the material available.

Part II has two chapters. The first chapter ("National Efforts for CII Analysis") illustrates country-specific approaches to the analysis of CII. The second chapter ("Models for CII Analysis") introduces models that help to analyze diverse aspects of CII in the abstract, detached from a country-specific context. Important concepts, approaches, and terms are included in the "Glossary of Key Terms" in the appendix. Entry in the glossary is marked by an arrow (→).

Table 1 serves as a reading aid for part II. It includes the following information:

- The top part of the table shows all models discussed in the chapter "Models for CII Analysis",
- The bottom part of the table lists selected methods and models frequently used in the surveyed countries, with entry in the glossary,
- The right column lists those surveyed countries ("National Efforts for CII Analysis") that use the respective models and methods.

* Purely IT-security focused models such as the IT Baseline Protection Manual developed by the German Bundesamt für Sicherheit in der Informationstechnik (http://www.bsi.bund.de/gshb/english/menue.htm) have been omitted. We also were unable to get information on concrete approaches used in Sweden.

Models for CII Analysis		National Efforts for CII Analysis	
Technical IT-Security Models,	p 146–147		
Risk Analysis Methodology,	p 148–151		
Infrastructure Risk Analysis Model (IRAM),	p 152–154		
Leontief-Based Model of Risks ,	p 155–157		
Sector Model,	p 158–159	Switzerland,	p 134–136
Layer Model,	p 158–159	Canada, Netherlands, United States,	p 121–126 p 127–130 p 137–141
Sector Analysis,	p 160–162	Australia, The Netherlands,	p 118–120 p 127–130
Process and Technology Analysis,	p 163–164	Switzerland,	p 134–136
Dimensional Interdependency Analysis,	p 165–166		
Causal Mapping			
Cluster Analysis			
Dependency/Interdependency Matrix		Canada,	p 121–126
Event Tree Analysis			
Expert Assessment/Interviews			
Fault Tree Analysis			
Hierarchical Holographic Modeling			
Infrastructure Profiles		Canada,	p 121–126
Interdependency/Vulnerability Matrix		Australia, Canada,	p 118–120 p 121–126
Multi-Criteria Decision Approach		Norway,	p 131–133
Multi-Objective Trade-off Analysis			
Partitioned Multi-objective Risk Method (PMRM)			
Scenario Technique			
Seminar Games			
Vulnerability Assessment Process		Australia, United States,	p 118–120 p 137–141
Vulnerability Rating Table		Australia,	p 118–120
Vulnerability Profile Chart		Australia,	p 118–120

Table 1: Overview Part II

National Efforts for CII Analysis

Introduction

This chapter introduces country-specific efforts to analyze and evaluate various aspects of CII. This not only serves as a country guide but also provides examples for various methodological elements mentioned throughout the book.

Table 2 shows specific approaches developed in the surveyed countries and the examples they provide for methodological elements.

Country	Approach	Examples for
Australia	• PreDICT (Predict Defence Infrastructure Core Requirements Tool)	• Interdependency/Vulnerability Matrix • Sector Analysis • Vulnerability Assessment Process • Vulnerability Profile Chart • Vulnerability Rating Table
Canada	• National Contingency Planning Group Model • Infrastructure Protection Process	• Dependency/Interdependency Matrix • Infrastructure Profiles • Layer Model • Risk Rating Matrix • Risk/Impact Scattergram
The Netherlands	• BITBREUK Model • KWINT Report Model	• Layer Model • Sector Analysis • Vulnerability Analysis
Norway	• Multi-Criteria Model of the "Protection of Society" Projects (BAS)	• Multi-Criteria Decision Approach • Vulnerability Analysis
Switzerland	• InfoSurance Sector Model and CIIP Framework	• Process and Technology Analysis • Sector Model
United States	• Department of Energy (DoE) Layer Model • CIAO Vulnerability Assessment Process/ Project Matrix	• Layer Model • Vulnerability Assessment Process

Table 2: Outline of Approaches Used in Surveyed Countries

Australia

A number of studies have been conducted in Australia on threats to, and vulnerabilities of, CII. Among the official methodologies in use is the risk assessment methodology as introduced in the *Australian Communications-Electronic Security Instruction – Protective Security Manual (PSM)*.[1] Another important publication suggests a hierarchy of threats facing Australia's CI in descending order of probability of serious damage.[2] An official governmental assessment of 1998 (*Protecting Australia's National Information Infrastructure*) also suggests measures to protect Australia's information infrastructures.[3] The most comprehensive report to date, however, is an effort by the Australian National Support Staff and KPMG to study Australia's most important infrastructure sectors, with special relevance to defense. The methodology employed is presented in more detail below.

Predict Defence Infrastructure Core Requirements Tool (PreDICT)

In 1998, government officials decided to analyze the Australian national defense-related infrastructure in order to develop strategies to remove, ameliorate, or avoid identified vulnerabilities. A multi-step →*Vulnerability Assessment* Process was developed for the project.[4] In a first phase, the study identified vulnerabilities in fifteen infrastructure sectors and highlighted their interdependence. A second phase of the project identified preliminary strategies aimed at removing the vulnerabilities, with a special focus on defense needs.

1 Commonwealth of Australia, Information Security Group. *Australian Communications-Electronic Security Instruction 33 (ACSI 33)*. http://www.dsd.gov.au/infosec/acsi33/HB3.html.

2 Cobb, Adam. *Thinking about the Unthinkable: Australian Vulnerabilities to High-Tech Risks*. Foreign Affairs, Defence and Trade Group, Research Paper 18. (29 June 1998).

3 Attorney-General's Department. *Protecting Australia's National Information Infrastructure. Report of the Interdepartmental Committee on Protection of the National Information Infrastructure*. (Canberra, December 1998). http://www.law.gov.au/publications/niireport/niirpt.pdf, 13.

4 See KPMG / National Support Staff. Predict Defence Infrastructure Core Requirements Tool (PreDICT). http://www.defence.gov.au/predict/general/predict_fs.htm.

One key output of the process was the web-based decision support tool entitled *PreDICT (Predict Defence Infrastructure Core Requirements Tool*), which presents the data gathered during the project, and makes it available to defense planners and other interested parties. PreDICT is a tool that records the background, vulnerability, and interdependencies of ten national critical infrastructure sectors of relevance to defense.[5]

Methodology: Interdependency and Vulnerabilities Charts

Sector interdependencies in all sectors were discussed and rated by experts (both industry and defense representatives). The interdependencies were charted over the three time periods of 1999, 2005, and 2020, with additional summary pages detailing the nature of the interdependency and reasoning behind each rating (Figure 1 is an example of an interdependency chart).

Next, industry vulnerability profiles for each of the ten sectors were developed, based on industry analysis and interviews, with a focus on the critical interdependencies that exist between them. The vulnerabili-

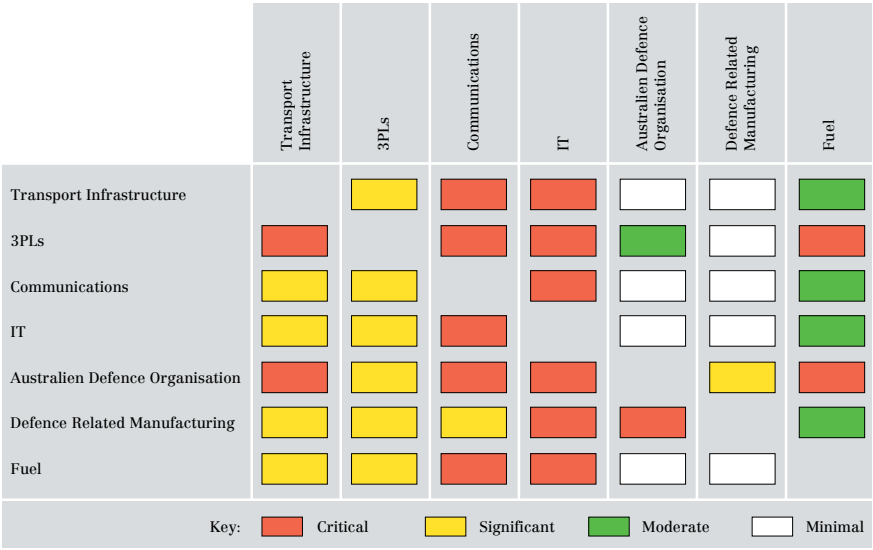

Figure 1: Interdependency Chart (Source: PreDICT)

5 The ten sectors are Transport, Fuel, IT, Utilities, Health, 3PL Providers, Education and Training, Communications, Defense-Related Manufacturing, and Financial Services.

ties were grouped into twelve "Broad Risk Areas" in order to compare and contrast vulnerabilities between industry sectors and defense and to group the vulnerabilities identified into common areas for analysis. The majority of the Broad Risk Area titles were drawn from →*Sector Analysis* (PEST, Porter's analysis, and SWOT analysis).[6]

The magnitude of each vulnerability was rated first by quantifying its consequence by degree (→*Categories*: "insignificant", "minor", "moderate", "major", "catastrophic"), and then by determining the likelihood of its occurrence. The vulnerability rankings for each Broad Risk Area were calculated using a →*Vulnerability Rating Table* and were visually represented on a →*Vulnerability Profile Chart*. (Figure 2)

Vulnerabilities with the highest rating by sector using this method were prioritized for the development of mitigation strategies.[7]

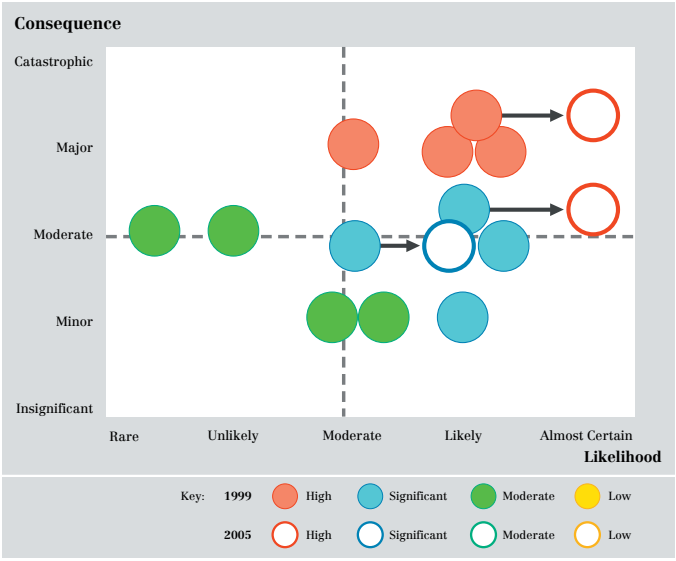

Figure 2: Vulnerability Profile for the Technology Sector (Source: PreDICT)

6 The twelve "Broad Risk Areas" are: Political, Economic, Social/Environmental/Cultural, Technological, Supplier, Customer, Substitutes, Competitor, Barriers to Entry, Operations – HR, Operations – Training, and Flexibility/Adaptability.

7 KPMG / National Support Staff. Predict Defence Infrastructure Core Requirements Tool: Methodology. http://www.defence.gov.au/predict/general/methodology_fs.htm.

Canada

In Canada, the key efforts to analyze the nation's CII are: The National Contingency Planning Group's (NCPG) assembly of an overall picture of infrastructure elements, which resulted in the book "*Canadian Infrastructures and their Dependencies*", and the comprehensive *Infrastructure Protection Process*, with a strong focus on interdependencies, developed by the Critical Infrastructure Protection Task Force (CIPTF).

The National Contingency Planning Group (NCPG) Model

When the National Contingency Planning Group (NCPG) was formed in October 1998, part of its mandate was the production of a National Infrastructure Risk Assessment (NIRA). The NIRA's objective was to better position the country for the transition to the year 2000 by finding out which infrastructures were most at risk. It set out to examine important Canadian infrastructure elements, determine their criticality, and assess the probability of their failure.[8] To determine the criticality, two criteria were used:

- The possible impact on four tenets (direct impact on individual Canadians);
  - No loss of life,
  - Basic community needs are met,
  - Business continues as usual,
  - Confidence in government is maintained.
- The degree of dependency (direct impact on Canadian government, industry, and business).[9]

Thirty-six infrastructure elements were agreed upon, ranging from physical systems (such as electricity, telecommunications, or airports) to services (such as health or finances). An expert panel was assembled

8 Charters, David. *The Future of Canada's Security and Defence Policy: Critical Infrastructure Protection and DND Policy and Strategy.* Research Paper of the Council for Canadian Security in the 21st Century. http://www.ccs21.org/ccspapers/papers/charters-CSDP.htm.

9 National Contingency Planning Group. *Canadian Infrastructures and their Dependencies.* (March 2000), preface.

to rank the criticality of the infrastructure elements against each of the criteria.[10]

A group formed under the auspices of the NCPG, called the Infrastructure Analysis Group (IAG),[11] subsequently produced a number of →*Infrastructure Profiles (IPs)*. Fifteen are collected in a compendium entitled "Canadian Infrastructure and Their Dependencies". The profiles include a description of the infrastructure, statistics, maps, contacts, references, and jurisdictions, as well as a detailed analysis of the interdependencies.

Infrastructure Protection Process

In spring 2000, the NCPG was converted into the Critical Infrastructure Protection Task Force (CIPTF). The Task Force, which was established within the Department of National Defence, developed an extensive process to review critical infrastructures in Canada (Figure 3).

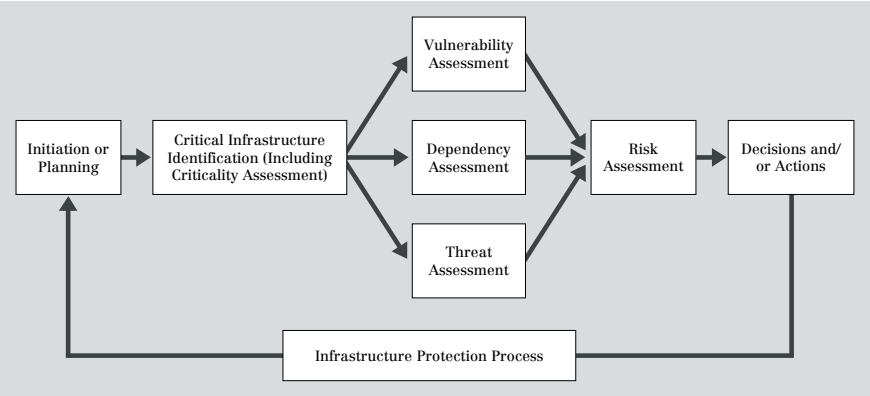

Figure 3: Canadian Infrastructure Protection Process (Source: Presentation by J. Grenier)

10 National Contingency Planning Group. Canadian Infrastructures and their Dependencies.

11 The IAG's mandate was to predict potential impacts on the Canadian infrastructure and critical government functions resulting from any year 2000 failures.

One of the main aims of this process was to understand and picture interdependencies.[12] Important steps within this approach are discussed below.

Canadian Layer Model

Based on six sectors identified as crucial,[13] the CIPTF developed a multi-dimensional →*Layer Model* that takes into consideration the responsibilities of five sectors: the international, federal, provincial, municipal, and the private level. Each of these areas of responsibility consists of three vertical sector-specific layers (operations layer, technical application layer, and control layer), which in turn rest on two "Common foundation layers":

- A "Terrain layer" that considers components such as vegetation, hydrography, geology, etc.,
- A "Feature layer" that considers components such as cities, buildings, roads, tunnels, airports, harbors, etc.

Figure 4 shows the layer model at an initial phase. At this step, only the specific layer of the international sector has been added onto the common foundation layers. With each additional step, the federal, provincial, municipal, and private-sector layers are added.

The CIPTF used this model to draw up a detailed dependency analysis based on input from approximately sixty experts (Figure 5). It became obvious that there was an immense number of interdependencies, which could not be plotted concisely this way.

12 Canada has not officially moved forward with this model and so far, there is no final model in Canada: see speech by Jacques Grenier: "The Challenge of CIP Interdependencies." *Conference on the Future of European Crisis Management.* (Uppsala, Sweden, 19–21 March 2001). http://www.ntia.doc.gov/osmhome/cip/workshop/ciptf_files/frame.htm.

13 These six sectors are: Governments, Energy and Utilities; Services; Transportation; Safety; Communications.

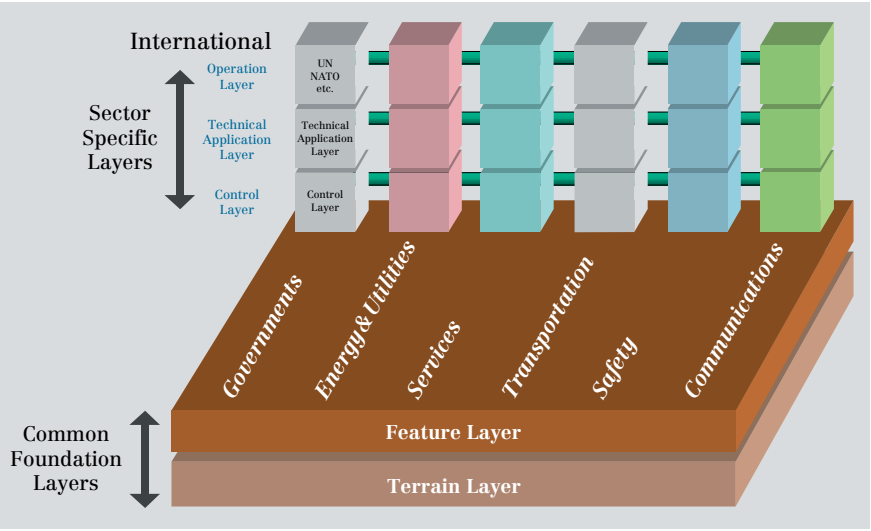

Figure 4: Canadian Critical Infrastructure Model (Source: Presentation by J. Grenier)

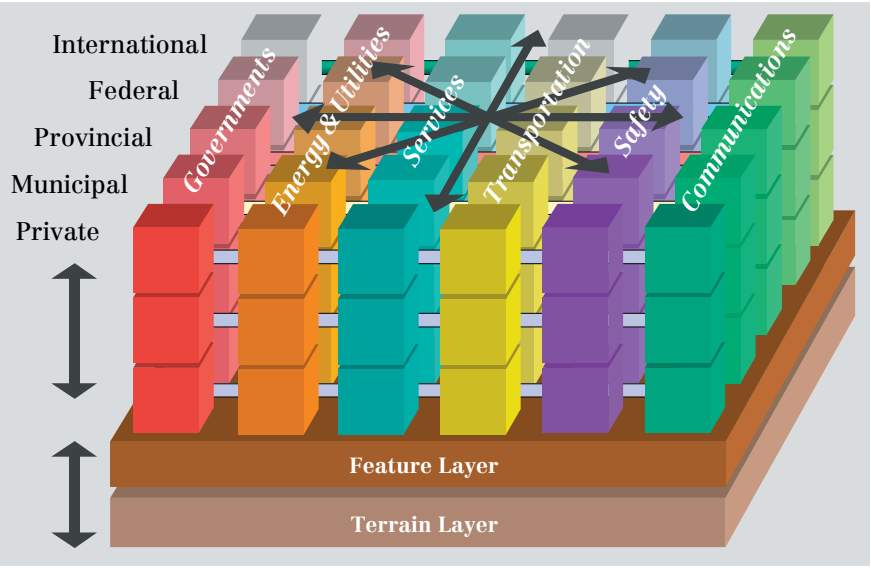

Figure 5: Canadian Critical Infrastructure Model: Dependencies (Source: Presentation by J. Grenier)

Sector	Element	Energy & Utilities					Services		
		Electrical Power	Water Purification	Sewage Treatment	Natural Gas	Oil Industry	Customs and Immigration	Hospital & Health Care Services	Food Industry
Energy & Utilities	Electrical Power		L			M			
	Water Purification	H				M			
	Sewage Treatment	M	H			H			
	Natural Gas	L				L			
	Oil Industry	H	L						
Services	Customs & Immigration	H	L	L	L	L		L	
	Hospital & Health Care Services	H	H	L	H	H	M		H
	Food Industry	H	H	H	L	M	M	L	
		Key:	H	High	M	Medium	L	Low	

Figure 6: Portion of the Indefinite Matrix (Source: Presentation by J. Grenier)

To better show and evaluate the level of interdependency between the different infrastructure elements, a →*Dependency Matrix* was developed (Figure 6). The extent of direct dependency between infrastructure elements is assigned the →*Values* "high", "medium", "low", and "none".

An application called *Relational Analysis For Linked Systems (RAFLS)* was developed to measure and model the ripple effects of these direct dependencies.[14]

Further Steps in the Infrastructure Protection Process

The Canadian Infrastructure Protection Process further evaluates threats and vulnerabilities in the physical dimension as well as in cyberspace for each component of an infrastructure element in all layers of the model. Risks can then be determined based on a →*Risk Rating Matrix* that multiplies threat values with vulnerability values. This method allows for a comparison of relative risks between components of an infrastructure

14 RAFLS, which is based on an algorithm, uses scored interdependencies and iteratively determines the dependencies and impacts. It shows high and medium dependencies and can demonstrate second-, third-, fourth-, and fifth-level dependencies. It can help to trace linkages and potentially interdict a path in time of crisis. (See Grenier, The Challenge of CIP Interdependencies).

element, between layers in the infrastructure model, and between infrastructure elements, which are called specific risks.

It is noted that risks accumulate when the risks of dependencies are propagated. Therefore, the Canadian process conducts a →*Cumulative Risk Assessment* through dependencies. The assessment of impacts then can be done with the use of a →*Risk/Impact Scattergram*, which ultimately helps to propose a framework for future action in terms of protection.[15]

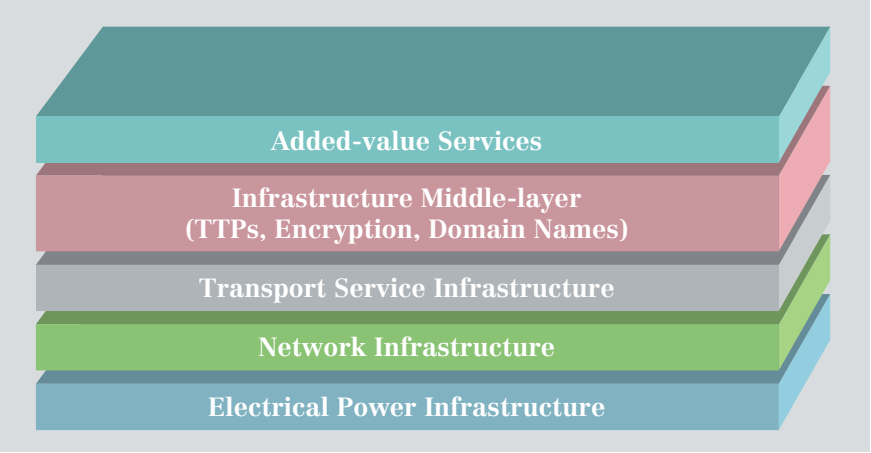

Figure 7: Bitbreuk Layer Model (Source: BITBREUK-Report)

15 Grenier, The Challenge of CIP Interdependencies, slide 25.

The Netherlands

In the Netherlands, the key studies on interdependency are *BITBREUK* ("In Bits and Pieces") by Infodrome[16] and a report on the vulnerability of the Internet by Stratix Consulting Group/TNO FEL. In both studies, qualitative models are described.[17]

BITBREUK Model

The model proposed by the BITBREUK report, which focuses on the Information and Communication Technologies (ICT) infrastructure, is a →*Layer Model* with vertically stacked elements of CII with focus on the IT sector (Figure 7).

Electrical power supply is considered the single factor underlying all ICT. Above this first layer are four more layers. The infrastructure middle layer is located on the fourth level. This layer provides added-value services such as domain name registration or Internet servers between different underlying national and international infrastructures. This middle layer is the basis for the provision of more advanced chains of services for government and the public and commercial organizations. These added-value services are dependent on the availability and integrity of the underlying infrastructure layers. This indicates vertical dependence on the one hand, and, on the other hand, also involves horizontal information flows and information service chains between the different public and private actors, individuals, and society as a whole.[18]

16 Luiijf, Eric., M. Klaver. *In Bits and Pieces: Vulnerability of the Netherlands ICT-Infrastructure and Consequences for the Information Society.* (Translation of he Dutch Infodrome essay "BITBREUK", de kwetsbaarheid van de ICT-infrastructuur en de gevolgen voor de informatiemaatschappij). (Amsterdam, March 2000).

17 Luiijf, Eric., M. Klaver, J. Huizenga. *The Vulnerable Internet: A Study of the Critical Infrastructure of (the Netherlands Section of) the Internet.* (The Hague, 2001). http://www.tno.nl/instit/fel/refs/pub2001/kwint_paper1048.pdf. (KWINT Paper).

18 Luiijf, Klaver, In Bits and Pieces, 8–10 and Luiijf, Eric. "Critical Info-Infrastructure Protection in the Netherlands". *ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead.* (Zurich, 8–10 November 2001). http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/luiijf/sld001.htm.

KWINT-Report by Stratix Consulting Group / TNO FEL

The aim of the study was to analyze the current vulnerabilities of the Dutch section of the Internet,[19] to identify possible consequences of threats, and to determine appropriate measures to reduce the vulnerabilities.[20]

The Four Models of the KWINT-Report

In order to address and clarify the roles of various actors, as well as the diversity, interdependencies, and vulnerabilities, four models with different orthogonal points of view were proposed (Figure 8).

- The social level model was used to discuss the motives and economics behind developments in the Internet,
- The functional level model was used as an intermediate between the functions experienced by the user of ICT and the more abstract and technical processes that form the basis for the functioning of the Internet (Figure 9).
- The structural level model was used to investigate the market environment of service providers and of product suppliers,
- The physical level model takes into account that the physical location of the operational facilities is of importance when analyzing vulnerabilities.[21]

Vulnerability Analysis

The vulnerability analysis was conducted for each of the four layers in Figure 8 and for two additional layers (interaction layer for infrastructures; physical environment). For each of the six layers, the weaknesses, the threat probability, and the possible impact were evaluated using three →*Values (*"high", "medium", and "low"). The vulnerabilities were investigated with respect to four →*IT-Security Objectives*, and with respect to natural causes, deliberate attacks by insiders, and deliberate attacks by outsiders.

19 'Internet' was defined end-to-end in this study, to include workstations, private and public IP networks, and information systems on servers.

20 Luiijf, Klaver, Huizenga, The Vulnerable Internet.

21 Luiijf, Klaver, Huizenga, The Vulnerable Internet, 3–5.

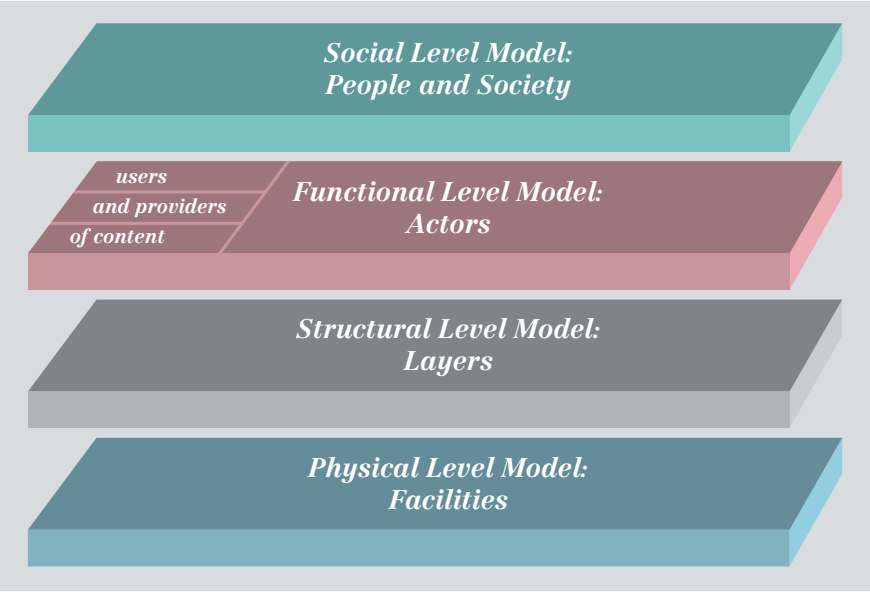

Figure 8: Four Levels of Models (Source: KWINT-Report)

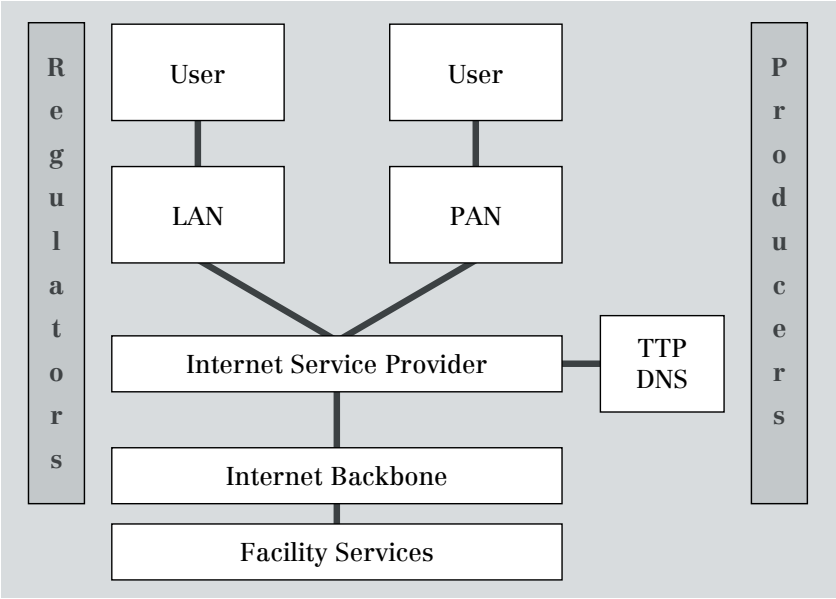

Figure 9: Functional Model with Types of Actors (Source: KWINT-Report)

This resulted in six tables that were aggregated and condensed. The final outcome is a table showing the most important vulnerabilities of the (Netherlands' section of the) Internet (Figure 10). In this table, the impact of selected vulnerabilities on citizens, enterprises, the nation, and society were assessed, as were vulnerabilities with global impact (geographical impact area). These results were used to devise a number of measures that were subsequently proposed to the Dutch government.

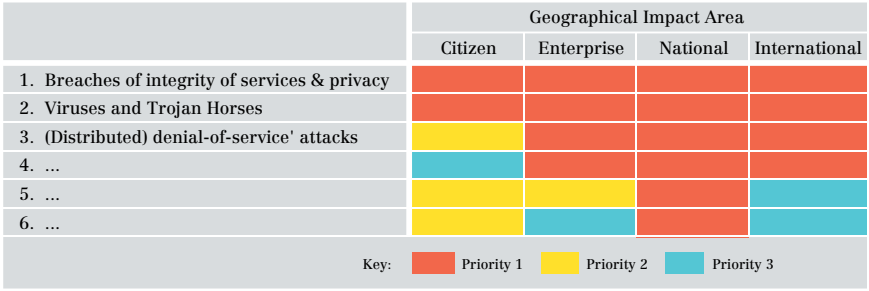

Figure 10: Geographical Impact Area Matrix (Source: KWINT-Report)

Norway

According to Norwegian experts, the BAS matrix is the only available model for analysis of Norwegian CII. However, the need to return to research agendas is well known in Norway and additional efforts can be expected.[22]

Multi-Criteria Model of the "Protection of Society" Projects (BAS)

"Protection of Society" (BAS) is a joint project between the Directorate for Civil Defense and Emergency Planning (DSB) and the Norwegian Defense Research Establishment (FFI). The project uses a methodology for cost-benefit/ cost-effectiveness analysis to design and evaluate civil emergency measures.

The same methodology was applied in the project "Protection of Society 2" (BAS2).[23] The purpose of the BAS2 project was to study vulnerabilities in the telecommunication system and to suggest cost-effective measures to reduce these vulnerabilities. The analysis proceeded in four interlinked steps (Figure 11).

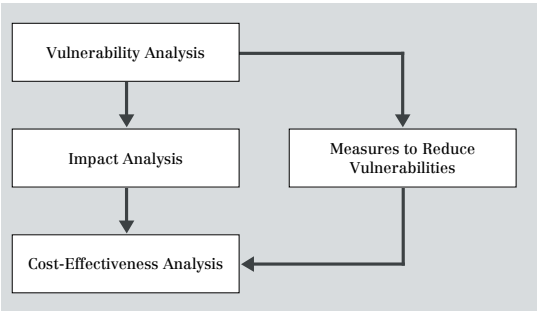

Figure 11: Steps of the Norwegian Vulnerability Analysis (Source: Hagen, Fridheim)

22 Interview with representative of the Norwegian Commission on the Vulnerability of Society.

23 Hagen, Janne Merete, Håvard Fridheim. *Cost-Effectiveness Analysis of Measures to Reduce Vulnerabilities in the Public Telecommunication System*. Paper presented at the 16 ISMOR, The Royal Military College of Science, Norwegian Defense Research Establishment. (United Kingdom, 1-3 September, 1999). http://www.isn.ethz.ch/crn/extended/workshop_zh/Norway_Tel.pdf.

At first, a →*Vulnerability Analysis* was conducted. By using →*Seminar Games*, BAS2 mapped the dependency of modern society upon telecommunication services in crisis and war-like situations. Secondly, an impact analysis was conducted. Next, measures that might reduce the vulnerabilities were evaluated. Lastly, the actual cost-effectiveness analysis was undertaken.

Because no single method was able to handle all the problems BAS2 had to analyze, a combination of several techniques and methods was employed to calculate the most cost-effective protection strategy for the telecommunication system. These other approaches include seminar games; use of →*Scenarios*, →*Causal Mapping*, →*Fault Tree Analysis*, and Probabilistic Cost Estimation, as well as a →*Multi-Criteria Model*.

The Multi-Criteria Model

Calculating the effectiveness of measures to reduce the vulnerabilities proved to be a challenge. Rather than applying mathematical simulation models, the BAS2 study used the →*Multi-Criteria Decision Approach*. This approach systematically maps out subjective expert evaluations and combines them into a quantitative measure of effectiveness.

The multi-criteria approach involves structuring the problem in a multi-criteria hierarchy, where measures are linked to a top-level goal through several levels of decision criteria. The multi-criteria model used in BAS2 is a hierarchy with two interlinked parts. The top part of the hierarchy describes the "societal sub-system" of the analysis, while the lower part of the hierarchy describes the "technical sub-system". The two sub-systems are connected to each other, so that the top criteria in the technical sub-system are identical to the bottom criteria in the societal sub-system. (Figure 12).

The ultimate goal is to maximize the protection of society. This goal can be distilled into three sub-criteria, which are:

- to minimize loss of life,
- to minimize economic losses, and
- to minimize the danger of a loss of sovereignty.

These criteria can be further divided into more specialized criteria. Figure 13 shows parts of the social hierarchy. The relationships between the criteria on different levels are then quantified by experts. The experts weigh the different criteria in the model relative to each other. These preferences serve as a measure of the effectiveness of one criterion compared to the others on the same level.

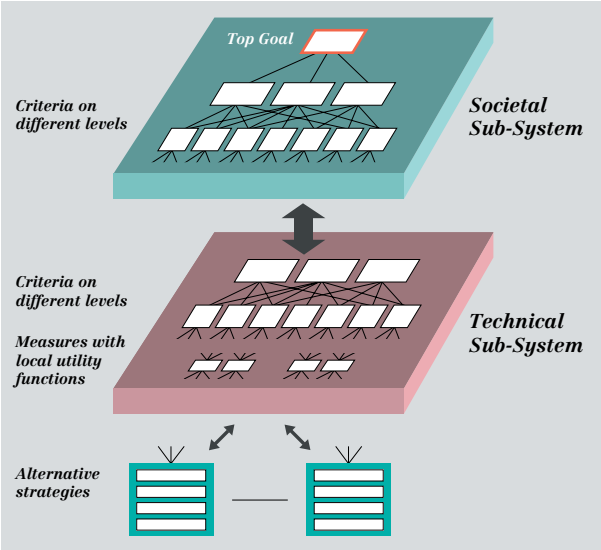

Figure 12: Multi-criteria Hierarchy (Source: Hagen, Fridheim)

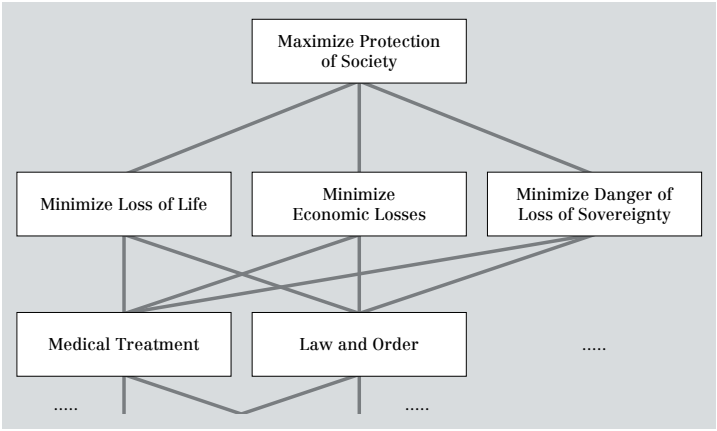

Figure 13: Parts of the Social Hierarchy for the Multi-Criteria Analysis (Source: Hagen, Fridheim)

Switzerland

Although Switzerland's authorities recognize the increasing vulnerability of Swiss CII, appropriate measures for gathering, structuring, and managing the emerging risks are yet to be accomplished. There are few attempts to model the dependencies of critical infrastructures on the information infrastructure, or on the interdependencies between CII. Existing models are predominantly qualitative. One model is described: The InfoSurance Sector Model. Overall, there is a great need to return to the research agenda.

InfoSurance Sector Model and CIIP Framework

Representatives of the InfoSurance foundation defined fourteen infrastructure sectors as being critical to Switzerland, and explored possible interdependencies between these sectors. The resulting picture shows the crucial sectors on a circle and the expected one-way or two-way interdependencies between them. At the center of the model are the two main recipients of the services provided by these critical sectors: enterprises and the individual inhabitants of Switzerland (Figure 14).

The InfoSurance →*Sector Model* is only the starting point for a more comprehensive CIIP framework that encompasses seven methodological elements (Figure 15).[24] The combined analysis in a step-by-step procedure provides a rough picture of interdependencies between CII sectors, impacts, threat patterns, and risk management procedures. To a large extent, this model is still theoretical.

- Element 1: *Sector Model:* Switzerland is defined as a complex of fourteen interdependent sectors.
- Element 2: →*Process and Technology Analysis:* This element identifies the interdependencies within a single sector by assessing different layers of a sector. Figure 16 shows a process and technology analysis for the telecommunications sector.
- Element 3: *Dependability Analysis:* The next element identifies the interdependencies between two and more sectors, using the results of the →*Process and Technological Analysis*. The degree of depen-

24 InfoSurance, Ernst Basler + Partner AG. *Einflussfaktoren und Abhängigkeiten im Umgang und Einsatz von Informationssicherheit* (Zollikon, 2000). http://www.infosurance.ch/de/ppt/Krisenverstaendnis.ppt.

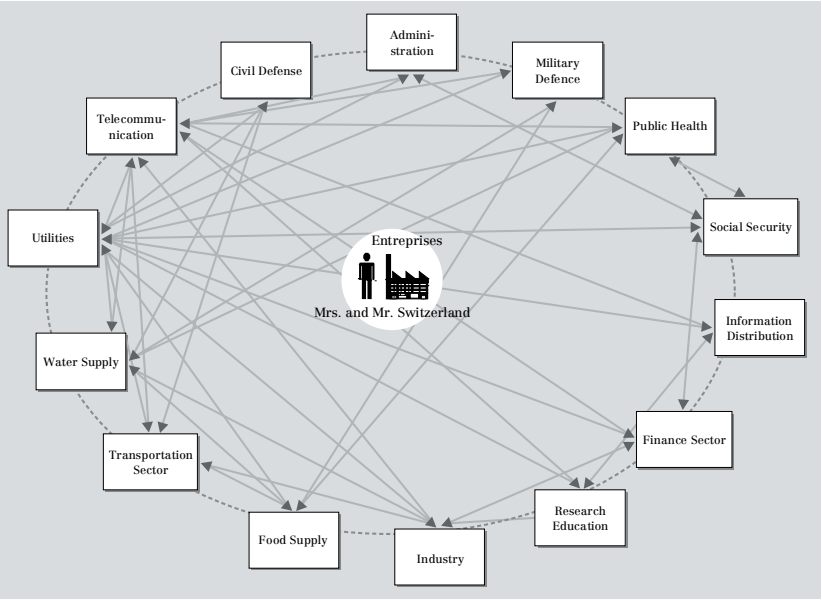

Figure 14: InfoSurance Sector Model (Source: InfoSurance/ Ernst Basler + Partner AG)

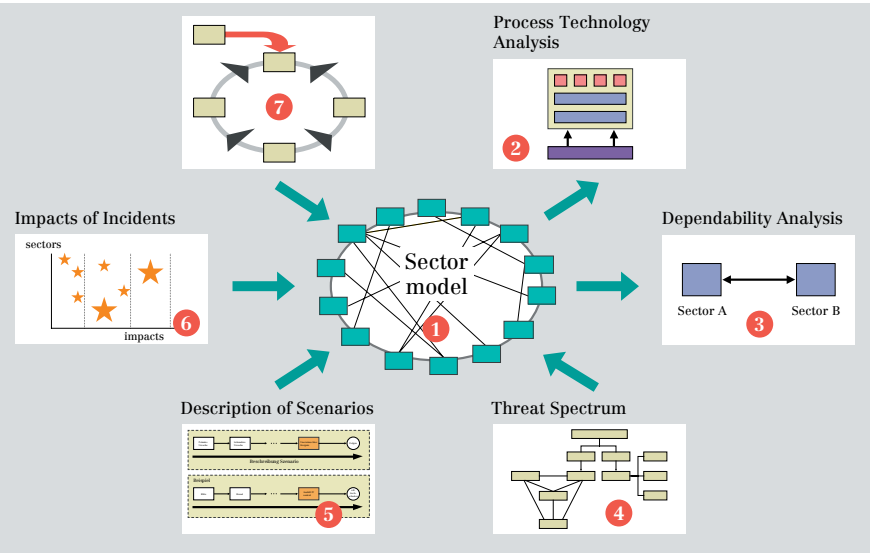

Figure 15: The CIIP Framework Switzerland (Source: InfoSurance/ Ernst Basler + Partner AG)

dency may be determined by identifying the nodes and linkages between sectors.

- Element 4: *Spectrum of Possible Threats:* This element structures the threat spectrum, and also includes an analysis of possible actors and their motives.
- Element 5: *Description of Scenarios:* Possible scenarios are described using →*Scenario Technique* or scenario software.
- Element 6: *Impacts of a Single Event:* A risk analysis approach identifies the impact of incidents within critical infrastructure sectors.
- Element 7: *Risk Management Process:* The risk management process helps to analyze and assess risks and is useful in the planning, implementation, and control of measures.

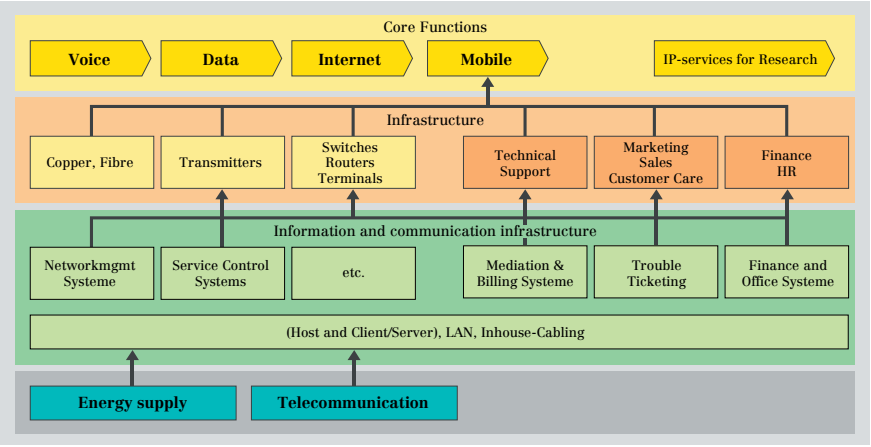

Figure 16: Process and Technology Analysis for the Telecommunication (Source: InfoSurance/ Ernst Basler + Partner AG)

United States

Even though many official US papers discuss the concept and importance of interdependencies,[25] none of them provides a methodological guideline for analyzing this phenomenon. However, over the years, the US has consistently focused on interdependency research. For example, efforts are underway to model and simulate complex interdependencies. One modeling approach, currently developed at the Sandia National Laboratories, utilizes an agent-based methodology to predict interactions among critical infrastructure elements.[26] Also, a comprehensive toolset for interdependence analysis is being developed by the Department of Energy (DoE), which is very active due to the extensive experience its Argonne National Laboratory has accumulated in the field. Below, a →*Layer Model* as developed by the DoE is presented together with the →*Vulnerability Assessment* Process designed by the Critical Infrastructure Assurance Office (CIAO).

The Department of Energy (DoE) Layer Model

The Department of Energy (DoE) uses a →*Layer Model* for the energy sector that shows interdependencies with other sectors and sector components (Figure 17).

Each sector is pictured as a grid on which the individual critical system components are located. Each component must be mapped in detail. The aim is to define critical system components and attendant vulnerabilities, interdependence propagation pathways and the degree of coupling, spatial and temporal system behavior, and the evaluation of protection, mitigation, response, and recovery options.[27]

In addition, a comprehensive toolset for interdependence analysis is being developed by the DoE. It is composed of early alert screening tools, interdependency simulation tools, and a broad range of supporting analytic tools. Its aim is to model the interaction among system components and analyze how disruptions to one infrastructure can affect or propa-

25 Cf. The President's Commission on Critical Infrastructure Protection (PCCIP). *Critical Foundations: Protecting America's Infrastructures.* (Washington, D.C., October 1997).

26 See http://www.sandia.gov/Surety/Facts/Modeling.htm.

27 Scalingi, Paula. *Critical Infrastructure Protection Activities. Department of Energy.* (March 2001). http://www.naseo.org/events/outlook/2001/presentations/scalingi.pdf.

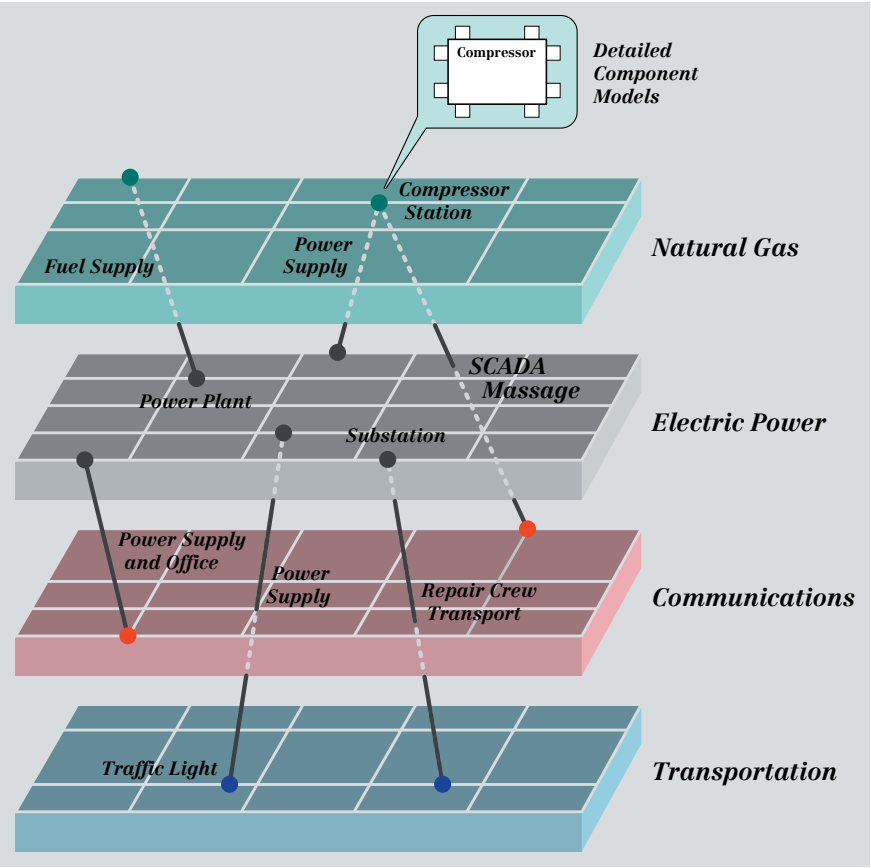

Figure 17: DoE Layer Model (Source: Buehring, Argonne National Laboratory) [28]

gate to other infrastructures. These tools also help to examine protection, mitigation, response, and recovery strategies.[29] The DoE has also developed a three-step →*Vulnerability Assessment* Process.[30]

28 Buehring, Bill. *Natural Gas Security Issues Related to Electric Power Systems*. (28 November 2001). http://wpweb2k.gsia.cmu.edu/ceic/presentations/Buehring.pdf, slide 19.
29 Buehring, Natural Gas Security Issues Related to Electric Power Systems.
30 Scalingi, Critical Infrastructure Protection Activities.

CIAO Vulnerability Assessment Process/Project Matrix

On the basis of Presidential Decision Directive (PDD) 63 and the National Plan 1.0, CIAO developed "Project Matrix™", a program designed to identify and characterize the assets and associated infrastructure dependencies and interdependencies that the US government requires to fulfill its most critical responsibilities to the nation. Project Matrix™ involves a three-step process in which each civilian federal department and agency identifies (1) its critical assets; (2) other federal government assets, systems, and networks on which those critical assets depend to operate; and (3) all associated dependencies on privately owned and operated critical infrastructure elements.[31] The exact methodology is confidential, but the similar approach of the "Vulnerability Assessment Framework" (VAF) developed for CIAO is publicly available.[32] The methodology consists of three main steps, as shown in Figure 18.

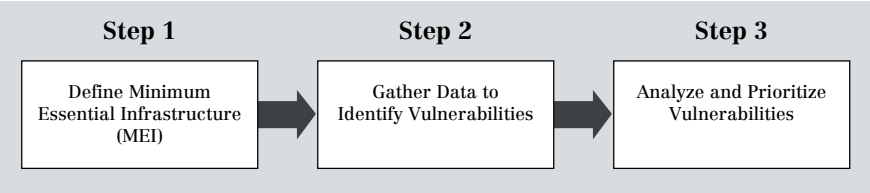

Figure 18: Steps of the VAF Evaluation Process (Source: KPMG/ Marwick)

Step 1: Define Minimum Essential Infrastructure (MEI)

In step 1, the assessment team will define the so-called "Minimum Essential Infrastructure" (MEI) for the organization, with focus on the specific infrastructure components that support essential processes. It is recommended that this first step consist of a broad, department- or agency-level macro vulnerability assessment of both the internal agency MEI and the agency's relationship to, and connection with, the national MEI.

31 Critical Infrastructure Assurance Office, Project Matrix: http://www.ciao.gov/federal/.

32 KPMG, Peat Marwick. *Vulnerability Assessment Framework 1.1. Prepared under contract for the Critical Infrastructure Assurance Office*. (October 1998). http://www.ciao.gov/resource/vulassessframework.pdf. The VAF methodology has drawn heavily on other processes for measuring information technology (IT) system controls, such as: the Control Objectives for Information Technology (COBIT) process of the Information Systems Audit and Control Foundation (ISACF); the May 1998 publication "Executive Guide Information Security Management" of the US General Accounting Office (GAO); and the GAO's standards for auditing federal information systems (Federal Information Systems Control Audit Manual (FISCAM)).

Step 2: Gather Data to Identify Vulnerabilities

The objective of step 2 is to identify the vulnerabilities in the organization related specifically to the MEI. The outcome will be the identification and reporting of flaws or omissions in controls that may affect the integrity, confidentiality, accountability, and/or availability of resources that are essential for achieving the organization's core mission(s). The criteria used to identify these vulnerabilities are depicted in Figure 19, showing the so-called "VAF Cube".

Step 3: Analyze and Prioritize Vulnerabilities

In step 3, vulnerabilities identified in step 2 are defined and analyzed. This allows a first order of prioritization for purposes of remediation or minimization. Figure 20 shows the activities conducted under step 3.
Step 3 includes four sub-steps: (1) Each vulnerability is examined to determine if it has an impact on more than one MEI core process; (2) vulnerabilities are sorted by core process; (3) a graphical summary of

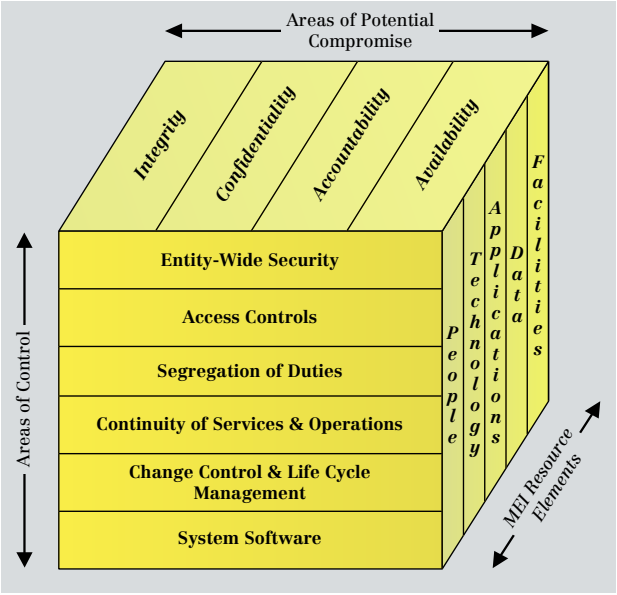

Figure 19: The VAF Cube (Source: KPMG/ Marwick)

the number of vulnerabilities by core process is generated; (4) an analysis of the likelihood that a vulnerability will be exploited is conducted, taking into consideration the potential threats to the agency. Using these four parameters, priorities are assigned for vulnerability remediation or minimization.

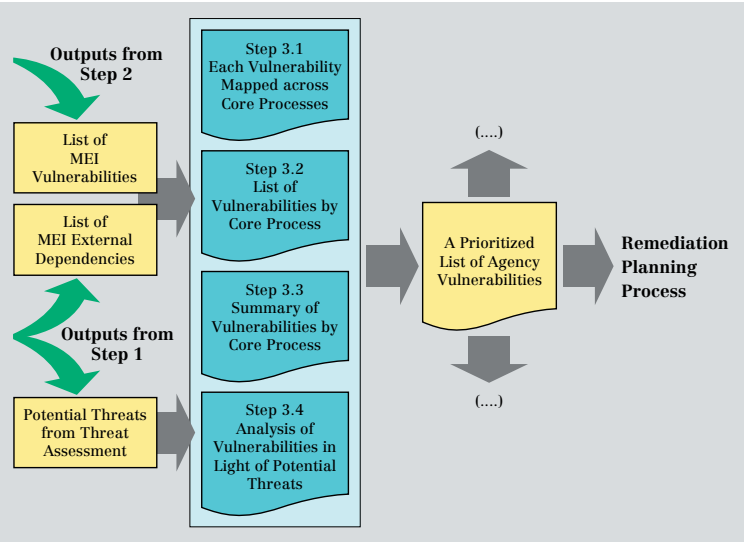

Figure 20: Step 3 Activities (Source: KPMG/ Marwick)

Models for CII Analysis

Introduction

This chapter discusses models and methods used for CII analysis on a generic level. The following models are introduced:

- Technical IT-Security Models,
- Risk Analysis Methodology,
- Infrastructure Risk Analysis Model (IRAM),
- Leontief-Based Model of Risks,
- Sector and Layer Model,
- Sector Analysis,
- Process and Technology Analysis,
- Dimensional Interdependency Analysis.

For each approach, four elements are considered:

- *Application Area*: to what level of analysis or to what component of the analysis of CII can the discussed approach be applied (e.g., technical systems level, infrastructure component, infrastructure, infrastructure sector, complex (critical) infrastructure system)?
- *Objective*: what is the declared objective of the approach?
- *Work Process*: what steps does the approach include? (If no process description is available, this step is omitted)
- *Reference Material*: lists additional reference material, often developed in the surveyed countries, with a short comment.

Technical IT-Security Models

Application Area

Technical IT-security models aim at ensuring security at the technical systems level.

Objective

Predominantly, this category of models covers locally applied measures with a localized focus in a business, agency, or organizational context. The models are based on the supposition that sufficient protection at the technical system level nullifies threats to the larger system of critical infrastructures. Technical protection manuals recommend security measures for exemplary IT systems.[1] The aim of these recommendations is to achieve a security level for IT systems that is reasonable and adequate to satisfy protection requirements ranging from a normal to a high degree of protection. Others provide models for the design, the development, or the implementation of secure IT systems taking into consideration the four →*IT-Security Objectives*.[2]

Reference Material

- Stoneburner, Gary. *Computer Security. Underlying Technical Models for Information Technology Security. Recommendations of the National Institute of Standards and Technology.* NIST Special Publication 800–33. (Washington, D.C.: U.S. Government Printing Office, December 2001). http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf.

The National Institute of Standards and Technology (NIST) has issued a number of guidelines or recommendations for information technology security. Proposed technical models provide a description of the technical foundations that underlie secure information technology and are

1 Bundesamt für Sicherheit in der Informationstechnik. *IT Baseline Protection Manual. Standard Security Safeguards*. Updated July 2001. http://www.bsi.de/gshb/english/menue.htm.

2 Stoneburner, Gary, Alice Goguen, and Alexis Feringa. *Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology.* NIST Special Publication 800-30. (Washington, D.C.: U.S. Government Printing Office, January 2002). http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

intended as blueprints that should be considered in the design and development of technical security capabilities.

- Bundesamt für Sicherheit in der Informationstechnik. *IT Baseline Protection Manual. Standard Security Safeguards*, updated July 2001, http://www.bsi.de/gshb/english/menue.htm.

The IT Baseline Protection Manual contains standard security safeguards, implementation advice, and aids for numerous IT configurations that are typically found in IT systems. This information is intended to assist with the rapid solution of common security problems, to help raise the security level of IT systems, and to simplify the creation of IT security policies.

- Commonwealth of Australia, Information Security Group. *Australian Communications-Electronic Security Instruction 33 (ACSI 33)* Handbook 3. Risk Management, Version 1.0, http://www.dsd.gov.au/infosec/acsi33/HB3.html.

ACSI 33 is intended to provide guidance to all Australian government departments, organizations, and personnel in the task of protecting classified or unclassified computer information and equipment. Specifically, it describes the steps to be taken to plan and implement computer security measures.

Risk Analysis Methodology (for IT Systems)

Application Area

Risk analysis/assessment helps to consider the security implications of electronic information systems and to devise policies and plans to ensure the systems are appropriately protected. The assessment can address any degree of complexity or size of system.

Objective

As a decision-making tool for the security sector, risk assessment methodologies aim to assure that the priority or appropriateness of measures used to counter specific security threats is adequate for the risks.[3] The outcomes of the risk assessment are used to provide guidance on the areas of highest risk.[4] Risk analysis is a widely used approach that includes a number of subsequent steps. Standard definitions show which elements need to be included in the process: Risk is a function of the *likelihood* of a given *threat source* displaying a particular potential *vulnerability*, and the resulting *impact* of that adverse event.[5]

Work Process

Risk assessment methodologies are often step-by-step processes. The number of steps may vary slightly and can be adjusted to specific needs.

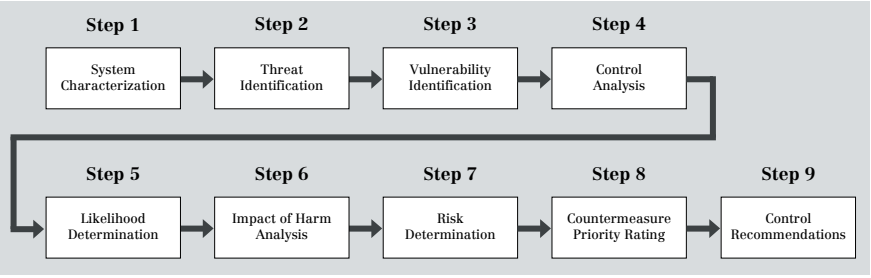

Figure 21: Steps in Risk Assessment Methodology

3 Commonwealth of Australia, Australian Communications-Electronic Security Instruction 33.
4 Commonwealth of Australia, Australian Communications-Electronic Security Instruction 33.
5 Stoneburner, Goguen, Feringa. Risk Management Guide for Information Technology Systems, 8.

However, in order to identify all the necessary sub-elements, no less than five steps must be undertaken. Figure 21 shows a possible nine-step risk analysis approach.[6]

Step 1: System Characterization

Definition of the scope of the effort and the boundaries of the system assessed. This includes identification of all kinds of resources, assets,[7] and information that constitute the system.

Step 2: Threat Identification

Determination of (1) the nature of external and internal threats,[8] (2) their source, and (3) the probability of their occurrence. The threat probability is a measure of the likelihood of the threat being realized.

Step 3: Vulnerability Identification

The next step is to develop a list of system vulnerabilities that could be exploited by the potential threat-sources.[9] There are several sophisticated approaches to a separate →*Vulnerability Assessment.*

Step 4: Control Analysis

Analysis of the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat exploiting a system vulnerability.

Step 5: Likelihood Determination

In determining the likelihood of a threat, one must consider threat sources (step 2), potential vulnerabilities (step 3), and existing controls (step

6 It is a mixture of an American approach described in: Stoneburner, Goguen, Feringa, Risk Management Guide for Information Technology Systems, and an Australian approach described in: Commonwealth of Australia, Australian Communications-Electronic Security Instruction 33.

7 An "asset" can be a tangible item (such as hardware), a grade or level of service, staff, or information.

8 Information on the nature and source of external threats can be derived in quantitative form from police reports, computer security surveys and bulletins, results of an audit analysis, or actuarial studies. Information on internal threats can be estimated using previous experience, generic statistical information, or a combination of the above.

9 Recommended methods for identifying system vulnerabilities are the use of vulnerability sources, the performance of system security testing, and the development of a security requirements checklist.

4). The likelihood that a potential vulnerability could be exploited by a given threat source can be described by different →*Categories*.

Step 6: Impact or Harm Analysis

The grade of possible harm to an asset is best determined by an executive, an asset owner, or an asset manager, and strongly reflects the actual value of the asset. The adverse impact of a security event can be described in terms of loss or degradation of any, or combination of, the →*IT-Security Objectives*. Other categories might be applied if risk analysis is conducted for more abstract systems.

Step 7: Risk Determination

Assessment of the level of risk to the system. The determination of risk can be expressed as a function of the likelihood that a given threat source will attempt to exploit a given vulnerability (step 5) and the magnitude of the impact should a threat source successfully exploit the vulnerability (step 6). To measure this resultant risk, a →*Risk Scale* and a →*Risk Level Matrix* are needed.

Step 8: Countermeasure Priority Rating

The countermeasure rating expresses the difference between the required risk (desired "risk level" as set by the management authority of the system) and the resultant risk (step 7), and is used to provide guidance as to the importance that should be placed on security countermeasures. Again, applied values and categories might vary widely. Table 3 is an example of a risk assessment table.

Step 9: Control Recommendations

Provision of controls that could mitigate or eliminate the identified risks. The goal of the recommended controls is to reduce the level of risk to the system and to its data to an acceptable level.

Reference Material

- Stoneburner, Gary, Alice Goguen, and Alexis Feringa. *Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology.* NIST Special Publication 800–30. (Washington, D.C.: U.S. Government Printing Office, January 2002), http://csrc.nist.gov/publications/nistpubs/800–30/sp800–30.pdf.

This guide provides a foundation for the development of an effective risk management program; it contains both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems.

- Commonwealth of Australia, Information Security Group. *Australian Communications-Electronic Security Instruction 33 (ACSI 33)* Handbook 3. Risk Management, Version 1.0, http://www.dsd.gov.au/infosec/acsi33/HB3.html.

The objective of this handbook is to present a risk assessment strategy that is consistent with the operation of information systems. The risk assessment methodology used in this manual has been adapted from the Protective Security Manual (PSM), and the Australian Standard AS/NZ 4360:1999 titled "Risk Management".

- Haimes, Yacov Y. *Risk Modeling, Assessment, and Management*. (New York: Wiley Publications, 1998).

A comprehensive description of the state of the art of risk analysis, including basic concepts as well as advanced material.

Column 1 Asset Identification	C 2 Threat to the Asset	C 3 Threat Likelihood	C 4 Harm	C 5 Resultant Risk	C 6 Required Risk	C 7 Countermeasure(s) Priority Rating
Row 1: Reliability of e-commerce-related website	Accidental electrical power or equipment failure	Medium	Grave	Critical	Nil	4
Row 2: Accuracy of publicly available web information	Loss of confidence or goodwill due to "hacking" of web page	High	Minor	Medium	Low	1
Row 3: Secure access to internal network services by authorized staff, from external networks	Loss of crypto token or keys required to access the secure channel(s)	Very Low	Serious	Medium	Low	1

Table 3: Risk Assessment Table[10]

10 Example from: Commonwealth of Australia, Australian Communications-Electronic Security Instruction. http://www.dsd.gov.au/infosec/acsi33/HB3A.html.

Infrastructure Risk Analysis Model (IRAM)[11]

Application Area

The IRAM is a probabilistic infrastructure risk analysis model that provides an analytical methodology for quantifying risk and a systematic process to conduct risk modeling, assessment, and management of specific infrastructure components or whole infrastructure sectors.

Objective

The IRAM is a complex approach to model the interconnectedness and interdependencies of an infrastructure system. The focus is on the modeling and assessment aspects and provides means for calculating critical and relevant measures of effectiveness needed to allocate scarce resources for improving system security. Through modeling expected as well as extreme risk, the IRAM provides activities of the system under normal as well as unusual workloads.

Work Process

The IRAM process consists of four phases, shown in Figure 22.

Phase I: Identify Threats and Vulnerabilities

Phase I identifies the risks to the infrastructure by structuring the system (Figure 23). Borrowing from the →*Hierarchical Holographic Modeling* (HHM) philosophy, the infrastructure is dissected with respect to

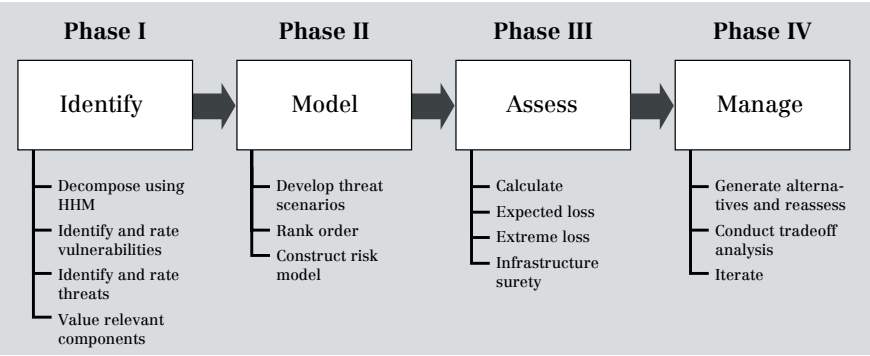

Figure 22: The four Phases of the Infrastructure Risk Analysis Model

11 Ezell, Barry C., John V. Farr, and Ian Wiese. "Infrastructure Risk Analysis Model" In: *Journal of Infrastructure Systems*. (vol. 6, 3, September 2000): 114–117.

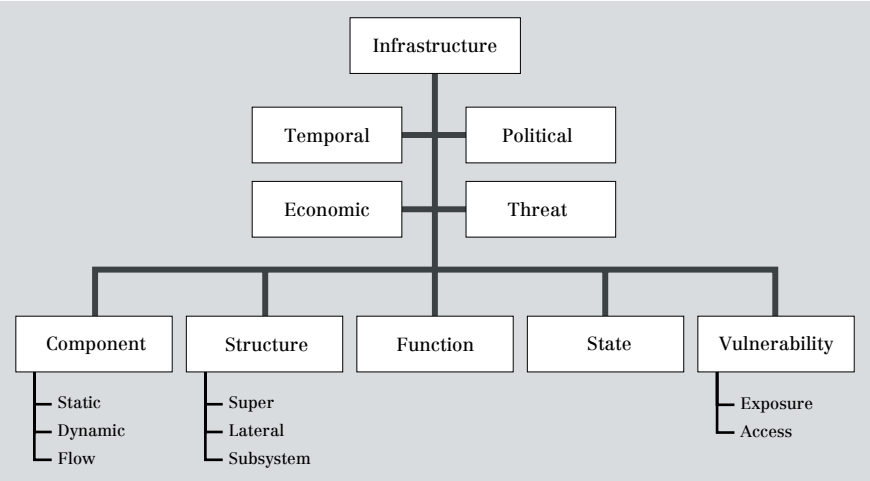

Figure 23: Generic Systems Decomposition (Source: Ezell, Farr, Wiese) [12]

- Components: structural (static), operating (dynamic), and flow components of the infrastructure,
- Hierarchical structure: refers to the relationship between components at different hierarchies such as super-system, lateral system, and sub-system,
- Function: described (in active verb phrases) in terms of purposeful actions that each component, element, or subsystem contributes,
- State: the various states (idle, busy, pumping, etc.) the system can be in at any given time,
- Vulnerability: identified for each system and addressed in terms of exposure, access, and threat.

Phase I culminates with a ranking of vulnerabilities for further assessment: Once the system has been dissected and its vulnerabilities and threats identified, the results are ordered in a ranking system. Next, the risk sources are defined. This decision may be based on research results, surveys, or other sources.

Phase II: Model Risks

The first step in Phase II is developing scenarios for models. The goal of the risk model is to provide information on consequences of a scenario executed against the system under study. →*Event Trees* can be used as a

12 Based on Ezell, Farr, Wiese, Infrastructure Risk Analysis Model, Figure 2, 115.

tool for constructing the risk model. Phase II ends with the construction of a probabilistic model to assess risks associated with a given scenario. As in Phase I, scenarios are ranked, and the experts decide on scenarios that will serve as initiating events for the risk model.

Phase III: Assess Loss

Phase III is the assessment phase, where infrastructure security, mean expected loss, and extreme loss are calculated using the →*Partitioned Multi-objective Risk Method* (PMRM).[13] This not only allows to see the expected extent of damage, but adds understanding of low-probability/high-impact events. It also serves as a useful tool to demonstrate the security of a system.

Phase IV: Manage

Phase IV is the management phase, where alternatives are generated and the risk model is reassessed to predict infrastructure performance. It culminates with a →*Multi-Objective Trade-off Analysis*. The trade-offs provide information to determine the level of accepted risk.

Reference Material

- Ezell, Barry C., John V. Farr, and Ian Wiese. "Infrastructure Risk Analysis Model" In: *Journal of Infrastructure Systems*. (vol. 6, 3, September 2000): 114–117.

This paper introduces a probabilistic infrastructure risk analysis model developed for a small community's water supply and treatment systems.

- Ezell, Barry C., John V. Farr, and Ian Wiese. "Infrastructure Risk Analysis of Municipal Water Distribution System" In: *Journal of Infrastructure Systems*, (vol. 6, 3, September 2000): 118–122.

This paper shows how an infrastructure risk analysis model can be applied to a small municipality. Based on a vulnerability analysis and expert opinion, a scenario for an intentional water contamination is developed and then modeled using an event tree. Expected and extreme risk are then measured using exceedence probability. Lastly, alternatives are generated and the results are presented in a multi-objective framework.

13 See Haimes, Yacov Y. *Risk Modeling, Assessment, and Management.* (New York: Wiley Publications, 1998): 312–321, 404–414, 437–483.

Leontief-Based Model of Risk in Complex Interconnected Infrastructures

Application Area

This approach to the input-output dynamics of complex infrastructure systems has a special focus on interdependencies and the effects of change in one component on another.

Objective

The purpose of this model is to improve understanding of the operability of critical infrastructure under all plausible conditions to help forecast the effect of one segment of a change in another. This is done by exploring intra-connectedness within each infrastructure, as well as the interconnectedness among them.

The original Leontief input-output model[14] is a framework for studying the equilibrium of an economy. Leontief's model assumes that the inputs of both goods and resources required to produce any commodity are proportional to the output of that commodity. Furthermore, the output of any commodity is used either as input for the production of other commodities or to satisfy final demands.

The adapted model considers a system consisting of critical complex interconnected and interconnected infrastructures, with the output being the risk of their inoperability that can be triggered by one or multiple failures due to complexity, accidents, or acts of terrorism. The input to the system can be failures due to accidents, natural hazards, or acts of terrorism. (Figure 24)

The system is in a perfect condition when all components are operating flawlessly. In this case, the system is in a state of equilibrium.

Work Process

The unit used in the Leontief input-output model for the economy is the dollar. The adapted infrastructure model uses units of risk of inoperability, where the risk of inoperability is measured as the probability (likelihood) and the degree (percentage) of the inoperability of a system.

14 Leontief, W. W. *Input-Output Economics, 2nd Edition.* (New York, Oxford University Press: 1986).

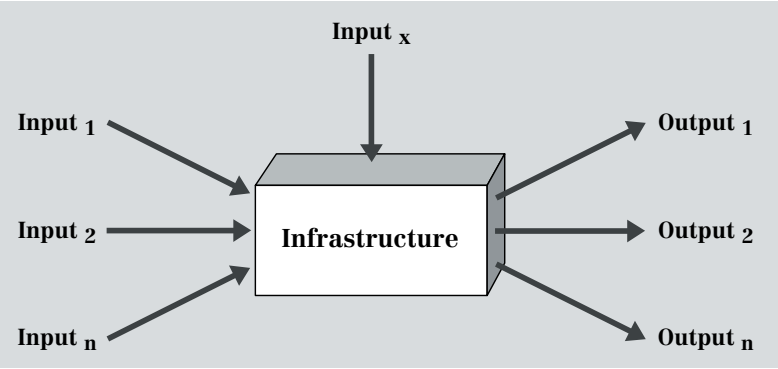

Figure 24: Input-Output Relationship

When the model is applied to any specific infrastructure system, one of the very first tasks is to define, for each infrastructure, the inoperability and the associated risk in a manner that can describe the behavior of the infrastructure as precisely as possible. First and foremost, one must define inoperability for each of the subsystems in such a way that the essence of the problem is captured and the characteristics of all subsystems pertinent to the objectives of the problem are appropriately and effectively represented. The inoperability of an infrastructure may be defined using various criteria, e.g., geographical, functional, temporal, or political. Each may justify the construction of a different Leontief-based model addressing a specific dimension.

After inoperability is clearly defined, the next step is to determine the Leontief equilibrium matrix. Extensive data collecting and data mining may be required to complete this step. The resource allocation problem is introduced in the Leontief economy model as a single-objective linear programming model, where the gross national product is maximized subject to the constraints imposed by limited resources. In the Leontief-based linear infrastructure model, multiple objectives can be analyzed. One example is minimizing the inoperability of more than one infrastructure. Further questions are how the equilibrium is achieved and how the system would react to an initial perturbation. This is asking how the state of the infrastructure would evolve over time.

Reference Material

- Haimes, Yacov Y. and Pu Jiang. "Leontief-Based Model of Risk in Complex Interconnected Infrastructures". In: *Journal of Infrastructure Systems*. (vol. 7, 1, March 2001): 1–12.

This paper introduces the adapted Leontief Model to be applied to infrastructures. It briefly discusses the dynamics of risk of inoperability using such a model, and presents several examples to illustrate the theory and its applications.

- Leontief, W. W. *Input-Output Economics*. (New York: Oxford University Press, 1986).

This collection of writings provides a comprehensive introduction to the input-output model for which Leontief was awarded the Nobel Prize in 1973. It includes twenty essays.

Sector and Layer Models

Application Area

Sector and layer models show parts of infrastructure systems or the totality of critical infrastructure elements and their relationship to each other and often serve to illustrate interdependencies between the elements.

Objective

Sector and layer models are mainly used as illustrations for how critical infrastructures are organized or serve as a basis for additional steps in the determination of interdependencies. They vary considerably from country to country.

Plain sector models do not scale different sectors as to their importance, but interdependencies might be shown between the sectors (→"National Efforts for CII Analysis: Switzerland").

The Canadian layer model (→"National Efforts for CII Analysis: Canada") addresses responsibilities of the international, federal, provincial, municipal, and private sectors. These areas of responsibility consist of the three vertical sector-specific layers: (1) operations layer, (2) technical application layer, and (3) control layer. The whole system in turn rests on two basic foundation layers.

The Dutch model (→"National Efforts for CII Analysis: Netherlands"), which focuses on the Information and Communication Technologies (ICT) infrastructure, stacks different segments in order of their importance. At the bottom is the electrical power supply and at the top added-value services, which are dependent on the availability and integrity of the underlying infrastructure layers. This points to a vertical dependence plus horizontal information flows and information service chains between the different public and private actors, individuals, and society as a whole.

Reference Material

- Luiijf, Eric, M. Klaver. *In Bits and Pieces: Vulnerability of the Netherlands ICT Infrastructure and Consequences for the Information Society.* (Translation of the Dutch Infodrome essay "BIT-BREUK", de kwetsbaarheid van de ICT-infrastructuur en de gevolgen voor de informatiemaatschappij). (Amsterdam, March 2000).

This essay was written in March 2000 on behalf of Infodrome as a basis for discussion in the Infodrome workshop "Vulnerabilities of ICT networks". This paper introduces a model for vertically stacked infrastructures.

- Luiijf, Eric, M. Klaver, J. Huizenga. *The Vulnerable Internet: A Study of the Critical Infrastructure of (the Netherlands Section of) the Internet*. (The Hague, 2001). http://www.tno.nl/instit/fel/refs/pub2001/kwint_paper1048.pdf.

This paper introduces four models with different points of view in order to address and clarify the roles of various actors, as well as the diversity, interdependencies, and vulnerabilities emerging in critical information infrastructures, mainly the Internet.

- InfoSurance, Ernst Basler + Partner AG. *Einflussfaktoren und Abhängigkeiten im Umgang und Einsatz von Informationssicherheit* (Zollikon, Zürich: 2000). http://www.infosurance.ch/de/ppt/Krisenverstaendnis.ppt.

This presentation introduces the CIP framework for Switzerland, including the sector model.

- Grenier, Jacques. "The Challenge of CIP Interdependencies". *Conference on the Future of European Crisis Management*. (Uppsala, Sweden, 19–21 March 2001). http://www.ntia.doc.gov/osmhome/cip/workshop/ciptf_files/frame.htm.

This presentation gives a step-by-step introduction to the Canadian Infrastructure Protection Process and includes the Canadian CI layer model.

Sector Analysis

Application Area

Sector analysis adds to an understanding of the functioning of single sectors by highlighting various important aspects of the sector.

Objective

There are many aspects that might be analyzed in connection with individual sectors. The Dutch approach (→"National Efforts for CII Analysis: Netherlands") develops four models with different points of view in order to address and clarify the roles of various actors, as well as the diversity, interdependencies, and vulnerabilities that exist. Another approach (→"National Efforts for CII Analysis: Australia") mainly considers the economic environment and highlights industry sector information such as trends, points of strength and weakness, the impact of the external environment, and the role of competitive forces in a bid to understand the sector under investigation. The methodological approach used are PEST, Porter's analysis, and SWOT analysis.

PEST (Political, Economic, Social, Technological) Analysis

A PEST analysis is usually conducted to obtain an understanding of the macro environment affecting the business or sector under consideration (political, economic, social, and technological factors). The concept of the PEST analysis is to look at external factors that influence the business. Table 4 shows an example of a PEST analysis table.

	Political	Economic	Social	Technological
Macro Overview	• Globalization • Privatization	• Economic development • Inflation • Unemployment	• Population • Education	• PC penetration • Reliance of key infrastructure on technology systems • Internet access
Specific Sector Drivers	• Establishment of federal ministries • Organizations	• Importance of industry • R&D	• Improve quality of life • Global community • Knowledge-sharing	• Technological breakthroughs

Table 4: PEST Example

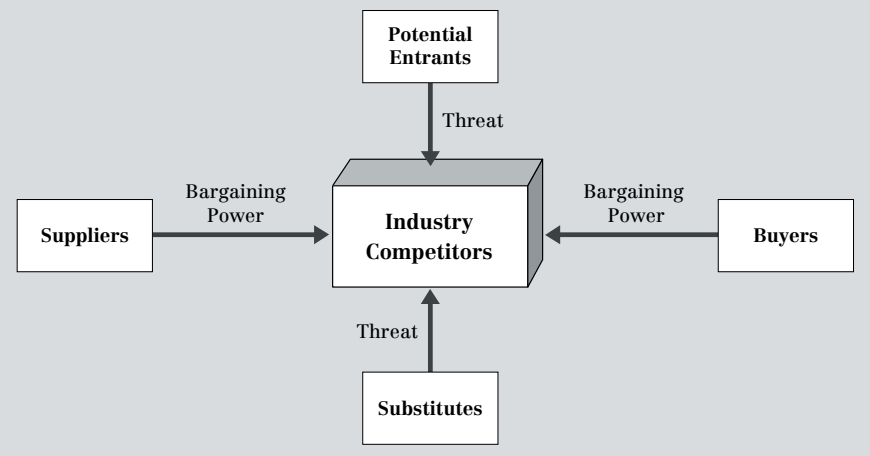

Figure 25: Michael Porter's Five Forces Model

Porter's Analysis

Porter's analysis looks at the competitive forces at work in a particular sector or industry. Important criteria in this analysis are intensity of rivalry; competitors, barriers to entry, threat of substitutes; supplier power, and buyer power. Figure 25 shows Porter's five forces model.

SWOT (Strength, Weakness, Opportunities, Threats)

A SWOT analysis, which focuses on strength, weakness, opportunities, and threats, is usually conducted at the micro-level, or business unit level, but can also be conducted at the sector level. Table 5 shows a typical SWOT worksheet.

		Environment Analysis	
		Opportunities (1) Opportunity 1 (2) Opportunity 2 (n) Opportunity n	Threats (1) Threat 1 (2) Threat 2 (n) Threat n
Situation Analysis	Strengths (1) Strength 1 (2) Strength 2 (n) Strength n	SO-Strategies Examples: S1O1: Specific strategy S1SnO1: Specific strategy ...	ST-Strategies Examples: S1S3T2: Specific strategy ...
	Weaknesses (1) Weakness 1 (2) Weakness 2 (n) Weakness n	WO-Strategies Examples: W1O1O2: Specific strategy ...	WT-Strategies Examples: W2T2: Specific strategy ...

Table 5: Typical SWOT Worksheet

Reference Material

- KPMG / National Support Staff. *Critical Infrastructure Project. Phase 2. Information Technology Report.* Predict Defense Infrastructure Core Requirements Tool (PreDICT). (April 2000).

This study has ten parts, each dealing with one of ten industry sectors. A PEST, Porter's analysis, and SWOT analysis is conducted in each of these sectors.

- Porter, Michael. *Competitive Strategy. Techniques for Analyzing Industries and Competitors* (New York: Free Press, 1980).

This book introduces Porter's analysis of industries, based on the identification of five underlying forces that drive industry competition.

- Luiijf, Eric., M. Klaver, J. Huizenga. *The Vulnerable Internet: A Study of the Critical Infrastructure of (the Netherlands Section of) the Internet.* (The Hague, 2001), http://www.tno.nl/instit/fel/refs/pub2001/kwint_paper1048.pdf.

This paper introduces four aspects that might be applied to the analysis of sectors: the social, functional, structural, and physical aspects.

Process and Technology Analysis

Application Area

The process and technology analysis helps to identify critical infrastructure sectors dependencies on information infrastructure and across multiple sectors.

Objective

This approach assesses different layers of a sector in order to examine the dependency on information and communication technology in one critical sector and across multiple sectors by highlighting core functions, core components, and their interdependencies.

Work Process

The analysis follows a six-step process (Figure 26).
Steps 1 to 4 are conducted for each sector defined as critical. After core functions and processes have been identified for each sector, step 5 and 6 help to define the dependencies on other sectors and assess the manner of dependencies.

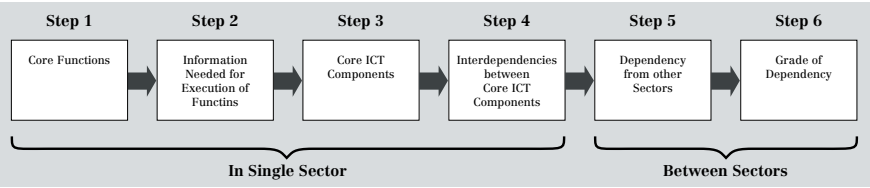

Figure 26: Steps of the Process and Technology Analysis

Step 1: Identify Core Functions of a Sector

To identify core functions, a basic understanding of the values chains and core functions within the sector is necessary.

Step 2: Identify Information Needed for Execution of Function

The information needed can be divided into two functional groups: (1) Business information management: Define what kind of information must be available at all times to assure sector functions, (2) Service and system management: Define availability of systems, performance, etc., and define necessary IT functions.

Step 3: Identify Core ICT Components

This step aims to identify "single points of failure" and the importance of individual infrastructure components within a sector.

Step 4: Show Interdependencies Between Core ICT Components

Define dependencies of core infrastructure components that could lead to cascading effects of failure. The knowledge of these dependabilities allows forecasts of cascading failures.

Step 5: Define Dependency from Other Sectors

The degree of dependency may be determined by identifying nodes and linkages between the sectors. The following questions have to be answered:

- What dependencies exist between functions of different sectors?
- What dependencies exist between infrastructure components of different sectors?

Step 6: Establish Grade of Dependencies

In order to better understand the interdependencies, the grade of the dependency between sectors is defined for each interface according to the following criteria:

- Type of dependency: is it a functional or a direct dependency?
- Impact of dependency: what if the functions are only partly available?
- Transfer time: how long does it take until impacts become visible?
- Redundancy: what kind of redundancies exist within the different sectors?

Reference Material

- InfoSurance, Ernst Basler + Partner AG. *Einflussfaktoren und Abhängigkeiten im Umgang und Einsatz von Informationssicherheit* (Zollikon, Zürich: 2000). http://www.infosurance.ch/de/ppt/Krisenverstaendnis.ppt.

This presentation introduces the CIP framework Switzerland, including detailed process and technology analysis for different sectors.

Dimensional Interdependency Analysis

Application

This descriptive approach portrays six dimensions of infrastructure interdependencies.

Objective

The dimensional interdependency analysis is a descriptive approach to facilitate the identification, understanding, and analysis of interdependencies. It provides the foundation for a comprehensive set of orthogonal interdependency metrics. It addresses a broad range of interrelated factors and system conditions that are represented and described in terms of six "dimensions" (Figure 27).

The dimensions include the technical, economic, business, social/political, legal/regulatory, public policy, health and safety, and security concerns that affect infrastructure operations. The six "dimensions" that can be distinguished are:

- Environment, Coupling/Response Behavior,
- Infrastructure Characteristics,
- Types of Interdependencies,
- State of Operation,
- Type of Failure.

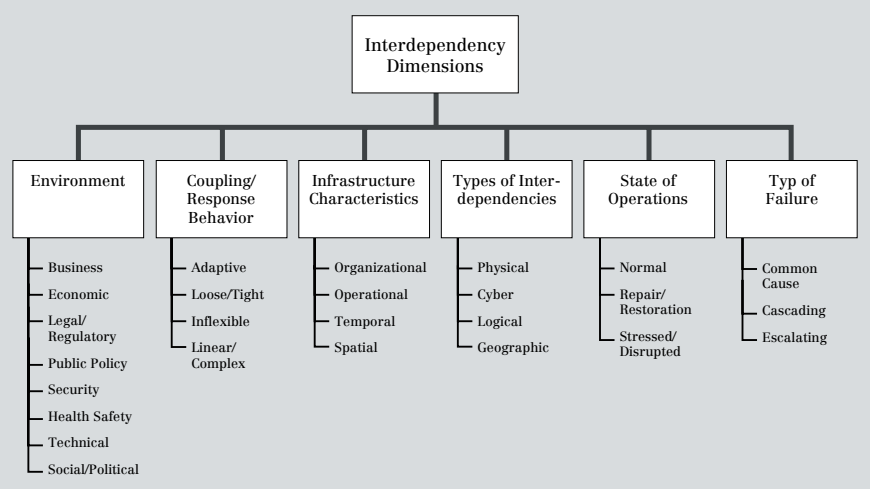

Figure 27: Interdependency Dimensions

The environment comprising these concerns influences normal system operations, emergency operations during disruptions and periods of high stress, and repair and recovery operations. The degree to which the infrastructures are coupled, or linked, strongly influences their operational characteristics. Some linkages are loose and thus relatively flexible, whereas others are tight, leaving little or no flexibility for the system to respond to changing conditions or failures that can exacerbate problems or cascade from one infrastructure to another. These linkages can be physical, cyber, related to geographic location, or logical in nature. Interdependent infrastructures also display a wide range of spatial, temporal, operational, and organizational characteristics that can affect their ability to adapt to changing system conditions. And finally, interdependencies and the resultant infrastructure topologies can create subtle interactions and feedback mechanisms that often lead to unintended behavior during disruptions.[15]

Reference Material

- Rinaldi, Steven M., James P. Peerenboom, and Terrence K. Kelly. "Complex Networks. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies." In: *IEEE Control Systems Magazine*. (vol. 21, 6, December 2001): 11–25.

This article presents a conceptual framework for addressing infrastructure interdependencies. The authors use this framework to explore the challenges and complexities of interdependency and introduce the fundamental concept of infrastructures as complex adaptive systems. The focus is on interrelated factors and system conditions that collectively define the six dimensions.

15 Rinaldi, Steven M., James P. Peerenboom, and Terrence K. Kelly. "Complex Networks. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies." In: *IEEE Control Systems Magazine*. (vol. 21, 6, December 2001): 11–25.

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

Appendix

A1 Glossary of Key Terms

Categories

Categories of risks, likelihood, impact, and consequences vary considerably and need to be defined thoroughly at the beginning of any risk assessment. Categorization might depend on the desired level of precision in the assessment, or on whether it is a → *Qualitative* or a *Quantitative Risk Assessment*. The most simple ranking can be expressed using the categories "high", "medium", and "low".

Causal Mapping

Causal mapping refers to the use of directed node and link graphs to represent a set of causal relationships within systems of complex relationships. Causal relations are represented as nodes and links, and concepts of cause and effect are established with direct or inverse directions. The method can be used to explore cognition and to develop maps that can be the basis for confirmatory empirical testing.

Cluster Analysis

Cluster analysis is a collection of statistical methods that can be used to assign cases or data to groups (clusters). The aim is to classify what is being investigated in clusters in such a way that there is a strong association between "the object" in the same cluster, but a weak one with regard to objects in other clusters. Thus, the cluster analysis can expose links and structures in data that are not evident at first inspection.

Critical Information Infrastructure (CII)

Critical Information Infrastructure (CII) includes components such as telecommunications, computers/ software, Internet, satellites, fiber optics, etc. The term is also used for the totality of interconnected computers and networks and their critical information flows.

Critical Information Infrastructure Protection (CIIP)

Critical Information Infrastructure Protection (CIIP) is a subset of → *Critical Infrastructure Protection* (CIP). CIIP focuses on the protection of systems and assets including components such as telecommunications, computers/software, Internet, satellites, fiber optics, etc., and on interconnected computers and networks, and the services they provide.

Critical Infrastructure (CI)

Critical Infrastructure (CI) includes all systems and assets whose incapacity or destruction would have a debilitating impact on the national security, and the economic and social well being of a nation.

Critical Infrastructure Protection (CIP)

Critical Infrastructure Protection (CIP) includes measures to secure all systems and assets whose incapacity or destruction would have a debilitating impact on the national security, and the economic and social well being of a nation.

Cumulative Risk Assessment

A cumulative risk assessment is the process of evaluating the combined exposure and hazard of a subject from all factors that share a common mechanism of danger. In CIIP, the risk of dependencies propagates and the risk to infrastructures accumulates. In Figure 1, the cumulative risk to Infrastructure 1 rises from 1 to 2.5 to 3.0 (etc.) as one goes into more depth.

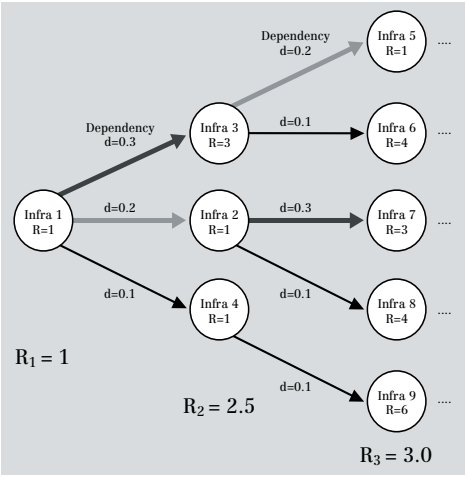

Figure 1: Cumulative Risk Tree (Source: Presentation by J. Grenier)

Dependency

Dependency exists between two components, often within a sector. It considers a specific, individual connection between two infrastructures. Usually, this relationship is unidirectional. Dependency is therefore a linkage or connection between two infrastructures, through which the state of one infrastructure influences or is dependent on the state of the other.

Dependency/Interdependency Matrices

Dependency/Interdependency Matrices often serve as a tool for visualizing the strength of interdependencies between different sectors (→"National Efforts for CII Analysis": Australia and Canada). Often, different colors representing values (→*Categories*) such as "high", "medium", "low", or "none" are used to show the strength of interdependencies. These matrices are read horizontally by industry sector, where each field describes the level of dependency on the sector in the vertical column.

Sector	Element	Energy & Utilities					Services		
		Electrical Power	Water Purification	Sewage Treatment	Natural Gas	Oil Industry	Customs and Immigration	Hospital & Health Care Services	Food Industry
Energy & Utilities	Electrical Power		L			M			
	Water Purification	H				M			
	Sewage Treatment	M	H			H			
	Natural Gas	L				L			
	Oil Industry	H	L						
Services	Customs & Immigration	H	L	L	L	L		L	
	Hospital & Health Care Services	H	H	L	H	H	M		H
	Food Industry	H	H	H	L	M	M	L	

Key: H High M Medium L Low

Figure 2: Dependency/Interdependency Matrix (Source: Presentation by J. Grenier)

Event Tree Analysis

Event tree analysis asks "what if" to determine the sequence of events that lead to consequences. From the event tree, one can deduce a probability density and excedence probability. Event trees help to understand how an outcome is determined by mitigating events. The failure of each mitigating event may be estimated through expert assessment or, in some cases, through an additional →*Fault-Tree Analysis*. Figure 3 is an example of an event tree.

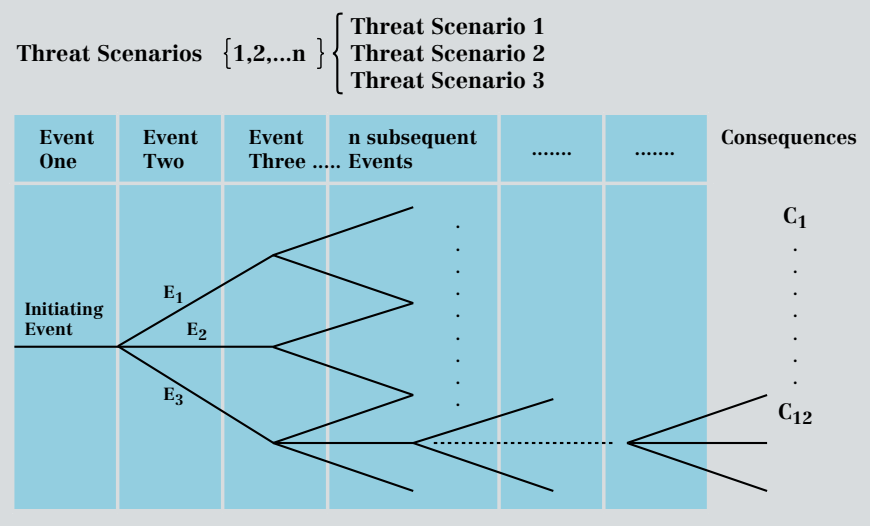

Figure 3: Event Tree (Source: Ezell, Farr, Wiese)

Expert Assessment/ Interviews

A very effective way of getting information on various aspects of CII is to circulate a questionnaire among key persons/experts or to interview them. A questionnaire can contain multiple-choice answers that can be assessed afterwards with the help of an evaluation key, or questions can be phrased to leave more latitude for semi-structured answers.

Factor Analysis

Factor analysis is a statistical method used to identify a small number of factors that represent situations between a list of interrelated variables. It is used to study the patterns of relationships among many dependent variables, with the goal of discovering something about the nature of the independent variables that affect them, even though those independent variables have not been measured directly. The main applications of factor analytic techniques are: (1) to reduce the number of variables and (2) to detect a structure in the relationships between variables – that is, to classify variables. Therefore, factor analysis is applied as a method for data reduction or structure detection.

Fault Tree Analysis

A fault tree analysis is a deductive, top-down method of analyzing system design and performance. It involves specifying an (often undesirable) top event for analysis, followed by the identification of all associated elements in the system that could cause that top event to occur. Fault trees can be used to assess the probability of failure of a system or of a top event occurring, to compare design alternatives, to identify critical events that will significantly contribute to the occurrence of the top event, and to determine the sensitivity of the probability of failure of the top event to various contributions of basic events. Fault tree analyses are generally performed graphically using a logical structure of AND and OR gates (Figure 4).

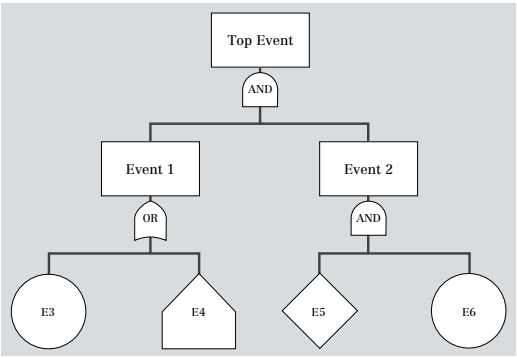

Figure 4: Example of a Simple Fault Tree

Hierarchical Holographic Modeling (HHM)

The HHM methodology takes into consideration the fact that in the process of modeling large-scale and complex systems, more than one mathematical or conceptual model is likely to emerge. Each of these models

may focus on a specific aspect, yet all may be regarded as acceptable representations of the infrastructure system. Therefore, HHM builds a family of models that address different identified aspects of the systems. Central to the HHM method is a particular form of diagram, as shown in Figure 5. The different columns in the diagram reflect different "perspectives" on the overall system.

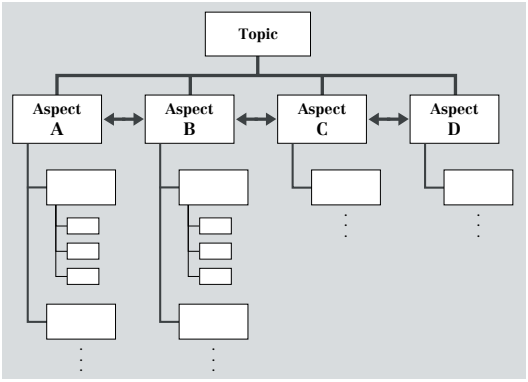

Figure 5: HHM Framework (Source: Y.Y. Haimes)

Information and Communication Technologies (ICT)

Information and Communication Technologies are characterized by (1) computing and telecommunications equipment, software, processes; and people that support the processing, storage, and transmission of data and information, (2) the processes and people that convert the data into information and information into knowledge, and (3) the actual data and information.

Infrastructure

The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services. Infrastructures provide a reliable flow of products and services essential to defense and economic security, the smooth functioning of governments at all levels, and society as a whole.

Infrastructure Profiles (IPs)

Infrastructure profiles such as the one developed by the National Contingency Planning Group (Canada) include a number of characteristics of certain infrastructures, such as description of the infrastructure, statis-

tics, maps, contacts, references, jurisdictions, and a detailed analysis of the interdependencies.

Interdependency

Interdependency is a bi-directional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other. More generally, two infrastructures are interdependent when each is dependent on the other.

IT-Security Objectives

There are four basic IT-security objectives:[1]

(1) Availability (of systems and data for intended use only):

Availability is a requirement to assure that systems work promptly and service is not denied to authorized users. This objective protects systems against intentional or accidental attempts to either perform unauthorized deletion of data or otherwise cause a denial of service or data, and against attempts to use system or data for unauthorized purposes.

(2) Integrity of system or data: Integrity is required on two levels:

- Data integrity (the requirement that data not be altered without authorization while in storage, during processing, or while in transit) or
- System integrity (the quality that a system has when performing the intended function in an unimpaired manner, free from unauthorized manipulation).

(3) Confidentiality of data and system information:

Confidentiality is the requirement that private or confidential information not be disclosed to unauthorized individuals. Confidentiality protection applies to data in storage, during processing, and while in transit.

1 Cf. Stoneburner, Gary. *Computer Security. Underlying Technical Models for Information Technology Security. Recommendations of the National Institute of Standards and Technology.* NIST Special Publication 800–33. (Washington, D.C.: U.S. Government Printing Office, December 2001). http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf.

(4) Accountability (to the individual level):

Accountability is the requirement that actions of an entity may be traced uniquely to that entity.

As a fifth objective, the assurance that the other four objectives have been met is sometimes mentioned.

Layer Model

Layer models show parts of infrastructure systems or the totality of a nation's critical infrastructures and their relationship to each other, and often serve to picture interdependencies between the elements. (→"Models for CII Analysis: Sector and Layer Models".)

Multi-Criteria Decision Approach

The multi-criteria decision approach (MCDA) is both an approach and a set of techniques, with the goal of providing an overall ordering of options, from the most preferred to the least preferred option. MCDA involves structuring the research problem in a multi-criteria hierarchy, where measures are linked to a top-level goal through several levels of decision criteria. The top-level goal is the overall objective of the system of analysis.

Multi-Criteria Model

See →*Multi-Criteria Decision Approach*; →"National Efforts for CII Analysis: Norway".

Multi-Objective Trade-off Analysis

The Multi-Objective Trade-off Analysis is closely linked to the →*Multi-Criteria Decision Approach* as it is based on the assumption that problems are characterized by multiple, non-commensurate, and often conflicting, objectives. It is used to identify this hierarchy of objectives and to avoid comparing and trading off objectives that belong to different levels. Ultimately, the goal is to present a number of alternatives. The decision-maker reviews the results and then makes a qualitative decision on system safety or security.

Partitioned Multi-objective Risk Method (PMRM)

The PMRM is a risk analysis method for solving multi-objective problems of a probabilistic nature. Instead of using the traditional expected value of risk, the PMRM generates a number of conditional expected-value functions, which represent the risk (given that the damage falls within specific damage ranges). It is therefore used to identify the risk of extreme and catastrophic events. This not only allows a decision-maker to see the expected value of damage, but adds understanding of low probability/high-damage events.

Process and Technology Analysis

One of the methodological elements of the InfoSurance CIIP framework. It helps to identify critical infrastructure sectors dependencies on information infrastructure and across multiple sectors. (→"Models for CII Analysis: Process and Technology Analysis; →"National Efforts for CII Analysis: Switzerland").

Qualitative and Quantitative Risk Assessment

A *quantitative* risk assessment expresses threat likelihood, impact, and risk in terms of a numeric value, whereas a *qualitative* assessment uses ratings such as "high", "medium", or "low" to express the value. The major advantage of the quantitative approach is that it is precise and provides a measurement that can be fed directly into a cost-benefit analysis. Many approaches today start out by using qualitative rankings ("high", "medium", or "low") and attribute a range of values to each.

Risk

Risk is the net negative impact of an event/incident, considering both the probability and the impact of occurrence.

Risk/Impact Scattergram

When assessing impact of incidents, a scattergram plotting the relative rated criticality of the infrastructure elements (increasing from bottom to top) against their relative risk value (increasing from left to right) can be used (Figure 6).

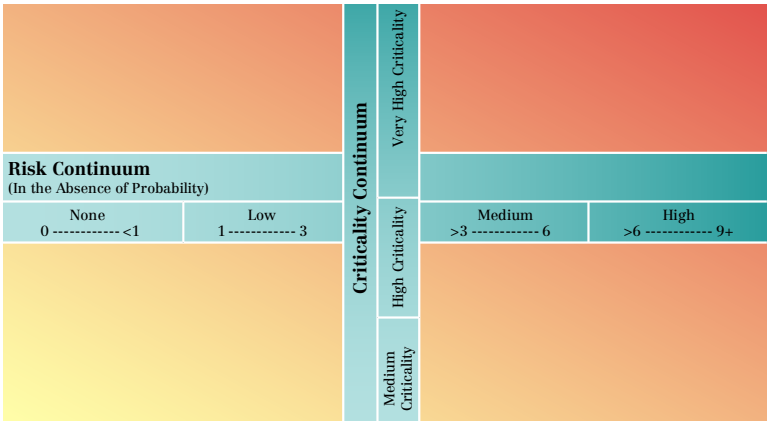

Figure 6: Risk/ Impact Scattergram (Source: Speech by J. Grenier)

This creates four quadrants in which crucial elements of a sector (e.g. communication satellites or telecom systems for the communications sector) can be positioned. This is a way to show which element needs special attention.

Risk Level Matrix

A risk level matrix is used in connection with a →*Risk Scale* to determine and describe the intensity of risk. It relates two categories (such as threat likelihood and impact) and multiplies assigned values to each category (Figure 7).

		Impact		
		Low (10)	**Medium** (50)	**High** (100)
Threat Likelihood	**High** (1.0)	**Low** (10 x 1.0 = 10)	**Medium** (50 x 1.0 = 50)	**High** (100 x 1.0 = 100)
	Medium (0.5)	**Low** (10 x 0.5 = 5)	**Medium** (50 x 0.5 = 25)	**Medium** (100 x 0.5 = 50)
	Low (0.1)	**Low** (10 x 0.1 = 1)	**Low** (50 x 0.1 = 5)	**Low** (100 x 0.1 = 10)
Key:		High	Medium	Low
Risk Scale:		> 50 - 100	> 10 - 50	> 1 - 10

Figure 7: Typical Risk Level Matrix

Risk Rating Matrix

After the evaluation of threat and vulnerability for single components of an infrastructure element, risks can be determined based on a matrix that multiplies the assigned values for threat and vulnerability (Figure 8). This method allows for a comparison of relative risks between components of an infrastructure element, between layers in the infrastructure model, and between infrastructures.

Figure 8: Basic Risk Rating Matrix

Risk Scale

A risk scale assigns numeric values to → *Categories* of risk, such as "high", "medium", "low". (See Figure 7).

Scenarios/ Scenario Technique

The scenario technique enables the generation of scenarios that serve to determine strategies in order to control or at least influence the unknown developments of complex systems as favorably as possible with regard to own objectives and interests. There are various techniques and even software tools to develop scenarios.[2]

Sector Analysis

Sector analysis adds to an understanding of the functioning of single sectors by highlighting various important aspects of the sector. (→"Methods and Models to Analyze CII: Sector Analysis").

2 Cf. von Reibnitz, Ute. *Szenario-Technik: Instrumente für die unternehmerische und persönliche Erfolgsplanung.* (Wiesbaden, 1992).

Sector Model

Sector and layer models are mainly used as illustrations for how critical infrastructures are organized. They vary considerably from country to country (→"Methods and Models to Analyze CII: Sector and Layer Models"; →"National Efforts for CII Analysis: Switzerland").

Seminar Games

Seminar gaming is an approach to understanding complex problems that capitalizes on the inherent expertise of groups of participants, which discuss complex topics by way of scenarios.[3]

Values

See →*Categories*.

Vulnerability

Vulnerability can be understood as the collective result of risks and the ability of a society, local municipal authority, company or organization to deal with and survive external and internal emergency situations. The vulnerability analysis covers a long-term perspective and gives focus to a sequence of events from the moment an emergency situation occurs until a new stabile situation has been reached (see also →*Vulnerability Assessment*).

Vulnerability Analysis

See →*Vulnerability Assessment*.

Vulnerability Assessment

There are two different understandings of vulnerability assessment:

1) Vulnerability assessment can be a step in risk analysis methodology. Its goal is to develop a list of vulnerabilities that could be

3 Cf. Strategic Leadership Exercise "Informo 2001", conducted by the Strategic Leadership Training in cooperation with Ernst Basler + Partner AG, http://www.admin.ch/ch/e/bk/sfa/sfa/rueckblick.html

exploited by a potential threat-source ("exposure analysis"). There are several sophisticated approaches to Vulnerability Assessment (→"National Efforts for CII Analysis: Australia"; →"National Efforts for CII Analysis: United States").

2) A second approach sees vulnerability as the collective result of risks and the ability of a society, local municipal authority, company, or organization to deal with and survive external and internal emergency situations. Vulnerability assessment is thus not part of risk analysis, but a combination of risk analysis and emergency management evaluation.[IV]

Vulnerability Profile Chart

A vulnerability profile chart visually represents vulnerability rankings, often with a focus on interdependencies. Each profile may represent a single sector. The vulnerability ranking is done in order to compare and contrast vulnerabilities between sectors. One possible approach is the definition of "risk areas" in order to group vulnerabilities into common areas for analysis. (→"National Efforts for CII Analysis: Australia"). (Example Figure 9)

Vulnerability Rating Table

Vulnerability is sometimes defined as a function of likelihood and consequences. Through the separate analysis of each, the vulnerabilities can be rated using the product of the "Consequence" and the "Likelihood" ratings, displayed as a rating table (Figure 10).

IV Cf. Nilsson, Jerry, Sven Erik Magnusson, Per-Olof Hallin, Bo Lenntorp. Vulnerability Analysis and Auditing of Municipalities (Lund University Centre for Risk Assessment and Management (LUCRAM)): 15–17. http://www.isn.ethz.ch/crn/basics/process/documents/vulnerability.pdf

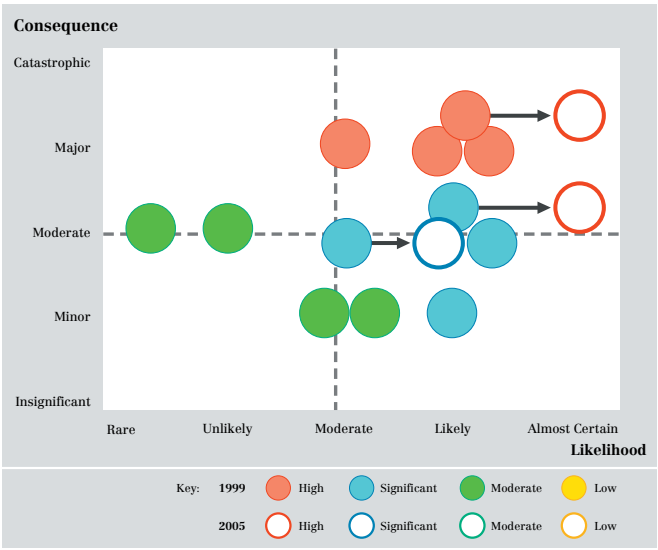

Figure 9: Vulnerability Profile Chart (Source: PreDICT)

Likelihood	Consequences: Insignificant	Minor	Moderate	Maior	Catastrophic
Almost Certain	Significant	Significant	High	High	High
Likely	Moderate	Significant	Significant	High	High
Moderate	Low	Moderate	Significant	High	High
Unlikely	Low	Low	Moderate	Significant	High
Rare	Low	Low	Moderate	Significant	Significant

Key: High Significant Moderate Low

Figure 10: Vulnerability Rating Table

A2 Bibliography

Australia

Attorney-General's Department. *Protecting Australia's National Information Infrastructure. Report of the Interdepartmental Committee on Protection of the National Information Infrastructure.* (Canberra, December 1998). http://www.law.gov.au/publications/niireport/niirpt.pdf

Budget 2001–2002 (Fact Sheet): Protecting the National Information Infrastructure: Part of the Government's E-security Initiative. http://www.asio.gov.au/Media/Contents/protecting%20NII.htm

Cobb, Adam. *Thinking about the Unthinkable: Australian Vulnerabilities to High-Tech Risks.* Foreign Affairs, Defence and Trade Group, Research Paper 18. (29 June, 1998).

Commonwealth Department of Communications, Information Technology and the Arts (DOCITA). *E-Commerce beyond 2000.* (Canberra, 2000). http://www.iwar.org.uk/e-commerce/resources/au/beyond2k_final_report.pdf

Commonwealth Department of Communications, Information Technology and the Arts (DOCITA). *A Strategic Framework for the Information Economy. Identifying Priorities for Action.* (Canberra, December 1998).

Commonwealth of Australia, Information Security Group. *Australian Communications-Electronic Security Instruction 33 (ACSI 33).* http://www.dsd.gov.au/infosec/acsi33/HB3.html

Dale, Tom. "Who's Who in eSecurity and eCrime". *eSecurity and eCrime Conference at Baker & McKenzie Cyberspace Law and Policy Centre.* (Sydney, 19–20 July, 2001). http://www.austlii.edu.au/au/other/CyberLRes/2001/17

Dependability Development Support Initiative (DDSI). *European Dependability Policy Environments*, *Country Report Australia.* (Version April 2002).

Etter, Barbara. "The Australasian Policing Response to Electronic Crime". *Australasian Centre for Policing Research to the FBI Global Economic Threats Conference.* (FBI Academy, Quantico, Virginia (USA), July 9–13, 2001).

KPMG / National Support Staff. *Critical Infrastructure Project. Phase 2. Information Technology Report.* Predict Defence Infrastructure Core Requirements Tool (PreDICT). (April 2000). http://www.defence.gov.au/predict/segments/it/pdf/it_full.pdf

Rathmell, Andrew. *Trip Note*, *Australian Business-Government Task Force on Critical Infrastructure*, 26–27 March 2002.

Canada

Canadian Security Intelligence Service (CSIS). *Protection of the Canadian Critical Infrastructure.* (17 July, 2001).

Charters, David. *The Future of Canada's Security and Defence Policy: Critical Infrastructure Protection and DND Policy and Strategy.* Research Paper of the Council for Canadian Security in the 21st Century. http://www.ccs21.org/ccspapers/papers/charters-CSDP.htm

Dependability Development Support Initiative (DDSI). *Global Overview – Countries, International and Inter-Governmental Organisations.* (Version April 2002).

Grenier, Jacques. "The Challenge of CIP Interdependencies". *Conference on the Future of European Crisis Management.* (Uppsala, Sweden, 19–21 March 2001). http://www.ntia.doc.gov/osmhome/cip/workshop/ciptf_files/frame.htm

National Contingency Planning Group. *Canadian Infrastructures and their Dependencies.* (March 2000).

"National Critical Infrastructure Protection Program". In: *Memo Quarterly Newsletter.* (Yukon Government and Emergency Preparedness Canada, vol. 7, Winter 2001).

ÖCB (ed.). *International CEP Handbook: Civil Emergency Planning in the NATO/EACP Countries 1999-2000.* (Stockholm, 2000).

Purdy, Margaret. *Cyber-Sabotage for Government. Speech at the Ottawa Congress Centre.* (Ottawa, 20 February, 2001). http://www.ocipep.gc.ca/pub_communi/speeches/cybersabotage_e.html

Germany

Act on the Protection of Personal Data Used in Teleservices. (Teleservices Data Protection Act – Teledienstedatenschutzgesetz, TDDSG) 22 July, 1997, amended last by Article 3 of the Bill on Legal Framework Conditions for Electronic Commerce.

Act on the Utilization of Teleservices. (Teleservices Act – Teledienstegesetz TDG) 22 July, 1997, amended last by Article 1 of the Bill on Legal Framework Conditions for Electronic Commerce.

Bewig, Frank. *Schutz kritischer Infrastrukturen in Deutschland: Kooperationen zwischen Staat und Privatwirtschaft.* (Semesterarbeit im Seminar "Militär- und Sicherheitspolitik im technologischen Wandel". (Berlin, September 2000). http://userpage.fu-berlin.de/~bendrath/hausarbeiten/kritis-D.rtf

Blattner-Zimmermann, Marit. "Kritische Infrastrukturen im Zeitalter der Informationstechnik". *Seminar on Information Warfare.* (Lucerne, 22 November, 2001).

Bundesamt für Sicherheit in der Informationstechnik (BSI). *IT-Sicherheitsstrukturen in der deutschen Kreditwirtschaft.* (SecuMedia Verlag: Ingelheim, 2002) http://www.bsi.de/presse/pressinf/itkredit.htm

Bundesministerium des Innern. *Zweiter Gefährdungsbericht der Schutzkommission beim Bundesminister des Innern. Bericht über mögliche Gefahren für die Bevölkerung bei Grosskatastrophen und im Verteidigungsfall.* (Berlin, October 2001).

Bundesministerium für Bildung und Forschung. "Online – Offline: IT in Education". *Innovationen Wissensgesellschaft.* (August 2000).

Dependability Development Support Initiative (DDSI). *European Dependability Policy Environments*, *Country Report Germany.* (Version April 2002).

Ennen, Günther. "CERT-Bund – eine neue Aufgabe des BSI". In: *KES Zeitschrift für Kommunikations- und EDV-Sicherheit.* Bundesamt für Sicherheit in der Informationstechnik (BSI). (Bonn, June 2001): 35–41.

Fischer, Wolfgang, Brigitta Krüger, Niels Lepperhoff, Regina Eich. *Was treibt die Entwicklung des Internet voran?* Programmgruppe Systemforschung und Technologische Entwicklung (STE). (Jülich, August 2001).

Hutter, Reinhard. "Cyber-Terror: Risiken im Informationszeitalter". In: *Aus Politik und Zeitgeschichte* (vol. 10/11, 2002): 31–39.

Informationstechnische Bedrohungen für Kritische Infrastrukturen in Deutschland. Kurzbericht der Ressortarbeitsgruppe KRITIS. (December 1999). http://www.iwar.org.uk/cip/resources/Kritis-12-1999.html

Jantsch, Susanne. "Critical Infrastructure Protection in Germany". *ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead.* (Zurich, 8–10 November, 2001). http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/jantsch/sld001.htm

"Kritische Infrastrukturen in Staat und Gesellschaft". In: *BSI-Kurzinformationen zu aktuellen Themen der IT-Sicherheit.* (January 2001). http:/www.bsi.bund.de/

Kühn, Klaus Dieter. "Katastrophenresistente Infrastrukturen". In: *Bevölkerungsschutz.* (vol. 4, 2001): 46–47.

Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations. Bundesgesetzblatt. (Part 1, 21 May, 2001: 876, Unofficial version for industry consultation).

Möhring, Michael. *Informationsgesellschaft.* (Universität Koblenz-Landau: Institut für Wirtschafts- und Verwaltungsinformatik, 2001).

Welzel, Carolin. "Vom Kalten Krieg zum Cyberwar: eBusiness, eGovernment – eWar?". In: *politik-digital.* (19 April, 2001). http://www.politik-digital.de/text/netzpolitik/cyberwar/bundeswehr.shtml

Netherlands

De Bruin, Ronald. "From Research to Practice: A Public-Private Partnership Approach in the Netherlands on Information Infrastructure Dependability". *Dependability Development Support Initiative (DDSI) Workshop.* (28 February, 2002).

Dutch Ministry of Transport, Public Works and Water Management / Dutch Ministry of Economic Affairs. *Internet Vulnerability.* (July 2001).

Evers, Joris. "The Netherlands adopts cybercrime pact". In: *CNN.com*. (30 November, 2000). http://www.cnn.com/2000/TECH/computing/11/30/dutch.cybercrime.idg/

House of Parliament (Tweede Kamer). Dossier 27925 – action line 10.

Infodrome. *De Overheid in de Informatiesamenleving: Mission September 1999.* (September, 1999). http://www.infodrome.nl/english/missie_eng.html

Luiijf, Eric "Critical Info-Infrastructure Protection in the Netherlands". *ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead.* (Zurich, 8–10 November, 2001). http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/luiijf/sld001.htm

Dependability Development Support Initiative (DDSI). *Public-Private Co-operation: Business Governmental Actions Towards Achieving a Dependable Information Infrastructure in Europe.* Issues and background paper for the DDSI workshop on Public-Private Co-operation (Stockholm, 6–7 June, 2002).

Luiijf, Eric. "Information Assurance and the Information Society". In: Gattiker, Urs E., Pia Pedersen and Karsten Petersen (Eds.). *EICAR 1999 Best Paper Proceedings.* (Aalborg, 1999).

Luiijf, Eric. "Information Assurance under Fire". *Information Assurance and Data Security, SMI conference.* (London, 2–3 February, 2000).

Luiijf, Eric. "Netherlands Defense Information Operations Policy". *Seminar on Information Warfare.* (Lucerne, 22 November, 2001).

Luiijf, Eric, M. Klaver, J. Huizenga. *The Vulnerable Internet: A Study of the Critical Infrastructure of (the Netherlands Section of) the Internet*. (The Hague, 2001).

Luiijf, Eric, M. Klaver. *In Bits and Pieces: Vulnerability of the Netherlands ICT-Infrastructure and Consequences for the Information Society.* (Translation of he Dutch Infodrome essay "BITBREUK", de kwetsbaarheid van de ICT-

infrastructuur en de gevolgen voor de informatiemaatschappij). (Amsterdam, March 2000).

Ministerie van Defensie, *Defensienota 2000*, (1999).

Stratix / TNO-FEL. *The Reliability of the Netherlands Internet: Consequences and Measures.* Report of Project Phase 3: Review of International Activities and Possible Actions. (English translation of "De Betrouwbaarheid van het Internet: Gevolgen en Maatregelen. Project KWINT – Rapportage Fase 3. (October 17, 2000, Version 2.2).

Norway

Dependability Development Support Initiative (DDSI). *European Dependability Policy Environments*, *Country Report Norway.* (Version April 2002).

Dependability Development Support Initiative (DDSI). *Public-Private Co-operation: Business Governmental Actions Towards Achieving a Dependable Information Infrastructure in Europe.* Issues and background paper for the DDSI workshop on Public-Private Co-operation (Stockholm, 6-7 June, 2002).

Hagen, Janne Merete, Håvard Fridheim. *Cost-Effectiveness Analysis of Measures to Reduce Vulnerabilities in the Public Telecommunication System*. Paper presented at the 16 ISMOR, The Royal Military College of Science, Norwegian Defence Research Establishment. (United Kingdom, 1-3 September, 1999).

Henriksen, Stein. "National Approaches to CIP Norway". *ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead*. (Zurich, 8–10 November, 2001). http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/Henriksen/sld001.htm

Hovden, Jan. *Public Policy and Administration in a Vulnerable Society.* Norwegian University of Science and Technology (NTNU). (Oslo).

Jervas, Gunnar, Ian Dennis, Richard Conroy (Eds.). *New Technology as a Threat and Risk Generator. Can Countermeasures Keep up with the Pace?* (Stockholm, March 2001).

Krohn Devold, Kristin. *The Government's Defence Challenges and Priorities. The Defence Minister's New Year Address to the Oslo Military Society, January 7, 2002. (Oslo, 2002).* http://odin.dep.no/fd/engelsk/aktuelt/taler/statsraad_a/010011-090053/index-dok000-b-n-a.html

Ministry of Defence. *Society's Security and Preparedness. Fact Sheet.* (March 2002). http://forsvar.regeringen.se/pressinfo/pdf/FB_p200102_158_eng.pdf.

Ministry of Industry, Employment and Communication. *An Information Society for All. Fact Sheet No. 2000.018.* (March 2000).

Ministry of Justice and Police. *Statement on Safety and Security of Society.* Report No. 17 to the Storting (2000-2001).

Ministry of Trade and Industry. *Society's vulnerability due to its ICT-dependence.* (Abridged version of the main report, Oslo, October 2000).

Nicander, Lars. "The Swedish Initiative on Critical Infrastructure Protection" *ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead.* (Zurich, 8–10 November, 2001). http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/nicander/sld001.htm

Nilsson, Jerry, Sven Erik Magnusson, Per-Olof Hallin, Bo Lenntorp. *Vulnerability Analysis and Auditing of Municipalities.* (Lucram: Lund University). http://www.isn.ethz.ch/crn/basics/process/documents/vulnerability.pdf

Norges offentlige utredninger. (2000:24) *Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet.* Statens forvaltningstjeneste Informasjonsforvaltning. (Oslo, 2000).

Svendsen, Per-Kare. *Internet Rights Country Report – Norway.* (January 2000). http://www.apc.org/english/rights/europe/countries/norway.html

Sweden

Dependability Development Support Initiative (DDSI). *European Dependability Policy Environments, Country Report Sweden.* (Version April 2002).

The Swedish Commission on Vulnerability and Security. *Vulnerability and Security in a New Era – A Summary.* (SOU 2001:41, Stockholm, 2001). http://forsvar.regeringen.se/propositionermm/sou/pdf/sou2001_41eng.pdf

The Swedish ICT Commission. *Basic Protection in Computer Hardware and Software. The Observatory for Information Security.* (2001).

The Swedish ICT Commission. *General Guide to a Future-Proof IT Infrastructure. Observatory for IT Infrastructure. Report 37/2001.* (Stockholm, 2001).

Wallstrom, Peter. "Methods for Infrastructure Protection". *MIS Training, InfowarCon '99.* (London, 1999).

Weissglass, Gösta (Ed.). "Planning a High-Resilience Society". *Papers and Proceedings from the Lövånger Symposium*, 18–20 August 1993. (Umeå, 1994).

Wik, Manuel W. "The Swedish Commission on Vulnerability and Security. Under Leadership of Special Investigator Åke Pettersson". *ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead.* (Zurich, 8–10 November, 2001). http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/Wik_135/sld001.htm

Switzerland

Bircher, Daniel. "Informationsinfrastruktur – Verletzliches Nervensystem unserer Gesellschaft". In: *Neue Zürcher Zeitung*, 7 *July*, *1999*.

Carrel, Laurent F. *Bericht des Projektleiters über die Strategische Führungsausbildung (SFU) 97.* (Bern, 1 July, 1998).

Generalsekretariat VBS (Ed.). *Risikoprofil Schweiz. Umfassende Risikoanalyse Schweiz.* (Draft, Bern, August 1999).

Groupe de Réflexion. *Für eine Informationsgesellschaft in der Schweiz. Zuhanden des Schweizerischen Bundesrates.* (Bern, June 1997).

Informatikstrategieorgan Bund. *Einsatzkonzept Information Assurance Schweiz. Melde- und Analysestelle Informationssicherheit (MELANI)*, *Sonderstab Information Assurance (SONIA)*. Schlussbericht vom 30. November 2001 (Zollikon: Ernst Basler + Partner AG, 2001).

ISPS News (Infosociety.ch). *Press Release: Gemeinsam die Cyber-Kriminalität bekämpfen. Bundesrat genehmigt Konvention des Europarats.* http://www.isps.ch.

Koordinationsgruppe Informationsgesellschaft (KIG). *Konzept "Information Assurance".* (Bern, May 2000).

Rytz, Ruedi. *Sonderstab Information Assurance – ein paar Gedanken.* (Bern, 11 September, 2001).

Schweizerische Bundeskanzlei. *Information Assurance: Die Verletzlichkeit der schweizerischen Informationsgesellschaft.* (Bern, 19 May, 1998).

Schweizerische Bundeskanzlei. *INFORMO 2001: Strategische Führungsausbildung.* Dokumentation für Teilnehmende und Medienschaffende. (Bern, 2001).

Schweizerische Bundeskanzlei. *Strategische Führungsübung 1997 – Kurzdokumentation über die SFU 97.* (Bern, 1997).

Security through Cooperation – Report of the Federal Council to the Federal Assembly on the Security Policy of Switzerland. (Bern, June 1999). http://www.vbs.admin.ch/internet/SIPOL2000/E/index.htm

Sibilia, Ricardo. "Informationskriegführung. Eine schweizerische Sicht". *Institut für militärische Sicherheitstechnik (IMS)*. (Nr. 97–6, Zurich, 1997).

Spillmann, Kurt R.; Libiszewski, Stefan; Wenger, Andreas; et al. "Die Rückwirkungen der Informationsrevolution auf die schweizerische Aussen- und Sicherheitspolitik". In: *NFP 42 Synthesis*, *Nr. 11. Schweizerischer Nationalfonds*, Bern, 1999). http://www.snf.ch/nfp42/public/resume/rspillmanninfo_d.html

Strategy of the Federal Council for an Information Society in Switzerland. (Bern, 18 February, 1998).

Trappel, Josef. *Informationsgesellschaft Schweiz – Bestandesaufnahme und Perspektiven.* Europäisches Zentrum für Wirtschaftsforschung und Strategieberatung. (Prognos, Basel, May 1997).

United States

Belcher, Tim, Elad Yoran. *Internet Security Threat Report: Attack Trends for Q3 and Q4 2001.* (Alexandria, January 2002).

Bendrath, Ralf. "Critical Infrastructure Protection in the United States". *ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead.* (Zurich, 8–10 November, 2001). http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/bendrath/sld001.htm

Brown, Evelyn. "Energy Systems Expertise is Key to Critical Infrastructure Center." In: *Logos* (No 17, vol. 2, Fall 1999). http://www.anl.gov/OPA/logos17-2/infra2.htm

Buehring, Bill. *Natural Gas Security Issues Related to Electric Power Systems.* (November 28, 2001). http://wpweb2k.gsia.cmu.edu/ceic/presentations/Buehring.pdf

Bush, George W. *Executive Order 13228. Establishing the Office of Homeland Security and the Homeland Security Council.* (Washington, D.C., October 8, 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, D.C., October 16, 2001). http://www.ncs.gov/ncs/html/eo-13231.htm

Clinton, William J. *Defending America's Cyberspace: National Plan for Information Systems Protection. An Invitation to a Dialogue.* Version 1.0. (The White House, Washington, D.C., 2000).

Clinton, William J. *Executive Order 13010 on Critical Infrastructure Protection.* (Washington, D.C., 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, D.C., 22 May, 1998). http://www.fas.org/irp/offdocs/pdd-63.htm

Clinton, William J. *Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities.* (The White House, Washington, D.C., January 2001).

Cyber Security – Full Committee Hearing on Cyber Security – How Can We Protect American Computer Networks From Attack? (Washington, D.C., Wednesday, 10 October, 2001). http://www.iwar.org.uk/cip/resources/house-oct-10-01/

Dacey, Robert F. *Critical Infrastructure Protection: NIPC Faces Significant Challenges in Developing Analysis, Warning, and Response Capabilities, before the Subcommittee on Technology, Terrorism, and Government Information, Senate Committee on the Judiciary.* GAO-01-769T (Washington, D.C., 22 May, 2001). http://www.iwar.org.uk/cip/resources/gao/d01769t.pdf

Davis, John (President's Commission on Infrastructure Protection). *Research and Development for Critical Infrastructure Protection.* (Washington, D.C., 5 September, 1997). http://www.ciao.gov/resource/pccip/ac_randd.pdf

Fisher, R., J. Peerenbaum. "Interdependencies: A DOE Perspective". *16th Annual Security Technology Symposium & Exhibition. Session IV: Infrastructure Interdependencies: The Long Pole in the Tent.* (Williamsburg, Virginia, 28 June, 2000).

Fisher, Ron, Jim Peerenbaum. "Lessons Learned from Industry Vulnerability Assessments and September 11th". *US Department of Energy Assurance Conference.* (Arlington, 12–13 December, 2001).

Government Electronics and Information Technology Association (GEIA). *Information Assurance and Critical Infrastructure Protection: A Federal Perspective.* (2001).

House Science Committee: *October 17, 2001 – Full Committee Hearing on Cyber Terrorism – A View From the Gilmore Commission.* (Washington, D.C., 17 October, 2001). http://www.iwar.org.uk/cip/resources/house-oct-17-01/

How Secure is Our Critical Infrastructure? U.S. Senate Committee on Governmental Affairs. (Washington, D.C., 12 September, 2001). http://www.iwar.org.uk/cip/resources/senate-sep-12-01/

Improving Our Ability to Fight Cybercrime: Oversight of the National Infrastructure Protection Center. Hearing before the Senate Committee on the Judiciary Subcommittee on Technology, Terrorism and Government Information. (Washington, D.C., 25 July, 2001). http://www.iwar.org.uk/cip/resources/nipc-oversight/hr072501st.htm

Kneso, Genevieve J., *CRS (Congressional Research Service) Report for Congress. Federal Research and Development for Counter Terrorism: Organization, Funding and Options.* (November 2001). http://www.ieeeusa.org/forum/PAPERS/CRSterrorismresearch.pdf

KPMG, Peat Marwick. *Vulnerability Assessment Framework 1.1. Prepared under contract for the Critical Infrastructure Assurance Office.* (October 1998). http://www.ciao.gov/resource/vulassessframework.pdf

League, Sarah Jane. "Critical Infrastructure Assurance Office: Protecting America's Infrastructures". *InfowarCon '99.* (London, 1999).

Legal Information Institute. *Code Collection. Sec. 1001. – Statements or entries generally.* http://www4.law.cornell.edu/uscode/18/1001.html

Little, Richard G., Paul B. Pattak, Wayne A. Schroeder (Eds.). *Use of Underground Facilities to Protect Critical Infrastructures, Summary of a Workshop.* (National Academy Press: Washington, D.C., 1998).

Moteff, John D. *CRS (Congressional Research Service) Report for Congress. Critical Infrastructures: Background, Policy, and Implementation.* (Updated 4 February, 2002). http://www.fas.org/irp/crs/RL30153.pdf

Moteff, John D. *RL30153: Critical Infrastructures: Background and Early Implementation of PDD-63.* (Updated 12 September, 2000). http://www.cnie.org/nle/crsreports/science/st-46.cfm

National Information Infrastructure. Risk Assessment: A Nation's Information at Risk. (Executive Summary, January 1999). http://www.ncs.gov/n5_hp/N5_IA_HP/HTML/RVWG/niirisk.htm (no longer available)

Office of the Undersecretary for Defense. *Protecting the Homeland – Report of the Defense Science Board Task Force on Defensive Information Operations 2000 Summer Study.* (Executive Summary, vol. I, March 2001). http://www.acq.osd.mil/dsb/protecting.pdf

Oversight hearing on Information Technology – Essential Yet Vulnerable: How Prepared Are We for Attacks. Subcommittee on Governmental Efficiency, Financial Management and Intergovernmental Relations. (26 September, 2001). http://www.iwar.org.uk/cip/resources/house-sep-26-01/witnesses.htm

Power, Richard. "2001 CSI/FBI Computer Crime and Security Survey." In: *Computer Security Issues & Trends.* (vol. 1, 2001).

Proceedings of the Infrastructure Interdependencies Research and Development Workshop. Hosted by the Department of Energy, Office of Critical Infrastructure Protection, and the White House, Office of Science and Technology Policy. (Mc Lean, 12–13 June, 2000).

Protecting America's Critical Infrastructures: How Secure Are Government Computer Systems? US Subcommittee on Oversight and Investigations Hearing. (Washington, D.C., 5 April, 2001). http://energycommerce.house.gov/107/action/107-13.pdf

Ryan, Julie. *The Infrastructure of the Protection of the Critical Infrastructure.* (1998). http://www.iwar.org.uk/cip/resources/pdd63/pdd63-article.htm

Sandia National Laboratories. *Modeling of Interdependencies. Critical Infrastructure Surety.* http://www.sandia.gov/Surety/Facts/Modeling.htm

Scalingi, Paula. *Critical Infrastructure Protection Activities. Department of Energy.* (March 2001). http://www.naseo.org/events/outlook/2001/presentations/scalingi.PDF

Stoneburner, Gary, Alice Goguen, and Alexis Feringa. *Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology.* NIST Special Publication 800–30. (Washington, D.C.: U.S. Government Printing Office, January 2002).

Stoneburner, Gary. *Computer Security. Underlying Technical Models for Information Technology Security. Recommendations of the National Institute of Standards and Technology.* NIST Special Publication 800–33. (Washington, D.C.: U.S. Government Printing Office, December 2001). http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf

The Department of Homeland Security. *Information Analysis and Infrastructure Protection.* http://www.whitehouse.gov/deptofhomeland/sect6.html

The President's Commission on Critical Infrastructure Protection (PCCIP). *Critical Foundations: Protecting America's Infrastructures.* (Washington, D.C., October 1997).

United States General Accounting Office (GOA). *Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities.* (GAO-01-323, 25 April, 2001).

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. (USA PATRIOT ACT) ACT OF 2001. http://www.cdt.org/security/usapatriot/011026usa-patriot.pdf

US Critical Infrastructure Assurance Office. *Practices for Securing Critical Infrastructure Assets.* (Washington, D.C., January 2000). http://www.iwar.org.uk/cip/resources/prac.pdf

White Paper on PDD-63. The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. (Washington, D.C., 22 May, 1998). http://www.cybercrime.gov/white_pr.htm

CII Methods and Models

Attorney-General's Department. *Protecting Australia's National Information Infrastructure. Report of the Interdepartmental Committee on Protection of the National Information Infrastructure.* (Canberra, December 1998). http://www.law.gov.au/publications/niireport/niirpt.pdf

Bundesamt für Sicherheit in der Informationstechnik. *IT Baseline Protection Manual. Standard Security Safeguards.* http://www.bsi.de/gshb/english/menue.htm

Charters, David. *The Future of Canada's Security and Defence Policy: Critical Infrastructure Protection and DND Policy and Strategy.* Research Paper of the Council for Canadian Security in the 21st Century. http://www.ccs21.org/ccspapers/papers/charters-CSDP.htm

Cobb, Adam. *Thinking about the Unthinkable: Australian Vulnerabilities to High-Tech Risks*. Foreign Affairs, Defence and Trade Group, Research Paper 18. (29 June, 1998).

Commonwealth of Australia, Information Security Group. *Australian Communications-Electronic Security Instruction 33 (ACSI 33*) Handbook 3. Risk Management, Version 1.0, http://www.dsd.gov.au/infosec/acsi33/HB3.html

Commonwealth of Australia. *Example of Risk Assessment*. http://www.dsd.gov.au/infosec/acsi33/HB3A.html

Critical Infrastructure Assurance Office, Project Matrix: http://www.ciao.gov/federal/

Ernst Basler + Partner AG. *Risikoorientierte Sicherheitsnachweise im Eisenbahnbetrieb. Leitfaden* (on behalf of the German Federal Ministry of Transport) (Zollikon, 1996).

Ezell, Barry C., John V. Farr, and Ian Wiese. "Infrastructure Risk Analysis Model". In: *Journal of Infrastructure Systems*. (vol. 6, 3, September 2000): 114–117.

Ezell, Barry C., John V. Farr, and Ian Wiese. "Infrastructure Risk Analysis of Municipal Water Distribution System" In: *Journal of Infrastructure Systems*, (vol. 6, 3, September 2000): 118-122.

Fraser, B. (ed.) *RFC2196 Site Security Handbook. The Internet Engineering Task Force (IETF) Network Working Group*. (September 1997). http://www.ietf.org/rfc/rfc2196.txt

Grenier, Jacques. "The Challenge of CIP Interdependencies". *Conference on the Future of European Crisis Management*. (Uppsala, Sweden, 19–21 March 2001). http://www.ntia.doc.gov/osmhome/cip/workshop/ciptf_files/frame.htm

Hagen, Janne Merete, Håvard Fridheim. *Cost-Effectiveness Analysis of Measures to Reduce Vulnerabilities in the Public Telecommunication System*. Paper presented at the 16 ISMOR, The Royal Military College of Science, Norwegian Defence Research Establishment. (United Kingdom, September 1–3, 1999).

Haimes, Yacov Y. and Pu Jiang. "Leontief-Based Model of Risk in Complex Interconnected Infrastructures". In: *Journal of Infrastructure Systems*. (vol. 7, 1, March 2001): 1–12.

Haimes, Yacov Y. *Risk Modeling, Assessment, and Management*. (New York: Wiley Publications, 1998).

Hutter, Reinhard. "Cyber-Terror: Risiken im Informationszeitalter". In: *Aus Politik und Zeitgeschichte*. (vol. 10/11, 2002): 31–39.

InfoSurance, Ernst Basler + Partner AG. *Einflussfaktoren und Abhängigkeiten im Umgang und Einsatz von Informationssicherheit* (Zollikon, Zürich: 2000). http://www.infosurance.ch/de/ppt/Krisenverstaendnis.ppt

KPMG / National Support Staff. *Critical Infrastructure Project. Phase 2. Information Technology Report.* Predict Defence Infrastructure Core Requirements Tool (PreDICT). (April 2000). http://www.defence.gov.au/predict/segments/it/pdf/it_full.pdf

KPMG / National Support Staff. Predict Defence Infrastructure Core Requirements Tool (PreDICT). http://www.defence.gov.au/predict/general/predict_fs.htm

KPMG, Peat Marwick. *Vulnerability Assessment Framework 1.1. Prepared under contract for the Critical Infrastructure Assurance Office.* (October 1998). http://www.ciao.gov/resource/vulassessframework.pdf

Leontief, W. W. *Input-Output Economics.* (New York: Oxford University Press, 1986).

Luiijf, Eric, M. Klaver, J. Huizenga. *The Vulnerable Internet: A Study of the Critical Infrastructure of (the Netherlands Section of) the Internet.* (The Hague, 2001).

Luiijf, Eric, M. Klaver. *In Bits and Pieces: Vulnerability of the Netherlands ICT-Infrastructure and Consequences for the Information Society.* (Translation of he Dutch Infodrome essay "BITBREUK", de kwetsbaarheid van de ICT-infrastructuur en de gevolgen voor de informatiemaatschappij). (Amsterdam, March 2000).

Luiijf, Eric. "Critical Info-Infrastructure Protection in the Netherlands". *ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead.* (Zurich, 8–10 November, 2001). http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/luiijf/sld001.htm

Masera, Marcelo, Wilikens, M. "Interdependencies with the Information Infrastructure: Dependability and Complexity Issues". *Conference Paper at the 5th International Conference on Technology, Policy, and Innovation.* (Ispra, 26-29 June, 2001). http://www.delft2001.tudelft.nl/paper%20files/paper1168.doc.

Maurer, Daniel. *Evaluation of the Integrated Complexity Management Instrument (ICI) for Generating Global Scenarios.* (Bern, June 2001). http://www.isn.ethz.ch/crn/basics/process/documents/ici_rapport_e.pdf

Merz, Hans, Thomas Schneider, and Hans Bohnenblust. *Bewertung von technischen Risiken. Beiträge zur Strukturierung und zum Stand der Kenntnisse. Modelle zur Bewertung von Todesfallrisiken* (Zürich: vdf Verlag der Fachvereine Zürich, 1995).

National Contingency Planning Group. *Canadian Infrastructures and their Dependencies.* (March 2000).

Nilsson, Jerry, Sven Erik Magnusson, Per-Olof Hallin, Bo Lenntorp. *Vulnerability Analysis and Auditing of Municipalities.* (Lucram: Lund University). http://www.isn.ethz.ch/crn/basics/process/documents/vulnerability.pdf

Porter, Michael. *Competitive Strategy. Techniques for Analyzing Industries and Competitors.* (New York: Free Press, 1980).

Protecting Australia's National Information Infrastructure. Report of the Interdepartmental Committee on Protection of the National Information Infrastructure. Attorney-General's Department. (Canberra, December 1998). http://www.law.gov.au/publications/niireport/niirpt.pdf

Rinaldi, Steven M., James P. Peerenboom, and Terrence K. Kelly. "Complex Networks. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies." In: *IEEE Control Systems Magazine.* (vol. 21, 6, December 2001): 11–25.

Stoneburner, Gary, Alice Goguen, and Alexis Feringa. *Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology.* NIST Special Publication 800-30. (Washington, D.C.: U.S. Government Printing Office, January 2002). http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Stoneburner, Gary. *Computer Security. Underlying Technical Models for Information Technology Security. Recommendations of the National Institute of Standards and Technology.* NIST Special Publication 800-33. (Washington, D.C.: U.S. Government Printing Office, December 2001). http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf

Stratix / TNO-FEL. *The Reliability of the Netherlands Internet: Consequences and Measures. Report of Project Phase 3: Review of International Activities and Possible Actions.* (English Translation of "De Betrouwbaarheid van het Internet: Gevolgen en Maatregelen. Project KWINT – Rapportage Fase 3. (October 17, 2000, Version 2.2). http://www.tno.nl/instit/fel/refs/pub2001/kwint_paper1048.pdf

von Reibnitz, Ute. *Szenario-Technik: Instrumente für die unternehmerische und persönliche Erfolgsplanung.* (Wiesbaden, 1992).

A3 Important Links

Australia

Attorney-General's Department (http://www.ag.gov.au)

Australian Computer Emergency Response Team (AusCERT) (http://www.auscert.org.au)

Australian Security Intelligence Organization (ASIO) (http://www.asio.gov.au)

Defense Science and Technology Organization (DSTO) (http://www.dsto.defence.gov.au)

National Office for the Information Economy (NOIE) (http://www.noie.gov.au)

Prime Minister of Australia (http://www.pm.gov.au)

Canada

Canada's National Computer Emergency Response Team (http://www.cancert.ca)

Canadian National Research Council (NRC) (http://www.nrc.ca)

Communication Research Centre (CRC) (http://www.crc.ca)

D-Net (http://www.dnd.ca)

Federal Association of Security Officials (http://www.faso-afrs.ca)

Government-on-Line (GoL) (http://www.gol-ged.gc.ca)

Institute for Information Technology (IIT) (http://www.iit.nrc.ca)

Networks of Centres of Excellence (NCE) (http://www.nce.gc.ca)

Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) (http://www.ocipep-bpiepc.gc.ca)

Treasury Board Secretariat (http://www.tbs-sct.gc.ca)

Germany

Arbeitskreis Schutz von Infrastrukturen (AKSIS) (http://www.aksis.de)

BKAonline – Bundeskriminalamt Wiesbaden (http://www.bka.de)

Bundesamt für Sicherheit in der Informationstechnik (BSI) (http://www.bsi.de)

Bundesministerium für Bildung und Forschung (BMBF) (http://www.bmbf.de)

Bundesnachrichtendienst (BND) (http://www.bundesnachrichtendienst.de)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) (http://www.bitkom.org)

CERT-Bund (http://www.bsi.bund.de/certbund/index.htm)

DCERT (http://www.dcert.de)

Deutsche Telekom AG (http://www.telekom.de)

Deutscher Bundestag (http://www.bundestag.de)

DFN-CERT (http://www.cert.dfn.de)

Europäisches Institut für IT-Sicherheit (http://www.eurubits.de)

Informations- und Kommunikationsdienste-Gesetz (http://www.iid.de/iukdg/)

Initiative D21 (http://www.initiatived21.de)

Initiative Informationsgesellschaft Deutschland (http://www.iid.de)

juris GmbH (http://www.juris.de)

secunet Security Networks AG (http://www.secunet.de)

Sicherheit im Internet (http://www.sicherheit-im-internet.de)

SIZ – Informatikzentrum der Sparkassenorganisation GmbH (http://www.s-cert.de)

The Netherlands

Binnenlandse Veiligheidsdienst (BVD) (National Intelligence and Security Agency) (http://www.fas.org/irp/world/netherlands/bvd.htm)

Directoraat-Generaal Telecommunicatie en Post (http://www.minvenw.nl/dgtp/home/)

INFODROME (http://www.infodrome.nl)

Ministerie van Verkeer en Waterstaat (http://www.minvenw.nl)

Ministry of the Interior and Kingdom Relations (http://www.minbzk.nl)

NLIP – Brancheverenigingen van Nederlandse Internet Providers (http://www.nlip.nl)

Rathenau Instituut (http://www.rathenau.nl)

SURFnet Computer Security Incident Response Team (http://cert-nl.surfnet.nl/home-eng.html)

The General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst, AIVD) (http://www.aivd.nl)

The Platform for Electronic Business in the Netherlands (ECP.nl) (http://www.ecp.nl/ENGLISH/index.html)

TNO Web (http://www.tno.nl)

Norway

Direktoratet for Sivilt Beredskap (DSB) (http://www.dsb.no)

Ministry of Trade and Industry (http://odin.dep.no/nhd/engelsk/)

Okokrim (http://www.okokrim.no)

The Norwegian Network for Research & Education – Computer Emergency Response Team (http://cert.uninett.no)

Sweden

Försvars Departementet (http://forsvar.regeringen.se)

KTH Royal Institute of Technology (http://www.kth.se/eng/)

Överstyrelsen för Civil Beredskap (http://www.ocb.se)

Swedish Alliance for Electronic Commerce (GEA) (http://www.gea.nu)

Swedish Defense Research Agency (http://www.foi.se/english/)

Swedish Emergency Management Agency (SEMA) (http://www.krisberedskapsmyndigheten.se/english/index.jsp)

Swedish National Defense College (http://www.fhs.mil.se)

The National Board of Psychological Defence (http://www.psycdef.se/english/)

Switzerland

Bundesamt für Berufsbildung und Technologie BBT (http://www.bbt.admin.ch)

CERT SWITCH (http://www.switch.ch/cert/)

Center for Security Studies and Conflict Research (FSK) (http.//www.fsk.ethz.ch)

Commission for Technology and Innovation (CTI) (http://www.snhta.ch/www-support/institutions/cti_fopet.htm)

Comprehensive Risk Analysis and Management Network (CRN) (http://www.isn.ethz.ch/crn/)

Division for Information Security and Facility Protection (DISFP) (http://www.vbs.admin.ch/internet/GST/AIOS/e/index.htm)

Federal Office for Communication (OFCOM) (http://www.bakom.ch/en/index.html)

Federal Office for National Economic Supply (NES) (http://www.bwl.admin.ch/)

Federal Office for Police (FOP) (http://internet.bap.admin.ch)

Federal Office of Information Technology, Systems and Telecommunication (FOITT) (http://www.informatik.admin.ch)

Federal Strategy Unit for Information Technology (FSUIT) (http://www.isb.admin.ch)

Foundation InfoSurance (http://www.infosurance.org)

IBM Zurich Research Laboratory (http://www.zurich.ibm.com)

Information and Communication Management Research Group (http://www.ifi.unizh.ch/ikm/research.html)

Information Society Coordination Group (http://www.isps.ch)

International Relations and Security Network (ISN) (http://www.isn.ethz.ch)

National Emergency Operations Center Agency (NAZ) (http://www.naz.ch)

Security and Cryptography Laboratory (LASEC) (http://lasecwww.epfl.ch)

Softnet (http://www.softnet.ch)

Strategische Führungsausbildung (http://www.sfa.admin.ch)

Symposium on Privacy and Security (http://www.privacy-security.ch)

United States

Center for Democracy and Technology (http://www.cdt.org)

Critical Infrastructure Assurance Office (CIAO) (http://www.ciao.gov)

Department of Homeland Security (http://www.whitehouse.gov/deptofhomeland)

Energy Information Sharing and Analysis Center (ENERGY-ISAC) (http://www.energyisac.com)

Federal Bureau of Investigation (FBI) (http://www.fbi.gov)

Federal Computer Incident Response Center (http://www.fedcirc.gov)

Federation of American Scientists (http://www.fas.org)

Financial Services Information Sharing and Analysis Center (FS-ISAC) (http://www.fsisac.com)

Information Technology Information Sharing and Analysis Center (IT-ISAC) (https://www.it-isac.org)

National Coordinating Center for Telecommunications (http://www.ncs.gov/ncc/)

National Infrastructure Protection Center (NIPC) (http://www.nipc.gov)

North American Electric Reliability Council (NERC) http://www.nerc.com

Partnership for Critical Infrastructure Security (PCIS) (http://www.pcis.org)

Stay Safe Online (http://www.staysafeonline.info)

Surface Transportation Information Sharing and Analysis Center (ST-ISAC) (http://www.surfacetransportationisac.org)

Miscellaneous

Cryptome (http://cryptome.org)

Dependability Development Support Initiative (DDSI) (http://www.ddsi.org)

European Warning and Information System Forum (EWIS) (http://ewis.jrc.it)

Global Business Dialogue on Electronic Commerce (http://www.gbde.org)

A4 Experts Involved

Australia

Ivan Timbs, National Office for the Information Economy (NOIE), E-Security Policy Section (http://www.noie.gov.au)

Canada

Jacques L. Grenier, Office of Critical Infrastructure Protection and Emergency Preparedness (http://www.ocipep-bpiepc.gc.ca)

Colin Knight, Office of Critical Infrastructure Protection and Emergency Preparedness (http://www.ocipep-bpiepc.gc.ca)

Germany

Ralf Bendrath, Scientist

Dr. Jörn Brömmelhörster, Consultant

Dr. Susanne Jantsch, Industrieanlagen-Betriebsgesellschaft (IABG) (http://www.iabg.de)

Dr. Christine Scharz-Hemmert, Industrieanlagen-Betriebsgesellschaft (IABG) (http://www.iabg.de)

Netherlands

Ronald de Bruin, KWINT, ECP.nl (http://www.ecp.nl)

Eric Luiijf, TNO Physics and Electronics, Laboratory (http://www.tno.nl)

Norway

Cort Arch Dreyer, Ministry of Trade and Industry (http://odin.dep.no)

Havard Fridheim, Norwegian Defence Research Establishment (http://www.mil.no/felles/ffi/start)

Arthur Gjengstö, Secretary to the Norwegian Commission on the Vulnerability of Society

Stein Henriksen, Directorate for Civil Defence and Emergency Planning (http://www.dsb.no)

Sweden

Lars Nicander, Director National Office of IO/CIP Studies, Swedish National Defence College (http://www.fhs.mil.se)

Jan Lundberg, Swedish Emergency Management Agency (SEMA) (http://www.krisberedskapsmyndigheten.se), former ÖCB

Manuel W. Wik, Swedish National Defence College (http://www.fhs.mil.se)

Peter Westrin, PH.D., FOI, Swedish Defence Research Agency (http://www.foi.se)

Dr. Peter Stern, Swedish Emergency Management Agency (SEMA) (http://www.krisberedskapsmyndigheten.se), former ÖCB

Peter Wallström, Cell Network (http://www.cellnetwork.se)

Switzerland

Dr. Michel Dufour, Dufour Consulting

Thomas Köppel, Federal Office for Police (http://internet.bap.admin.ch)

Kurt Haering, Director Foundation InfoSurance (http://www.infosurance.ch)

Dr. Ruedi Rytz, Federal Strategy Unit for Information Technology (FSUIT) (http://www.isb.admin.ch)

Dr. Ueli Haudenschild, Federal Office for National Economic Supply (http://www.bwl.admin.ch)

United States

Scott C. Algeier, U.S. Chamber of Commerce (http://www.uschamber.com)

A5 Abbreviations

ACSI 33:	Australian Communications-Electronic Security Instruction 33, (Australia)
AG KRITIS:	Interministerielle Arbeitsgruppe Kritische Infrastrukturen, (Germany)
AgIO:	Cabinet Office Workgroup on Information Operations, (Sweden)
AIOS:	Bureau for Security of Information and Objects, (Switzerland)
AKSIS:	Arbeitskreis Schutz Kritischer Infrastrukturen, (Germany)
ASIO:	Australian Security Intelligence Organisation, (Australia)
AusCERT:	Australian Computer Emergency Response Team, (Australia)
BIT:	Federal Office of Information Technology, Systems and Telecommunication, (Switzerland)
BITKOM:	Bundesverband für Informationswirtschaft, Telekommunikation und Neue Medien, (Germany)
BKA:	Bundeskriminalamt, (Germany)
BMBF:	Bundesministerium für Bildung und Forschung (Federal Ministry for Education and Research), (Germany)
BMWi:	Bundesministerium für Wirtschaft and Technologie, (Germany)
BND:	Bundesnachrichtendienst, (Germany)
BSI:	Bundesamt für Sicherheit in der Informationstechnik, (Germany)
BZK:	Ministry of the Interior and Kingdom Relations, (The Netherlands)
CanCERT:	Canadian Computer Emergency Response Team, (Canada)
CART:	Computer Analysis and Response Team, (United States)
CERT:	Computer Emergency Response Team
CERT SWITCH:	Computer Emergency Response Team of the Swiss Academic & Research Network, (Switzerland)
CERT-Bund:	German Computer Emergency Response Team für Bundesbehörden, (Germany)
CERT-NL:	Computer Emergency Response Team of the Netherlands, (The Netherlands)
CERT-RO:	Computer Emergency Response Team – Central Government, (The Netherlands)
CFAA:	Computer Fraud and Abuse Act, (United States)
CHO:	Chief Headquarter of Defense, (Norway)

CI:	Critical Infrastructure
CIAO:	Critical Infrastructure Assurance Office, (United States)
CIF:	Consultative Industry Forum, (Australia)
CIIP:	Critical Information Infrastructure Protection
CIP:	Critical Infrastructure Protection
CIPG:	Critical Infrastructure Protection Group, (Australia)
CIPTF:	Critical Infrastructure Protection Task Force, (United States)
CIS:	Center for International Studies, (Switzerland)
CRC:	Communications Research Centre, (Canada)
CRN:	Comprehensive Risk Analysis and Management Network, (Switzerland)
CTI:	Commission for Technology and Innovation, (Switzerland)
CWIG:	Critical Infrastructure Working Group, (United States)
CYTEX:	Cyber Terror Exercise, (Germany)
DDPS:	Swiss Federal Department of Defense, Civil Protection and Sports, (Switzerland)
DISFP:	Division for Information Security and Facility Protection, (Switzerland)
DJP:	Federal Department of Justice and Police, (Switzerland)
DoD:	Department of Defense, (United States)
DoE:	Department of Energy, (United States)
DSB:	Directorate for Civil Defense and Emergency Planning, (Norway)
DSD:	Defence Signals Directorate, (Australia)
DSTO:	Defence Science and Technology Organisation, (Australia)
EO:	Executive Order, (United States)
ECP-NL:	Platform Electronic Commerce in the Netherlands, (The Netherlands)
ESCG:	E-Security Coordination Group, (Australia)
ETH:	Swiss Federal Institute of Technology (ETH Zurich), (Switzerland)
FBI:	Federal Bureau of Investigation, (United States)
FDEA:	Federal Department of Economic Affairs, (Switzerland)
FDF:	Swiss Federal Department of Finance, (Switzerland)
FedCIRC:	Federal Computer Incident Response Center, (United States)
FFI:	Norwegian Defense Research Establishment, (Norway)
FIRST:	Forum of Incident and Security Response Team, (Canada)
FOI:	Swedish Defense Research Agency, (Sweden)

FOITT:	Federal Office of Information Technology, Systems and Telecommunication, (Switzerland)
FOP:	Federal Office for Police, (Switzerland)
FS/ISAC:	Financial Services Information Sharing and Analysis Center, (United States)
FSUIT:	Federal Strategy Unit for Information Technology, (Switzerland)
FSK:	Forschungsstelle für Sicherheitspolitik und Konfliktanalyse (Center for Security Studies and Conflict Research), (Switzerland)
GEA:	Swedish Alliance for Electronic Commerce, (Sweden)
GoL:	Government-on-line, (Canada)
HERT:	Hacking Emergency Response Team, (The Netherlands)
HHM:	Hierarchical Holographic Modeling
I&C:	Information and Communications
IAG:	Infrastructure Analysis Group
ICT:	Information and Communication Technologies
IDC:	Interdepartmental Committee on the Protection of the National Information Infrastructure, (Australia)
IIT:	Institute for Information Technology, (Canada)
IMS:	Institute for Microstructural Sciences, (Canada)
IOWG:	The Information Operations Working Group
IPs:	Infrastructure Profiles
IRAM:	Infrastructure Risk Analysis Model
ISACs:	Information Sharing and Analysis Centers
ISN:	International Relations and Security Network (Switzerland)
ISP:	Internet Service Provider
IT:	Information Technology
ITM:	Institut für Informations-, Telekommunikations- und Medienrecht, (Germany)
IWG:	CIP R&D Inter-Agency Working Group, (United States)
KLPD:	Korps Landelijke Politiediensten, (Dutch Police), (The Netherlands)
KTH:	Royal Institute of Technology, (Sweden)
LKA:	Landeskriminalamt, (Germany)
MCDA:	Multi Criteria Decision Approach
MIE:	Minimum Essential Infrastructure
MISA:	Municipal Information Systems Association, (Canada)

NAZ:	National Emergency Operations Center Agency, (Switzerland)
NCC:	National Coordinating Center
NCE:	Networks of Centres of Excellence, (Canada)
NCIPP:	National Critical Infrastructure Protection Program, (Canada)
NCPG:	National Contingency Planning Group, (Canada)
NCSA:	National Cyber Security Alliance, (United States)
NCSIP:	National CIO Sub-Committee on Information Protection, (Canada)
NERC:	North American Electricity Reliability Council, (United States)
NES:	Federal Office for National Economic Supply, (Switzerland)
NII:	National Information Infrastructure
NIPC:	National Infrastructure Protection Center, (United States)
NIRA:	National Infrastructure Risk Assessment, (Canada)
NIST:	National Institute of Standards and Technology, (United States)
NLIP:	Consortium of Dutch Internet Providers, (The Netherlands)
NOIE:	National Office for the Information Economy, (Australia)
NRC:	Canadian National Research Council, (Canada)
NSD:	Industry Security Delegation, (Sweden)
ÖCB:	Swedish Agency for Civil Emergency Planning, (Överstyrelsen för Civil Beredskam), now KBM (Sweden)
OCIIP:	Office of Computer Investigations and Infrastructure Protection, (United States)
OCIPEP:	Office of Critical Infrastructure Protection and Emergency Preparedness, (Canada)
OFCOM:	Federal Office For Communication, (Switzerland)
OGIT:	Office of Government Information Technology, (Australia)
OGO:	Office for Government On-line, (Australia)
OPET:	Office for Professional Education and Training, (Switzerland)
OSTP:	Office of Science and Technology Policy, (United States)
PCCIP:	Presidential Commission on Critical Infrastructure Protection, (United States)
PCIS:	Partnership for Critical Infrastructure Security, (United States)
PDD:	Presidential Decision Directives, (United States)
PEST:	Political, Economic, Social, Technological (Analysis)
PMRM:	Partitioned Multi-objective Risk Method

PreDICT:	Predict Defence Infrastructure Core Requirements Tool, (Australia)
PSCIOC:	Public Sector Chief Information Officer's Council, (Canada)
PSM:	Protective Security Manual, (Australia)
R&D:	Research and Development
RAFLS:	Relational Analysis For Linked Systems, (Canada)
SAVI:	Säkring Av Viktig Infrastructure, (Sweden)
SCNS:	Secretaries' Committee on National Security, (Australia)
SEMA:	Swedish Emergency Management Agency, (Sweden)
SFU:	Strategic Leadership Exercise, (Switzerland)
Sigint:	Signals Intelligence
SII:	Strategic Infrastructure Initiative, (Canada)
SIS:	Ministry of Trade and Industry Initiative, (Norway)
SLT:	Strategic Leadership Training, (Switzerland)
SWOT:	Strength, Weakness, Opportunities, Threats (Analysis)
USA PATRIOT:	(Act) Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, (United States)
V&W:	Ministry of Transport, Public Works and Water Management, (The Netherlands)
VAF:	Vulnerability Assessment Framework, (United States)
ZES:	Zentrum für Strategische Studien, (Germany)